Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

Mezei Kitti

A kiberbűnözés egyes büntetőjogi szabályozási kérdései

Doktori (PhD) értekezés

Témavezetők:
Prof. Dr. Tóth Mihály DSc. professor emeritus
Dr. Nagy Zoltán András habil. egyetemi docens

Pécs, 2019

TARTALOMJEGYZÉK

I. BEVEZETÉS

1. A témaválasztás indokolása, aktualitása[1]

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. Az információs társadalom egyik jellemzőjévé vált az infokommunikációs eszközök számának, sokféleségének a növekedése és használatuk széleskörű elterjedése.

A gyors ütemű informatikai fejlődésnek a nyilvánvaló előnyei mellett megvannak a maga veszélyei is, hiszen lehetőséget teremt a bűnözés eddig ismeretlen formái számára. Éppen ezért a kiberbűnözés jelenti napjaink egyik legnagyobb kihívását. Az új technológiák megjelenése (pl. mobilinformatikai és okoseszközök, Internet of Things[2]), a megvalósítható funkciók bővülése, illetve az információs hálózatok használatának az elterjedése magukkal hozzák az újabb elkövetési módokat, illetve büntetendő cselekmények körét.[3] A tisztán informatikai bűncselekményeken kívül (pl. hacking, adatmanipuláció, számítógépes vírusok) ma már szinte bármelyik hagyományos bűncselekmény (pl. csalás, zsarolás, pénzmosás) is elkövethető az információs rendszerek használatával, az interneten keresztül. Mindez kihívások elő állítja mind a jogalkotást a büntetőjogi szabályozásra tekintettel, mind a jogalkalmazást a büntetendő magatartások minősítéseinek kérdéseiben.

A büntető igazságszolgáltatás hatékonyságának növelése egyre sürgetőbben veti fel e téma kutatásának az igényét. Ennek ellenére a hazai szakirodalom keveset foglalkozik az informatikai bűnözés aktuális szabályozási kihívásaival a büntetőjogban, ezért a témát érintő tudományos kutatás hiánypótlónak tekinthető.

---

[1] A doktori értekezés az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV és ÚNKP-17-3-I kódszámú Új Nemzeti Kiválóság Programjának keretében készült.

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

[3] NAGY Zoltán András: Bűncselekmények számítógépes környezetben. Ad librum Kft. Budapest, 2009. 23-24. o.

Az internetnek számos olyan jellemzője van, amelyek egyben a használatával összefüggő visszaélések térnyerésére, illetve a bűncselekmények hatékonyabb elkövetésére is lehetőséget teremtenek. Az internetre csatlakozott eszközök és felhasználók száma évről évre növekvő tendenciát mutat. Mivel egy egész világra kiterjedő hálózatról van szó, amely azonnali és valós idejű kapcsolatteremtésre nyújt lehetőséget, a kiterjedt online jelenlét lehetővé teszi a tömeges informatikai támadások végrehajtását. A lényegét az elektronikus formában megjelenő nagy mennyiségű adat, információ jelenti („Big Data" jelenség)[4]. 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 lehetőséget nyújt a határon átívelő bűnözés számára. 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, a bűnözői infrastruktúrájukat is különböző államokból irányíthatják. Ez pedig olyan összetett joghatósági és illetékességi kérdéseket vet fel a büntető eljárásjogban, amelyek a mai napig megválaszolásra várnak.

Az internet egyben decentralizált és rugalmas hálózatok létrehozására ad lehetőséget, amelyek az elkövetők laza szerveződését segítik elő például, hogy egymás között megoszthatják a szakmai tudásukat és jártasságukat, valamint az általuk kifejlesztett technikai eszközöket. Az internet egyben egy kommunikációs csatornaként is szolgál, amely a különböző bűncselekmények elkövetésében is fontos szerepet tölthet be. Ennek következtében napjainkra a kiberbűnözés egy profit-orientált, szolgáltatás-alapú üzleti modellé nőtte ki magát, amelynek motorját az online feketegazdaság adja (pl. Darknet fórumok), ahol a különböző kibertámadásokat elősegítő eszközök és egyéb illegális szolgáltatások is elérhetőek. 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, de a terrorizmus képviselői is előszeretettel használják az internetet, legyen szó illegális online kereskedelemről vagy propagandaterjesztésről.

Azzal, hogy a sértettekkel egy távoli kapcsolatfelvételt garantál, az internet megszünteti azokat a szociális akadályokat is, amelyekkel az elkövetőknek a valóságban, akár egy személyes találkozáskor kellene szembenézniük. Az ilyen típusú bűnözésre magas látencia

[4] A „Big Data" kifejezés az interneten megjelenő hatalmas mennyiségű adatmennyiségre utal, amely új társadalmi jelenségként a jogalkotást és a jogalkalmazást is kihívások elé állítja. Lásd ZŐDI Zsolt: Jog és jogtudomány a Big Data korában. Állam- és Jogtudomány 2017/1. 95. o.

jellemző, mert a gyanútlan felhasználók sokszor nem is észlelik, hogy bűncselekmény áldozatává váltak és a hatóságok felé nem jelentik az esetet (pl. bankkártya visszaélések, pénzintézetek ellen intézett támadások), amely tovább nehezíti a felderítést.

Az információs rendszerek segítségével és az internet közbeiktatásával könnyedén lehet végrehajtani adat- vagy program manipulációt minimális költségek mellett, mert az információk 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 (pl. a WannaCry zsarolóvírus), vagy egy botnet-hálózat segítségével az elkövetők nagyszabású támadásokat tudnak végrehajtani, amely akár az adott rendszer teljes leállásához is vezethet.[5]

2017-ben a kiberbűnözés által okozott kár 600 milliárd dollár értékben realizálódott a különböző sértetti köröknél (pl. vállalatok, pénzintézetek, kormányzati szervek stb.) és a szakértők szerint ez 2021-re meg fog duplázódni. Mindez úgy gondolom, rávilágít arra, hogy mekkora lehetőség rejlik az új technológiák által nyújtott előnyök bűnelkövetési célú felhasználásában, ugyanakkor mekkora veszélyt és kockázatot hordoz a felhasználókra nézve.[6]

Az utóbbi években Magyarországon is jelentős emelkedés tapasztalható az informatikai bűncselekmények számában. Míg öt évvel ezelőtt csak 250 csalást követtek el információs rendszer felhasználásával, addig 2017-ben ez megközelítette a 4 és fél ezret. Ez idő alatt az információs rendszer vagy adat megsértésével kapcsolatos regisztrált bűncselekmények száma megtízszereződött, 52-ről 580-ra nőtt.[7]

2. Az értekezés tárgya és szerkezete

A disszertációmban elsősorban büntető anyagi jogi, és csak érintőlegesen büntető eljárásjogi kérdésekkel foglalkozom. Továbbá kizárólag az ún. tisztán informatikai bűncselekményekre, valamint a technológiai fejlődésnek az egyes – tágabb értelemben vett – gazdasági bűncselekményekre gyakorolt hatására fókuszálok.

[5] KOOPS, Bert-Jaap: The Internet and its Opportunities for Cybercrime. Tilburg School Legal Studies Paper Series No. 2011/9. 740-741. o.
[6] MCAFEE: Economics Impact of Cybercrime – No Slowing Down Report February 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf [2018.05.23.]
[7] LAJTÁR István: A kiberbűnözésről. Ügyészek Lapja 2019/1. 49. o.

Az értekezés négy nagy szerkezeti részre tagolódik. A bevezetést követő II. fejezetben a kiberbűnözés fogalmának a tisztázásával foglalkozom, ami azért is különösen fontos, mert máig nincs egy általánosan elfogadott jogi definíciója. Törekedtem mind a nemzetközi, mind a hazai szakirodalmi álláspontok széleskörű bemutatására, amelyek összevetése alapján meghatározható az informatikai bűnözés tágabb és szűkebb értelemben vett fogalmába tartozó bűncselekményi kör.

Ezt követően a kiberbűnözés elleni fellépés nemzetközi és uniós vonatkozásaival foglalkozom. Továbbá kiemelten vizsgálom az Egyesült Államok szabályozás történetét, amely elsőként szankcionálta és határozta meg az informatikai bűncselekmények széleskörét, ezért a kutatási téma szempontjából megkerülhetetlen.

A történeti részt követően az egyes kiberbűncselekményeket részletesen elemzem. Összehasonlítom a nemzetközi és uniós rendelkezéseket, valamint a hatályos hazai és amerikai szabályozás szerinti tényállásokat. Az alábbi három fő kibertámadás büntetőjogi minősítésével kezdem: a jogosulatlan belépéssel, illetve a DDoS-támadásokkal és a rosszindulatú programokkal. Ezután, az informatikai környezetben elkövetett csalással és zsarolással, valamint az egyéb informatikai visszaélésekkel kapcsolatos kérdésekkel (pl. személyes adatokkal és jelszavakkal való visszaélés) folytatom.

A III. fejezetben a modernizációnak a gazdasági bűncselekményekre gyakorolt hatásával kapcsolatos problémakört vizsgálom. Kiemelten érintem a bankkártyákkal összefüggő deliktumokat, ezen kívül a szervezett bűnözés megjelenését az interneten és a pénzmosás aktuális kérdéseit. A témakört a kriptovaluták büntető anyagi és eljárásjogi kihívásainak bemutatásával zárom.

A IV. fejezetben kiemelt szerepet kap az elektronikus bizonyítékokkal összefüggő szabályozási újdonságok bemutatása, így a hazai büntetőeljárásról szóló törvény[8] (a továbbiakban: Be.) hatályos rendelkezései és az erre vonatkozó uniós jogalkotási törekvések. Kiemelten foglalkozom továbbá a titkosítást és az anonimitást biztosító technológiák nyomozásra gyakorolt hatásával, valamint a joghatósági kérdésekkel a kiberbűncselekmények elkövetése esetén.

[8] 2017. évi XC. törvény a büntetőeljárásról

3. A kutatás módszerei

Az értekezés elkészítése során a témakör szempontjából lényeges nemzetközi, uniós, magyar és angolszász jogforrások kerültek felhasználásra. A joganyagok elemzése mellett az egyes részeknél hangsúlyt fektettem a vonatkozó joggyakorlatok bemutatására, valamint az adott kérdésköröket tárgyaló, releváns nemzetközi, hazai jogirodalmat és kutatási eredményeket dolgoztam fel.

A téma sajátos jellegéből adódóan interdiszciplináris keretek között tekintem át a technológiai fejlődés következtében megjelenő új kihívásokat és az ezekre adható válaszokat a büntetőjogban. A jogösszehasonlító módszertan szintén jelen van az értekezésben. Összevetem a különböző szabályozási szinteket és azok rendelkezéseit, illetve a vonatkozó joggyakorlatot, különös figyelemmel azok hasonlóságaira és különbözőségeire.

A kutatás során alkalmazom még továbbá a normatív és a dogmatikai módszert, valamint a az egyes részeknél a logikai és kritikai elemzés is szerepet kap is.

4. A kutatás célja, problémafelvetés

Az értekezésemben a következő kutatási kérdésekre keresem a választ:

1. Alkalmas-e a jelenlegi szabályozási környezet nemzetközi, uniós és hazai szinten, valamint az Egyesült Államokban a kiberbűnözés elleni fellépésre?
2. Képes-e a hazai büntetőjogi szabályozás és jogalkalmazás reagálni, alkalmazkodni a technológiai fejlődés következtében bekövetkezett változásokra az egyes gazdasági bűncselekmények esetén?
3. Alkalmasak-e az uniós és a hazai törekvések a büntetőeljárás során felmerülő technológiai kihívásokkal kapcsolatos aktuális szabályozási kérdések megoldására, különös tekintettel az elektronikus bizonyítékokra?

II. AZ INFORMATIKAI BŰNCSELEKMÉNYEK

1. A kiberbűnözés (informatikai bűnözés) fogalma

A kibertér (cyberspace) fogalmát először William Gibson amerikai író fogalmazta meg az 1984-ben megjelent „Neuromancer" című regényében, amikor elnevezést keresett a globális számítógépes hálózatra, amely összeköti az embereket, a számítógépeket és az információforrásokat. Az ebből képzett angolszász cybercrime[9] kifejezésből 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[10] (a továbbiakban: Budapesti Egyezmény) is ezt alkalmazza (Convention on Cybercrime). Az értekezésem során az informatikai bűnözést és kiberbűnözést mint szinonim fogalmakat fogom használni, mert ezek a szakirodalomban elfogadottak. Azonban fontos megjegyezni, hogy a kiberbűnözésnek még nincs egy általánosan elfogadott és egységes jogi definíciója.

Kezdetben eltérő elnevezéseket használtak, így a számítógépes bűnözést (computer crime), amely kizárólag a számítógépre helyezi a hangsúlyt (sőt egyes országok máig ezt használják a hazai szabályozásuk keretében[11]), illetve az internetes vagy virtuális bűnözést (internet crime[12] vagy virtual crime), amely kizárólag az internetre fókuszál, valamint a csúcstechnológiás bűnözést (high-tech crime) és elektronikus vagy digitális bűnözést, azonban utóbbi elnevezések túl tág fogalmi keretet adnak.

David Wall írt először az informatikai bűnözés „evolúciójáról", amely alapján megkülönbözteti az informatikai bűnözés fejlődésének több generációját:

- az első generáció közé tartoznak azon hagyományos bűncselekmények, amelyek elkövetéséhez a számítógépet és az internetet használták fel;
- a második generáció esetén a klasszikus bűncselekmények mellett megjelentek már az új típusú informatikai bűncselekmények is;

[9] Érdekesség, hogy a „cybercrime" fogalmát az Oxford Dictionary úgy határozza meg, hogy olyan büntetendő cselekményeket foglal magában, amelyeket a számítógépek vagy az internet segítségével követnek el.
[10] Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye, amelyet a 2004. évi LXXIX. törvénnyel hirdettek Magyarországon
[11] Például az Egyesült Államok, Kína, az Egyesült Királyság és Szingapúr. Lásd ehhez WANG, Qianyun: A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. Erasmus University of Rotterdam. Rotterdam, 2016. 7. o.
[12] Lásd JEWKEY, Yvonne – YAR, Majid (eds.): Handbook of Internet Crime. Willan Publishing, 2010.

- a harmadik generációba pedig azok a modern kori informatikai bűncselekmények tartoznak, amelyek az informatikai eszközök használata nélkül nem lehetne elkövetni.[13]

A Budapesti Egyezmény ugyan a kiberbűnözés fogalmát nem határozza meg, de útmutató jelleggel a bűncselekményeket csoportosítja a következőképpen:

- számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények (offences against the confidentiality, integrity and availability of computer data and systems),
- a számítógéppel kapcsolatos bűncselekmények (computer-related offences),
- a számítástechnikai adatok tartalmával kapcsolatos és szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények (content-related offences).

A kiberbűncselekményeket különböző szempontok mentén lehet csoportosítani, ezek közül kiemelném az Alisdair A. Gillespie által használtat:

- a számítógépekkel szembeni bűncselekmények (pl. informatikai bűncselekmények),
- vagyon elleni bűncselekmények (pl. csalás, virtuális tárgy „lopás”),
- a tiltott tartalommal kapcsolatos bűncselekmények (pl. gyermekpornográfia),
- valamint a személy elleni bűncselekmények (pl. zaklatás, cyberbullying).[14]

Megállapítható, hogy az informatikai környezetben elkövetett bűncselekmények motívumai, céljai nem térnek el a valós térben elkövetett bűncselekményekétől, mert ugyanúgy elkövethetők haszonszerzés vagy károkozás céljából, valamint az adatok, titkok kifürkészése végett vagy akár szexuális indíttatásból.[15]

Marije T. Britz a számítógépes bűncselekmény fogalmát általánosan határozza meg, amelybe beletartozik minden olyan bűncselekmény, amelyet számítógép használatával követnek el.[16] Hasonlóan értelmezi Eoghan Casey is, de pontos meghatározással nem szolgál, csak utal arra, hogy ebbe a kategóriába kizárólag azon bűncselekmények tartoznak, amelyek elkövetésekor a számítógép a bűncselekmény eszközeként vagy tárgyaként jelenik meg.[17] Britz emellett még a számítógéppel kapcsolatos bűncselekmény (computer-related crime) fogalmát használja és szerinte a számítógéppel kapcsolatos minden olyan bűncselekmény ebbe a körbe tartozik, amelynek az elkövetése során a számítógép bármilyen módon, akár közvetetten is jelen (pl. a zsarolás e-mail útján történik).[18]

[13] WALL, David: Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. International Review of Law, Computers and Technology 2008/1-2. 45-63. o.
[14] GILLESPIE, A. Alisdair: Cybercrime – Key Issues and Debates. Routledge, 2016. 7-8. o.
[15] NAGY (2009): i.m. 34. o.
[16] BRITZ, Marija T.: Computer Forensics and Cyber Crime: An Introduction. Pearson. London, 2013. 6. o.
[17] CASEY, Eoghan: Digital Evidence and Computer Crime. Elsevier. Amsterdam, 2012. 37. o.
[18] BRITZ: i.m. 6. o.

A szakirodalomban több szerző is, így Jonathan Clough[19], Peter Grabosky[20] és Susan W. Brenner[21] is a kiberbűnözésre mint egy gyűjtőfogalomként tekint, amelynek két fő kategóriája különböztethető meg: az egyik azon deliktumok csoportja, amelyeket kizárólag információs rendszerekkel (pl. számítógépekkel, azok hálózatával vagy egyéb ICT eszköz használatával) követhetők el. Jellemzően ezeknek a bűncselekményeknek a tárgya az információs rendszer. Ezek a tisztán informatikai bűncselekmények vagy kiberbűncselekmények, az ún. cyber-dependent crime (pl. számítógépes vírusok használata, hacking stb.). A második tágabb kategóriába tartoznak azok a hagyományos bűncselekmények, amelyeket az információs rendszerek felhasználásával követnek el, mint például a csalás, a zsarolás, a gyermekpornográfia, szerzői jogi jogsértések, a zaklatás és még sorolhatnánk. Ez az ún. cyber-enabled crime esetköre, amikor az információs rendszer a bűncselekmény elkövetésének az eszköze.[22] Az Europol is éves jelentéseiben azonos jelentéstartalommal használja ezeket a fogalmakat, de részben eltérő elnevezéssel, így a cyber-dependent crime-ot, valamint a cyber-facilitated crime-ot.

Egy harmadik kategória is megkülönböztethető, ami a bűncselekmény elkövetésének járulékos hozamaként jelenik meg, azonban ennek inkább csak büntető eljárásjogi szempontból van jelentősége, például amikor a számítógép vagy az adat mint bizonyíték használható fel (pl. gyermekpornográf tartalom vagy a bűncselekménnyel összefüggésbe hozható digitális nyomok mint például a keresési előzmény, üzenetváltás, kép-, videó-, és hangfelvétel stb.).

Ezen csoportosítást – vagy ezek változatait – használják az angolszász jogrendszert (common law) alkalmazó országokban is, többek között az Egyesült Államokban[23], az Egyesült Királyságban[24] és Ausztráliában[25].

A hazai szakirodalomban is több szerző foglalkozott az informatikai bűnözéssel kapcsolatos fogalommeghatározásokkal. Kezdetben Polt Péter, Pusztai László és Nagy Zoltán András[26] -

[19] CLOUGH: i.m. 10-11. o.
[20] GRABOSKY, Peter: Cybercrime. Oxford University Press, 2016. 8-9. o.
[21] BRENNER, W. Susan: Cybercrime – Criminal Threaths From Cyberspace. Praeger, 2010. 39-47 o.
[22] CLOUGH: i.m. 10-11. o.; A „cyber-related crime" elnevezést használja az Egyesült Államok Igazságügyi Minisztériuma, amikor a hagyományos bűncselekmény elkövetésének az 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
[23] COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION: The National Information Infrastructure Protection Act of 1996.
[24] MCGUIRE, Mike – DOWLING, Samantha: Cyber crime: A review of evidence, Summary, 2013. 5. o.
[25] ATTORNEY'S GENERAL'S DEPARTMENT (Australia): National plan to compay cybercrime. 2013. 4-5. o.
[26] PUSZTAI László: Számítógép és bűnözés. In: Gödöny József (szerk.): Kriminológiai és Kriminalisztikai Tanulmányok 26. OKRI, Budapest, 1989. 85. o.

Ulrich Sieber nyomán[27] - az elkövetési tárgyakat a német joghoz hasonlóan alapvetően két részre, a hardverre és a szoftverre különítették el, és utóbbival összefüggésben foglalkoztak a számítógépes visszaéléssel, a számítógép-kikémleléssel, a számítógépes szabotázzsal, valamint a gépidőlopással.[28]

Parti Katalin és Kiss Tibor szerint a számítástechnikai bűnözést, a számítástechnikai rendszerekkel kapcsolatos bűnözést, az internetes bűnözést és az informatikai bűnözést az egyes szerzők eltérően határozzák meg. Nincs azonban egységes definíciójuk, és nincs egyetértés arra vonatkozólag, hogy az egyes cselekmények mennyiben kapcsolódnak a számítástechnikai rendszerekhez és mennyiben az internethez, továbbá, hogy e két felülettel való kapcsolatuk mennyiben kizárólagos, valamint meghatározó. Az informatikai bűnözést a következőképpen definiálják: „az informatikai bűnözés a számítástechnikai bűnözés és az internetes bűnözés csoportjába tartozó magatartásokat kizárólagos módon magában foglaló kategória, amely egyben a kétfajta bűncselekmények közös halmazát is tartalmazza. A számítástechnikai bűnözés a számítástechnikai rendszerek és hálózatok integritását sérti, míg az internetes bűnözés esetében az internet mint elkövetési színtér, médium jelenik meg".[29]

Szathmáry Zoltán az informatikai bűncselekmények védett jogi tárgyaira és elkövetési tárgyaira tekintettel a következő fogalmat határozta meg: „azon bűncselekmények, melyek az információs rendszerek zavartalan működését, a bennük tárolt adatok megbízhatóságához, hitelességéhez, titokban maradásához, illetve az ezekhez fűződőt egyéb (nemzetbiztonsági, államigazgatási, gazdasági vagy személyes érdeket) sértik, vagy veszélyeztetik."[30]

A magyar jogirodalomban a külföldi szerzőkhöz hasonló fogalmat dolgozott ki Szabó Imre, aki úgy határozta meg a számítástechnikai bűncselekményeket, mint azok a „deliktumok, melyek egy számítógépes rendszerrel vagy számítástechnikai adattal kapcsolatba hozhatók, akár úgy, hogy az elkövetés eszközeként jelennek meg, vagy pedig a bűncselekmény elkövetési tárgyát képezik".[31]

Mindezekre tekintettel megállapítható, hogy a kiberbűnözés esetén egyrészt olyan új típusú bűncselekményekről beszélhetünk, amelyek kizárólag az információs rendszerek segítségével

[27] SIEBER, Ulrich: A számítógépes bűnözés és más bűncselekmények az információtechnológia területén. Magyar Jog 1993/2. 105-109. o.
[28] NAGY Zoltán András: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda. Belügyi Szemle 1999/11. 16-27. o.
[29] PARTI Katalin – KISS Tibor: Az informatikai bűnözés. In: Borbíró Andrea - Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft., 2017. 491-493. o.
[30] SZATHMÁRY Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. Doktori Értekezés (PTE ÁJK) Budapest, 2012. 79-80. o.
[31] SZABÓ Imre: Informatikai bűncselekmények. In: Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve. Budapest, Complex, 2008. 547. o.

követhetők el és olyan speciális védett jogi tárggyal rendelkeznek, mint amilyen az információs rendszer vagy adat. Másrészt ide tartoznak azok a már meglévő, hagyományos bűncselekmények is, amelyek sokkal könnyebben elkövethetők az új elkövetési eszközök segítségével.

Az informatikai bűnözés fogalmán kívül fontos vizsgálni a kapcsolódó alapvető fogalmakat is, így különösen a számítógépét. A modern technológiák rendkívül gyors fejlődésének következtében a definiálása egyre nagyobb kihívást jelent, mert a fogalmi keretet tágítja az új informatikai eszközök megjelenése. Manapság már az okostelefonok is rendelkeznek olyan processzorral, mint egy hagyományos asztali számítógép, valamint egyre több más „okos" eszköz is erős kapacitással bír. Éppen ezért az elkövetők már a különböző IoT eszközöket, például routereket, biztonsági kamerákat vagy akár az okostelevíziókat, gépjárműveket és egészségügyi berendezéseket veszik célba egy-egy kibertámadás során.

A jogalkotók részéről két megközelítés figyelhető meg a számítógép fogalmával kapcsolatban: vagy nem határozzák meg (pl. az Egyesült Királyság, Ausztrália és Kanada), vagy egy átfogó definíciót alkalmaznak (pl. az Egyesült Államok).[32]

A Budapesti Egyezmény köztes megoldást alkalmaz, mert ugyan a számítógép fogalmát nem, de a „számítástechnikai rendszerét" (computer system) definiálja a következőképpen: „a számítástechnikai rendszer minden olyan eszköz, illetőleg egymással kapcsolatban lévő vagy összekötött eszközök összessége, amelyek, illetőleg amelyeknek egy vagy több eleme egy adott programnak megfelelően adatok automatikus feldolgozását végzi". Röviden összefoglalva a számítógép egy program által vezérelt – hardver és szoftver részekből álló – eszköz, amely automatikus adatfeldolgozást végez. Ez magában foglalhatja a beviteli-kiviteli és adattároló eszközöket is. A hálózat pedig kettő vagy több számítástechnikai rendszer közötti kapcsolat, amelynek típusa közömbös, lehet akár vezetékes vagy vezeték nélküli, a lényeg, hogy információcserére kerüljön sor a hálózaton belül.[33]

Az Európai Parlament és Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról[34] (a továbbiakban: 2013-as irányelv) már a kor kívánalmainak megfelelően, technikai értelemben is tágabb információs rendszer (information system) fogalmát használja. Ez azt jelenti, hogy nem szűkíti le a fogalmi kört kizárólag a számítógépre (személyi számítógépekre), hanem az új meghatározás alkalmasabb arra, hogy kifejezze azt, hogy egy

[32] CLOUGH: i.m. 59. o.
[33] COUNCIL OF EUROPE: Explanatory Report to the Convention on Cybercrime. European Treaty Series – No. 185. 2001.
[34] 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.

szélesebb eszközkör tartozik ide, és már az olyan új modern eszközök is mint a táblagépek, az okostelefonok vagy az egyéb adattovábbítást és a kapcsolatfelvételt biztosító informatikai berendezések és ez a kör idővel még bővülni fog.[35]

A 2013-as irányelv alkalmazásában az „információs rendszer" magában foglal „minden olyan eszközt, illetve összekapcsolt vagy kapcsolódó eszközökből álló eszközcsoportot, amelyek közül egy vagy több valamely program alapján automatikus adatfeldolgozást hajt végre számítógépes adatokon, valamint a működése, használata, védelme és karbantartása céljából az ezen eszköz vagy eszközcsoport által tárolt, feldolgozott, helyreállított vagy továbbított számítógépes adatokon." Ezt a fogalmat vette át a hatályos 2012. évi C. törvény a Büntető Törvénykönyvről (a továbbiakban: Btk.) is a 459. § 15. pontjában, amelynek értelmében „információs rendszer minden olyan berendezés – vagy egymással kapcsolatban lévő ilyen berendezések összesége –, amely automatikusan végez adatfeldolgozást, azaz adatok bevitelét, kezelését, tárolását, továbbítását látja el."[36] Az információs rendszerek körébe tartoznak a számítástechnikai adatfeldolgozásra épülő memóriával rendelkező olyan egységek is, amelyek megjelenésükben eltérnek a „hagyományos" számítógépektől (pl. közcélú távbeszélő-szolgáltatás, információs rendszerek felhasználásával működő hírközlési, telekommunikációs rendszerek stb.).[37]

Az amerikai Computer Fraud and Abuse Act (a továbbiakban: CFAA) pedig a „számítógép" (computer) fogalmát a 1030. § (e)(1) pontjában az alábbiak szerint határozza meg: „olyan elektronikus, mágneses, optikai, elektrokémiai vagy egyéb nagysebességű adatfeldolgozó eszközt jelent, amely logikai, matematikai vagy tárolási funkciókat lát el, ezen felül magában foglal olyan adattárolásra vagy kommunikációra szolgáló egységet is, amely közvetlenül kapcsolódik az eszközhöz vagy párhuzamosan működik azzal, kivéve az automatizált írógépeket, zsebszámológépeket és hasonló eszközöket."

Ez a definíció a számítástechnikai rendszer fogalmára ugyan nem utal, azonban magában foglalja az „olyan adattárolásra vagy kommunikációra szolgáló egységet, amely közvetlenül kapcsolódik vagy párhuzamosan működik" a számítógéppel így például egy router is ide tartozik.

[35] SORBÁN Kinga: Vírusok és zombik a büntetőjogban - Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. In Medias Res 2018/2. 372. o.
[36] Btk. 459. § (1) bekezdés 15. pont
[37] MOLNÁR Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Kónya Sándor (szerk.): Magyar Büntetőjog - Kommentár a gyakorlat számára (Harmadik kiadás). HVG-ORAC Budapest, 2016. 946. o.

A CFAA-ban szabályozott kiberbűncselekmények elkövetési tárgyának általában védett számítógépnek kell lennie, ezért ezzel kapcsolatban fontos vizsgálni ennek a fogalmát is. A 1030. § (e)(2) bekezdés (A) pontja szerint olyan számítógép, amely „pénzintézet, vagy az Egyesült Államok kormányának kizárólagos használatában áll, illetőleg olyan számítógép, amely nem áll kifejezetten ilyen használatban, de pénzintézet vagy az Egyesült Államok kormánya által vagy annak érdekében használják, és e cselekmény befolyásolja a számítógépnek a használatát.” Továbbá a (B) pont szerint, „amelyet államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve államközi vagy nemzetközi kommunikációra használnak, illetve amelynek a használata érinti ezeket, beleértve azt a számítógépet is, amely az Egyesült Államokon kívül található, azonban olyan módon használják, hogy az hatással van az Egyesült Államok államközi kereskedelmére vagy nemzetközi kereskedelmére vagy kommunikációjára.”

Orin Kerr kritikával illette a „védett számítógép” elnevezést, mert valamennyi internetre csatlakoztatott számítógépet államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve kommunikációra használnak, hiszen az internet egy nemzetközi hálózat, amit kifejezetten ilyen célokra alkalmaznak. Ezt szem előtt tartva bármely internetre csatlakoztatott számítógép lehet a CFAA-ban szabályozott bűncselekmény elkövetésének az eszköze vagy tárgya, így megfelelőbb lenne a „számítógép” elnevezés használata a „védett számítógép” helyett.[38]

[38] WANG (2016): i.m. 72-73. o.; 110–111. o.

2. Történeti áttekintés

2.1. A kiberbűnözés elleni nemzetközi és uniós szintű fellépés

2.1.1. Az OECD jelentés

Az első fontos nemzetközi jogi dokumentum a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) által kibocsátott 1986-os jelentés volt. Ezzel iránymutatást kívántak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez, valamint a kodifikáció elősegítéséhez. A büntetendő cselekmények körét is már rendszerezte a következőképpen azonban még a számítógépes csalás nélkül:

- számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elrejtése jogtalan vagyoni eszközök vagy más értékek megszerzése céljából;
- számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elrejtése hamisítás céljából;
- számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elrejtése vagy a számítógépbe történő bármely más beavatkozás abból a célból, hogy a számítógépes vagy telekommunikációs rendszerek funkcióinak megakadályozása céljából;
- a védett számítógépes programok tulajdonosainak exkluzív jogainak megsértése a program jogosulatlan hasznosítása vagy forgalomba hozatala révén;
- a számítógépes vagy telekommunikációs rendszerbe az arra jogosult engedélye nélkül vagy a biztonsági intézkedések megsértésével vagy más tisztességtelen vagy bűnös szándékkal történő belépés vagy annak lehallgatása.

2.1.2. Az Európa Tanács 9. (89.) és 95. (13.) számú ajánlása

Az Európa Tanács a 1980-as évek második felében állított fel egy szakértői bizottságot a számítógépes bűncselekményekkel kapcsolatos ismeretek összegyűjtésére és a veszélyek felmérésére. A bizottság kiemelt célja volt, hogy egy - a kriminalizálandó magatartásokat tartalmazó - ajánlást dolgozzanak ki a tagállamok számára. Az első uniós dokumentum így az Európa Tanács (a továbbiakban: ET) 9 (89). számú ajánlása (Computer-Related Crime) lett, amely tartalmaz egy minimum listát. Ez a lista iránymutatásként szolgált a tagállamok jogalkotói számára, amennyiben az ilyen típusú bűncselekmények esetében új jogszabályokat hoznak, vagy a meglévőket módosítani kívánják, akkor abban az esetben kötelezve vannak arra, hogy az ajánlással összhangban járjanak el. Az ajánlás felhívja a figyelmet arra is, hogy

kizárólag egy egyetemes, kötelező erejű jogi dokumentum megalkotásával és elfogadásával tudnak hatékonyan fellépni lépni az új típusú bűnözéssel szemben.

A minimumlista a következőket tartalmazza:

- a számítógépes csalást,
- a számítógépes hamisítást,
- a számítógépes adatokban és programokban történő károkozást,
- a számítógépes szabotázst,
- a jogellenes behatolást (a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén),
- a jogellenes titokszerzést és
- a védett számítógépes programok jogellenes másolását.

Továbbá tartalmaz egy fakultatív listát is, amelynek az elemei pedig a következők:

- a számítógépes adatok és/ vagy programok megváltoztatása,
- a számítógépes kémkedés,
- a számítógép jogellenes használata és
- a védett programok jogellenes használata.[39]

Henrik W. K. Kaspersen kiemelte, hogy a büntető anyagi szabályozás mellett az eljárásjogi kérdésekkel is együttesen foglalkozni kell.[40] Ulrich Sieber is felhívta a figyelmet a határon átnyúló együttműködés fontosságára, különösen a különböző szervezetek közötti összehangolt tevékenységekre az informatikai bűnözés leküzdéséhez, mert eddig hiányozott a kölcsönös bűnügyi jogsegély és a nemzetközi nyomozás megteremtésének az alapja.[41] A büntető eljárásjogi aggodalmakra válaszul megszületett az ET. 95. (13.) számú ajánlása, amely kifejezetten az információs technológiákkal kapcsolatos eljárási problémákra törekedett megoldást nyújtani, így például érinti a házkutatást és lefoglalást, a technikai megfigyelést, a kötelezettséget a nyomozó hatóságokkal való együttműködésre, az elektronikus bizonyítékokat, a titkosítás használatát, a statisztikát és képzéseket, valamint a nemzetközi együttműködés során felmerülő kérdésekre ad választ.[42]

---

[39] GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN kód megadása vagy biztonságosan az Internet? Pécsi Határőr Tudományos Közlemények XIII. 237-238. o.

[40] KASPERSEN, Henrik W.K.: Implementation of Recommendation No. R (89) 9 on Computer-related Crime. Strasbourg, March 1997, Doc. CDPC (97) 5 and PC-CY (97) 5, 106. o.

[41] SIEBER, Ulrich: Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study. prepared for the European Commission, 1 January 1998.

[42] SCHJOLBERG, Stein: The history of global harmonization on cybercrime legislation – the road to Geneva. 2008. 5. o., https://cybercrimelaw.net/documents/cybercrime_history.pdf [2017.06.21.]

2.1.3. A Számítástechnikai Bűnözésről Szóló Egyezmény

2001 novemberében Budapesten írták alá az Európa Tanács által előkészített Számítástechnikai Bűnözésről Szóló Egyezményt[43] (a továbbiakban: Budapesti Egyezmény). A Budapesti Egyezmény az Európa Tanács tagjain kívüli országok előtt is nyitva áll, akik szintén aláírhatják és ratifikálhatják. Az eddigi ajánlásokhoz képest továbblépést jelentett és újabb jogi normákat fogalmazott meg. A számítógépes technikai fogalmakat már definiálja és ezáltal egységes értelmezést nyújt. A következő fogalmakat határozza meg: a számítástechnikai rendszer (computer system), számítástechnikai adat (computer data), szolgáltató (service provider), illetve átmenő adat (traffic data). Mind az anyagi, mind az eljárásjogi szabályozást tartalmazza. Az anyagi jogban a tényállások köre bővült, újabb jogsértéseket szabályoz (pl. eszközökkel való visszaélés, a gyermekpornográfiával kapcsolatos bűncselekmények). Az egyes bűncselekménytípusokat logikusan csoportokba rendezi.

A Budapesti Egyezmény négy részre osztható fel: 2-13. Cikk a büntető anyagi jogi részt tartalmazza, a 14-22. Cikk a büntetőeljárás jogi résszel foglalkozik (14 - 22. Cikk), amely magában foglalja az eljárásjogi rendelkezések alkalmazási körét, a forgalmi adatok valós idejű összegyűjtését az internetes szolgáltatók részéről, valamint a joghatósági kérdésekkel zárul. A 23-35. Cikk pedig a nemzetközi együttműködésre vonatkozó irányelveket fogalmaz meg. Valamennyi aláíró felet kötelezi a kölcsönös jogsegélynyújtásra, illetve a nyomozások és eljárások során történő együttműködésre, különösen az elektronikus bizonyítékok összegyűjtése érdekében. Végül a 36-48. Cikk a záró rendelkezésekben az egyezmény hatályára, a fenntartásokra, a módosításokra, a viták rendezésére és az egyezmény felmondására vonatkozó részekre térnek ki.

Az anyagi jogi szabályozás terén kimondja, hogy minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, amelyek ahhoz szükségesek, hogy a belső jogával összhangban bűncselekménynek minősüljenek az alábbi cselekmények jogosulatlan és szándékos elkövetése: a számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények (I. cím) körében a jogosulatlan belépés (2. cikk), a jogosulatlan kifürkészés (3. cikk), a számítástechnikai adat megsértése (4. cikk), valamint a számítástechnikai rendszer megsértése (5. cikk), végül az eszközökkel való visszaélés (6. cikk).

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

A második bűncselekménycsoportot a számítógéppel kapcsolatos bűncselekményekként határozza meg (II. cím), amelyek körében a számítógéppel kapcsolatos hamisítást (7. cikk) és a számítógéppel kapcsolatos csalást (8. cikk) különbözteti meg.

Végül a harmadik csoportot a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények (III. cím) képezik: a gyermekpornográfiával kapcsolatos bűncselekmények (9. cikk) és a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények (10. cikk).

Továbbá kötelezi a szerződő feleket, hogy kijelöljenek egy éjjel-nappal, a hét minden napján elérhető kapcsolattartási pontot[44], annak érdekében, hogy lehetővé tegye az informatikai bűncselekményekkel kapcsolatos nyomozásokkal vagy az elektronikus bizonyítékok összegyűjtésével kapcsolatos azonnali segítségnyújtást, valamint technikai tanácsok és jogi információk átadására is lehetőség van, ezenkívül még a gyanúsítottak tartózkodási helyének meghatározását és az adatok megőrzését is segíthetik (35. Cikk).

2003-ban a Budapesti Egyezményt kiegészítették a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló jegyzőkönyvvel.

A rendelkezéseivel összhangban a Büntető Törvénykönyvről szóló 1978. évi IV. törvény (a továbbiakban: 1978. évi Btk.) 300/C. §-ába a számítástechnikai rendszer és adatok elleni bűncselekményt vezették be, valamint egyéb más törvényi tényállásokat kiegészítettek a meghatározottak szerint, azonban ennek részletes bemutatására a későbbiekben kerül sor.[45]

Ugyanebben az évben az Európai Tanács 2001/413/IB kerethatározatát fogadták el a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről.[46] A fizetőeszköz fogalmát a törvényes fizetőeszközök (bankjegyek, érmék) kivételével és példálózó jelleggel határozza meg (pl. hitelkártya, csekkek és váltók stb.). A kerethatározat kötelezi a tagállamokat, hogy harmonizálják a büntetőjogi szabályaikat, és bűncselekménynek minősítsék az alábbi fizetési eszközökkel kapcsolatos büntetendő magatartások körét:

- a fizetőeszköz ellopása vagy más módon történő jogellenes eltulajdonítása;
- fizetőeszköz jogosulatlan felhasználás céljából történő hamisítása vagy meghamisítása;

[44] Magyarországon az Országos Rendőr-főkapitányságnak a Nemzetközi Bűnügyi Együttműködési Központja, valamint a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya a kijelölt 24/7-es kapcsolattartási pont.
[45] NAGY (2009): i.m. 40-56. o.
[46] A Tanács 2001/413/IB kerethatározata (2001. május 28.) a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről. HL L 149/1. 2001.6.2.

- lopott vagy más módon jogellenesen eltulajdonított, illetve hamis vagy hamisított fizetőeszköz elfogadása, megszerzése, szállítása, más személy részére történő értékesítése vagy átruházása, illetve birtoklása jogosulatlan felhasználás céljából;
- lopott vagy más módon jogellenesen eltulajdonított, illetve hamis vagy meghamisított fizetőeszköz jogosulatlan felhasználása, valamint
- a számítógépes csalás, amikor az adatmanipuláció vagy a jogosulatlan beavatkozás útján pénz vagy pénzbeli érték átruházására vagy átruháztatására kerül sor, és ezzel másnak vagyoni hátrány okoznak jogtalan haszonszerzés céljából.

2002-ben az Európai Parlament és a Tanács 2002/58/EK elektronikus hírközlési adatvédelmi irányelvét[47] fogadták el, amelynek célja, hogy biztosítsa a felhasználóknak az elektronikus hírközlési és technológiai szolgáltatások iránti bizalmát. Ezek a szabályok különösen a „spamek" betiltására, a felhasználó előzetes beleegyezését kérő (opt-in) rendszerre és a cookie-ek telepítésére vonatkoznak. Ez az irányelv 2009-ben egészült ki az ún. „süti" (cookie) irányelvvel[48], amely alapján a viselkedésalapú reklám célba juttatásához használt sütik kizárólag az érintettek hozzájárulását követően helyezhetők el a felhasználók számítógépein.[49]

2011-ben az Európai Parlament és Tanács 2011/93/EU számú irányelvét fogadták el a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről[50]. 2012-ben ezzel szoros összefüggésben kezdetét vette egy nemzetközi összefogás a „Globális szövetség a gyermekek online szexuális kizsákmányolása ellen" elnevezéssel, amelyhez az uniós országokon kívül más országok is csatlakoztak.

[47] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv"). HL L 201/37. 2002.7.31.

[48] Az Európai Parlament és a Tanács2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról. HL L 337/11. 2009.12.18.

[49] http://adatvedelmiaudit.hu/2011/06/cookie-k-csak-hozzajarulassal/ [2017.09.21.]

[50] Az Európai Parlament és a Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról. HL L 335/1. 2011.12.17.

2.1.4. A 2005/222/IB tanácsi kerethatározat az információs rendszer elleni támadásokról

Újabb változás 2005-ben történt, amikor az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat elfogadására került sor. [51] A kitűzött célok között szerepelt, hogy a számítógépes bűnözés elleni küzdelmet és az információbiztonságot előmozdítsák az Európai Unióban. Ezen kívül a transznacionális bűnözés ezen új formáját tekintve az igazságügyi és egyéb illetékes hatóságok közötti együttműködés javítása az információs rendszerek elleni támadásokra vonatkozó büntetőjogi szabályok közelítésével, különösképpen az információs rendszerekhez és adatokhoz való jogsértő hozzáférés, valamint beavatkozás esetén. Fogalommeghatározásokat is tartalmaz (információs rendszer, számítógépes adatok, jogi személy, jogosulatlanul), ezeket azonban a kerethatározatot felváltó 2013-as irányelv is átveszi, ezért ezt a vonatkozó résznél ismertetem a későbbiekben.

Az Európai Unióról szóló és az Európai Unió működéséről szóló szerződés 83. cikk (1) bekezdése pedig kimondja és ezáltal jogalapot biztosítva, hogy „az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében elfogadott irányelvekben szabályozási minimumokat állapíthat meg a bűncselekményi tényállások és a büntetési tételek meghatározására vonatkozóan az olyan különösen súlyos bűncselekmények esetében, amelyek jellegüknél vagy hatásuknál fogva a több államra kiterjedő vonatkozásúak, illetve amelyek esetében különösen szükséges, hogy az ellenük folytatott küzdelem közös alapokon nyugodjék. Ezek a bűncselekményi területek a következők: terrorizmus, emberkereskedelem és a nők és gyermekek szexuális kizsákmányolása, tiltott kábítószer-kereskedelem, tiltott fegyverkereskedelem, pénzmosás, korrupció, pénz és egyéb fizetőeszközök hamisítása, számítógépes bűnözés és szervezett bűnözés.”

Erre tekintettel „A polgárokat szolgáló és védő, nyitott és biztonságos Európa” című 2010-ben kiadott a tamperei és hágai programot követő ún. stockholmi program az Európát érintő jövőbeli kihívások között említi a számítógépes bűnözést.

[51] A Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról. HL L 69/67, 2005.3.16.

2.1.5. Az ENISA és a Kiberbűnözés Elleni Európai Központ

A 460/2004/EK európai parlamenti és tanácsi rendelet[52] létrehozta az Európai Hálózat és Információbiztonsági Ügynökséget (a továbbiakban: ENISA) mint kiberbiztonsági szakértői központot, amely szervezettel a cél, hogy hozzájáruljon az Unión belüli magas és hatékony szintű hálózat- és információbiztonság biztosításához, valamint – a polgárok, a fogyasztók, a vállalkozások és a közigazgatási szervek érdekeit szem előtt tartva – a hálózat- és információbiztonsági kultúra kialakításához. Az ENISA megbízatását több alkalommal hosszabbították meg egészen 2020. június 19-ig.

2019 áprilisában elfogadták azt a kiberbiztonsági jogszabályként is ismert rendeletet[53], amely bevezeti az Európai Uniós Kiberbiztonsági Ügynökséget, amely átveszi a jelenlegi ENISA szerepét a jogutódjaként, valamint az egész EU-ra kiterjedő tanúsítási rendszerek keretét, amely az információs és kommunikációs technológiákkal (a továbbiakban: ICT) kapcsolatos termékekkel, szolgáltatásokkal és folyamatokkal szembeni megfelelőssági szabályok, műszaki követelmények, szabványok és eljárások uniós szinten meghatározott átfogó rendszere. A megújult ügynökség célkitűzései között az alábbiak szerepelnek:

- Az uniós intézmények, szervek és hivatalok, valamint a tagállamok számára segítséget nyújt a kiberbiztonsággal kapcsolatos uniós – többek között az ágazati – szakpolitikák kidolgozásában és végrehajtásában.
- Az Unión belüli kapacitásépítés és felkészültség támogatásához járul hozzá a kiberbiztonsági készségek és kompetenciák fejlesztése érdekében azáltal, hogy segítséget nyújt a hálózati és információs rendszerek védelmének fokozásában, a kiberellenálló képesség és a kiberbiztonsági eseményekre való kapacitások fejlesztésében és javításában.
- A kiberbiztonsággal kapcsolatos kérdésekben elő kell mozdítania az uniós szintű együttműködést – beleértve az információmegosztást – és koordinációt a tagállamok, az uniós intézmények, szervek és hivatalok, valamint a köz- és a magánszféra releváns érdekelt felei között.

[52] Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. HL L 77. 2004.3.13.

[53] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). HL L 151/15. 2019.6.7.

- Az uniós szintű kiberbiztonsági képességek növeléséhez járul hozzá annak érdekében, hogy támogassa a kiberfenyegetések megelőzése és az azokra való reagálás terén tett tagállami intézkedéseket, különösen a határokon átnyúló biztonsági események esetében.
- Az európai kiberbiztonsági tanúsítás használatának az előmozdítása a belső piac széttagoltságának elkerülése érdekében.
- A kiberbiztonsági tudatosság növelésének az elősegítése (pl. minden év októberében koordinálja az „Európai Kiberbiztonsági Hónap" elnevezésű kampányt).[54]

Emellett az ENISA a kiberbűnözés elleni hatékony küzdelem az európai biztonsági stratégiában is kiemelt fontosságot élvez, hiszen hozzájárul a magas szintű kiberbiztonság elérésének általános céljához.

Azonban fontos külön említést tenni az uniós szintű bűnüldöző hatóságokról és ezek szerepéről az informatikai bűnözés elleni küzdelemben. Először az Europol szervezetén belül 2002-ben hozták létre a Csúcstechnológiai Bűnözési Központot (High Tech Crime Centre).[55]

Később 2013. január 11-től kezdte meg működését a Kiberbűnözés Elleni Európai Központ (a továbbiakban: EC3), amely az európai polgárok és vállalkozások számítástechnikai bűnözéssel szembeni védelméhez nyújt segítséget. A központot az Europol hágai székhelyén hozták létre és az EU kiberközpontjaként működik. Az EC3 a következő bűncselekményekre fókuszál: amelyeket szervezett bűnözői csoportok követnek el, mint például az online csalás, illetve amelyek súlyos kárt okoznak az áldozataiknak (pl. gyermekpornográfia), továbbá amelyek kritikus infrastruktúrákat érintenek.[56] A központon belül a Focal Point Terminal nyomoz a nemzetközi fizetési csalásokkal kapcsolatban, együttműködve az érintett intézményekkel, az Európai Központi Bankkal és a nemzeti bankokkal, akik valós idejű hozzáférést biztosítanak az információs adatbázisukhoz és az igazságügyi informatikai vizsgálatokhoz. A Focal Point Cyborg harcol a high-tech bűncselekményekkel szemben, kiemelten kezelve azokat, amelyek a kritikus infrastruktúrákat támadják. A Cyborg az Europol malware elemző rendszerét (European Malware Analyst System, avagy EMAS) alkalmazza annak érdekében, hogy segítse az igazságügyi informatikai vizsgálatokat és az ún. Joint Investigation Teams munkáját, hogy hatékonyan feltudják deríteni a nagyobb horderejű, nemzetközi automatizált műveleteket, mint például a botnet-hálózatókat. Az említett elemző rendszer a sandbox technológiára épül, amelyre a rendvédelmi szervek a további vizsgálatok

[54] Kiberbiztonsági jogszabály 4. cikk (1)-(7) bekezdés
[55] SZALÁRDI Gábor: A csúcstechnológiai bűnözés elleni küzdelem támogatása. Belügyi Szemle 2012/6. 98-99.o.
[56] PARTI Katalin – KISS Anna: A számítástechnikai bűnözésről akkor és most. In: Bárd Petra – Hack Péter – Holé Katalin: Pusztai László emlékére. OKRI. Budapest, 2014. 300. o.

elvégzése érdekében elektronikus úton töltik fel a felderített ügyek során felmerülő kártékony program mintázatokat, valamint az ezekkel összefüggésben keletkezett adatokat, ami után az egység az általa tett megállapításokat egy részletes jelentésben küldi vissza (pl. a rosszindulatú program azonosítását).[57]

A Focal Point Twins pedig a gyermekek szexuális kizsákmányolásával és bántalmazásával kapcsolatos eseteket vizsgálja (pl. szexuális zsarolás, ún. grooming[58]). Emellett áldozatazonosítási munkacsoport (Victim Identification Task Force) is működik, amelynek célja az ismeretlen áldozatokkal kapcsolatban rendelkezésre álló anyagok elemzése.[59]

Aktív szerepet vállal több ügynökség is a központ portfóliójának a kialakításában. A legfőbb partnerek ebben: az ENISA, az Európai Unió Bűnüldözési Képzési Ügynöksége (CEPOL), European Cybercrime Task Force (EUCTF) és az Interpol. Az EC3 egyben összeköti a különböző bűnüldöző hatóságokat, a Számítástechnikai Sürgősségi Reagáló Egységeket (CERT), iparágakat és a tudományos közéletet. További kezdeményezés eredményeképpen az ún. Joint Cybercrime Action Taskforce (J-CAT) pedig összefogja a szakértelmet a különféle kapcsolatfenntartó hatóságokkal az EU-n kívül is, hogy koordinálják a nemzetközi választ az azonosított, magas fokú fenyegetésekre. A J-CAT 2014-ben indult köszönhetően az EC3, EUCTF, FBI és az Egyesült Királyság Nemzeti Bűnüldözési Ügynökség (NCA) közös együttműködésének (pl. az általuk végrehajtott sikeres akcióként könyvelhető el többek között a zsarolásban élenjáró DD4BC elnevezésű csoport tagjainak a kézre kerítése).

Az EC3-nak stratégiai funkciója is van, mert egybegyűjti a szaktudás és az információkat, támogatja a bűnügyi nyomozásokat és elősegíti az egész Unióra kiterjedő megoldásokat. A stratégiai elemzéseken keresztül átfogó tanácsokat nyújt a döntéshozók számára a jövőbeli kiberbűnözői trendekre és módszerekre vonatkozóan. Az EC3 egyéb stratégiai feladatai között szerepel a prevenció, a lakosság tudatosságának növelése és a partnerségi kapcsolatok

[57] SZONGOTH Richárd – VETTER Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. Belügyi Szemle, 2018/7-8. 9. o., valamint BUONO, Laviero: Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, Volume 4. No. 3. 2012. 340-342. o.

[58] Az ún. sextortion, vagyis a szexuális zsarolás során az elkövető a gyermek bizalmába férkőzik (pl. a felnőtt fiatalkorúnak adja ki magát és barátkozik a gyermekkel, kifejezetten szexuális tartalmú anyagot mutat neki, hogy csökkentse a szexualitáshoz kapcsolódó gátlásait) és kihasználja a sebezhetőségét annak érdekében, hogy a gyermeket ábrázoló szexuális jellegű képekhez vagy videókhoz jusson hozzá, amit végül a zsarolás fázisa követ. Az elkövető kényszeríti, zsarolja az áldozatát, hogy szexuális szívességet teljesítsen a részére, vagy további kompromittáló képeket vagy videókat küldjön magáról, amennyiben a kérésnek nem tesz eleget, akkor a már birtokában lévő felvételnek a megosztásával fenyeget (pl. a közösségi médián keresztül), és ezzel már irányítása alá vonja a gyermeket. A grooming, vagyis a szexuális célú kapcsolatfelvétel a gyermek szexuális bántalmazásának az előkészítését jelenti, amely során az elkövetőt az motiválja, hogy a gyermeket a saját szexuális vágyának a kielégítésére használja fel. Lásd DORNFELD László – MEZEI Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog, 2017/1. 32-37. o.

[59] SZONGOTH – VETTER: i.m. 10-11. o.

szélesítése uniós szinten.[60] Az EC3 szakértelme az igazságügyi informatika területén is figyelemre méltó, mert saját laboratóriumot hozott létre, amely a legkorszerűbb segítséget nyújt, és emellett saját független technológiai kutatást és fejlesztést is végez.[61]

Érdemes megemlíteni az Interpol szerepét is a kiberbűnözés elleni fellépésben, mert a nemzetközi színtéren hasonló módon hozzájárul a kölcsönös tapasztalatcsere, a rendvédelmi szervek állományának képzése, a kapacitás bővítés és az operatív, valamint forenzikus tevékenysége révén.[62]

2.1.6. Az Európai Parlament és Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról

Az Európai Unió fontos lépéseket tett a kiberbiztonság és a digitális technológiákba vetett bizalom növelése érdekében. 2013-ban elfogadásra került az EU kiberbiztonsági stratégiája, amely irányt szabott az Unió kiberbiztonsági fenyegetésekre és kockázatokra adott politikai válaszlépései kidolgozásának és célként kitűzi a számítástechnikai bűnözés drasztikus csökkentését. A stratégia következőképpen határozza meg a fogalmát: „A kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket.”

Ennek fényében elfogadásra került Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013 (III.21.) Korm.határozat is, amely a következő definíciót adja: „a kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.”

A kiberbiztonság tehát számos eszközt foglal magában, így jelentős szerep jut az ipari szereplőkkel való együttműködésnek, a technikai fejlesztésnek és a prevenciónak. A

[60] MEZEI Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. Jura 2018/1. 353. o.; valamint https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [2017.10.21.]
[61] EUROPEAN PARLIAMENT'S POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS: Cybersecurity in the European Union and Beyond: Exploring the Threaths and Policy Responses. 2015. 53-54. o.
[62] https://www.interpol.int/Crimes/Cybercrime [2019.04.30.]

büntetőjogi fellépés a jogi eszközök közé tartozik, de fontos hangsúlyozni, hogy kizárólag ultima ratio megoldásként alkalmazható.

2013 augusztusában az Európai Parlament és Tanács elfogadta a már említett 2013-as irányelvet az információs rendszerek elleni támadásokról, amely a korábbi kerethatározatot váltotta fel és célja a számítástechnikai bűnözés elleni küzdelem megerősítése az információbiztonság előmozdítása, a szigorúbb nemzeti büntetőjogi szankciók és az illetékes hatóságok hatékonyabb együttműködése révén. A jogszabály megalkotásával a fő cél az volt, hogy minimumszabályokat határozzanak meg az információs rendszer elleni bűncselekményekre, valamint az ezekkel kapcsolatos büntetőjogi szankciókra vonatkozóan és az együttműködést elősegítsék a nemzeti rendvédelmi szervek és az erre specializálódott uniós szervek között, nevezetesen az Europol, az EC3, az Eurojust és az ENISA között.

Újdonság az ún. botnetekkel – avagy a számítógép-hálózatok távoli irányítására tervezett rosszindulatú számítástechnikai programokkal – kapcsolatos szabályozás. A 2013-as irányelv felhívja a figyelmet arra, hogy hatékony fellépésre van szükség, ezért biztosítani kell, hogy ugyanaz a bűncselekmény valamennyi tagállamban büntetendő legyen. A bűnüldöző hatóságok számára biztosítani kell a fellépéshez szükséges, az egymás közötti együttműködést elősegítő eszközöket az alábbi büntetendő magatartások körében: az információs rendszerekhez való jogellenes hozzáférés, az információ rendszerekbe vagy adatokba való jogellenes beavatkozás, a jogellenes adatszerzés, valamint a kiberbűncselekmények elkövetéséhez használt eszközökkel kapcsolatos előkészületi magatartások. Az egyes bűncselekményeket a későbbiekben elemzem részletesen. A tagállamoknak olyan szankciókat kell megállapítaniuk az információs rendszer elleni bűncselekményekre, amelyek hatékonyak, arányosak és visszatartó erejűek.

A hatékony prevenció érdekében a hatóságoknak együtt kell működniük a magánszférával és a civil társadalommal, amely kiterjedhet a szolgáltatók által a potenciális bizonyíték megőrzésére, együttműködési és partnerségi hálózat kiépítésére velük és a gyártókkal. A kiberbűnözés elleni küzdelem terén kiemelt szerep jut a magánszektornak, ami túl mutat azon, hogy csak az elektronikus bizonyítékok megszerzését segítsék, hanem akár hozzájárulhatnak a jogsértő tartalmak eltávolításához, valamint a teljes bűnözői infrastruktúrák felszámolásához.[63]

A 2013-as irányelv a jogi személyek felelősségével kapcsolatos rendelkezéseket és a velük szemben alkalmazandó szankciókat is tartalmazza a kerethatározathoz hasonló módon, valamint a joghatósági kérdésekre is választ ad.

[63] Lásd bővebben ehhez TROPINA, Tatiana: Public-Private Collaboration: Cybercrime, Cybersecurity and National Security. In: Tropina, Tatiana – Callanan, Cormac (eds.): Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer, 2015. 1-37. o.

Ezeken kívül a hatékony fellépés érdekében a tagállamok gondoskodnak saját operatív nemzeti kapcsolattartó pontjuk létrehozásáról, és arról, hogy igénybe veszik a meglévő, a hét minden napján 24 órában rendelkezésre álló hálózatot. A tagállamok olyan eljárások működését is biztosítják, amelyek révén sürgős segítségkérés esetén az illetékes hatóság a kézhezvételtől számított 8 órán belül jelezheti legalább azt, hogy teljesíti-e a segítségkérést, valamint, hogy ezt milyen formában és várhatóan mikor teszi. Továbbá tagállamoknak biztosítani kell egy olyan rendszer meglétét, amely rögzíti, előállítja és rendelkezésre bocsátja az informatikai bűncselekményekre vonatkozó statisztikai adatokat. Az 2013-as irányelvet a tagállamoknak 2015. szeptember 4-ig kellett implementálniuk.

2.1.7. A NIS irányelv

Végül érdemes említést tenni a 2016-ban elfogadott hálózati és információs rendszerek biztonságáról szóló ún. NIS irányelvről[64] is, amely az uniós polgárok online védelmének javítását tűzte ki célul a kiberbiztonság területén. Ugyanis a kiberbiztonság fenntartásának egyik eszköze az elektronikus hálózati és információs rendszerek biztonsága, amely egyben lefedi az adatok és információs rendszerek biztonságát. A hálózati és információs rendszerek biztonsága az arra való képességet jelenti, hogy ellenálljon mindazon fenyegetéseknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított, kezelt adatok, vagy ezen rendszereken nyújtott, vagy a rajtuk keresztül elérhető kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát. A hálózat és információbiztonság, vagyis a szűken vett kiberbiztonság, kiterjed az elektronikus hírközlő hálózatokra vonatkozó adatvédelmi (tárolt, továbbított, kezelt adatok biztonsága) és hálózatok ellenállását növelő szabályokra.

Ez az első olyan uniós szintű szabályozás az információbiztonság területén, amely egy közös intézményt és eszköztárat biztosít a tagállamok számára, valamint egy európai szintű együttműködésnek az alapjait határozza meg. Ennek megfelelően elkülöníthetünk nemzeti, valamint közösségi szinten végrehajtandó feladatokat. Éppen ezért az ENISA kulcsfontosságú szerepet kapott a NIS irányelv végrehajtásának támogatásában, valamint minden tagállamnak ki kell jelölnie egy vagy több – akár szektoronként egy-egy – számítógép-biztonsági eseményekre reagáló csoportot (CSIRT), amely legalább az adott szektor incidenskezelésért felelős.

[64] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. HL L 194/1. 2016.8.19.

A NIS irányelv a hatályát tekintve két csoportra osztható. Elsőként definiálja a gazdaság és a társadalom számára létfontosságú, ún. alapvető szolgáltatásokat nyújtó szereplők csoportját, melybe – a kritikus infrastruktúrák meghatározott köre – a digitális infrastruktúrák, energetika, közlekedés, banki szolgáltatások, pénzügyi szolgáltatások, egészségügyi szektor tartozik, illetve a másik csoportba pedig a kulcsfontosságú digitális szolgáltatók tartoznak (keresőprogramok[65], felhőalapú számítástechnikai szolgáltatás[66], online piacterek[67]).[68] Az alapvető szolgáltatásokat nyújtó szereplőknek az alábbi kötelezettségeknek kell eleget tenniük:

- Megfelelő és arányos műszaki és szervezési intézkedéseket kell tenniük a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében (pl. a biztonsági kockázatmenedzsment keretében sérülékenységi teszteket végeznek). A hálózati és információs rendszerek tekintetében az említett intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell biztosítaniuk.
- A szolgáltatás nyújtása során megfelelő intézkedéseket tesznek az alkalmazott hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére annak céljából, hogy biztosítsák az említett szolgáltatások folytonosságát. A biztonsági esemény alatt minden olyan eseményt kell érteni, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára.
- Indokolatlan késedelem nélkül bejelentik az illetékes hatóságnak vagy a CSIRT-nek az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket.[69]

[65] NIS irányelv 4. cikk 18. pont: „online keresőprogram: olyan digitális szolgáltatás, amelynek segítségével a felhasználók elvben valamennyi weboldalon, illetve konkrét nyelvű weboldalakon kulcsszó, kifejezés vagy egyéb formában megadott lekérdezés alapján bármilyen témában kereséseket végezhetnek, és amely ennek eredményeként olyan hivatkozásokat ad meg, ahol a keresett tartalommal kapcsolatos információk találhatók."

[66] NIS irányelv 4. cikk 19. pont: „felhőalapú számítástechnikai szolgáltatás: olyan digitális szolgáltatás, amely megosztható számítástechnikai erőforrások méretezhető és rugalmas pooljához enged hozzáférést."

[67] NIS irányelv 4. cikk 16. pont: „online piactér: olyan digitális szolgáltatás, amely a 2013/11/EU európai parlamenti és tanácsi irányelv 4. cikke (1) bekezdésének a) és b) pontjában meghatározott fogyasztók és/vagy kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek."

[68] Magyarországon a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete látja el az eseménykezelési feladatokat a létfontosságú információs rendszerek és rendszerelemek esetén, illetve az az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben meghatározott bejelentés-köteles szolgáltatást – úgymint online piactér, internetes keresőszolgáltatás, valamint felhőszolgáltatás – nyújtó szolgáltatók esetében az eseménykezelési, valamint a hatósági felügyeletet.

[69] TÓTH András: Hálózati és információs rendszerek biztonsága európai szabályozásának alapjai. Infokommunikáció és jog 2017/1. 16-24. o.

A fent felsorolt szektorokban a tagállamoknak ki kell jelölniük a meghatározott szempontok figyelembevételével a hatálya alá eső vállalatokat, cégeket. Ehhez szektoronként pontosítani, specializálni kell a NIS irányelv rendelkezéseiben megfogalmazott kijelölés kritériumait.[70]

2.2. A kiberbűnözés elleni fellépés az Egyesült Államokban

2.2.1. A kezdeti szabályozási törekvések 1984-ig

Az Egyesült Államokban szövetségi rendszer működik, ezért a kiberbűnözés elleni fellépés is kétszintű. A szövetségi szintű szabályozás egységes, területi hatálya az Egyesült Államok egész területére kiterjed, míg az egyes állami szintek egymástól eltérhetnek és csak az adott államok területén érvényesek. Az értekezésben kizárólag előbbit mutatom be, méghozzá a Computer Fraud and Abuse Act vonatkozó rendelkezéseit, amely kifejezetten az informatikai bűncselekmények szabályozását célozza.[71]

A törvényt 1984-ben fogadták el „Counterfeit Access Device and Computer Fraud and Abuse Act" elnevezéssel, amelyet később 1986-ban az első módosítással egybekötve változtattak meg „Computer Fraud and Abuse Act"-re. A CFAA-t megelőzően néhány jogtudós azon a véleményen volt, hogy a számítógépes bűncselekmények lényegében hagyományos bűncselekményeknek tekinthetők, amelyeket különböző technológiai eszközök használatával követnek el, ezért velük szemben a tradicionális büntetőjogi rendelkezések alkalmazását megfelelőnek gondolták. Mások úgy vélték, hogy ezek nem nyújtanak segítséget a számítógépes bűnözéssel szemben, éppen ezért új törvény megalkotására van szükség, mert a korábbi szabályozásnál még nem vették figyelembe az informatika felértékelődött szerepét a bűnelkövetésben, és alkalmazásuk nem megfelelő a számítógépes bűncselekmények esetében. Például erre először a United States vs. Seidlitz-ügy[72] hívta fel a figyelmet, amelyet követően fokozatosan felismerték, hogy a jelenlegi szabályozás nem bizonyul hatékonynak, illetve ezen bűncselekmények, amelyek a számítógépeket célozták vagy azok felhasználásával követtek el, lényegesen különböznek más bűncselekményektől, ezáltal egy új és egyedülálló kategóriát alapoztak meg. 1977-ben, végül konszenzus eredményeképpen született meg a „Bill of the

[70] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, HL L 194/1. 2016.7.19.

[71] CASEY: i.m. 85. o.

[72] Az első számítógépes csalás ügy, amelynél felmerült, hogy a hagyományos wire fraud (18 U.S.C. 1343. §) rendelkezései nem alkalmazhatóak megfelelően, és a terheltet nem lehetett volna felelősségre vonni, amennyiben a bűncselekményt nem az állami határon átnyúlóan követte el.

Federal Computer Systems Protection Act" (a továbbiakban: BFCSPA), ami azonban túlságosan tágan határozta meg a kriminalizált magatartások körét és a számítógép fogalmát is kritika illette, illetve nem nyújtott megfelelő adatvédelmet. Mindezt figyelembe véve végül nem fogadták el a törvényt. Az új típusú bűncselekmények szabályozására, így egészen a CFAA-ig kellet várni, amely kezdetben három bűncselekményt vezetett be.[73] Az első 1030. § (a)(1) bekezdésben szabályozott bűncselekmény a nemzetbiztonsági titok biztonságához fűződő érdek védelmét biztosította, amelynek értelmében büntették a számítógéphez való jogosulatlan hozzáférést abból a célból, hogy az illető nemzetbiztonsági információt szerezzen meg, azzal a szándékkal, hogy az Egyesült Államoknak ártson ezzel vagy külföldi kormányt előnyhöz juttasson. A második bűncselekményt a személyes pénzügyi információk védelmében alkották meg a 1030. § (a)(2) bekezdésében, amely tényállás büntetni rendeli azt, aki a számítógéphez jogosulatlanul hozzáfér, abból a célból, hogy a pénzintézet pénzügyi nyilvántartásában vagy a fogyasztóvédelmi ügynökség számítógépén tárolt pénzügyi információt szerezzen meg. A harmadik bűncselekmény pedig kifejezetten az Egyesült Államok kormányzati számítógépeinek védelméhez kapcsolódott, így a 1030. § (a)(3) bekezdése értelmében bűncselekményt követ el, aki a számítógéphez jogosulatlanul fér hozzá azért, hogy az Egyesült Államok kormányzati számítógépén tárolt információt használja, módosítsa, megsemmisítse, közzé tegye, és ezáltal a számítógép működését befolyásolja.[74]

Azonban a CFAA egyik fő hiányossága kezdetben az volt, hogy nem lehetett megfelelően alkalmazni, vagyis a gyakorlatban nem bizonyult hatékonynak, ezt jelzi, hogy a kihirdetésétől kezdve két évig nem indult a hatálya alá tartozó büntetőeljárás. Először is, a BFCSPA hibáiból okulva, a CFAA megalkotásakor már ügyeltek arra, hogy korlátozzák a BFCSPA-hez képest a törvény hatályát és elkerüljék a magánélet védelméhez fűződő jogok, valamint a szabadságjogok csorbítását. Ezt figyelembe véve a CFAA a védelmet kizárólag a pénzügyi nyilvántartások és fogyasztói információk, illetve a kormányzati tulajdonban lévő azon számítógépek számára biztosította, amelyekhez kormányzati vagy gazdasági érdek fűződött. Emiatt kritika is érte, mert a magánszektorhoz, illetve a magánszemélyekhez tartozó számítógépek[75], valamint azok, amelyek nem a fent említett információkhoz kapcsolódtak kívül estek a törvény tárgyi hatálya alól, vagyis a személyi számítógépeken tárolt személyes információk vagy pénzügyi nyilvántartásokon kívül eső hitelkártyák nem voltak a CFAA által

[73] WANG (2016): 99-100. o.
[74] KERR, Orin: Vagueness Challenges to the Computer Fraud and Abuse Act. Minnesota Law Review 2010. 1564. o.
[75] BRENNER, Susan W.: Cybercrime and the law: Challenges, issues and outcomes. Northeastern University Press, 2012. 25. o.

védve. A törvény további hiányossága, hogy nem tudott mit kezdeni azzal az esettel, ha a számítógéphez a jogosultságainak kereteit túllépve fértek hozzá az adott információhoz, ezért ezt később orvosolni kellett.[76]

2.2.2. A CFAA első módosítása 1986-ban

1986-ban módosították és kiterjesztették a CFAA hatályát, amelynek köszönhetően könnyebben lehetett alkalmazni a gyakorlatban. A törvényt ért kritikák miatt az első módosítás a bűnösségre terjedt ki, ugyanis a „tudatos" (knowingly) elkövetést felváltotta a „szándékos" (intentionally) a 1030. § (a)(2) és a (a)(3) bekezdésekben szabályozott bűncselekményeknél, illetve a jogosulatlan hozzáférés mellett már (actus reus kiterjesztése) a jogosultság kereteinek túllépését is szankcionálták.

Az angolszász jog szerint akkor állapítható meg a bűncselekmény elkövetése, ha megtörtént a bűnös cselekmény (actus reus, a bűnös tett), és arra az elkövető tudatállapota kiterjedt, azaz a cselekményt ő követte el, annak megtörténtét kívánta (mens rea, a bűnös tudat). Mindkét fogalmi elemnek meg kell valósulnia ahhoz, hogy a bűncselekmény megállapítható legyen.

„A common law országaiban a bűnösség a mens rea tág értelmű fogalma, amely szubjektív vagy objektív kritériumokon vagy a kettő kombinációján nyugszik. A büntetőeljárás során azt kell bizonyítani, szubjektív értelemben, hogy az elkövetőnek tempore criminis volt szubjektív viszonyulása a cselekményhez, míg objektív értelemben azt, hogy az elkövetés idején ilyen szubjektív viszonyulással nem rendelkező elkövetőre az értelmes, elvárható magatartást folytató személy tesztjét lehet alkalmazni (és elítélni)."[77]

Ezzel összevetve a bűnösség megnyilvánulási formáinál a következők vizsgálandók a hazai büntetőjogban: a tudati oldal, amely az elkövetőnek azon képességét jelenti, hogy képes előre látni a cselekményének következményeit és átlátja (tudata átfogja) az objektív tényállási elemeket, valamint az akarati (érzelmi) oldal, amely pedig a cselekményhez, illetve annak következményeihez való érzelmi viszonyulását jelenti.

A mens rea főbb formái 1030. § passzusai alkalmazásában a következők: „intentionally", „knowingly", „recklessly" és a „negligently".[78] Az amerikai jogban használt szándékosság (intentionally) és tudatosság (knowingly) hasonlóságot mutatnak a magyar büntetőjog szerinti

[76] WANG (2016): i.m. 102-106. o.
[77] KARSAI Krisztina: Az alapelvek rendszere az európi büntetőjogban. MTA doktori értekezés. Szeged, 2015. 75. o.
[78] A szövetségi jog általában nem követi a Model Penal Code rendelkezéseit, azonban a 1030. § rendelkezéseiben a jogalkotó átvette annak a mens rea-ra vonatkozó részét [2.02 General Requirements of Culpability Art. (2) (a)-(d)]. Lásd KERR Orin S.: Computer Crime Law. Fourth Edition. West Academic Punlishing 2018. 113. o.

szándékosság két formájához. A szándékosság direkt formája is a magatartás következményének a kívánásán alapul, míg a tudatos elkövetés esetén a következményébe való belenyugváson. Gondatlanságból követi el a bűncselekményt, aki előre látja cselekményének lehetséges következményeit, de könnyelműen bízik azok elmaradásában (recklessly, avagy tudatos gondatlanság), vagy cselekménye lehetséges következményeit azért nem látja előre, mert a tőle elvárható figyelmet vagy körültekintést elmulasztja (negligently, avagy hanyagság). Azonban különbség, hogy az eshetőleges szándék és a tudatos gondatlanság meghatározásánál és egymástól való megkülönböztetésénél már nem az elkövető magatartásának (lehetséges) következményeihez való érzelmi akarati viszonyulását, hanem az eredmény bekövetkezésének valószínűségét veszik figyelembe. A szándékosság megállapítását kívánás hiányában csak az eredmény bekövetkezésének gyakorlatilag teljes bizonyossággal való előre látása alapozza meg. Az ennél alacsonyabb valószínűség már a tudatos gondatlanság körébe tartozik. Előfordulhat az is, hogy valamelyik tényállási elem tekintetében a felelősség bűnösségre tekintet nélküli (strict liability), míg a többi tényállási elemre kiterjed valamelyik bűnösségi forma. A strict felelősség egy sajátos, a magyar jogban nem létező kategória.[79]

A módosítás további három új tényállást is kodifikált a 1030. § (a)(4)-(6) bekezdésekben. Az 1030. § (a)(4) bekezdés büntetendővé tette a számítógéphez való jogosulatlan hozzáférést csalási szándékkal, amely alapvetően, a hagyományos „wire fraud" elkövetésének felel meg számítógéppel. 1030. § (a)(5) bekezdés értelmében felelősségre vonható az, aki jogosulatlanul hozzáfér a számítógéphez és információt módosít, megrongál, megsemmisít vagy az engedélyezett használatot megakadályozza. A 1030. § (a)(6) bekezdés a számítógépes jelszavakkal való visszaélést tiltja. Az 1030. § (a)(4) és (5) bekezdés a szövetségi érdekű számítógépek (federal interest computers) védelmére korlátozódott. Ezek közé tartoznak azok a számítógépek az (A) pont szerint, amelyeket az Egyesült Államok kormánya vagy a pénzintézetek használnak, vagy a (B) pont szerint azok, amelyek több államot átívelő számítógépes hálózat részeként jelennek meg. Az (A) pont a korábbi szabályozást fedi le, míg a (B) pont új, bár korlátozott alapot jelentett, mert csak akkor alkalmazható, ha több államot érintő bűncselekményt követnek el, az államok közötti hálózaton keresztül. Ekkor azonban az internet használata még nem terjedt el széleskörben, így kevés bűncselekmény tartozott ebbe a körbe.[80]

[79] MISKOLCI László: A bűnösség alapkategóriái az angol büntetőjogban. Magyar Jog 2002/2. 100-117. o.
[80] WANG (2016): i.m. 106-107. o.

2.2.3. Az 1988 és 1990 közötti módosítások

Az 1988 és 1990 közötti időszakban három módosítása is volt a törvénynek, amelyek szintén a CFAA hatályát terjesztették ki, és elsődlegesen a pénzügyi biztonság, illetve a különböző pénzintézetek védelmét voltak hivatottak megerősíteni. Az 1988-as módosítás a pénzintézet (financial institution) fogalmát bővítette azáltal, hogy a korábbiaktól eltérően nemcsak kizárólag a hitelkártya kibocsátókat, hanem valamennyi pénzintézetet a törvény hatálya alá vonta. A 1989-es módosítás a bank kifejezés helyett a pénzintézetet használja, amely világosan meghatározza, hogy azon intézetek tartoznak ide, amelyeknek a betétjei biztosítva vannak a Federal Savings and Loan Insurance Corporation által. Az 1990-es módosítás további két ponttal bővítette a pénzintézet fogalmát.

2.2.4. A CFAA ötödik módosítása 1994-ben

A CFAA 1994-es módosítása révén bővült a bűnösség (mens rea) köre és büntetendővé vált a gondatlanságból (recklessness) történő elkövetése a 1030. § (a)(5) bekezdésben szabályozott bűncselekménynek, amely tényállásnak a törvényi megfogalmazása is változott a korábbihoz képest. Ez az ún. vírus rendelkezés, amely alapján büntetőjogilag felelősségre vonható, aki jogosulatlanul továbbít programot, információt, kódot vagy parancsot – ez különösen a számítógépes kártékony programokra vonatkozik –, és ezáltal szándékosan kárt okoz, illetve amennyiben gondatlanságból okoz kárt, azt is büntetni rendeli egy másik bekezdés keretében.[81]

A módosítás lehetővé tette a sértettek számára az elkövetővel szembeni polgári jogi kártérítési igényt az őket ért informatikai bűncselekmény következtében bekövetkezett kár és veszteség megtérítéséért.[82]

2.2.5. The National Information Infrastructure Protection Act 1996

Kezdetben a 1030. § (a)(2) bekezdés csak azokat az eseteket szankcionálta, amelyek során az elkövetők olyan információt szereztek meg, amit a pénzintézet pénzügyi nyilvántartásában vagy a fogyasztóról a fogyasztóvédelmi szerv nyilvántartásában tároltak. Az 1996-os módosítás révén azonban bármely információ megszerzése büntetendővé vált, amennyiben egynél több államot érintett.

[81] WANG (2016): i.m. 108. o.
[82] BRENNER (2012): i.m. 27. o.

A módosítás továbbá a 1030. § (a)(7) bekezdésben új bűncselekményt vezetett be, a számítógépes zsarolást, amelyet a későbbiekben a hatályos szabályozásnál részletesen elemzek.

A minősített esetek körét is bővítette a 1030. § (a)(4) bekezdésben, hozzáadva a következőket: „a fizikai sérülés bármely személynél következik be", illetve „a közegészségügyet és közbiztonságot érintő fenyegetés".

Végül a módosítás érintette a „szövetségi érdekű számítógép" fogalmát, mert ezt az új „védett számítógép" elnevezés váltotta fel, amely az (A) pont értelmében az a számítógép, amely „a pénzintézet vagy az Egyesült Államok kormányának kizárólagos használatában áll, illetve olyan számítógép, amely nem áll kifejezetten ilyen használatban, de pénzintézet vagy az Egyesült Államok kormánya által vagy annak érdekében használják, és e cselekmény befolyásolja a számítógépnek a használatát." Továbbá a módosítás révén a (B) pont szerint, „amelyet államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve államközi, illetve nemzetközi kommunikációra használnak".[83]

Az Economic Espionage Act pedig a kár fogalmának alkalmazását kiterjesztette a CFAA hatálya alá tartozó bűncselekményekre is, amelynek a meghatározása tartalmilag azonos a hatályos törvényben beépítettel.[84]

2.2.6. USA PATRIOT Act 2001

2001-ben az Egyesült Államok is aláírta és ratifikálta a Budapesti Egyezményt. Ugyanebben az évben a szeptember 11-ei terrortámadást követően az USA PATRIOT Act 2001 [85] elfogadására is sor került. A módosítás bővítette a védett számítógépnek minősülő gépek körét, kiegészítve a következőkkel: „amelyet államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve államközi vagy nemzetközi kommunikációra használnak, beleértve azt a számítógépet is, amely az Egyesült Államokon kívül található, azonban olyan módon használják, hogy az hatással van az Egyesült Államok államközi kereskedelmére vagy nemzetközi kereskedelmére vagy kommunikációjára". A definíció kiterjesztésével a cél az volt, hogy a törvény hatálya alá tartozzanak azok a számítógépek is, amelyek az Egyesült Államokon kívül találhatók.

[83] WANG (2016): i.m. 110. o.
[84] BRENNER (2012): i.m. 28. o.
[85] Az USA PATRIOT a törvény címének a rövidítése, amely a következő: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 és egyben hazafias törvényként is említik.

A 1030. § (a)(5) bekezdés új minősített esettel kiegészülve tiltja az Egyesült Államok kormányának szervei által vagy érdekében használt számítógépekben történő károkozást, különösen, amely az igazságszolgáltatást, a honvédelemet és a nemzetbiztonságot érinti.[86]

2.2.7. The Identity Theft and Enforcement and Restriction Act 2008

A törvény legaktuálisabb módosítására 2008-ban került sor, amely a 1030. § hatályát terjesztette ki azáltal, hogy törölték az államközi vagy nemzetközi kereskedem vagy kommunikáció (interstate or foreign communication) kitételt a 1030. § (a)(2)(C) pontból, és a módosítást követően a következőképpen néz ki: büntetendő az olyan védett számítógéphez történő jogosulatlan hozzáférés, amely – államok közötti vagy államon belüli – információt képes helyreállítani. További újdonság, hogy a minősített esetek körét is tovább bővítették, és bekerült az 5,000 $ értékhatár, illetve a tíz vagy több számítógépben okozott kár.[87]

A harmadik legjelentősebb változtatás a védett számítógép definíciójának (B) pontját érintette, és a hatályos törvény is ezt tartalmazza: „olyan számítógép, amelyet államközi kereskedelemre vagy nemzetközi kommunikációra, illetve államközi vagy nemzetközi kommunikációra használnak, illetve amelynek a használata érinti ezeket, beleértve azt a számítógépet is, amely az Egyesült Államokon kívül található, azonban olyan módon használják, hogy az hatással van az Egyesült Államok államközi kereskedelmére vagy nemzetközi kereskedelmére vagy kommunikációjára.” A korábbi szabályozáshoz képest a változást nehéz észrevenni, de lényegesen változott, mert azok a számítógépek is már ebbe a körbe tartoznak, amelyek hatással vannak – nem csak, amelyeket erre a célra használnak – az Egyesült Államok államközi kereskedelmére vagy nemzetközi kereskedelmére vagy kommunikációjára.[88]

2008-ig a 1030. § (a)(5) szakasz egy (A) és (B) bekezdésre volt tagolva. Az (A) további három pontot tartalmazott, amelyek közül az (1) a vírus és a DDoS-támadásokat szankcionálta, míg a (2) és a (3) a jogosulatlan hozzáféréssel okozott károkozó magatartásokat. Ezt a szabályozási felépítést azonban a módosító törvény megváltoztatta, ugyanis a 1030. § (a)(5)(A) pont alatt szabályozott bűncselekményt további alpontokra osztotta, és így alakult ki a hatályos szabályozás szerinti felosztás: a DDoS-támadásokra és a vírusokra vonatkozó 1030. § (a)(5)(A), a szándékos jogosulatlan hozzáférés gondatlan károkozással 1030. § (a)(5)(B), valamint a

[86] U.S. DEPARTMENT OF JUSTICE: Computer Crime and Intellectual Property Section Criminal Division: Prosecuting Computer Crimes. 2015. 5. o.; valamint WANG (2016): i.m. 111. o.
[87] WANG (2016): i.m. 111. o.
[88] KERR (2010): i.m. 1568-1571. o.

szándékos hozzáférés károkozással 1030. § (a)(5)(C). A korábbi (B) pont pedig a vonatkozó minősített esetek körét szabályozta.[89]

A hatályos CFAA-ban szabályozott kiberbűncselekmények, amelyeket a későbbiekben részletesen elemzek a következők:

- Nemzetbiztonsági információval való visszaélés [1030. § (a)(1)],
- Számítógéphez való jogosulatlan hozzáférés és információval való visszaélés [1030. § (a)(2)],
- Kormányzati számítógéphez való jogosulatlan hozzáférés [1030. § (a)(3)],
- Számítógépes csalás [1030. § (a)(4)],
- Számítógép vagy információ megsértése [1030. § (a)(5)],
- Hozzáférést biztosító jelszavakkal vagy egyéb információkkal való visszaélés [1030. § (a)(6)],
- Számítógépes zsarolás [1030. § (a)(7)].

A 1030. § (b) szakasz értelmében büntetendő a 1030. § (a) szakasz rendelkezéseiben szabályozott valamennyi bűncselekménynek a kísérlete és az elkövetésükben való megállapodás – mint előkészületi cselekmény – is.

A kiberbűncselekmények felderítése és nyomozása során az alábbi szövetségi bűnüldöző szerveknek van kiemelt szerepük: az Egyesült Államok Igazságügyi Minisztériuma alá tartozó Computer and Intellectual Property Section, valamint a Szövetségi Nyomozó Iroda (Federal Investigation Bureu, FBI), amelynek szervezetén belül ún. Cyber-Digital Task Force munkacsoportok működnek.[90]

[89] BRENNER (2012): i.m. 28-29. o.

[90] Lásd ehhez részletesen SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban. Themis 2016/1. 166-169. o.

3. A jogosulatlan belépés, avagy a hacking a büntetőjogban

3.1. Általános bevezető

Az első büntetendő magatartás, amivel részletesen foglalkozom az a jogosulatlan belépés vagy másnéven hacking, mely utóbbi elnevezés gyakran előfordul a nemzetközi és a hazai szakirodalomban is egyaránt. A „hacker" kifejezést általában azokra az informatikai szakemberekre használják, akik kiemelkedően magas fokú szaktudással és gyakorlattal rendelkeznek. Az egyik legnépszerűbb nézet szerint a hackerek között különbséget lehet tenni aszerint, hogy milyen szándékkal törik fel a rendszert. Ez alapján beszélhetünk az ún. „white" hat vagy fehér kalapos hackerekről, akik jóhiszeműen az adott rendszer biztonságát és sebezhetőségét tesztelik. Emellett vannak az ún. „black hat" vagy fekete kalapos hackerek, illetve másnéven „crackerek", akik többek között azért hatolnak be a rendszerbe, hogy kárt okozzanak, vagy épp az értékes információkhoz jussanak hozzá. Végül az utolsó csoportot képezik az ún. „grey hat" vagy szürke kalapos hackerek, akik nehezen behatárolható módon az előző két csoport között helyezkednek el valahol.

A bemutatott terminológiáknak a használata azonban vitatható. Általában egyetértés van a tekintetben, hogy az etikus hackerek[91] tevékenysége a fehér kalapos csoportba tartozik, azonban nehezíti a helyzetet, hogy hiányzik ennek a megfelelő szabályozása, valamint nincs kialakítva egy széles körben elfogadott gyakorlata. Ennek ellenére már megjelentek különböző információbiztonsági cégek a piacon, akik kifejezetten ilyen képzést kínálnak.

Közelebbről megvizsgálva ezt a problémakört felmerül a kérdés, hogy a jogosultság hiánya esetén beszélhetünk-e egyáltalán etikus hackelésről. Steven Furnell rámutat arra, hogy a „biztonság fejlesztése" érdekében végzett hacking megítélése esetén a főkérdés, hogy mi történik a megszerzett információval. Amennyiben ezt a hacker diszkréten bejelenti a cégnek, akkor az etikus hozzáállásnak tekinthető. Azonban, ha ettől eltérő módon a hacker a nagy nyilvánosság előtt tárja fel a biztonsági rést, akkor ez a részéről nehezen tekinthető etikusnak, különösen azért, mert ezzel felhívja figyelmet a rendszerben található hibára, de facto arra, hogy mások is használják ki a rendszer sebezhetőségét. Furnell szerint további megválaszolandó kérdésként merül fel, hogy egy diszkrét bejelentés esetén is etikusnak tekinthető-e, ha a rendszerbe valaki engedély nélkül belép és mindezt úgy teszi, hogy más informatikai műveletet nem végez. Álláspontja szerint a hacker ebben az esetben is hátrányt okozhat a jogosulatlan

[91] FURNELL, Steven: Hackers, viruses and malicious software. In: Jewkes, Yvonne – Yar, Majid: Handbook of Internet Crime. Willan Publishing, 2010. 43-45. o.

hozzáféréssel anélkül, hogy a rendszerben bármit megváltoztatna vagy megzavarná annak a működését, ellenben például könnyedén láthat olyan szenzitív információt (pl. személyes adatot vagy üzleti titkot), amivel később visszaélhet.[92] Erre tekintettel a jogosulatlan belépés azon esetei, amelyek károkozási szándék nélkül történnek jó példaként szolgálnak a szürke kalapos hackelésre. A fehér kalapos típusa pedig kizárólag azokra az esetekre korlátozódik, amikor a hacker erre kifejezetten speciális vagy általános felhatalmazást kap. Ezért azok a személyek, akik csak saját elhatározásukból, jogosultság hiányában keresnek programhibákat vagy biztonsági réseket, nem tekinthetők etikus hackernek, hanem csak azok, akik rendelkeznek jogosultsággal valamilyen formában (pl. az információs rendszer tulajdonosa kifejezetten megbízza őket a rendszer tesztelésére és támadására).

A jogosulatlan belépés alapvetően megvalósulhat egyszerűen vagy összetettebb módon is például, ha az elkövetők egy számítástechnikai-hálózatot használnak fel arra, hogy távoli hozzáférést szerezzenek, és ez gyakran különböző joghatóság alá tartozó számítógépek közbeiktatásával történik. A hozzáférés megszerzése történhet alap felhasználói szintű műveletekkel, vagy ún. „root level access", illetve „god level access" szintűvel, amikor ugyanazokkal a jogosultságokkal rendelkeznek mint a rendszergazda, és ezáltal a rendszerben tárolt valamennyi adat elérhetővé válik a számukra, sőt módosításokat hajthatnak végre vagy akár (rosszindulatú) programokat futtathatnak.

A szoftverek gyors ütemű fejlesztése elkerülhetetlenül magában hordozza a programhibákat is, amiket az elkövetők gyakran kihasználnak mielőtt még ezeket a szoftverfejlesztők észrevennék és kijavítanák. Ezek az ún. nulladik napi (zero-day) támadások, amelyek a programkészítők és a felhasználók által még nem ismert olyan sebezhetőséget használnak ki, amelynek eredményeképpen könnyedén hozzáférhetnek az információs rendszerekhez.

Emellett gyakran olvashatunk a felhasználói fiókok (pl. e-mail, közösségi oldalak) feltöréséről szóló híreket, azonban érdemes felhívni a figyelmet arra, hogy a jogosulatlan belépések többségének a célpontjai elsősorban a nagyobb cégek, gazdasági szereplők vagy állami szervek, és nem a magánszemélyek.

A jogosulatlan hozzáféréssel az elkövető célja továbbá az is lehet, hogy arra használjon fel több számítógépet, hogy a közbeiktatásuk révén elrejtse a személyazonosságát, a bűncselekmény elkövetésének a helyét vagy éppen bűncselekmények elkövetésére, így gyermekpornográf tartalmakhoz való hozzáférésre, vagy spam küldésre, amire különösen alkalmasak a nyilvános Wi-Fi hozzáférési pontok (HotSpot).[93]

[92] GILLESPIE: i.m. 44-45. o.
[93] CLOUGH: i.m. 37. o.

Megállapítandó, hogy az egyes hacking-jellegű cselekmények mögött leggyakrabban a következő motivációk húzódnak: hozzáférés az információhoz, az adat megváltoztatása, illetve törlése, valamint az információs rendszer használata.[94] 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 egyészségügyi adatokat szereznek meg (pl. név és születési idő, telefonszámok, e-mail címek, felhasználói adatok[95], jelszavak és bankkártya adatok). Az elkövetők ezeket gyakran nem saját maguk részére szerzik meg, hanem azért, hogy ezeket később a Darknet fórumokon értékesítsék.

3.2. A jogosulatlan belépés nemzetközi és uniós szintű szabályozása

A Budapesti Egyezmény értelmében a jogosulatlan belépés bűncselekményét követi el, aki a számítástechnikai rendszerbe vagy annak bármely részébe (pl. legyen az tárolt vagy forgalmi adat, mappák, egyéb komponensek, adathordozók stb.) jogosulatlanul és szándékosan belép. Azonban nem minősül jogosulatlan belépésnek például egy e-mail küldés vagy fájl továbbítás, ellenben bűncselekményt valósít meg, aki olyan számítógépbe lép be, ami a nyilvános telekommunikációs hálózatra csatlakozik vagy ugyanazon hálózaton belül található, mint például egy szervezeten belül elérhető helyi hálózat (LAN) vagy intranet. E tekintetben a kommunikáció módja közömbös (pl. lehet vezetékes vagy vezeték nélküli). A szerződő felek kiköthetik, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy számítástechnikai adatok megszerzésére irányuló, illetve más tisztességtelen céllal kövessék el.[96]

A büntetendő cselekményt jogosulatlanul kell elkövetni, ami azt jelenti, hogy ez a rendszer vagy a rendszer egy részének a jogosultjának vagy egyéb jogosultjának az engedélye nélkül történik (pl. a már említett engedélyezett tesztelés nem minősül ennek). Nem büntetendő azonban, ha a számítástechnikai rendszerhez ingyenes és nyilvános hozzáférés áll rendelkezésre.

---

[94] CLOUGH: i.m. 33. o.
[95] http://www.europarl.europa.eu/news/hu/headlines/society/20180418STO02004/facebook-cambridge-analytica-botrany-zuckerberg-valaszoljon-az-europaiaknak [2018.07.21.]
[96] COUNCIL OF EUROPE: Explanatory Report to the Convention on Cybercrime. European Treaty Series – No. 185. 2001. 9-10. o.

A 2013-as irányelv is hasonlóan határozza meg a jogosulatlanul belépés fogalmát, mert jogosulatlannak minősül minden olyan magatartás, - ideértve a belépést, beavatkozást vagy adatszerzést is - amelyet a rendszernek vagy a rendszer részének tulajdonosa vagy egyéb jogosultja nem engedélyezett, vagy amelyet a nemzeti jog nem tesz lehetővé.

A rendszert érintő jogellenes beavatkozással (3. cikk) kapcsolatban kimondja, hogy tagállamoknak meg kell hozni a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszerhez vagy annak egy részéhez való, szándékosan és jogosulatlanul történő hozzáférés legalább a súlyosabb esetekben bűncselekménynek minősüljön akkor, ha a bűncselekményt valamely biztonsági intézkedés megsértésével követték el.

A tagállamok kötelesek az informatikai bűncselekményeket (3-7. cikk) szabadságvesztéssel büntetni, amelynek a felső határa – legalább a súlyosabb esetekben – két év, valamint biztosítaniuk kell, hogy az ezekre való felbujtás, vagy az elkövetésükhöz nyújtott bűnsegély is bűncselekménynek minősüljön.

Azonban a 2013-as irányelv nem állapít meg büntetőjogi felelősséget abban az esetben, ha a bűncselekmény objektív kritériumai teljesülnek, de a cselekményt nem jogsértő szándékkal követték el, például az érintett személy nem tud arról, hogy az adott hozzáférés jogosulatlannak minősül, vagy az információs rendszerek tesztelésével vagy védelmével bízták meg (pl. egy cég kijelöl valakit a biztonsági rendszerének a tesztelésére). Ezen kívül az információs rendszerekhez való hozzáférést felhasználói szabályzat vagy szolgáltatási feltételek révén korlátozó szerződéses kötelezettségek vagy megállapodások, valamint a munkáltató információs rendszereihez való magáncélú hozzáféréssel és azok magáncélú használatával kapcsolatos munkaügyi jogviták nem vonhatnak maguk után büntetőjogi felelősséget, amennyiben a hozzáférés az említett körülmények között minősülne jogosulatlannak, és ezáltal a büntetőeljárás kizárólagos alapját képezné. Nem érinti az információhoz való hozzáférésnek a nemzeti és az uniós jogszabályokban meghatározott jogát, ugyanakkor ez a jog nem szolgálhat az információhoz való jogellenes vagy önkényes hozzáférés igazolásául.

3.3. A jogosulatlan belépés hazai szabályozása

Az 1980-as évek második felében a hazai büntető törvénykönyvbe először a számítógépes csalás tényállását iktatták be, amelynek a megfogalmazásakor rendszerint a hagyományos csalás tényállásának szerkezetét követték beépítve a magatartások megtévesztő jellegét és a jogtalan haszonszerzési célzatot. Kezdetben a Legfelsőbb Bíróság döntésében például a befejezett csalásként értékelte azt a büntetendő magatartást, amikor a számítógépkezelő terhelt

az őt terhelő hátralék összegét valótlan adat betáplálásával egyenlítette ki.[97] Rövid időn belül azonban egy új és önálló tényállás megalkotása vált szükségessé, ezért a számítógépes csalás az 1978. évi Btk. 300/C. §-ába lett beiktatva. Emellett a bankkártyával elkövetett tényállásokat is beemelték, amelyek ugyancsak a számítástechnikai eszközökkel elkövetett, illetve azok ellen irányuló bűncselekmények büntethetőségét teremtették meg. Már ebben az időszakban is felmerült a számítógépes adatok kikémlelésének szankcionálása, illetve az "elektronikus betörés" önálló bűncselekménnyé nyilvánítása. Azonban még hiányoztak a Btk.-ból a számítógépes elkövetéssel kapcsolatos speciális definíciók is, mint például a számítógépnek, a számítógépes adatnak és az adatfeldolgozásnak a fogalma. Jelentős változásokat még az 1999. évi CXX. törvény hozott, mert a nagy nyilvánosság általános részi fogalmát kiterjesztette az elektronikusan rögzített információ távközlő hálózaton való közzétételére is.

Végül a Budapesti Egyezményben foglalt büntetőjogi rendelkezésekkel összhangban léptette életbe a 2001. évi CXXI. törvény a számítástechnikai rendszer és adatok elleni bűncselekmény (1978. évi Btk. 300/C. §), valamint a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása elnevezésű bűncselekménynek (1978. évi Btk. 300/D. §) a tényállásait, amely koncepcionálisan új szabályozást teremtett meg. Ezeket a bűncselekményeket azonban ekkor még a gazdasági bűncselekmények című fejezetben (XVII. fejezet) helyezték el, de ezt a megoldást kritikaként érte, hogy nem juttatta megfelelően kifejezésre a védendő értékek sokféleségét.

A számítógépes csalás helyébe iktatott új tényállás már büntetni rendelte a számítástechnikai rendszerbe történő jogosulatlan belépést, valamint a számítástechnikai rendszer és az abban tárolt, feldolgozott, kezelt vagy továbbított adatok sértetlensége elleni cselekményeket is. Ezt kiegészítette a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása, amely már az alapcselekmények elkövetését lehetővé tévő feltételek biztosítását is sui generis bűncselekményként rendelte büntetni.[98]

Az egyes országok az informatikai bűncselekményeket külön törvényben szabályozzák (pl. Egyesült Államok), míg mások azt a szabályozási megoldást alkalmazzák, hogy a nemzeti büntető törvénykönyvükbe, vagy egy önálló fejezetben (pl. Franciaország), vagy a különös részben szétszórtan helyezik el a tényállásokat (pl. Németország).

[97] BH 1989/184.
[98] MOLNÁR Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Kónya Sándor (szerk.): Magyar Büntetőjog - Kommentár a gyakorlat számára (Harmadik kiadás). HVG-ORAC Budapest, 2018. 971-972. o.

Az információs társadalom jellemző indikátora, az infokommunikációs eszközök általános elterjedtsége és használata, amely változásokat eredményezett szinte valamennyi társadalmi viszony területén. Az informatikai környezet egyrészt a már létező társadalmi értékek új szféráját, másrész egészen új a büntetőjog által védett értékeket hozott létre.[99]

2009-ben Nagy Zoltán már azt az álláspontot képviselte, hogy az informatikai bűncselekmények a tárgyi oldalon mutatkozó hasonlóságok, szoros összefüggések miatt a Btk. önálló fejezetét fogják alkotni.[100] Erre egészen a Btk.-ig kellett várni, amely már a 2013-as irányelvnek megfelelően – eleget téve a jogharmonizációs kötelezettségnek – átalakította a kiberbűncselekményekre vonatkozó szabályozást mind elnevezésben és mind tartalmilag, mert már a gazdasági bűncselekményektől külön, a XLIII. fejezetbe kerültek a „A tiltott adatszerzés és információs rendszerek elleni bűncselekmények" címmel. A korábbi „számítástechnikai rendszer" terminológia helyébe az „információs rendszer" lépett.

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.[102] Nagy álláspontja szerint e tényállás különböző bekezdései eltérő jogi tárgyat hivatottak védeni, így az (1) bekezdés az információs rendszerek integritását és biztonságát. A (2) bekezdés (a) pontja az e rendszer biztonságos működését, míg a (b) pont az elektronikus adatok megbízhatóságához, hitelességéhez fűződő érdeket, valamint a tartalmától függően az azok által megtestesített értéket és utóbbiak minősülnek a súlyosabb jogtárgy sértésnek.[103]

Lényeges azonban kiemelni, hogy ez a tényállás továbbra is csak a számítástechnikai jellegű, szoftveres úton elkövetett támadások ellen biztosít büntetőjogi védelmet. A számítógépnek a mechanikus védelmét ma is a rongálás törvényi tényállása látja el.[104] A büntető kódex három külön fordulattal határozza meg a bűncselekmény elkövetési magatartásait és valamennyi fordulatának az elkövetési tárgya az információs rendszer, amelynek a betöltött funkciója a meghatározó.[105]

---

[99] SZATHMÁRY (2012): i.m. 16. o.
[100] NAGY (2009): i.m. 61. o.
[102] KARSAI Krisztina: XLIII. fejezet Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz. Complex Kiadó. Budapest, 2013. 898. o.
[103] NAGY Zoltán András: XLIII. fejezet tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Tóth Mihály – Nagy Zoltán András (szerk.): Magyar Büntetőjog: Különös rész. Osiris Kiadó, Budapest 2014. 594-595. o.
[104] MOLNÁR (2016): i.m. 946. o.
[105] TÓTH Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In: Gál István László – Nagy Zoltán András (szerk.): Informatika és büntetőjog. PTE ÁJK. Pécs, 2006. 184. o.

A Btk. 423. §-ában a tisztán informatikai bűncselekménynek minősülő információs rendszer vagy adat megsértésének tényállását találjuk, amelynek (1) bekezdése értelmében büntetendő, 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.

Az (1) bekezdésben meghatározott enyhébb súlyú alapeset az információs rendszerbe történő jogosulatlan belépést nyilvánítja büntetendő cselekménnyé, amelynek két esete különböztethető meg. A jogosulatlan belépés irányulhat az elkövető által felhasznált számítógépre vagy a rajta keresztül elérhető védett számítógépes hálózatra (pl. intézményi belső hálózat, ún. intranet vagy az internet részét képező hálózat mint ilyen egy banki rendszer).

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, tűzfallal 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 konjuktív feltételek a bűncselekmény megállapíthatóságához.[106] Meghatározásra került továbbá az elkövetési mód is, így a bűncselekmény megvalósul akkor, ha a belépés a védelmi intézkedés megsértésével vagy ennek kijátszásával történik például a biztonsági rendszer hiányosságait kihasználva lépnek be jogosulatlanul vagy a jogosult jelszavával vagy belépési kódjával, amelynek megszerzési módja azonban közömbös (pl. történhet megtévesztéssel, kifürkészéssel, kódtörő programmal, social engineering, vagyis pszichológiai manipulációval vagy elképzelhető, hogy a felhasználó hanyagsága folytán jut hozzá az elkövető). Például a német Büntető Törvénykönyv (a továbbiakban: StGb.) 202a. §-a is hasonlóan megköveteli a hacking megállapításához, hogy a jogosulatlan belépést a rendszer technikai védelmének a kijátszásával valósítsák meg.[107]

A kiberbiztonságban a leggyengébb láncszem az ember. Az esetek döntő többségében ugyanis minden sikeres támadás mögött a sértetti közrehatás áll, és éppen ezért az elkövetők gyakran előnyben részesítik a social engineering támadásokat – mint például az adathalászatot (phishing) – a technikai-jellegű megoldások alkalmazása helyett. Kevin Mitnick szerint a

[106] NAGY (2014): i.m. 594-595. o.
[107] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany

pszichológiai manipuláció könnyedén megkerüli a technológiai akadályokat (pl. tűzfalat vagy egyéb védelmet) a manipuláció, befolyásolás és megtévesztés segítségével.[108]

A bűncselekmény nem célzatos, ezért nem feltétele az elkövetésnek 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 beleolvad a súlyosabb jogtárgysértésre figyelemmel.[109]

A jogosulatlan belépésnek egy tipikus eseteként említhető az ún. wardriving vagy wireless hacking, ami a vezeték nélküli hálózatok jogosulatlan használatát jelenti. A Wi-Fi kapcsolatok kialakításának több formája van: vannak a nyilvános hálózatok, amelyekhez bárki szabadon csatlakozhat, mindenféle korlátozás nélkül. Nyilvános, de zárt hálózatok is rendelkezésre állhatnak, amelyek esetében egy speciális szoftver gondoskodik arról, hogy a hálózatot egy kód ismeretében lehet használni korlátozott ideig. Emellett vannak privát hálózatok, amelyeknél a hozzáférést titkosítják, általában tűzfal és jelszó használatával korlátozzák. Ezek a hálózatok saját használatra lettek kialakítva és jelszóvédelemmel vannak ellátva, ezért kizárólag a jelszó ismeretében lehet ezekhez csatlakozni. Azonban előfordul, hogy a tulajdonos akaratlanul a hálózatot védelem nélkül „nyitva" hagyja. Amennyiben a felhasználó az adatforgalom után fizet a szolgáltatója felé, akkor jelentős kárt okozhat nála a jogosulatlanul rácsatlakozó személy. A Wi-Fi hálózatok további veszélyforrást jelentenek, mert rajtuk keresztül jogosulatlanul betudnak lépni az információs rendszerekbe, illetve lehetőség van a hálózaton keresztül továbbított kommunikáció kifürkészésére is. Azonban csak akkor valósítja meg a hálózatot jogosulatlanul használó személy a 423. § (1) bekezdését a „Wi-Fi-lopással"[110], ha a hálózat aktív védelemmel van ellátva és ezt sérti meg, különben nem.[111]

Érdekességként megemlítendő az első nagy média visszhangot keltő hazai hacker ügy, az Elender-per. 1999 decemberében az elkövetők beléptek a szolgáltató rendszerébe,

---

[108] MITNICK, Kevin D.: A megtévesztés művészete című könyvnek a borítója: „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."

[109] SZATHMÁRY Zoltán: A számítástechnikai bűncselekmények és rendszertani elhelyezésük. Jogtudományi Közlöny 2012/4. 173-174. o.

[110] Lásd BLUTMANN László - KARSAI Krisztina - KATONA Tibor: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? Bűnügyi Szemle 2008/1. 42-49.o.

[111] NAGY (2009): i.m. 272-273. o.

feltelepítettek egy lehallgató programot, és így később megszerezték az Elender mintegy 35 000 ügyfelének azonosítóját. A jelszavak birtokában a cég honlapját kicserélték egy maguk által szerkesztettre, amin közzétették a birtokukba jutott felhasználói jelszavakat. A cég emiatt kénytelen volt leállítani a szervert, ezáltal a sokezer ügyfél által igénybe vett szolgáltatások szüneteltek. Miután birtokukba jutott a cég egyik informatikai igazgatójának jelszava, nyilvánosságra tudtak hozni rendszergazda jogosultságot biztosító jelszavakat is, akkor emiatt már három napra leállt a teljes rendszer. A hatályos szabályozás szerint bűncselekményt valósítottak meg, azonban a cselekmény elkövetésének időpontjában még az 1978. évi Btk. nem szabályozta az informatikai bűncselekményeket, ezért az ügyészség közérdekű üzem működésének megzavarása és magántitok jogosulatlan megismerése miatt emelt vádat, azonban ez alól a bíróság másodfokon felmentette őket.[112]

A jogosulatlan belépéssel kapcsolatban fontos a már korábban vizsgált etikus hacking kérdését is áttekinteni a hazai szabályozás fényében, ami különösen aktuálissá vált, mert az elmúlt években több magyarországi esetre is fény derült, amelyek éles vita tárgyát képezték.

Az első eset során egy fiatal hacker 50 Ft-ért vett bérlettel mutatott rá a BKK és T-Systems által üzemeltetett e-jegyrendszer hiányosságára, ami végül feljelentéssel zárult a jegyértékesítési rendszert ért informatikai támadás miatt. A vádemelésre végül nem került sor, mert az ügyészség megállapította, hogy a célja valóban a biztonsági rés feltárása és ennek közlése volt a BKK felé. A rendszerhibáról való kétséget kizáró meggyőződéshez szükség volt a vásárlás befejezésére. Mindezekre tekintettel az ügyészség szerint a cselekménye nem volt veszélyes a társadalomra, amely a bűncselekmény megállapításának a feltétele. Emellett a megtett bejelentése közérdekű bejelentésnek minősül, ami büntethetőséget kizáró ok.[113]

A másik esetben egy programozónak tanuló hallgató a Magyar Telekom oldalán található nyilvános dokumentumban talált információk alapján jutott hozzá egy rendszergazdai jelszóhoz, amellyel hozzá tudott férni a Telekom teljes belső hálózatához, és erről a biztonsági résről később tájékoztatta a céget. Ezt követően azonban további, újabb sebezhetőséget talált és ezt kihasználva lépett be újból a rendszerbe, a vállalat kifejezett kérésére ellenére, aminek eredményeképpen a Telekom ismeretlen tettes ellen tett feljelentést. Az ügyészség vádat emelt az információs rendszer megsértéséért, még hozzá annak minősített esetéért, mert a meghackelt szerver a hírközlő hálózat része volt, ezért a Btk. 459 § (1) bekezdés 21. pontja alapján

[112] VARGA Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In Medias Res 2019/1. 163-164. o.
[113] https://jogaszvilag.hu/napi/bkk-botrany-fellelegezhet-az-etikus-hacker/ [2017.11.21.]

közérdekű üzemnek minősül.[114] Végül a Szolnoki Járásbíróság folytatólagosan elkövetett információs rendszer vagy adat megsértése bűntettében mondta ki bűnösnek, és 600 ezer forint pénzbüntetésre ítélte nem jogerős ítéletében.

Mindezekre tekintettel a bírónak a konkrét esetben joga van megvizsgálni, hogy ha a törvényi tényállást kimerítette-e ugyan az illető, van-e olyan társadalmilag fontos és méltányolható érdek, ami miatt a cselekményének a jogellenessége hiányzik, és ezért nem veszélyes a társadalomra. Karsai Krisztina szerint büntetőjogi értelemben azt kell vizsgálni, hogy mihez fűződik nagyobb társadalmi érdek a személyes adatok biztonságához vagy a biztonsági rések fenntartásához. A bíró tehát vizsgálja ezt a kérdést, és a bizonyítékok alapján kialakult belső meggyőződése szerint megállapíthatja a társadalomra veszélyesség hiányát, és így felmentheti az illetőt. Azonban az e tevékenység mögött húzódó szándékot is mindig figyelembe kell venni.

Ambrus István véleménye szerint a bíróság a vizsgálat tárgyává teheti például azt is, hogy a terhelt eljárása tekinthető-e közérdekű bejelentésnek-e vagy sem.[115] A közérdekű bejelentés olyan körülményre hívja fel a figyelmet, amelynek orvoslása vagy megszüntetése a közösség vagy az egész társadalom érdekét szolgálja, vagyis a bejelentő jelen esetben a közérdek védelme érdekében realizálja magát az elkövetési magatartást. A közérdekű bejelentés javaslatot is tartalmazhat.[116]

A bűncselekmény alanya az első fordulatban a belépésre jogosultsággal nem rendelkező személy lehet, míg a második fordulat esetén az adott személy rendelkezik erre vonatkozó engedéllyel.

Áttérve a jogosulatlan belépés második fordulatára, ami akkor valósul meg, ha az elkövető az engedélyezett belépést követően a jogosultságának terjedelmi vagy időbeli kereteit meghaladja, illetve a jogosultságot más módon megsérti az információs rendszerben való bennmaradással szándékosan. E fordulat alaki bűncselekményt határoz meg.[117]

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

[114] http://ugyeszseg.hu/valasz-a-tarsasag-a-szabadsagjogokert-tasz-etikus-hacker-ugyeben-tett-allitasaira/ [2019.02.05.]
[115] https://qubit.hu/2019/02/04/torvenyt-sertett-az-etikus-hacker-de-ha-nem-jelent-veszelyt-a-tarsadalomra-a-birosagnak-fel-kell-mentenie [2019.02.05.]
[116] 2013. évi CLXV. törvény a panaszokról és a közérdekű bejelentésekről 1. § (3) bekezdése
[117] MOLNÁR Gábor Miklós: XL. fejezet – A pénzmosás. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (szerk.): Büntetőjog II. – Különös Rész. HVG-Orac Lap- és Könyvkiadó Kft. Budapest, 2018. 947. o.

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.

Az említett eset során a védelem utalt a jelenlegi rendőrségi gyakorlatra is, amely szerint bárkit megbízhatnak felettesei a tevékenységi körétől eltérő, bármilyen kiegészítő vagy akár érdemi feladat elvégzésével is szóbeli parancs, utasítás útján, írásbeli nyom nélkül, így álláspontja szerint kizárólag szubjektív elhatározás kérdése, hogy az ilyen, nem az adott munkakörhöz tartozó feladatok elvégzése során történő informatikai rendszerbe való belépés miatt mikor és kit vonnak felelősségre.[118]

3.4. A jogosulatlan hozzáféréssel összefüggő bűncselekmények szabályozása az Egyesült Államokban

A CFAA-ban szabályozott bűncselekmények egy része a „jogosulatlan hozzáférést" követeli meg [1030. § (a)(3), (a)(5)(B), (a)(5)(C)], míg más rendelkezések a „jogosulatlan hozzáférést" vagy a „jogosultságának kereteit túllépve" történő elkövetést [1030. § (a)(1), (a)(2), (a)(4)] is. A törvény azonban a „jogosulatlan hozzáférés" (unauthorised access) fogalmának meghatározásával adó maradt. Azonban a széleskörben elfogadott álláspont szerint a hozzáférés nem csak szűken vett „belépést" foglalja magában, hanem többek között a számítógép használatát is.

A CFAA általában a „jogosulatlan hozzáférés" keretében azokat az eseteket szabályozza, amelyek során az elkövetők mint „kívülálló" személyekként (outsiders) követik el a bűncselekményeket mint például a külső támadást indító hackerek, míg a „jogosultság kereteinek túllépésével" elkövetett magatartások esetén olyan engedéllyel rendelkező, „bennfentes" személyekről (insiders) van szó mint például az alkalmazottak. A megkülönböztetés alapját a rendszerhez való hozzáférési jogosultság jelenti. Azok a személyek,

[118] BH 2017.12.392.; Ezzel kapcsolatban Parti Katalin vizsgálta, hogy a hacking szabálysértésként való felfogása mennyiben lenne hatékonyabb és nagyobb visszatartó erejű szankció. Lásd PARTI Katalin: Gondolatok a számítástechnikai adatok és rendszerek elleni bűncselekmények tényállásairól. Büntetőjogi Kodifikáció 2005/2. 38. o.

akik hozzáférési jogosultsággal rendelkeznek a számítógéphez, általában büntetőjogi felelősségre akkor vonhatók kizárólag, ha szándékosan okoznak kárt. Ezzel szemben a kívülállók a szándékos károkozáson kívül, a gondatlanságból bekövetkezett eredményért is büntethetők.[120]

Fontos, hogy a bűncselekményeket megalapozó hozzáférésnek jogosulatlannak kell lennie, amelynek alapját a Budapesti Egyezménynél tárgyalt fogalom képezi, vagyis annak minősül, ha az adott magatartást a tulajdonos vagy egyéb jogosult nem engedélyezi.

A hozzáférésnek a korlátozása vagy megtagadása két módon történhet: a technikai védelem alkalmazásával (code-based restriction) vagy szerződés (contract-based restriction) alapján.[121] A „kód" szerinti szabályozás esetén a tulajdonos valamilyen technikai intézkedést tesz annak érdekében, hogy a hozzáférést korlátozza, mint például a fiók hozzáféréshez felhasználónevet és jelszót ad meg. Aki ezt kijátssza akár csak jelszó találgatással vagy technikai eszköz használatával, az jogosulatlanul fér hozzá.

A szerződéssel történő szabályozás gyengébb alapokon nyugszik, amely alapján a tulajdonos határozza meg a hozzáférés feltételeit, amely történhet formálisan vagy informálisan, valamint kifejezetten vagy hallgatólagosan. Például ilyen lehet a munkaszerződés vagy használati feltételeket tartalmazó szabályzat. A szerződéssel történő korlátozás nagymértékben attól függ, hogy a szerződési feltételek mennyiben vannak pontosan és részletesen meghatározva.

Kerr azzal a hasonlattal él, mely szerint a kettő között a különbség úgy ragadható meg, hogy a kód-alapú korlátozás esetén az ajtót becsukjuk, és egyben bezárjuk az ajtót, hogy idegenek ne tudjanak bejönni, míg a szerződés-alapú korlátozáshoz hasonlítható, azaz eset, amikor az ajtót nyitva hagyjuk és kirakunk egy táblát, hogy „idegeneknek belépni tilos".[122]

Kerr felhívja a figyelmet arra, hogy ez esetben különösen jelentős szerepe van a mens rea vizsgálatának. Általánosságban a CFAA a szándékos vagy tudatos elkövetést követeli meg a felelősségre vonáshoz. Ez azt jelenti, hogy az illető tudatának át kell fognia, hogy az általa tanúsított magatartás nem engedélyezett a számára. További kérdéseket vet fel például, ha egy alkalmazottat elbocsátanak – egyúttal a jogosultságát is megvonják –, és ezt követően fér hozzá a volt munkáltatójának a rendszeréhez. Ehhez példaként említendő a United States vs. Shahulhameed-ügy, amikor a Toyota Motors elbocsátotta az informatikus alkalmazottját,

[120] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 5-6 o.
[121] Orin S. Kerr szerint a jogosulatlan belépés esetén kizárólag a kód-alapú védelem jöhet szóba, mert a szerződés-alapút nehezebb meghatározni ez esetben. Azonban a jogosultság kereteinek túllépése esetén elismeri a szerződés alapú korlátozás létjogosultságát. KERR, Orin S.: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes. 78 N.Y.U. L. Rev. 1596 (2003). 1662-1663. o.
[122] KERR (2003): i.m. 1662-1663. o.

azonban még a vállalati hozzáférését nem vonták vissza technikai értelemben, így ezt kihasználva a rendszerbe belépve adatokat módosított és a szerverek működését akadályozta. A bíróság ezt úgy értékelte, hogy jogosulatlanul fért hozzá a rendszerhez és felelősségre vonta ezért.[124] Ezen kívül említi a Steele-ügyet, amikor az elbocsátott alkalmazottól elvették a céges laptopját, belépőkártyáját és aláírattak vele egy nyilatkozatot, hogy a jövőben már nem férhet hozzá a volt munkáltatójának a számítógépes rendszeréhez. Ennek ellenére ezután több alkalommal használta azt és ezért felelősségre vonták. Ez azzal magyarázható, hogy a hozzáférési jogosultságának a visszavonása megtörtént és a körülményekből tudott erre következtetni, azonban vannak olyan esetek, amikor ez nem ennyire nyilvánvaló.[125]

A másik érdekes kérdés miként minősíthető az ún. port scanning, amely tesztelést általában mind a kiberbiztonsági szakértők és crackerek is szokták elvégezni annak érdekében, hogy feltérképezzék a hálózatnak a nyitott és sebezhető portjait, azonban a bíróság szerint ez nem minősül a 1030. § szerinti jogosulatlan hozzáférésnek.[126]

A CFAA a „jogosultságának keretének túllépését" a 1030. § (e)(6) pontjában definiálja, melynek értelmében azt jelenti, hogy az adott személy „jogosultsággal rendelkezik a számítógéphez történő hozzáféréshez, és e jogosultság felhasználásával információt szerez meg vagy módosít a számítógépen, azonban a jogosultsága a megszerzésre vagy a módosításra nem terjed ki". Ennek megfelelően a vádhatóság részéről azt kell bizonyítani, hogy az adott személy hozzáférési jogosultsága hogyan lett korlátozva, valamint e korlátozást hogyan lépte túl annak érdekében, hogy megszerezze vagy módosítsa az információt a számítógépen. Előbbi bizonyítása egyszerű, ha a terhelt jogosultságának kereteit írásban foglalták, így például számítógép használati szabályzatban, munkaszerződésben vagy titoktartási szerződésben.

A legvitatottabb kérdésként merül fel a jogirodalomban és a joggyakorlatban egyaránt, hogy vajon az adott személy túllépi-e a jogosultságainak a keretét, ha nem a meghatározott célból fér hozzá a számítógéphez. Ez különösen három esetben gyakori, ha:

(1) az engedélyező fél kifejezetten megtiltotta a terheltnek, hogy meghatározott célból férjen hozzá a számítógéphez,

(2) az engedélyező fél kifejezetten megtiltotta a terheltnek, hogy az adataihoz meghatározott célból férjen hozzá, azonban a számítógéphez való hozzáférést ennek megfelelően nem tiltotta meg,

[124] KERR, Orin S.: Computer Crime Law. Fourth Edition. West Academic Publishing 2018. 48-51. o.
[125] KERR, Orin S.: Norms of computer trespass. Columbia Law Review Volume 116. 2016. 1182. o.
[126] KERR (2018): i.m. 37. o.

(3) az engedélyező fél nem tiltotta meg kifejezetten, hogy a terhelt használja az adatait „nem megfelelő” célra, de a terhelt az engedélyező fél érdeke ellen tanúsított magatartást.

Az első eset a legkevésbé ellentmondásos, mert egyértelműen meghatározásra kerül a cél alapú korlátozás a terhelt hozzáférési jogosultságával kapcsolatban. A második eset már kérdéses, mert például sértett az érintett személlyel ugyan aláírathat egy titoktartási szerződést, amelyben hozzájárul ahhoz, hogy nem használja fel a sértett információját személyes haszonszerzésre, de probléma merülhet fel, ha a megállapodás nem tartalmazza kifejezetten, hogy az illető nem férhet hozzá a sértett számítógépes rendszeréhez. Ugyan korlátozva lett az információ személyes felhasználása, de az nem, hogy az illető jogosultsága nem terjed ki a számítógépen található adatok megszerzésére vagy módosítására.[127]

3.4.1. Számítógéphez való jogosulatlan hozzáférés és információval való visszaélés (Accessing a computer and obtaining information)

Általában a hacking cselekmények vonatkozásában átfedés mutatkozik az általános 1030. § (a)(2) bekezdés szerinti és a speciálisabb tényállások között, de a büntetőeljárások döntő többsége előbbi miatt indul, ezért először ezzel foglalkozom részletesen. A jogosulatlan belépések sérthetnek több bekezdést is, például egy szövetségi szerv számítógépébe történő „betörést” a (B) és (C) bekezdéseket egyaránt megvalósíthatja.

(a)(2) bekezdése alapján vétség miatt büntetendő, „aki szándékosan, jogosulatlanul vagy jogosultságának keretét túllépve hozzáfér a számítógéphez és információt megszerez

(A) pénzintézet pénzügyi nyilvántartásából vagy fogyasztóvédelmi szervtől;

(B) az Egyesült Államok kormányzati szervétől (department or agency);

(C) védett számítógépről.”

„Aki gazdasági előnyért, anyagi haszonszerzésért, vagy más bűncselekmény, illetve jogszabály által tiltott cselekmény elkövetésének elősegítése érdekében követi el a bűncselekményt, vagy 5,000 $ értéket meghaladó információt szerez meg bűntett miatt büntetendő.”

1030. § (a)(2) bekezdés szerinti alapesetben nincs egy monetáris küszöbérték meghatározva, amely azzal indokolható, hogy vannak olyan esetek, amikor a jogosulatlan belépéssel okozott sérelemnek az értékét nehezen lehet pénzben kifejezni például, ha az elkövető jogosulatlanul szerzi meg egy kórháztól az egyészségügyi adatokat vagy személyes adatokat a bűnügyi

[127] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 8-11. o.

nyilvántartási rendszerből. Azonban, ha ez a 5,000 $ értéket eléri, akkor vétség helyett bűntett miatt vonható felelősségre az elkövető.

1986-ban a Kongresszus a bűnösség tekintetében a tudatosan kitételt megváltoztatta a szándékosra annak érdekében, hogy kiemelje e bűncselekmény körében a jogosulatlan hozzáféréshez a szándékos elkövetés szükségességét, és ezért kizárja azokat az eseteket, amelyek tévedés, figyelmetlenség folytán vagy gondatlanságból következnek be.

Az információ megszerzése egy tág fogalmat takar, amibe beletartozik az is, hogy az elkövető csak megnézi az adott fájlt akár annak letöltése vagy átmásolása nélkül. Ezen bűncselekménynek az elkövetési magatartása a jogosulatlan hozzáférés.

Az osztály (department) magában foglalja a szövetségi kormányzati entitásokat, mint a törvényhozó vagy bírósági, és a végrehajtó hatalomhoz tartozó szerveket. Az ügynökség (agency) egy szűkebb kört foglal magában, mint az osztály, mert ebbe bármely, az Egyesült Államok tulajdonában lévő hivatal tartozik.

Az alapesetet kimerítő magatartás miatt az elkövető pénzbüntetéssel és/vagy egy évig terjedő szabadságvesztéssel büntethető. Amennyiben a minősített esetet valósít meg, vagyis aki gazdasági előnyért, anyagi haszonszerzésért, vagy más bűncselekmény, illetve jogszabály által tiltott cselekmény elkövetésének elősegítése érdekében követi el bűncselekményt, vagy 5,000 $ értéket meghaladó információt szerez meg, akkor bűntett miatt öt évig terjedő szabadságvesztéssel büntetendő, valamint pénzbüntetést is kiszabhat a bíróság.[128]

Utóbbi esetben problémát jelenthet az információ értékének a pontos meghatározása, mert jelen tényállás tágan védi a bármely „megszerzett információt a védett számítógépről”, és az esetek döntő többségében az érintett információ immateriális és nem rendelkezik egy könnyen meghatározható piaci értékkel. Kerr szerint ezért bármely ésszerű módszer alapján meghatározható az információnak az értéke (pl. a bíróság egy reklámanyagot tartalmazó videó esetén a gyártási költséget vette figyelembe).[129]

3.4.2. Nemzetbiztonsági információval való visszaélés (Obtaining national security information)

1030. § (a)(1) bekezdés értelmében bűntett miatt büntetendő, „aki tudatosan, jogosulatlanul hozzáfér a számítógéphez vagy jogosultságainak kereteit túllépi azért, hogy nemzetbiztonsági információt megszerezzen, és okkal feltételezhető, hogy az információ arra használható, hogy

[128] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 16-22. o.
[129] KERR (2018): i.m. 93. o.

az Egyesült Államoknak kárt okozzon vagy más idegen nemzetet előnyhöz juttasson és ezért szándékosan közli, átadja, továbbítja vagy ezekre kísérletet tesz, vagy visszatartja az információt."

A bűncselekmény megvalósulásának feltétele, hogy az elkövető tudatosan jogosulatlanul vagy jogosultságainak keretei túllépve férjen hozzá a számítógéphez. A jogosultság terjedelme esetenként eltérhet, ezért a konkrét eset összes körülményét mérlegelve állapítható meg a jogosultság hiánya vagy éppen a jogosultság kereteinek a túllépése. Azonban érdemes megemlíteni, hogy azok a számítógépek vagy számítógép-hálózatok, amelyek nemzetbiztonsági információt tárolnak általában titkosítottak, valamint rendelkeznek megfelelő védelemmel és belső szabályzattal a hozzáféréssel kapcsolatban, ezért önmagában az is elegendő lehet, ha ezeket az elkövető kijátszotta vagy megsértette.

A megszerzett információnak felhasználhatónak kell lennie az Egyesült Államokkal szemben, ehhez elegendő annak a bizonyítása, hogy az elkövetés tárgya minősített (classified) vagy korlátozott (restricted) nemzetbiztonsági információ és az elkövetőnek tudomása volt erről.

Végül a szankcionált elkövetési magatartások a következők: a nemzetbiztonsági információ közlése, átadása, továbbítása vagy ezek előidézése; valamint ezen magatartásokra kísérletet tesz; végül visszatartja az információt attól a személytől, aki jogosult az átvételre a feladata ellátása során. Az elkövető pénzbüntetéssel, valamint tíz évig terjedő szabadságvesztéssel büntethető.[130]

3.4.3. Kormányzati számítógéphez való jogosulatlan hozzáférés (Tresspassing in a government computer)

A 1030. § (a)(3) bekezdése szerint büntetendő, „aki szándékosan, jogosulatlanul hozzáfér olyan nem nyilvános számítógéphez, amely kizárólag az Egyesült Államok kormányának használatában van, vagy abban az esetben, ha nincs kizárólagos használatában, akkor azt az Egyesült Államok kormánya használja, vagy érdekében használják, és ez befolyásolja a számítógép működését."

Jelen tényállás azt az esetkört hivatott szankcionálni, amikor kívülállók hatolnak be szövetségi kormányzati számítógépekbe, még abban az esetben is, ha eközben nem szereznek meg semmilyen információt. A bűncselekmény elkövetési tárgya kizárólag a nem nyilvános (nonpublic) számítógép lehet, amely magában foglalja a kormányzati számítógépeket, de

[130] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 12-16. o.

például azokat a kormányzati szervereket nem, amelyek (köz)szolgáltatást nyújtanak a lakosság számára (pl. ilyen a kormányzati webszerver). További feltétel, hogy a számítógép a kormány tulajdonát kell, hogy képezze vagy legalább a kormány használja, vagy az érdekében használják, erre példaként említhető, ha az Egyesült Államok fiókkal rendelkezik egy magáncégnek a szerverén, akkor azt már az Egyesült Államok használja és a bűncselekmény elkövetésének a tárgyát képezheti, annak ellenére, hogy az nem a saját tulajdona.

A számítógép működését a jogosulatlan hozzáférés már önmagában befolyásolja, mert sérti a kormányzati hálózat integritását és titkosságát. Ezért a bűncselekmény megállapításához nincs szükség annak bizonyítására, hogy az illető bármely információt megszerzett vagy kárt okozott.

A bűncselekmény elkövetői csak „kívülálló" személyek lehetnek az adott kormányzati szervre tekintettel. Mindez abból következik, hogy a Kongresszus döntése alapján a kormányzati alkalmazottak esetében közigazgatási szankciók alkalmazását tartotta megfelelőnek. Azonban ez csak az adott kormányzati szerven belül alkalmazható, ha egy másik kormányzati szerv rendszeréhez fér hozzá az alkalmazott, akkor a cselekménye e szakasz értelmében büntetendő, mert az adott szervre nézve kívülálló.

A törvény e bűncselekmény elkövetőjét egy évig terjedő szabadságvesztéssel rendeli büntetni, valamint emellé vagy ehelyett pénzbüntetés is megállapítható. Amennyiben korábban már elítélték informatikai bűncselekményért, akkor a kiszabható büntetés tíz évig terjedő szabadságvesztésre emelkedik.[131]

[131] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 23-25. o.

4. A DDoS-támadások és a számítógépes vírusok

4.1. A DDoS-támadásokról általában

A szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek a célja az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében[132] (pl. e-mail, banki vagy egyéb fiókokhoz való hozzáféréshez, vagy a weboldal elérésében) – innen a szolgáltatásmegtagadással járó elnevezés is –, amelynek a leggyakoribb formája a webszerver elérését és rendeltetésszerű használatát gátolja a mesterségesen generált és megnövelt adatforgalommal.[133]

Az elnevezés a támadás angol megfelelőjének rövidítéséből ered, amely során az említett támadás egyetlen számítógéptől származik, több közbeiktatott gép nélkül: Denial of Service (rövidítve: DoS). Amennyiben a támadás összetettebb, mert összekapcsolt rendszerek csoportjától, egyszerre sok – lehetőleg minél több – helyről indul, akkor a Distributed Denial of Service (rövidítve: DDoS), vagyis az elosztott szolgáltatásmegtagadással járó támadás használandó. Ebben az esetben feladatot nem egyetlen eszköz végzi el, mint a DoS- támadásnál, hanem a rendszert alkotó – egymástól akár nagy távolságban lévő - eszközök (pl. asztali gépek, okos mobiltelefonok, vagy routerek stb.) párhuzamosan.[134]

A támadás technikai alapja leegyszerűsítve a következőképpen néz ki: a DDoS-támadás során a támadó egy hálózatot alkotó számítógépek adatcsomagjaival elárasztja a célzott szervert akkora forgalommal, hogy az képtelen lesz az adatcsomagok fogadására, illetve válaszolására, ezzel akár a rendszer teljes leállását is eredményezhetik, azonban a funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik.[135]

A felhasználó tudta nélkül megfertőzött számítógépeket, 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 irányítója,

[132] NAGY (2009): i.m. 115. o.
[133] http://www.cert-hungary.hu/ddos [2017.09.21.]
[134] GYÁNYI Sándor: Az információs terrorizmus által alkalmazott támadási módszerek és a velük szemben alkalmazható védelem. PhD értekezés tervezet. Budapest, 2011. 88. o.
[135] NAGY Zoltán András: A sértett szerepe néhány kibertérben elkövetett bűncselekményben – alkalmazott viktimológia. In: Finszter Géza – Kőhalmi László – Végh Zsuzsanna (szerk.): Egy jobb világot hátrahagyni… Tanulmányok Korinek László professzor tiszteletére. PTE ÁJK. Pécs, 2016. 487. o.

aki kiosztja a feladatot a fertőzött eszközöknek, az ún. botmaster, illetve több irányító esetén a botherder. A botnet-hálózat tagjait a fertőzött zombi számítógépek alkotják. Azt a központi vezérlő eszközt, amely vezérli a botnet-akciókat controllernek hívják. A controller általában az ún. drop serverre csatlakozik, amely a botnet által gyűjtött adatok tárolására szolgáló tárhely, és ez hozzáférhető a botnet-hálózat valamennyi tagja és a botmaster számára. A botmaster és botnet közti kapcsolatot és az utasítások eljuttatását biztosító kommunikációs útvonal az ún. Command&Control (C&C) szerver.[136]

A botnetek a kiberbűnözői infrastruktúrának az alapját képezik, mérhetetlen erőforrást biztosítanak a rendelkezésre álló számítógép kapacitás és sávszélesség tekintetében.[137] A botnetek a DDoS-támadások indításán kívül alkalmasak spamküldésre, adathalászatra, hálózat-figyelésre, billentyűzet-figyelésre, a rosszindulatú programok (pl. gyakori a ransomware, vagyis zsarolóvírus) terjesztésére, illetve az internetes reklámokhoz a klikkelések begyűjtésére.

A DDoS-támadásokat a botok terjeszkedési fázisa előzi meg, amely során a malware eljuttatása a cél, hogy megfertőzzenek vele minél több rendszert, amelynek révén végül átveszik a gépek feletti irányítást és az összehangolt támadáshoz felhasználják azokat. Minél több, illetve nagyobb erőforrással rendelkező fertőzött taggal bővül a botnet-hálózat, annál nagyobb szabású támadást lehet végrehajtani.[138]

Fontos megjegyezni, hogy bármely felhasználó számítógépe bármikor válhat könnyedén zombigéppé. A káros botnet kódok ugyanúgy jutnak el az óvatlan felhasználó számítógépeire, mint bármely más fertőzések. A számítógépek az internetre történő csatlakozással már ki vannak téve a veszélynek, a kockázat pedig különösen megnövekedett az új mobilinformatikai és IoT eszközök elterjedésével (pl. Mirai botnetvírus közel 150 000 routert és biztonsági kamerát fertőzött meg, a segítségével szokatlanul erős DDoS-támadást hajtottak végre az Egyesült Államok egész keleti partján, ahol több óráig az internet szolgáltatás szünetelt).[139]

---

[136] GYÁNYI (2011): i. m. 89. o.

[137] EUROPEAN PARLIAMENT'S POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS: Cybersecurity in the European Union and Beyond: Exploring the Threaths and Policy Responses. 2015, 36. o. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf [2017.09.24.]

[138] GYÁNYI Sándor: A botnetek, a túlterheléses támadások eszközei. Magyar Rendészet, 2013. Különszám 24. o.; Az Europol felhívja a figyelmet arra, hogy ezek a nagyszabású támadások már könnyen megvalósíthatók kisebb számú, de ellenállóbb botnetekkel is. Kezdetben 100 Gbps támadások voltak megfigyelhetők, napjainkra a 300 Gbps-ot is meghaladja, sőt a jelentése szerint már 600 Gbps erősségű támadásra is sor került és ez 24 óránál tovább is tarthat. EUROPOL: The Internet Organised Crime Assessment (europol) 2016. 35. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 [2017.10.24.]

[139] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf [2017.11.05.]

Napjainkban a botnetek a technológiai fejlődésnek köszönhetően már fájlmegosztó rendszereken, Peer-to-Peer (P2P) hálózatokon, közösségi oldalakon keresztül is terjedhetnek.

A túlterheléses támadások mögött húzódó motivációk általában különböznek. Előfordulhat, hogy egy támadás azt a célt szolgálja, hogy a célpontot érintő súlyosabb betöréseket elfedje. Ezen kívül a DDoS-támadásokat egyre gyakrabban anyagi haszonszerzés céljából például zsarolás során használják fel. Emellett történhet károkozási szándékkal, mint például az üzleti versenytársak technológiai folyamatai ellen intézett támadásokkal. Ebben az esetben a támadók általában tudatosan, jól időzítve olyan időpontokat választanak a támadásokhoz, amikor az adott célpont nagyobb bevételre számíthat. Ennélfogva nagyobb kárt is tudnak okozni például ilyen a Cyber Monday, Black Friday, karácsonyi időszak vagy a sportfogadásokra tekintettel az amerikai Super Bowl. A weboldalak működésének a megszakítása költséges terhet jelent bármely oldal üzembentartója számára legyen szó kis- és középvállalkozásról vagy nagy vállalatról.[140] A támadással járó pénzügyi veszteség esetenként különbözhet és nem kizárt az sem, hogy az megtámadott vállalkozás működésére hosszútávon is hatással van. Ez megnyilvánulhat a kieső és pótolhatatlan bevételben, illetve a presztízsveszteségben, mivel az ügyfelek nem tudják elérni a támadással célzott cég honlapját, sem igénybe venni az általa kínált szolgáltatást, ezért inkább a konkurens vállalkozásokat választják és lemorzsolódnak (pl. a pénzügyi ágazaton belül, ez különösen a tőzsdei kereskedésben pillanatok alatt súlyos és jelentős kárt okozhat).[141]

Az informatikai támadások hátterében politikai[142] vagy ideológiai indíttatás is állhat, amit az ún. hacktivizmus[143] elnevezéssel illetek. A hacktivista nem egy csalárd hacker, aki profit érdekében személyes információkat szerez meg vagy egyéb súlyos kárt okoz, hanem tevékenységével az a célja, hogy felhívja a figyelmet egy aktuális politikai vagy társadalmi ügyre. Számára a hacktivizmus egy internet által biztosított stratégia, amely lehetővé teszi a polgári engedetlenség gyakorlását (pl. a DDoS-támadások indításával, a weboldal felülírásával

[140] Például a DDoS-támadások következtében egy órányi kényszer offline állapot a nagyvállalatok számára jelentős gazdasági veszteséget okozott: a Google-nek több mint 100 millió dollárt, az Amazonnak közel 750 millió dollárt és a PayPalnek 250 millió dollárt. Lásd JOUGLEUX, Philippe – SYNODINOU, Tatiana-Eleni – MITROU, Lilia: Chapter 2: Criminalization of Attacks against Information Systems. In: Iglezakis, Ioannis (ed.): The Legal Regulation of Cyber Attacks. Wolters Kluwer, 2019. 21. o.

[141] URCUYO, Michael S.: From Internet trolls to seasoned hackers: protecting our financial interests from Distributed-Denial-Of-Service attacks. Rutgers Computer & Technology Law Journal Volume 42., 2016, 300–330. o.

[142] A 2016-os amerikai elnökválasztás, illetve az azt megelőző kampány hívta fel a figyelmet arra, hogy az informatikai támadásokat és a médiaeszközöket, különösen a közösségi médiát, akár a választás eredményének befolyásolására is használhatják. Lásd részletesen erről KOVÁCS László – KRASZNAY Csaba: „Mert az övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-s amerikai elnökválasztás során. Nemzet és Biztonság 2017/3. szám 3-15. o.

[143] A hacktivizmus, avagy a „hactivism” elnevezés a „hacking” és az „activist” szavak összevonásából ered.

az ún. „defacement”-tel, információk jogosulatlan megszerzésével, illetve azok későbbi nyilvánosságra hozatalával, vagy egyéb virtuális szabotázs akciókkal).[144]

A túlterheléses támadások szolgálhatják a kiberhadviselést[145] és hozzájárulhatnak a kiberháborúkhoz. Egyre gyakrabban megfigyelhető, hogy a hackerek nem önállóan cselekednek, hanem mögöttük már felsorakoznak a nemzetállamok is, így az államok által szponzorált kibertámadásokról van szó, amelyek stratégiai és katonai célt szolgálnak. Ezeket általában a hivatásos állományban lévő informatikusok vagy a megbízott white hat hackerek hajtják végre[146] (pl. az Egyesült Államok Védelmi Minisztériuma 2010-ben létrehozta a katonai Kiberparancsnokságot, míg Kína és Oroszország tagadja, hogy rendelkeznének „kiberhadsereggel”[147]). Példaként említhető a 2007-es első tallini kiberháború, amikor a DDoS-támadások napokig megbénították a kormányzati rendszert, a telekommunikációs és a pénzügyi hálózat működését. 2008-ban az öt napos orosz-grúz konflikus volt az első olyan összecsapás, amikor a fegyveres harc mellett, azzal párhuzamosan a kibertérben is küzdelem folyt. Azonban ezeknek a támadásoknak a forrása – vélhetően Oroszország volt –, de ezt egyértelműen a mai napig nem tudják bizonyítani.[148] Reagálva ezekre az eseményekre a NATO Kibervédelmi Kiválósági Központ munkatársai elsőként készítették el a kibervédelmi kézikönyvet (Talinn Manual), ami ugyan csak ajánlásnak tekinthető, de jogi keretet nyújt az informatikai hadviseléshez a már meglévő nemzetközi jogi rendelkezések megfelelő alkalmazásával.[149]

Emellett már, ha még nem is számottevően ugyan, de a terrorista csoportok eszköztárában is felsorakozhatnak a különböző informatikai támadások, ezért a nemzetközi és hazai szakirodalom is már egy ideje foglalkozik az ún. kiberterrorizmus (cyberterrorism) kérdésével.[150] Azonban ennek részletes elemzése nem képezi az értekezés részét.

---

[144] https://www.techopedia.com/definition/2410/hacktivism [2017.10.21.]

[145] Kiberhadviselésnek nevezik azt a jelenséget, amikor egy állam egy másik állam ellen informatikai támadást indít, amelynek célja az adott ország társadalmi és gazdasági működésének akadályozása vagy ellehetetlenítése. Ez általában egy átfogó támadássorozat, amelynek a kiterjedése jelentős és az okozott kár oly mértékű, hogy akár egy egész országot veszélyeztethet. Például a túlterheléses támadások kivitelezése a kibertérben stratégiai és taktikai jelentőségű lehet, mert a valós térben zajló katonai támadásokkal okozott „káoszhoz” hozzájárulhat, és további potenciált adhat a fizikai támadásokhoz. Lásd STEPHENSON, Peter – GILBERt, Keith: Investigating computer-related crime. CRC Press, 2013. 35. o.

[146] NAGY Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! Magyar Jog 2016/1. 21-22. o.

[147] BERKI Gábor: Kiberháborúk, kiberkonfliktusok. In: Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – Pintér István: Műhelytanulmányok – A virtuális tér geopolitikája. Geopolitikai Tanács Közhasznú Alapítvány. Budapest, 2016. 274. o.

[148] APPAZOV, Artur: Legal aspects of cybersecurity. University of Copenhagen, Faculty of Law, 2014. 21–22. http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf [2017.10.21.]

[149] Lásd bővebben SCHMITT, Michael N. – VIHUL L, Liis (eds.): Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

[150] Lásd ehhez részletesen CHEN, Thomas M. – JARVIS, Lee - MACDONALD, Stuart: Cyberterrorism – Understanding, Assessment, and Response, Springer, New York, 2014.; A kiberbűnözést, a kiberterrorizmust és a

4.2. A malware támadásokról általában

A támadások másik gyakori típusát a különféle ún. malwarek vagyis rosszindulatú programok képezik, amelyeket az elkövetők továbbítanak, és ezáltal a gyanútlan felhasználók rendszereit fertőzhetik meg. A malware a „malicious" és „software" vagyis a rosszindulatú szoftver szavak összevonásából áll, ami utal egyben arra, hogy általában ezeket a kártevő programokat arra használják, hogy jogosulatlanul behatoljanak az információs rendszerekbe, vagy módosításokat végezzenek, kárt okozzanak az adatokban a felhasználó tudta és hozzájárulása nélkül, de egyre gyakoribb, hogy abból a célból használják fel ezeket, hogy bizalmas adatokhoz férjenek hozzá, amelyek elősegítik a további csalásokat vagy egyéb jogsértéseket (pl. zsarolás, személyazonosság-lopás stb.).[151]

Különböző típusú rosszindulatú programokat ismerünk és sokszor alig különböznek egymástól, ezért nehéz csoportosítani őket, de az alábbi fő kategóriák határozhatók meg: vírusok (virus), férgek (worm), trójai programok (Trojan) és kémprogramok (adware, spyware).

Általában, hogy mikor tekinthető egy szoftver rosszindulatúnak az attól is függ, hogy milyen céllal készítik és telepítik. Például az adware és spyware programok gyakran inkább a „nemkívánatos" kategóriába sorolhatók, mert reklámozási célt szolgálnak vagy kereskedelmi célú információ gyűjtésre használják őket (pl. böngészési szokásaink megfigyelésére és megszerzett információk alapján célzott reklámokat és hirdetéseket küldenek). A kémprogramok azonban alkalmasak a bizalmas adatok gyűjtésére is (pl. jelszavak, személyazonosító, banki vagy más személyes adatok) vagy a rendszer sebezhetőségének feltérképezésére, és az így megszerzett információk további visszaélések alapját képezhetik. A billentyűzetfigyelők (keylogger) pedig a billentyű leütések valós idejű rögzítését teszik lehetővé.

Az elkövetők gyakran számítógépes vírusokat és férgeket használnak. Előbbi képes önmagának a lemásolására és megfertőzni az információs rendszereket, amelyhez szüksége van egy „hordozóra", gazdagépre tehát lényegében úgy viselkedik, mint a biológiai vírus. A számítógépes férgek ezzel szemben önmagukat reprodukálják, kihasználják a hálózatok hibáit, vagy hiányos biztonsági beállításokat, hogy tovább terjeszkedjenek. Manapság a legveszélyesebb programok ebből a típusból kerülnek ki. Az önsokszorosításon kívül a férgek

kiberhadviselést hasonlítja össze: BRENNER, Susan W.: Cybercrime, Cyberterrorism and Cyberwarfare. Relations internationales 77(3). 453-471. o.; valamint DORNFELD László: Kiberterrorizmus – A jövő terrorizmusa? In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019. 46-63. o.; illetve SZABÓ Imre: Az informatikai terrorizmus veszélyei. Belügyi Szemle 2011/2. 5-20. o.

[151] CLOUGH: i.m. 36-38. o.

többféle dologra is programozhatóak. Egyik jellemző következményük, hogy a támadók jogosulatlanul hátsó ajtót (backdoor) nyitnak a rendszerekbe, amin keresztül adatokat szerezhetnek meg, illetve botnet-hálózat részévé tehetik a megtámadott számítógépet.

A trójai programok ártalmatlannak tűnnek – sőt sokszor más hasznos programnak álcázzák magukat, így a gyanútlan felhasználó saját maga tölti le ezeket –, de ezek rejtett káros tevékenységet végeznek anélkül, hogy önmagukat sokszorosítanák. A trójai is alkalmas lehet a hátsó ajtó létrehozására a megfertőzött rendszerben, amelynek köszönhetően a támadónak lehetősége az irányítást átvenni az egész gép felett (pl. a mikrofon és a webkamera is felhasználható).

Emellett még megemlítendő, hogy vannak az ún. „logikai bomba" elnevezésű kártékony programok, amelyek például egy adott időpontban vagy meghatározott program indításakor aktiválják magukat.

A malware terjesztés történhet közvetlenül például egy megfertőzött adathordozóval való rácsatlakozással (pl. pendrive), vagy az interneten, valamint más számítógép-hálózaton keresztül egy végrehajtható fájl segítségével. Gyakran e-mail mellékletként küldenek rosszindulatú programokat vagy egy weboldalra irányítanak át, de megjelent már az ún „drive-by-downloads" is, ami azért különösen veszélyes, mert ekkor a malware magától letöltődik, kihasználva a rendszer sebezhetőséget a weboldalba vagy alkalmazásba illesztve. Az ún. „clickjacking" esetében pedig a káros kód el van rejtve a „kattintható" tartalmakban például a letöltés gomb formájában.

A legnagyobb veszélyt az elmúlt években a zsarolóvírusok (ransomware) jelentették, mely kártékony programok úgy működnek, hogy a megfertőzött számítógépen vagy mobil eszközökön tárolt fájlokat, akár a teljes adatállományt letitkosítják, 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 kilétének megismerése szinte lehetetlen, mert általában a „váltságdíjat" a nehezen lenyomozható ún. kriptovalutában[152] – például bitcoinban – kérik. A pénz kifizetése sem garancia arra, hogy a zsaroló a titkosítást feloldja. 2017-ben a WannaCry zsarolóvírus az egész világon végig söpört, mert egyedi módon féregként viselkedve egy hálózaton belül valamennyi számítógépet megfertőzött így például Nagy-Britanniában kórházak, illetve Németországban a

[152] Lásd részletesen „A kriptovaluták büntető anyagi és eljárásjogi kérdései" című fejezetben.

vasútvállalat rendszerét blokkolta teljesen.[153] Ezt pedig követték az újabb ransomware-ek a Petya és a NotPetya. A felhasználók gyakran fizetnek is például a Hollywood Presbyterian Hospital Medical Center 17,000 $ értékű bitcoint fizettet ki, mert a vírus napokig megbénította a kórház működését. Részben ennek a támadásnak köszönhető, hogy Kalifornia állam büntető törvénykönyvébe önálló bűncselekményként jelent meg a ransomware felhasználása.[154]

2014-ben fedezték fel a Tyupkin elnevezésű malware-t, amely számos ATM-es fertőzött meg világszerte, és lehetővé tette az elkövetőknek, hogy közvetlen manipulációval kiürítsék az automatákat, mindezt bankkártya használata nélkül sikerült végrehajtani, és így több millió dollárhoz jutottak hozzá.[155]

További kiberbiztonsági kockázatot jelentenek különösen az egyedi hatású és célzott támadásokra kifejlesztett rosszindulatú programok jelentik különösen, amelyek a kritikus infrastruktúrákat támadják. 2010-ben a Stuxnet volt az első komoly célzott támadás, melyet ipari rendszerek ellen vetettek be. Az első kártékony kód volt, amely a kritikus infrastruktúra elemeinek a fizikai károkozásával is járt – sőt kifejezetten ezzel a céllal fejlesztették ki – és ezáltal Irán atomprogramját lényegében megbénították, mert több év kellett ahhoz, hogy egy atomfegyver előállításához szükséges dúsított urán a rendelkezésükre álljon. Ma már tudjuk, a Stuxnet csak az első ilyen eszköz volt a sorban, testvérei a Duqu, a Gauss vagy a Flamer bizonyítják ezt.[156]

4.2.1. A célzott támadások

Fontosnak tartom, hogy külön említést tegyek az egyik legveszélyesebb támadási formáról az ún. „Advanced Persistent Threat", avagy rövidítve az APT támadásokról, amelyeket gyakran célzott támadásokként neveznek. Az elnevezés pedig abból ered, hogy nem véletlenszerűen választják ki a megtámadni kívánt rendszereket (pl. államigazgatási, védelmi vagy pénzügyi szervezeteket, így bankokat vagy tőzsdei cégeket), hanem tudatosan előre megtervezik azokat. Ezek általában támadások sorozatát foglalják magukban, amelyek gondosan előkészítettek és hosszú időn keresztül észrevétlenül hajtják végre őket.[157]

---

[153] NAGY Zoltán András – MEZEI Kitti: A zsarolóvírus és botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Szent Lászlótól a modernkori magyar rendészettudományig. Pécs, 2017. 167-168. o.

[154] https://www.bleepingcomputer.com/news/government/new-california-law-makes-ransomware-a-standalone-crime/ [2017.05.21.]

[155] https://www.theguardian.com/technology/2014/oct/08/cash-machine-atm-malware-tyupkin [2017.05.23.]

[156] NAGY Zoltán András: A kiberháború új dimenzió – a veszélyeztetett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). Pécsi Határőr Tudományos Közlemények XIII., 2012. 225–226. o.

[157] KOVÁCS László: A kibertér védelme. Dialog Campus Kiadó. Budapest, 2018. 151-153. o.

Az utóbbi évek egyik legnagyobb APT-alapú támadássorozata az ún. Carbanak volt[158], amely során az elkövetők kifinomult módszerekkel megközelítőleg 1 milliárd dollárt szereztek meg 30 országból, több mint 100 különböző pénzintézettől és mindezt úgy, hogy hónapokig észrevétlenül tudtak maradni a pénzügyi rendszerek hálózatában. A támadásra a nemzetközi bűnügyi együttműködésnek köszönhetően derült fény, amely a bűnüldöző hatóságok és a magánszféra – az Interpol, a Europol és a Kaspersky Lab – közös munkájának az eredménye.

Az APT támadások esetén a modus operandi alapja általában a social engineering megoldásokkal, főleg az ún. „spear phishing", azaz célzott adathalász támadásokkal kezdődik. Ez esetben is a támadás forrását a banki alkalmazottaknak küldött célzott adathalász e-mailek jelentették. A levelek a támadás alapját képező Carbanak elnevezésű malware-t tartalmazták, amely a Microsoft Office programcsomag biztonsági réseit kihasználva hátsó ajtót nyitott a banki rendszerhez. Ezáltal a támadók részére lehetőség nyílt a belső hálózat feltérképezésére, a pénzügyi rendszerekbe való belépéshez, valamint távoli hozzáférést biztosító szoftver telepítésére, amelynek köszönhetően az alkalmazottak képernyő aktivitását is megfigyelték, sőt ezt képernyővideóval rögzítették is. A támadás összetettségére utal, hogy az elkövetők a jogtalan haszonszerzés érdekében különböző módszereket alkalmaztak:

A támadók online banki rendszereken és a nemzetközi elektronikus fizetési megoldásokon keresztül utaltak át különböző összegeket a saját számláikra vagy más országok bankjaiba.

A másik esetben a belső banki rendszeren keresztül az ügyfelek bankszámláin megváltoztatták a számlaegyenleget, a különbséget pedig a saját számláikra utalták, így észrevétlenek tudtak maradni, mivel az ügyfél egyenlege változatlan maradt.

Továbbá átvették az irányítást az ATM automaták felett is, amelyeket úgy programoztak távolról, hogy előre meghatározott időpontban készpénzt adjanak ki, amit a pénzfutárok a megadott időpontban vártak az automatáknál és elhozták a megbízónak.[159]

[158] Ezen kívül a Cobant és FIN7 néven ismert ez az elkövetői csoport. Tagjainak egy részét sikerült az amerikai hatóságoknak letartóztatniuk, amiről sajtóközleményt is adott ki az Egyesült Államok Igazságügyi Minisztériuma lásd: https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

[159] EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2018. 23. o.; https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 [2018.09.21.]

4.3. A DDoS-támadásokkal és a számítógépes vírusokkal kapcsolatos nemzetközi és uniós rendelkezések

A DDoS-támadásokat és a rosszindulatú programok segítségével végrehajtott támadásokat is kriminalizálja a Budapesti Egyezmény, méghozzá a számítástechnikai adat (4. cikk), valamint a rendszer megsértése (5. cikk) keretében. Előbbi szerint bűncselekménynek minősül a számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megrongálása, megváltoztatása vagy megsemmisítése, azonban fenntarthatják a szerződő felek annak kikötését, hogy a meghatározott cselekmény eredményeként jelentős kár következzen be. A rendelkezés célja, hogy megfelelő védelmet biztosítson a számítástechnikai adatoknak és programoknak - mint a fizikai dolgok esetén - a velük szemben bekövetkező károkozó magatartások esetén. Utóbbi miatt büntetendő, aki a számítástechnikai rendszer működését a számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével, jogosulatlanul és szándékosan, jelentős mértékűen akadályozza. Az akadályozásnak jelentős mértékűnek kell lennie, azonban, hogy mi minősül ennek, azt a szerződő felek szabadon határozhatják meg. Például jelentősnek tekinthető az olyan mértékű, formájú és gyakoriságú adat küldés egy meghatározott rendszerre, amely jelentős hátrányt okoz a rendszer használatában vagy más rendszerekkel történő kommunikációra való alkalmasságára (pl. ilyenek a DDoS-támadások, kártékony kódok, amelyek lényegesen lassíthatják a rendszer működését vagy programok, amelyek nagy mennyiségű e-mailt küldenek a címzettnek annak érdekében, hogy akadályozza a kommunikációt).[160]

A 2013-as irányelv a rendszert érintő jogellenes beavatkozást (4. cikk) határozza meg – hasonlóan a Budapesti Egyezményhez –, amely magában foglalja valamely információs rendszer működésének súlyos akadályozását vagy megszakítását a számítógépes adatok szándékos és jogosulatlanul történő bevitelével, továbbításával, megrongálásával, törlésével, minőségi rontásával, megváltoztatásával vagy elrejtésével, vagy ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tételével, és ezen magatartásoknak legalább a súlyosabb esetekben bűncselekménynek kell minősülniük.

A 2013-as irányelv az adatot érintő jogellenes beavatkozást (5. cikk) büntetni rendeli, ezért a tagállamoknak meg kell hozni a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszer számítógépes adatainak szándékos és jogosulatlan törlése, megrongálása, minőségi rontása, megváltoztatása vagy elrejtése, vagy az ilyen adatok szándékos és

[160] COUNCIL OF EUROPE: i.m. 12. o.

jogosulatlan hozzáférhetetlenné tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön.

Továbbá felhívta a figyelmet a botnetekre mint veszélyforrásokra, mert felismerték, hogy általuk egyre veszélyesebb, ismétlődő és átfogó támadásokat tudnak végrehajtani, amelyek gyakran kulcsfontosságú információs rendszereket (pl. kritikus infrastruktúrákat) érintenek. E kockázat figyelembevételével állapít meg büntetőjogi szankciót a botnetek létrehozására, mivel a felhasználásukkal súlyos kárt képesek okozni, de ennek meghatározása, hogy mi minősül súlyosnak az a tagállamok döntési jogkörébe tartozik (pl. fontos és közérdekű rendszerszolgáltatások megzavarása, jelentős költségek okozása, vagy személyes adatok, illetve különleges adatok, információk elvesztése stb.).

Súlyosbító körülménynek minősül, ha a bűncselekményt bűnszervezetben követik el, illetve az súlyos kárt vagy alapvető érdeksérelmet okoz. Büntetendő és súlyosabb szankció megállapításának van helye, ha a támadás átfogó, azaz jelentős számú információs rendszert érint vagy súlyos kárt okoz, ideértve azokat a támadásokat is, amelyek célja egy botnet-hálózat létrehozása, vagy amelyeket botnet révén hajtanak végre. Helyénvaló arra az esetre is súlyosabb szankciókat megállapítani, ha a támadás valamely tagállam vagy az Unió kritikus infrastruktúrája[161] ellen irányul. Ez azért indokolt, mert a kritikus infrastruktúrák egyes elemeinek működése, illetve együttműködése oly mértékben függenek az információs rendszerektől, hogy azok összeomlása vagy megsemmisülése súlyos következményekkel járhat, nem csak az adott infrastruktúrára nézve, hanem más kritikus infrastruktúrákra tekintettel is. A támadások éppen ezért általában az infrastruktúrán belül az ún. kritikus információs infrastruktúra részeit célozzák. Ezek azok az infokommunikációs rendszerek, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra működésének szempontjából (pl. számítógép-hálózat és programok stb.).[162] Ezek védelme különösen fontos, mert a támadások érinthetik például az erőművek, vízellátó vagy újrahasznosító ún. SCADA rendszereit, vagyis az ipari vezérlő rendszereket.[163] Érdemes felhívni a figyelmet arra is, hogy az uniós rendvédelmi szervekhez bejelentett, kritikus

[161] 2008/114/EK tanácsi irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. HL L 345. 2008.12.23. 77.: „kritikus infrastruktúra: a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban."

[162] MUHA Lajos: a Magyar Köztársaság kritikus információs infrastruktúrájának védelme. PhD értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest, 2007. 36-37. o. [2017.12.19.]

[163] HOLT, Bossler – BOSSLER, Adam M. – SEIGFRIED-SPELLAR, Kathryn C.: Cybercrime and digital forensics: An introduction. Routledge, 2018. 402. o.

infrastruktúrákat érintő támadások között a DDoS-támadások dominálnak és egyre gyakoribbak a célzott támadások.[164]

A szankciókra vonatkozó rendelkezéseket egyben pontosítja is a következőképpen: amennyiben szándékosan az információs rendszert vagy adatot érintő jogellenes beavatkozással (4-5. cikk), valamint a kiberbűncselekmény végrehajtásához szükséges eszköz használata révén (7. cikk) jelentős számú információs rendszert érintenek, akkor ezen esetek büntetési tételének a felső határa legalább három évig terjedő szabadságvesztés legyen. Továbbá az említett bűncselekmények elkövetésének a kísérlete is büntetendő.

Ha az információs rendszer vagy adat elleni bűncselekményt bűnszervezetben követik el, vagy súlyos kárt okoztak, vagy azok valamely, a kritikus infrastruktúra részét képező információs rendszer ellen követték el, akkor szabadságvesztéssel legyenek büntetendő, és a felső határa legalább öt év.

Ezen kívül rögzíti, hogy a tagállamoknak meg kell hozni a szükséges intézkedéseket annak érdekében, hogy ha a 4. és 5. cikkben említett bűncselekményeket egy másik személy személyes adataival visszaélve követték el egy harmadik fél bizalmának elnyerése céljából, és ezáltal kárt okoztak a személyazonosság jogos tulajdonosának, akkor ezt a nemzeti joggal összhangban súlyosító körülménynek lehessen tekinteni, kivéve, ha e körülmény a nemzeti jog értelmében már egy másik bűncselekményt valósít meg.

Az informatikai bűncselekmények elkövetését megkönnyítheti számos körülmény például, ha az elkövetőnek alkalmazotti minőségében van - vagy volt - hozzáférése az érintett információs rendszerek részét képező biztonsági rendszerekhez. A nemzeti jog keretében a büntetőeljárás során a tagállamoknak gondoskodniuk kell arról, hogy a bírók az elkövető elítélésekor figyelembe vehessék e súlyosító körülményeket, mivel továbbra is a bíróság mérlegelési jogkörébe tartozik, hogy e körülményeket a konkrét esetek egyéb tényállási elemeivel együtt miként értékeli.

Az információalapú társadalmakban a vállalatok számára az egyik a legnagyobb értékké az adat, illetve az információ vált, amelyek viszont a digitális forradalomnak köszönhetően, egyre könnyebben szerezhetők meg jogtalan eszközökkel, így különösen elkövethetők a szervezetek terhére – vagy akár javára – az egyes informatikai bűncselekmények (pl. a vállalatok rendszereinek a biztonsági réseinek a kijátszásával, vagy éppen az adatvagyon vesztés a kilépő alkalmazottaknak köszönhető, mert magukkal viszik azt).[165] A Budapesti Egyezmény (12.

[164] EUROPOL (2017): i.m. 26.
[165] AMBRUS István – FARKAS Ádám: Whistleblowing és büntetőjog – szempontok a vállalati visszaélések megítéléséhez. Magyar Jog 2017/7-8. 442-443. o.

Cikk) és a 2013-as irányelv (10. cikk) is erre tekintettel érinti a jogi személyek[166] felelősségre vonhatóságát az informatikai bűncselekményekért, amelyeket akár saját nevében, akár a jogi személy valamely szervének tagjaként eljárva olyan személy követett el a jogi személy javára, aki a jogi személyen belül vezető tisztséget tölt be, amely a jogi személy képviseletének, vagy a nevében történő döntéshozatal, vagy a jogi személyen belüli ellenőrzés jogán alapul. Emellett szükséges intézkedéseket kell tenni annak értekében is, ha az említett személy általi felügyelet vagy ellenőrzés hiánya teszi lehetővé, hogy a neki alárendelt személy kiberbűncselekményt kövessen el a jogi személy javára. Mindez nem zárja ki azt, hogy a természetes személyek ellen is büntetőeljárást indítsanak. A felelősségre vont jogi személy esetén az alkalmazott szankció magában foglalhat büntetőjogi és nem büntetőjogi pénzbüntetéseket vagy bírságokat is.

4.4. A DDoS-támadások és a számítógépes vírusok hazai szabályozása

Az információs rendszerekben különböző módon képesek kárt okozni, mint például, aki jogosulatlan hozzáférést szerez a rendszer felett, képes olyan parancsot küldeni, ami a rendszer működéséhez szükséges fájlok törlését vagy annak a leállítását eredményezi. Ezeket az eseteket hivatott a Btk. 423. § (2) bekezdés a) pontja szabályozni, amelynek értelmében, aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

A törvény azonban nem határozza meg a releváns elkövetési magatartásokat, ezért bármely cselekmény tényállásszerű lehet, amely az információs rendszer működésének akadályozását eredményezi. Akadályozáson nem kizárólag azt kell érteni, hogy a rendszer nem működik, vagy nem megfelelően működik, hanem azt is, ha a rendszer nem alkalmas a rendeltetésének megfelelő feladat ellátására. Amennyiben az információs rendszer pl. közhiteles nyilvántartás vagy más, az adatok hiteles igazolására szolgáló nyilvántartás, akkor akár a valótlan, akár a valódi adat jogosulatlan bevitele, megváltoztatása, törlése e nyilvántartások rendeltetésszerű használatát, működését is gátolhatja. Az elkövető tudatának át kell fognia azt a tényt, hogy cselekményével jogosulatlanul akadályozza az információs rendszer működését. Az elkövetési magatartás megkezdésével a kísérlet valósul meg és az akadályozás bekövetkezésével válik befejezetté. A bűncselekmény e fordulatát nem csak az adatok bevitelére, megváltoztatására, törlésére és egyéb műveletek végzésére jogosulatlan személy, hanem arra jogosult személy is

[166] A 2013-as irányelv 2. cikk c) pontja meghatározza a jogi személy fogalmát, amelynek értelmében „bármely jogalany, amely az alkalmazandó nemzeti jog szerint jogi személynek minősül; ide nem értve a tagállamokat, harmadik országokat, az állami hatáskört gyakorló közjogi szerveket, valamint a nemzetközi közjogi szervezeteket."

elkövetheti, azonban ehhez feltétel, hogy a beavatkozást szándékosan nem a jogosultsága keretei között, nem a rendeltetésének megfelelően, hanem a reá vonatkozó rendelkezések megsértésével végezze.[167] A jogosulatlan akadályozásra a leggyakoribb esetként a DDoS-támadások említhetők. A honlaprongálás (defacement) is e fordulat szerint minősül, ha a weboldal tartalmát alakítják át, írják felül a saját – szöveges vagy vizuális – tartalommal.

Amennyiben a jogosulatlan belépést követően olyan meg nem engedett műveleteket hajt végre az elkövető, aminek következtében az információs rendszer működését akadályozza, akkor a (2) bekezdés a) pontja szerinti fordulatot valósítja meg, például akkor, ha az információs rendszer adatfeldolgozás eredményét a vírusok becsempészésével tudatosan befolyásolja, és ezáltal a programok működésre képtelenné váljanak.[168] További példaként említhető egy konkrét jogeset, amikor a terhelt egy weboldal biztonsági réseinek a megállapítására alkalmas programmal több esetben jogosulatlanul belépett egy internetszolgáltató cég szerverére, és e magatartása eredményeképpen annak teljesítményét csökkentve szolgáltatás-kiesést okozott.[169]

A (2) bekezdés b) pontja szerint, aki az információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

A harmadik fordulatnak az elkövetési tárgya az információs rendszerben lévő adat. Az (5) bekezdés szerint e § alkalmazásában adatnak minősül az „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."[170] Érdekességként említendő, hogy például Gellér Balázs és Ambrus István az elkövetési tárgy fogalmát a következőképpen határozza meg: az elkövetési tárgy a törvényi tényállásban meghatározott dolog, személy vagy más speciális tárgy, akire vagy amelyre az elkövetési magatartás hatása irányul. Utóbbira álláspontjuk szerint azért van szükség, mert a Btk. rendszerében léteznek olyan élettelen tárgyak, amelyek elkülönült legáldefiniciójuk miatt nem vonható a dolog büntetőjogi fogalma alá. A „más speciális tárgy" alatt érteni kell a virtuális

[167] MOLNÁR (2018): i.m. 948. o.
[168] BH 1999.145.
[169] KOVÁCS Mihály: A számítástechnikai rendszer és adatok elleni bűncselekmények a városi ügyészség gyakorlatában. Ügyészek Lapja 2011/5. 70. o.
[170] Ezt a fogalommeghatározást használja mind a Budapesti Egyezmény [1. Cikk b) pontja], mind a 2013-as irányelv is [2. cikk b) pont].

valóságban létező, kézzel nem fogható elkövetési tárgyakat is mint a számítástechnikai adatot.[171]

A szankcionált elkövetési magatartások a következők: az adat megváltoztatása, törlése vagy hozzáférhetetlenné tétele. Az adat megváltoztatásán az adat tartalmának bármilyen módon történő módosítását értjük, amely akár megvalósulhat az adat felülírásával, kiegészítésével vagy részleges törlésével. A Legfelsőbb Bíróság ezt az elkövetési magatartást állapította meg abban az ügyben, ahol az ETR rendszerben a nem teljesített vizsgát jelölő adatot az elkövető eredményes vizsgára változtatta meg és ehhez a megfelelő érdemjegyet is hozzárendelte. Az információs rendszer és adat megsértésének tényállását valósítja meg a főiskola számítástechnikai hálózatának felügyeletét ellátó informatikusa, aki a hallgatók vizsgakötelezettségét és vizsgaeredményeit nyilvántartó számítástechnikai rendszerben levő adatok jogosulatlan megváltoztatásával a vizsgát előírás ellenére nem tett hallgatóval kapcsolatban olyan adatokat rögzít a rendszerben, amelyek szerint a hallgató a meghatározott tantárgyból eredményes vizsgát tett.[172] A törlés az adat megsemmisítését, teljes eltávolítását jelenti. Az adat hozzáférhetetlenné tétele esetén nem valósul meg törlés, a rendszer továbbra is tárolja, de az elkövető az adatnak az elérhetőségét akadályozza meg például azzal, hogy jelszóval védett könyvtárban elrejti, titkosítja az adatállományt mint például a zsarolóvírusok esetében ez történik, vagy az általa ismert helyre (FTP-, cloud-, raid szerverre) másolja.[173]

A törvény már egyetlen adat megváltoztatását, törlését vagy hozzáférhetetlenné tételét büntetni rendeli. Az adat megváltoztatásának, törlésének, hozzáférhetetlenné tételének szándékos előidézésén túl a cselekmény tényállásszerűségének a megállapításához szükséges még, hogy e magatartásokat a megfelelő jogosultság (engedély) hiányában, illetve a jogosultság kereteit megsértve kövessék el. E körben a rendszergazda rendelkezése az irányadó.

A bűncselekmény az adat bármilyen módon történő módosításával befejezetté válik. Nem szükséges, hogy a cselekmény az adatfeldolgozás eredményét befolyásolja, vagy bármely egyéb hátrányos következmény bekövetkezzen.[174]

Azonban megemlítendő, hogy e fordulat keretében az adatbevitel önmagában nem büntetendő, csak akkor, ha az további nem kívánt következményekhez vezet, mint például az információs rendszer működését akadályozza, valamint, ha azt jogtalan haszonszerzés végett végzik, és ezzel kárt okoznak. Az adatbevitelt a Budapesti Egyezmény sem nevesíti.

---

[171] GELLÉR Balázs - AMBRUS István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017. 205-206. o.
[172] EBH 2009.2033. I.; BH 2009.264. I.
[173] COUNCIL OF EUROPE: i.m. 11. o.
[174] MOLNÁR (2018): i.m. 947-948. o.

A minősített eset állapítható meg és bűntett miatt egy évtől nyolc évig terjedő szabadságvesztéssel büntetendő, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint, azonban a törvény nem határozza meg, hogy mi tekinthető jelentős számúnak, tehát a jogalkalmazókra hárul ez a feladat, hogy egy erre vonatkozó gyakorlatot dolgozzanak ki.[175] A minősített esetre a DDoS-támadás jó példa, hiszen a végrehajtása során a támadó sok száz vagy több ezer felhasználó gépei felhasználásával kísérel meg kapcsolatot létesíteni a megtámadott számítógéppel. E sok száz vagy ezer zombigép egy botnetet alkot, amit a támadó vezérel távolról. Az egyszerre küldött nagy mennyiségű adatkérés és továbbítás bénítja a megtámadott információs rendszert, ami kimerítheti a jelentős számú információs rendszer fogalmát.[176] A másik minősített eset megvalósulásakor a büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el. A Btk. az értelmező rendelkezések között a 459. § 21. pontjában meghatározza exemplifikatív felsorolással, hogy mi minősül közérdekű üzemnek: a közmű, a közösségi közlekedési üzem, az elektronikus hírközlő hálózat, az egyetem és a postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok (pl. pénzintézetek) és üzemek. Ezzel a probléma az, hogy a közérdekű üzem és a 2013-as irányelv szerint alkalmazott kritikus infrastruktúra fogalma[177] nem fedi egymást, így a cselekmény minősítése vitatott lehet, különösen a szociális jólét, a közegészség intézményei ellen intézett támadások esetében. Erre azért is fontos felhívni a figyelmet, mert 2017 óta hazánkban is bevezetésre került az elektronikus egészségügyi rendszer, ami azt jelenti, hogy ettől kezdve valamennyi személyes adatot és az intézményi ellátási dokumentumokat elektronikus úton tárolnak, ezáltal fokozott veszélynek vannak kitéve az esetleges informatikai támadásokkal szemben.

[175] MOLNÁR (2018): i.m. 950. o.

[176] NAGY (2014): i.m. 598. o.; Külön érdekesség, hogy a magyarországi botnet fertőzöttségre figyelmeztető 2015-ös Symantec-tanulmány szerint Magyarország a vírussal fertőzött számítógépek számát tekintve a 6. legfertőzöttebb ország a világon – Kína, USA, Tajvan, Törökország és Olaszország előz meg minket –, és a 2. helyet foglalja el az európai országok között. Lásd Internet Security Threat Report. 2015/20.; 2016-ban pedig a magyar kormányzati informatikai rendszert és oldalakat is sorozatos DDoS-támadás érte, és ennek következtében több óráig nem voltak elérhetőek a szolgáltatások. Lásd Belügyminisztérium által közzétett jelentést: http://www.kormany.hu/hu/belugyminiszterium/hirek/
senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast [2017. 09. 09.]

[177] A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklet 3.2. pontja: „kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére”.

A bűncselekmény valamennyi fordulata szándékos bűncselekmény, amely egyenes és eshetőleges szándék mellett egyaránt tényállásszerű. A tettes bárki lehet, aki a tényállásszerű elkövetési magatartásokat tanúsítja. Ennek megfelelően valamennyi fordulatát a megfelelő jogosultsággal rendelkező, illetve az ilyen jogosultsággal nem rendelkező személy tettesként egyaránt elkövetheti.

A bűncselekmények rendbelisége az informatikai rendszerek számához igazodik. A törvény valamennyi informatikai rendszer önálló büntetőjogi védelmét biztosítja függetlenül attól, hogy azok tulajdonosa, illetőleg üzemeltetője azonos vagy különböző természetes vagy jogi személy, illetőleg jogi személyiség nélküli szervezet.

Az egyes informatikai rendszerek sérelmére megvalósított akár azonos, akár különböző elkövetési magatartások száma a rendbeliséget rendszerint nem érinti. A következetes ítélkezési gyakorlatnak megfelelően a természetes egység keretében nyerhet értékelést.[180] Folytatólagosan elkövetett információs rendszer vagy adat megsértésének bűncselekménye állapítható meg, ha az elkövető egységes akaratelhatározásból az azonos helyzetből (hozzáférésből) fakadó lehetőséget kihasználva, azonos információs rendszer sérelmével, különböző alkalmakkal követi el a vizsgált bűncselekményt.[181]

Az információs rendszer vagy adat megsértésének bűncselekménye alapesetének három fordulata egymás mellett, illetve egymást követően is megvalósulhat. Az azonos jogtárgysértés a valódi alaki halmazat megállapítását rendszerint kizárja. A különböző alkalmakkal elkövetett, egymással összefüggésben nem álló cselekmények esetén azonban a valódi anyagi halmazat megállapítását nem zárja ki önmagában az a körülmény, hogy az egyes bűncselekményeket azonos informatikai rendszer használatával (felhasználásával, sérelmével) hajtották végre.[182]

Érdemes végül áttekinteni a halmazati és elhatárolási kérdéseket a bírósági gyakorlat alapján. Amennyiben a hivatalos személyként eljáró ügyintéző anyagi ellenszolgáltatásért valótlan adatokat jegyez be közhiteles nyilvántartásba, és ezzel összefüggésben valótlan tartalmú közokiratok kerülnek kiadásra, akkor egyetlen magatartással – a valótlan adatok bevitelével – a már abban rögzített közokiratokra vonatkozó adathalmazokat jogosulatlanul megváltoztatja. Egységes cselekménye a Btk. 413. § (1) bekezdésének b) pontja szerinti információs rendszer és adat megsértésének bűntettét, valamint a Btk. 343. § (1) bekezdés b) pontja szerinti hivatalos személy által elkövetett közokirat-hamisítás bűntettének törvényi tényállását egyaránt megvalósítja, mert sérti mindkét bűncselekmény védett jogi tárgyát,

[180] MOLNÁR (2016): i.m. 950-951. o.
[181] Legfelsőbb Bíróság Bf. II. 74/2008/5.
[182] MOLNÁR (2016): i.m. 951. o.

feltéve, ha a bűncselekményt egyenes szándékkal, magatartásának előre látott következményeit kívánva hajtja végre.[183]

Az információs rendszer és adat elleni bűncselekmény, valamint a közokirat-hamisítás és a vesztegetés bűncselekményeinek anyagi halmazata valóságos, ha az információs rendszer és adat megsértésének bűncselekményét az EBH 2033.I. alatti módon megvalósító elkövető ezért a tevékenységéért az érintett hallgatóktól előnyt kér, továbbá a számítástechnikai rendszerben valótlanul rögzített adatok közlésével közreműködik abban, hogy a valóságban le nem tett vizsgáról valótlan adat kerüljön a leckekönyvbe.[184]

Ha a pénzintézet ügyintézője az ügyfelek által a pénzintézetnél lekötött vagy lekötni kívánt pénzösszegeket a sajátjaként kezeli és a sikkasztás leplezése érdekében az információs rendszerben e betétekre vonatkozó adatokat jogosulatlanul megváltoztatja, akkor a sikkasztással (Btk. 372. §) halmazatban a Btk. 423. § (1) bekezdés b) pont szerint minősülő és büntetendő információs rendszer és adat elleni bűntett megállapításának van helye. Az elkövető cselekménye két, egymástól független védett jogi tárgyat sért, és a két bűncselekmény nem kapcsolódik szükségszerűen egymáshoz. Mindkét bűncselekmény egyaránt elkövethető a másik nélkül. Ez irányadó lehet más bűncselekmények (pl. csalás) mellett megvalósult információs rendszer és adat elleni bűncselekmény halmazatának a megítélése körében is.[185]

Másik uniós ország kiberbűncselekményekkel kapcsolatos büntetőjogi szabályozását is indokoltnak tartom példaként bemutatni, ezért a német StGb. rendelkezéseire is kitérek az egyes részeknél. A StGb. 303b. §-ában a számítógépes szabotázsként szankcionálja a DDoS-támadást, illetve a rosszindulatú program alkalmazásával indított támadást, valamint adatmanipulációt kimerítő magatartásokat. E szerint, aki más számára fontos adatfeldolgozó rendszer működését akadályozza az adat törlésével, elrejtésével, módosításával, hozzáférhetetlenné tételével vagy adatbevitellel, vagy továbbításával azért, hogy másnak ezzel kárt okozzon, akkor ezért három évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntetendő. Amennyiben más üzleti vállalkozásának, vállalatának vagy közműnek az adatfeldolgozó rendszerével szemben követi el, akkor a büntetés öt évig terjedő szabadságvesztéssel is sújtható. Abban az esetben, ha az elkövető ezáltal jelentős pénzügyi veszteséget okoz vagy üzletszerűen követi el vagy olyan csoport tagjaként, amelynek a célja, hogy rendszeresen számítógépes szabotázst kövessenek el, vagy a támadás kritikus

[183] Legfelsőbb Bíróság Bfv. II. 74/2008/5.
[184] EBH 2009.2033. II.; BH 2009.264. II.
[185] Szegedi Ítélőtábla Bf. I. 180/2006/3.

infrastruktúrát érint, akkor hat hónaptól kezdve tíz évig terjedő szabadságvesztés is kiszabható vele szemben. A törvény e bűncselekmény kísérletét is büntetni rendeli.[186]

Az információs rendszerben végzett műveletekkel a jogtalan haszonszerzés célzata nélkül is jelentős kárt lehet okozni, ezért úgy gondolom, hogy – mind az amerikai, mind a német szabályozásra is figyelemmel – indokolt lenne egy külön fordulatba iktatni ezt az információs rendszer vagy adat megsértése bűncselekményének deliktumába is, amennyiben az elkövető a tényállásszerű magatartásának eredményeképpen kárt okoz.

Az informatikai környezetben elkövetett bűncselekmények esetén azt a fontos jogalkotási megfontolást is figyelembe kell venni, hogy ne kerüljön sor a tényállások duplikálására, hiszen szűkül azon bűncselekmények köre, amelyeket az információs rendszerek segítségével ne lehetne elkövetni. Például a közlekedés biztonsága elleni bűncselekményt a közlekedési lámpákat vezérlő információs rendszerbe történő illetéktelen beavatkozással, vagy – extrém példát említve – emberölést az intenzív osztály számítógépeinek manipulálásával is el lehet követni.[187] További példaként említhető, azaz eset, amikor az elkövető akár egy önvezető járművet is az elkövetés eszközeként használhat, amennyiben a hackertámadás során az önvezető járművet arra programozza be, hogy a sértettet megölje (pl. nagy sebességgel falnak vezeti a járművet), akkor e magatartása büntetőjogi értelemben vett cselekménynek tekinthető ugyanúgy, mintha egy lőfegyverrel vagy szúró-vágó eszközzel próbálna meg végezni vele.[188] Emellett az élet kioltására alkalmasak lehetnek a hadászati céllal kifejlesztett drónok is, amelyek már arcfelismerő szoftverrel rendelkeznek, így könnyedén beprogramozhatók arra, hogy a kiválasztott személyt megöljék. Az IoT eszközök is különböző jogsértő cselekményekhez szolgálhatnak eszközül vagy éppen annak tárgyául is, mert általuk könnyedén lehet szenzitív adatokat gyűjteni a felhasználókról. Gondoljunk egy okosotthonra, amelyet ugyanúgy érhet támadás mint bármely más informatikai eszközt, és ennek következében az elkövető áttudja venni az irányítást felette és különböző parancsokat továbbíthat, ezáltal alkalmas lehet a sértett megfigyelésére vagy akár az otthonába történő be vagy onnan a kizárására.[189] Az autólopás is új szintre lépett a technológiai újításoknak köszönhetően, mert

[186] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019.
[187] NAGY Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: Homoki-Nagy Mária - Karsai Krisztina - Fantoly Zsanett - Juhász Zsuzsanna - Szomora Zsolt - Gál Andor (szerk.): Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Szeged, 2018. 755. o.
[188] AMBRUS István: Az autonóm járművek és a büntetőjogi felelősségre vonás akadályai. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019. 10-11.o.
[189] SCHJOLBERG, Stein: The history of cybercrime 1976-2014. Cybercrime Research Institute, 2014. 148-149. o.

már az sem példa nélküli, hogy nagy értékű autókat lopnak el úgy, hogy a kulcs nélküli indítórendszerüknek a védelmét jeltovábbító eszközökkel kijátsszák.[190]

Vadász Viktor álláspontjával egyetértek, hogy megfontolandó az, amennyiben az adott bűncselekmény elkövetésekor az információs rendszer mint elkövetési eszköz kerül alkalmazásra, akkor ez jelentős mértékben növeli az ilyen jellegű cselekmények társadalomra veszélyességét, ezért indokolt lenne a jogalkotó részéről, hogy ezt az egyes bűncselekmények (pl. csalás, zsarolás esetén) minősített eseteként külön szabályozza.[191]

4.5. A számítógép vagy információ megsértése (Damaging a computer or information) a CFAA-ban

A CFAA 1030. § (a)(5) szakasza szerint vétség miatt büntetendő az (A) bekezdés szerint, „aki tudatosan továbbít programot, információt, kódot vagy parancsot, és ezzel szándékosan, jogosulatlanul kárt okoz a védett számítógépben;

A (B) bekezdés értelmében, aki szándékosan, jogosulatlanul hozzáfér a védett számítógéphez és gondatlanságból kárt okoz; valamint

A (C) bekezdés alapján, aki szándékosan, jogosulatlanul hozzáfér a védett számítógéphez és ezzel kárt és veszteséget okoz."

Amennyiben az (A) és (B) bekezdésben szabályozott bűncselekményeket úgy követi el, hogy az alábbi minősített esetek közül legalább egyet megvalósít, akkor bűntett miatt büntetendő a 1030. § (c)(4)(A)(i) (I)-(VI) alapján, aki:

(1) „legalább 5,000 $ értékű veszteséget okoz egy év alatt;
(2) az egészségügyi ellátást akadályozza;
(3) fizikai sérülést okoz;
(4) fenyegetést jelentsen a közegészségre vagy közbiztonságra nézve;
(5) az igazságszolgáltatásban, a honvédelemben, a nemzetbiztonságban használt számítógépet érint;
(6) a károkozás tíz vagy több védett számítógépet érint egy év alatt."

A három bekezdés között a törvény az elkövetési magatartás és az ehheu, valamint az eredményhez kapcsolódó bűnösségi forma alapján differenciál. Az (A) bekezdés megtiltja, hogy bárki tudatos (knowingly) továbbítással és szándékosan (intentionally) kárt okozzon a védett számítógépben, míg a (B) és (C) bekezdés esetében közös, hogy a felelősségre vonáshoz

[190] https://www.dailymail.co.uk/news/fb-5472209/How-thieves-steal-car-without-keys-The.html [2019.01.21.]
[191] VADÁSZ Viktor: A számítógép demisztifikálása. Ügyészek Lapja 2010/2. 16. o.

szükséges feltétel, hogy az elkövető szándékosan férjen hozzá, azonban a (B) bekezdés esetén gondatlanságból (recklessly) okozzon kárt. A (C) bekezdés szerint pedig károkozáson kívül további feltétel, hogy veszteséget is okozzon, ami érdekesség, hogy az Igazságügyi Minisztérium kézikönyve szerint ebben az esetben az eredménynek hanyagságból (negligently) kell megvalósulnia, míg Kerr szerint e fordulatból hiányzik a bűnösségi elem, vagyis a srict felelősség érvényesül.[192] A (B) és (C) esetekben tehát, a szándékos és jogosulatlan hozzáférés a feltétel, amely alapján felelősségre vonható az elkövető, akkor is, ha nem terjedt ki a szándéka a károkozásra. Ezzel ellentétben az (A) bekezdésben szabályozott esetben csak a tudatos továbbítás és a szándékos károkozás mint eredmény a feltétele a bűncselekmény megvalósulásának, ami történhet a számítógéphez való hozzáférése nélkül is, például amikor a támadó eláraszt egy weboldalt nagy mennyiségű adatcsomaggal egy DDoS-támadás révén, amelynek eredményeképpen a honlap hozzáférhetetlen lesz, akkor a károkozás szándékos, azonban az elkövető a támadás során nem fér hozzá a számítógéphez. A 1030. § (a)(5)(A) bekezdés szerint felelősségre vonható az, aki a DDoS-támadást végrehajtja, illetve az is, aki a rosszindulatú programot e célból felhasználja vagy továbbítja. Ez következik abból, hogy a DDoS-támadás általában magában foglalja a káros kód továbbítását is, amellyel a számítógépeket zombigépekké változtatja és azon kód továbbítását, amit arra használ fel az elkövető, hogy az irányítása alá vont zombik számára kiadja a parancsot a támadásra a meghatározott célponttal szemben.[193] A bűncselekmény elkövetési tárgya a védett számítógép, amelynek fogalmát korábban már ismertettem.

A 1030. § (a)(5)(A) bekezdés megállapításához kettő feltétel együttes teljesülése szükséges: a továbbításnak a megvalósulása, illetve a kár bekövetkezte. Ez a tényállás a tudatos, károkozási célzatú informatikai támadás végrehajtását szankcionálja. A törvény szövegben szereplő „program, információ, kód vagy parancs” továbbítása tág értelemben magában foglalja azokat az eseteket, amikor a továbbítás képes a számítógép működését befolyásolni. Ilyenek lehetnek a program kódok (pl. számítógépes férgek vagy vírusok), parancsok (pl. információ törlésére irányuló), és a hálózati adatcsomagok, amelyek elárasztják a hálózatot vagy a rendszer sebezhetőségeit használják ki, mint például a DDoS-támadások.

Az eljárás során a következők bizonyítása szükséges: a terhelt és a továbbításért felelős személy megegyezik, valamint a továbbítás tényét is, amelyhez elegendő a közvetett bizonyíték megléte. Továbbításnak minősül például a rosszindulatú programnak a telepítése is. Az elkövetőnek nem kell közvetlenül a sértett számítógépe felé a továbbítást végeznie ahhoz, hogy

[192] KERR (2018): i.m. 114. o.
[193] BRENNER (2012): i.m. 49. o.; valamint U.S. DEPARTMENT OF JUSTICE (2015): i.m. 36-37. o.

megsértse ezt a rendelkezést például az egyik konkrét esetben az elkövető káros kódot helyezett el egy programba, ami a munkáltatója rendszerében futott és egy idő után aktiválta magát, és ennek következtében további káros kódokat töltött le, és a többi alkalmazott által használt gépet is használhatatlanná tette.

A következő feltétel, hogy az elkövető kárt okozzon a számítógépben, ami magában foglalja az információ vagy számítógép hozzáférhetetlenné tételét. A kár fogalma a 1030. § (e)(8) pont szerint a következő: „bármely olyan károsodás, amely az adat, program, rendszer vagy információ hozzáférhetőségét vagy integritását sérti". Kár akkor is keletkezik, amikor az adott cselekmény a szolgáltatónál lassulást vagy csökkentett kapacitást eredményez. A túlterheléses támadásnál pedig elsősorban erről van szó, mert a szerver vagy weboldal – és ennek következtében a rajta található információ is – elérhetetlenné válik és ezáltal a sértettnél kár realizálódik. Károkozás következik be akkor is, ha a magatartás sérti az adat, program, rendszer vagy információ integritását például az adatot vagy információt törlik, módosítják, vagy éppen titkosítják (pl. rendszerbe betörnek és hozzáférnek a naplófájlokhoz vagy a bank adatbázisában módosítanak az egyenlegen). Ugyanúgy kár keletkezik, ha a számítógép működését befolyásolják (pl. keylogger telepítése az otthoni számítógépre) vagy az információt, illetve a számítógépet elérhetetlenné teszik. Továbbá az is károkozásnak minősül, ha az elkövető a rendszerbe jogosulatlanul belép és a login fájlokat megváltoztatva kinyeri a rendszerhez tartozó jelszavakat, majd elfedve tevékenységére helyreállítja az eredeti állapotot. Ebben az esetben ugyan az adat fizikailag nem lett megváltoztatva vagy törölve, azonban az integritása sérült ezáltal.[194] Kárként értékelhető ezen kívül az is, ha az elkövető megváltoztatja a biztonsági szoftvert (pl. vírusirtót), aminek következtében az nem észleli a behatolást a rendszerbe.[195]

A veszteség a (C) bekezdésben és az egyik minősített eset körében is előkerül, ezért ennek meghatározásával foglalkozom a következőkben. A CFAA 1030. § (e)(11) pontja tágan definiálja a veszteség fogalmát: „bármely olyan kiadás a sértett részéről, ami magában foglalja a jogsértésre adott válaszokat, kárfelmérést, illetve az adatnak, a programnak, a rendszernek vagy az információnak a jogsértés előtti állapotra történő helyreállításával kapcsolatban felmerült költségeket, és bármely olyan bevétel kiesést, költséget, vagy egyéb károsszeget, amely a szolgáltatás szünetelésével összefüggésben keletkezett". Ez általában azt a pénzösszeget jelenti, amitől elesik a sértett a szolgáltatás szüneteléséből adódóan. Ha a leállás minél hosszabb ideig tart, annál nagyobb veszteség keletkezik. A bíróság azonban a cég jó hírnevét kizárta a veszteségi körből, de például idetartozik azoknak az alkalmazottaknak a

[194] CLOUGH: i.m. 130. o.
[195] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 39. o.

munkadíja és munkabére, akiket a helyreállítással megbíztak, vagy éppen a leállás miatt a munkájukat nem tudják végezni, továbbá a weboldalon elszalasztott hirdetési és értékesítési bevételek is ide tartozhatnak.[196] A Middleton-ügy során a bíróság kimondta, hogy a kár magában foglal bármely olyan veszteséget, amely a terhelt magatartásának az előrelátható következménye (natural and foreseeable result), így azt a költséget is, amely észerűen szükséges a rendszer újbóli biztonságának a helyreállításához például ez érintheti az (elveszett) adatokat, programokat, rendszer beállításokat.[197] Azonban a korábbinál jobb és biztonságosabb rendszer felállításának érdekében tett intézkedések már nem. A sértett, avagy a károsult lehet természetes vagy jogi személy is.[198]

Végül a (A) és (B) bekezdés minősített eseteinek a részletes elemzésével folytatom. Az első esetben a törvény legalább 5,000 $ értékben okozott veszteség bekövetkeztének feltételét határozza meg, valamint az erre vonatkozó időkeretet is, hogy ennek egy év alatt kell történnie. Ennek a részletes elemzésétől azonban eltekintek, mert egyebekben az előző bekezdés vonatkozik rá.

A törvény azokkal a támadásokkal szemben is véd, amelyek akadályozzák „az egy vagy több személynek az orvosi vizsgálatát, diagnózisát, kezelését vagy gondozását". Ennek nem kell jóvátehetetlennek vagy jelentősnek lennie, illetve pénzügyi veszteségnek sem kell bekövetkeznie. Ez a rendelkezés a kórházak, klinikák és más egészségügyi intézmények rendszerei és a bennük tárolt érzékeny adatok számára nyújt védelmet. A megállapításához elegendő, ha az elkövető cselekménye legalább egy betegnek az egészségügyi nyilvántartását potenciálisan érintette.

A harmadik eset akkor valósul meg, ha „a fizikai sérülés bármely személynél következik be". Például a forgalmi jelzőlámpák működésének megzavarásával autóbaleset történik és ennek következtében a gépjárművezetők megsérülnek.

A negyedik minősített esetnél elegendő, ha a közegészség és közbiztonság veszélybe kerül a támadás eredményeképpen, például a forgalmi jelzőlámpák működésének leállása következik be - a közlekedési infrastruktúra elleni támadásnak köszönhetően -, azonban az nem jár fizikai sérüléssel, de az elkövető felelősségre vonható már azért, mert veszélyhelyzetet idézett elő. Ez a rendelkezés elsősorban a kritikus infrastruktúrák[199] elleni támadásokkal szemben lép fel, ugyanis ezeknek a fokozott védelme különösen indokolt.

[196] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 41-43. o.
[197] KERR (2018): i.m. 125. O.
[198] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 42-43. o.
[199] Az Egyesült Államok 1998-ban elnöki irányelvben határozta meg kritikus infrastruktúra fogalmát, amely 2001-ben lépett hatályba a PATRIOT törvénnyel: „mindazon fizikai vagy virtuális rendszerek és berendezések, amelyek

A CFAA kiemelten tiltja az Egyesült Államok kormánya által vagy érdekében használt számítógépekkel szembeni támadásokat, különösen, amelyek, az igazságszolgáltatást, a honvédelemet és a nemzetbiztonságot érintik (pl. a bíróságok, ügyészségek számítógépes rendszere, valamint a katonai és védelmi magánvállalkozások is). A Kongresszus célja ezzel a ponttal az volt, hogy fokozottan védje a kormányzati funkciók, illetve valamennyi kormányzati ág zavartalan működését és a felelősségre vonásra abban az esetben is sor kerüljön, ha a támadás sikertelen, ezért nem szükséges, hogy tényleges kár következzen be.

Végül az utolsó pont a leggyakoribb eset, amely a tíz vagy több védett számítógépben való károkozást határozza meg egy év alatt. Ezt az esetkört a DDoS-támadás könnyen kimeríti, mert minden támadás végrehajtásához általában több fertőzött számítógépre van szükség. Tehát ez a rendelkezés akkor alkalmazható, amikor az elkövetés botnethez köthető vagy egyéb esetben is, ha több számítógép érintett, azonban a károkozás természete miatt nem lehet, vagy nehezen meghatározható az okozott kár mértéke az egyes számítógépek tekintetében, vagy nem bizonyítható, hogy a megállapított veszteség meghaladta a 5,000 $ értéket.[200]

A szankciók pedig a következőképpen alakulnak: aki szándékosan vagy gondatlanságból kárt okoz a védett számítógépben, és ezzel megsérti a 1030. § (a)(5)(A) vagy (B) bekezdését, akkor vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

Amennyiben az elkövető valamelyik minősített esetet a 1030. § (a)(5)(A) pontjába ütköző magatartásával kimeríti, akkor bűntett miatt tíz évig terjedő szabadságvesztéssel és/vagy pénzbüntetéssel, míg a 1030. § (a)(5)(B) pont esetén öt évig terjedő szabadságvesztéssel és/vagy pénzbüntetéssel büntethető. A törvény azonban nem határoz meg a minősített esetekre tekintettel szándékot, ezért elegendő annak bizonyítása, hogy az elkövető magatartása és a bekövetkezett kár vagy veszélyhelyzet között okozati összefüggés áll fenn.

Aki a 1030. § (a)(5)(A) vagy (B) pont megsértésével bűncselekményt követ el és korábban már a 1030. § hatálya alá tartozó más bűncselekmény elkövetéséért is elítélték, akkor ez esetben húsz évig terjedő szabadságvesztés szabható ki, míg a (C) pont megsértése esetén, ha korábban szintén informatikai bűncselekmény elkövetőjeként már felelősségre vonták, akkor ez tíz évig terjedő szabadságvesztést vonhat maga után.

2002-ben a Kongresszus további rendelkezést vezetett be, amennyiben az informatikai támadás következében súlyos fizikai sérülés vagy halál következik be eredményként. Ha az

oly létfontosságúak az Egyesült Államok számára, hogy azok korlátozása vagy megsemmisülése meggyengítő hatással lenne a nemzetbiztonságra és a nemzetgazdaság biztonságára, a közegészségre, közbiztonságra vagy ezek bármely kombinációjára". https://www.selectagents.gov/resources/USApatriotAct.pdf [2017.12.29.]

[200] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 45–47. o.

elkövető a 1030. § (a)(5)(A) pont szerint szándékosan kárt okoz a védett számítógépben és ezáltal tudatosan vagy gondatlanságból súlyos fizikai sérülést okoz, vagy erre kísérletet tesz, akkor húsz évig terjedő szabadságvesztés szabható ki. Végül a bíróság büntetésként életfogytig tartó szabadságvesztést állapíthat meg, ha az elkövető tudatosan vagy gondatlanságból halált okoz, vagy erre kísérletet tesz.[201]

[201] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 47–49. o.

5. A számítógépes csalás

5.1. A számítógépes csalás nemzetközi, uniós és hazai szabályozása

A Budapesti Egyezmény a számítógéppel kapcsolatos bűncselekmények (II. fejezet) körében a számítógépes csalást (8. cikk) szabályozza, előírva a szerződő feleknek, hogy belső jogukkal összhangban bűncselekménynek minősítsék:

a) a másnak jogosulatlanul és szándékosan történő vagyoni károkozást, amelyet számítástechnikai adatok bármilyen bevitelével, megváltoztatásával, törlésével vagy megsemmisítésével,
b) vagy a számítástechnikai rendszer működésébe való bármilyen beavatkozással, anyagi haszon saját vagy más részére történő jogosulatlan megszerzésének céljából követnek el.

A 1978. évi Btk. a számítógépes csalást egyrészt még a számítástechnikai rendszer és adatok elleni bűncselekmény (300/C. §) keretében szabályozták, másrészt a készpénz-helyettesítő fizetési eszközzel visszaélés egyik korábbi alakzatából (313/C. §), és ez tartalmilag megfelelt a nemzetközi elvárásoknak. A Btk.-ban azonban nóvumként jelent meg már külön tényállásként az információs rendszer felhasználásával elkövetett csalás elnevezéssel (Btk. 375. §), a vagyon elleni bűncselekmények között, amelyet a Btk. miniszteri indokolása az eltérő jogtárgy védelemmel magyarázott. E szerint az információs rendszer felhasználásával elkövetett, kárt okozó csalások elsősorban vagyoni érdekeket sértő cselekmények, illetve ezek a csalásszerű magatartások azért kerültek a csalástól eltérő önálló tényállásba, mert hiányzik belőlük a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás. A kárt az információs rendszer jogtalan befolyásolása okozza. Ennélfogva az információs rendszer felhasználásával elkövetett csalás nem speciális bűncselekmény a csaláshoz viszonyítva, hanem egyszerűen egy olyan másik bűncselekmény, amelynek elkövetése esetén a csalás nem is állapítható meg.[203]

Az információs rendszerek sokrétű funkciójából következik, hogy e rendszerek ellen intézett támadások más társadalmi viszonyt is sérthetnek, így ezen bűncselekmények kettő – vagy akár több – jogtárggyal is rendelkezhetnek, mint az információs rendszer felhasználásával elkövetett csalás is ilyen, mert az információs rendszerek integritása, biztonsága mellett a vagyoni viszonyokat is védi.[204]

A hatályos Btk. 375. § (1) bekezdésében szabályozott károkozó adatvisszaélési alakzat szerint, aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt

[203] A Btk. javaslatának 375. §-ához fűzött indokolás
[204] NAGY (2009): i.m. 60. o.

adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. Jelen deliktum elkövetési magatartásai megegyeznek a korábban az információs rendszer vagy adat elleni bűncselekménynél részletesen elemzett cselekményekkel. Azonban különbség, hogy ez már eredmény-bűncselekmény, ezért akkor tényállásszerű, ha az elkövető magatartását jogtalan haszonszerzés céljából fejti ki, amelynek eredményeként kár[205] is bekövetkezik. Nem szükségszerű, hogy a kár az információs rendszer tulajdonosánál vagy rendszergazdájánál következzen be. Gyakori elkövetési magatartás, hogy értékes adatokat törölnek vagy megváltoztatnak annak érdekében, hogy megtévesszenek másokat abból a célból, hogy jogtalan haszonhoz jussanak. Például jellemző, hogy az elkövető pénzügyi rendszerhez fér hozzá és a bankszámla egyenleget vagy hitelkeretet manipulálja. A bíróság az egyik ügyben azért marasztalta az elkövetőt, mert a számítástechnikai rendszerbe vitt be olyan adatokat, amelyek valótlanok voltak, és nem rendelkezett jogosultsággal ehhez. E cselekményét folytatólagosan elkövetve gyakorlatilag egy évtizeden keresztül, havi rendszerességgel valósította meg, kihasználva a bér és munkaügyi előadói munkaköréből adódó lehetőséget. E magatartásával az volt a célja, hogy őt meg nem illető jövedelemhez jusson, azaz cselekményét jogtalan haszonszerzés végett fejtette ki. Az átutalások megtörténte után az adatokat törölte, amit azért tett, hogy a jogtalan haszonszerzés érdekében véghez vitt magatartására ne derüljön fény, így végső soron a törlés célzata is a jogtalan haszonszerzés volt.[206]

Másik döntésében a bíróság kimondta, hogy a pénzintézet internetes felületén végrehajtott olyan pénzügyi műveletek, amelyek a pénzintézettel megkötött NET számlacsomagnak, illetve az internetbanki szerződésben foglaltaknak megfelelnek, a számítógépes rendszer rendeltetésszerű igénybevételét jelentik, ezért az információs rendszer felhasználásával elkövetett csalás különös részi tényállását nem valósítják meg.[207]

Károkozó magatartás lehet még például a különböző kártékony programok bejuttatása a célzott adatbázisba.

A bűncselekmény célzatos, ezért csak egyenes szándékkal követhető el. A bűncselekmény eredménye, a kár bekövetkezése tekintetében azonban elegendő az eshetőleges szándék is. A haszonszerzés mindig jogtalan, ha más megtévesztésével károkozásra irányul. A jogtalan

[205] A Btk. 459. § (1) bekezdésének 16. pontja értelmében: a kár e törvény eltérő rendelkezése hiányában a bűncselekménnyel a vagyonban okozott értékcsökkenés.
[206] Fővárosi Törvényszék B.687/2012/11.
[207] BH 2017.8.252.

haszon megszerzése azonban nem szükséges, már a tényállás körén kívül esik. A cselekmény rendszerint a jogellenes számítógépes manipuláció megkezdésével jut a kísérlet szakaszába, és a kár bekövetkezésével fejeződik be.[208]

Az elkövető bárki lehet, aki a jogosultsággal rendelkezik valamennyi magatartás tanúsítására, azonban ezeket szándékosan nem az engedélyezett cél elérése érdekében, hanem jogtalan haszonszerzés céljából másnak kárt okozva valósítja meg, vagy aki egyáltalán nem rendelkezik jogosultsággal.

A (2)-(4) bekezdés a bűncselekmény súlyosabban minősülő eseteit – a vagyon elleni bűncselekmények szabályozási technikájához hasonlóan – a bekövetkezett kár összegéhez[209] igazodóan határozza meg. A minősítési rendszert a kár összegén kívül még a bűnszövetségben, illetve az üzletszerűen történő elkövetés határozza meg. Az alapeset átfogja mind a kisebb, mind a nagyobb kár bekövetkezését, a minősített esetek a jelentős kártól kezdődnek. A bűncselekmény bármely csekély összegű kár bekövetkezte esetén tényállásszerű, tehát nincs alsóértékhatára. Ennek a tényállásnak szabálysértési alakzata nincs.[210]

Az információs rendszer felhasználásával elkövetett csalás bűntettének szükségszerű eszközcselekménye a Btk. 423. § (2) bekezdésének pontjai szerinti információs rendszer vagy adat megsértésének bűntette, ezért bűnhalmazatot nem képeznek.

A hazai bírósági gyakorlatban már több esetben sor került a számítógépes csalásnak kártékony programok felhasználásával elkövetett eseteivel. Az egyik ügyben a bíróság számítógépes csalás bűntettében mondta ki a terhelt bűnösségét, aki a károsult gazdálkodó szervezet alkalmazásban állt, mint informatikus szakértő és a feladata volt a cég átfogó számítástechnikai rendszerének kidolgozása. A történeti tényállás szerint a munkaköri kötelezettsége alapján több programot is írt a cég részére, amelyek közül kettőbe egy olyan kódsorozatot épített be, ami az aktiválást követően a programokat fizikálisan megsemmisíti, a harmadikba pedig egy olyat, amely egy meghatározott naptári időpont bekövetkezése után a program működését lehetetlenné teszi. Erről munkáltatóját nem tájékoztatta, ezért a gazdálkodó szervezet azonnali hatállyal megszüntette a foglalkoztatását. Ezt követően a terhelt által készített programok részben megsemmisítették önmagukat, részben működésképtelenné váltak,

---

[208] SZOMORA Zsolt: XXXV. A vagyon elleni bűncselekmények. In: Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz. Complex Kiadó. Budapest, 2013. 788. o.

[209] Btk. 459.§ (6) bekezdése alkalmazásában az érték, a kár, valamint a vagyoni hátrány
a) ötvenezer-egy és ötszázezer forint között kisebb,
b) ötszázezer-egy és ötmillió forint között nagyobb,
c) ötmillió-egy és ötvenmillió forint között jelentős,
d) ötvenmillió-egy és ötszázmillió forint között különösen nagy,
e) ötszázmillió forint felett különösen jelentős.

[210] SZOMORA (2013): i.m. 789. o.

ezért a cégnél a termelés irányítása, regisztrálása és az árukiadás egy napra lehetetlenné vált. A számítógépes rendszer újra indításával, kijavításával a társaságnak megközelítőleg 6 millió Ft kára keletkezett. Az elsőfokú ítélet ellen bejelentett fellebbezések alapján a másodfokú bíróság annak ítéletét megváltoztatta akként, hogy a terhelt cselekményét számítógépes csalás bűntettének a Btk. 16. §-a szerinti kísérletének minősítette. Döntését azzal indokolta, hogy a kár fogalmát a Btk. a bűncselekménnyel a vagyonban okozott értékcsökkenésként határozza meg, ezért a gazdálkodó szervezet által a rendszer átprogramozásával összefüggésben a túlórákért kifizetett munkabér kárként nem értékelhető. Tekintettel arra, hogy a vádlott tisztában volt azzal, hogy cselekménye az adatfeldolgozás eredményét megváltoztatja, és belenyugodott abba, hogy magatartásával kárt okozhat, mely kár azonban a rendszer újraindítása miatt nem következett be, ezért a vádlott cselekménye a számítógépes csalás bűntettének kísérleteként értékelhető.[211]

Mindezekre tekintettel az információs rendszer felhasználásával elkövetett csalással okozott kár fogalma több kérdést is felvett. Amennyiben a cselekménnyel összefüggésben ténylegesen bekövetkezik az értékcsökkenés, abban az esetben egyszerűbb a helyzet, hiszen egyértelműen kárként értékelhetők például a tényleges befizetés nélkül jóváírt, vagy az egyik bankszámláról a másikra jogosulatlanul átutalt pénzösszegek. Ellenben problémát jelent, ha a tényállásszerű magatartás kifejtésével összefüggésben kár ténylegesen nem következik be például a kártékony programok által az információs rendszerben okozott működési zavarok elhárításával kapcsolatban felmerült kiadások megítélése – ahogy ez az ismertetett jogesetben is megmutatkozott – vagy a védett adatbázisból megszerzett – avagy "ellopott" – majd később értékesített, bizalmas gazdasági, üzleti információk értékének meghatározása, valamint a bűncselekmény stádiumának a megállapítása.[212]

A Btk. 459. § értelmező rendelkezései szerint a kár fogalma kizárólag az értékcsökkenést, míg a vagyoni hátrány az értékcsökkenést és az elmaradt vagyoni előnyt egyaránt magában foglalja.[213] A büntetőjogi értelemben vett kárfogalomnak, azonban nem része a károsultat ért vagyoni hátrányok kiküszöböléséhez szükséges költségek [Ptk. 6:522. § (2) bekezdés c) pont], amelyek például egy informatikai támadást követően a rendszer helyreállítása érdekében felmerülhetnek. Ez a polgári jog szabályai szerinti kártétel a káreseményt követően azokat a

[211] BH 1999/145.
[212] LACZI Beáta: A számítógép és a büntetőjog. Magyar Jog 2001/3. 137-152. o.
[213] Deák Zoltán megítélése szerint pedig felesleges és elvi alapon sem igazolható a kár büntetőjogi fogalmából az elmaradt haszonnak a kirekesztése, valamint az is, hogy a Btk. az egyes bűncselekményeknél a társadalomra veszélyesség fokmérőjének tekinti a tényleges vagyoncsökkenést, míg más büntetendő magatartásoknál az elmaradt vagyoni hasznot. Lásd DEÁK Zoltán: A kár büntetőjogi fogalmáról - megjegyzések egy eseti döntés margójára. Magyar Jog 2012/6. 371. o.

kiadásokat tartalmazza, amelyeket a károsult saját elhatározásából eszközöl abból a célból, hogy a vagyoni hátrány növekedését elkerülje vagy csökkentse.[214]

Hollán Miklós szerint az információs rendszer felhasználásával elkövetett csalás – és a hagyományos csalás – tényállásánál is büntetőjogi jelentőséget az elmaradt haszonnak kell tulajdonítani, és ezért ezek nem a kár, hanem a vagyoni hátrány fogalmán alapulnának. Továbbá felhívja a figyelmet arra is, hogy az információs rendszer felhasználásával elkövetett csalásra is alkalmazni kellene a csalás tényállásához fűzött értelmező rendelkezést, amelynek értelmében kárnak kell tekinteni az igénybe vett szolgáltatás meg nem fizetett ellenértékét is. Ez azzal magyarázható, hogy lehetnek olyan esetek, amikor az illető a vagyonban okozott értékcsökkenés hiánya miatt nem felel ezen deliktumért. A hatályos szabályozás lényegében eltérő védelmet biztosít, hogy a cselekmény információs rendszerrel végzett műveletekkel vagy természetes személy megtévesztésével valósul meg. Ez pedig nem összeegyeztethető a Btk. javaslatának indokolása szerinti szándékkal, amely a két bűncselekmény közötti különbséget az elkövetési magatartásban és nem az eredményben ragadja meg.[215]

A gyakorlatban még felmerülhet az is, hogy az információs rendszer felhasználásával elkövetett csalás és a hagyományos, a Btk. 373. §-ba ütköző csalás vagy más bűncselekmény (lásd előző részben ismertetett pénzintézeti alkalmazott által elkövetett sikkasztás esetét) elhatárolásának kérdése. Az elhatárolás alapját az jelenti, hogy az információs rendszer az elkövetésnek, vagy a leplezésnek az eszköze volt-e. A kérdés, hogy az elkövető csak felhasználta-e az információs rendszerben rejlő lehetőséget és úgy követte el a bűncselekményt, hogy azt annak segítségével kívánta eltitkolni, vagy már a bűncselekmény elkövetése érdekében manipulálta az adatokat.[216] Egyetértek azzal az állásponttal, mely szerint, ha az elkövető az információs rendszer üzembentartójának okozott kárt adatmanipulációval kívánta eltüntetni, akkor nem jogtalan haszonszerzés végett tanúsította az elkövetési magatartást, hanem annak leplezése céljából. Azonban, ha a jogtalan haszonnak a megszerzéséért szükséges jogcímet is informatikai művelettel teremti meg az elkövető (pl. valótlan adatokat visz be a rendszerbe) és ezzel kárt okoz, akkor már az információs rendszer felhasználásával elkövetett csalás állapítható meg.[217]

[214] KEMENES István: A kárfogalom a polgári jogi és a büntetőjogi kapcsolódási pontjai. Magyar Jog 2018/9. 487. o.
[215] HOLLÁN Miklós: A szolgáltatások megfizetés szándéka nélküli igénybevétele és a büntetőjog – Dogmatikai és jogpolitikai vizsgálódás egy empirikus kutatás hajnalán. Magyar Jog 2019/4. 207-208. o.
[216] SZATHMÁRY (2012): i.m. 93. o.
[217] SZABÓ (2008): i.m. 615. o.

Ezen kívül a közönséges és az információs rendszer felhasználásával elkövetett csalás büntetési tétele közötti különbség is tetten érhető, míg előbbi alapesetét vétségként, két évig, addig utóbbi alaptényállását már bűntettként, három évig terjedő szabadságvesztéssel fenyegeti a kódex.[218] Ezt a Btk. javaslat indokolása azzal magyarázza, hogy a törvény az információs rendszer vagy adat megsértését két évig terjedő szabadságvesztéssel fenyegeti. „Ez utóbbi szükségszerű eszközcselekménye az információs rendszer felhasználásával elkövetett csalásnak, így indokolt, hogy a csalási cselekményektől eltérően az alapesetben ennél súlyosabb, három évig terjedő szabadságvesztéssel fenyegetett legyen."

A német StGb. 202b. §-ban szabályozott phishing elnevezésű tényállás szerint öt évig terjedő szabadságvesztéssel büntetendő, aki technikai eszközök révén jogosulatlanul, nem nyilvános adatfeldolgozó rendszerből szerez meg adatokat. Amennyiben az adatot felhasználja jogtalan előny szerzés céljából – és ezáltal kárt okozzon – akkor a 263a. §-ában szabályozott számítógépes csalás miatt vonható felelősségre és öt évig terjedő szabadságvesztéssel rendeli büntetni.[219]

5.2. A számítógépes csalás (Accessing to defraud and obtain value) a CFAA-ban

A CFAA 1030. § (a)(4) bekezdése szerint büntetendő, „aki tudatosan, jogosulatlanul vagy jogosultságának kereteit túllépve, csalás szándékával (intent to defraud) hozzáfér a védett számítógéphez, és a számítógép felhasználásával csalást követ el azért, hogy értékkel bíró dolgot (anything of value) megszerezzen, vagy ha a csalás tárgyát a számítógép használata jelenti, akkor a használat értékének meg kell haladnia az 5,000 $-t egy év alatt."

A számítógépes csalás egy hibrid tényállás a jogosulatlan hozzáférés és a csalás között. A bűncselekmény célzatos, mert az elkövetőnek már a csalás szándékával kell a számítógéphez hozzáférnie, erre utal az „intent to defraud" és ezt a számítógépet használja fel arra, hogy csalást elkövessen és ezáltal értékkel rendelkező dolgot megszerezzen.

Például az elkövető egy nyilvántartásban elérhető információt módosít vagy töröl, ezt követően pedig vagyoni előnyben részesül attól, aki a nyilvántartás helyességében bízott. Az egyik esetben a terhelt a hitelinformációs ügynökség nyilvántartásához fért hozzá és a hitel értékelését számára kedvezőbb értékre módosította. Továbbá az elkövető megszerezhet olyan értékkel bíró információt, adatot, amelyet később csalásra használ fel. Például az egyik ügyben a terhelt a telefontársaság számítógépéhez fért hozzá és szerzett meg olyan kártyaszámokat,

[218] KONDOROSI András: Az információs rendszer felhasználásával elkövetett csalás. Infokommunikáció és jog 2014/2. 74. o.
[219] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019.

amelyekkel ingyen tudott nemzetközi hívásokat indítani. Másik esetben például a terhelt arra használta a számítógépet, hogy hamis, hamisított dokumentumokat állítson ki, amit később csalásra használt fel, így a lottó terminált használta fel arra, hogy visszadátumozott szelvényeket állítson ki a nyerő számokkal és utána átvette ezért a nyereményt.

A tényállásszerűséghez az elkövetőnek valamilyen értékkel bíró dolgot (pl. pénz, áru vagy szolgáltatás stb.) kell megszereznie, ami például lehet számítógépes adat és információ is, azonban ennek az elkövető számára értékesnek kell lennie a csalás megvalósításának szempontjából. Például a Czubisnki-ügy során az elkövető az adóhatóság egyik osztályán dolgozott és hozzáféréssel rendelkezett ahhoz a számítógépes rendszerhez, amely az adófizetőkkel kapcsolatos információkat tárolta. Ebben az adatbázisban a jogosultságainak kereteit túllépve több alkalommal keresést futatott le, annak ellenére, hogy tudta, hogy nem hivatali ügyben nem férhetne ehhez hozzá. Azonban az eljárás során nem nyert bizonyítást az, hogy bármilyen értékkel rendelkező dolgot megszerzett volna (pl. kinyomtatta, felhasználta vagy nyilvánosságra hozta volna) és az információ megtekintése puszta kíváncsiságból nem meríti ki a számítógépes csalás tényállását, hanem a 1030. § (a)(2) bekezdése alapján vonható ezért felelősségre.

Érdemes megemlíteni, hogy abban az időben, amikor a törvény megalkotására sor került, megszokott volt, hogy az ún. szuperszámítógépek használatát a tulajdonosuk bérbe adta, mert akkoriban kevés számítógép állt rendelkezésre, ezért értékelte úgy a jogalkotó, hogy a számítógép használata is gazdasági értékkel bír. A hatályos CFAA-ban is ez a fordulat még maradt, azonban manapság ez már idejét múltnak tekinthető.

A 1030. § (a)(4) bekezdésének a megsértése pénzbüntetést és/vagy öt évig terjedő szabadságvesztést vonhat maga után, ha az elkövetőt korábban már elítélték informatikai bűncselekményért, akkor tíz évig terjedő szabadságvesztést állapíthat meg a bíróság.[220]

[220] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 26-34. o.

5.3. A személyes adatok büntetőjogi védelme

A 2013-as irányelv először hívja fel a figyelmet arra, hogy a számítástechnikai bűnözésre alkalmazott integrált megközelítés egy másik fontos eleme a személyazonosság-lopás és a személyazonossághoz kapcsolódó egyéb bűncselekmények elleni hatékony fellépés. Ez különösen indokolt, mert a felhasználók sokszor nincsenek tisztában az online jelenléttel járó veszélyekre, a megosztott információkkal és képekkel járó fenyegetésekkel. Ennek eredményeképpen a szenzitív adatokat az erre illetéktelen személyek már egyre könnyebben tudják megszerezni (pl. erre a célra kifejlesztett malware, spam, phishing és hacking módszerek segítségével).[222]

Bert-Jaap Koops és Ronald Leenes tettek kísérletet a témakör szempontjából releváns fogalmak meghatározására és ezek egymástól való elhatárolására. Az álláspontjuk szerint a gyűjtőfogalomnak a személyazonossághoz kapcsolódó bűncselekmények (identity-related crimes) tekinthetők. Ezen büntetendő magatartásoknak az elkövetési tárgya vagy eszköze a személyazonossághoz köthető. 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.[223] Utóbbinak a definícióját hasonlóan határozzák meg szövetségi törvény szintjén az Egyesült Államokban is: „a személyazonosság-lopás fogalma alatt olyan csalást értünk, amely esetén más személynek a személyazonosító információját engedély nélkül használják fel, vagy erre kísérletet tesznek."[224]

A személyazonosság-lopás különösen azért veszélyes, mert általában az elkövető megszerzi valakinek az adatait és mások előtt ennek a személynek adja ki magát, majd olyan magatartást tanúsít, amelynek negatív következményei a sértettnél realizálódnak.[225]

Ugyanakkor a személyazonosság-lopást általában nem önálló deliktumként kezelik, hanem ezt az elnevezést is a különböző büntetendő magatartások körének a gyűjtőfogalmaként használják.[226] Az egyes országok büntető törvénykönyveiben jellemzően az alábbi

[222] OECD Policy Guidance on Online Identity Theft, 2008. 3. o.
[223] KOOPS, Bert-Jaap – LEENES, Ronald: ID Theft, ID Fraud and/or ID-related Crime. Definitions matter. Datenschutz und Datensickerheit 2006 (9), 556. o.
[224] 15 U.S.C. 1681a. § (q)(3)
[225] KORINEK László: Tendenciák korunk bűnözésében, bűnüldözésében. MTA székfoglaló előadás, 2013. 44. o.
[226] 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.

magatartásokat rendelik büntetni: a másnak a személyazonosságával összefüggő információinak a jogosulatlan megszerzését, valamint az ezekkel való kereskedést, vagy a személyazonosságra vonatkozó hamis információk létrehozását, illetve ennek elősegítését.[227]

Fontos vizsgálni továbbá a teljesség igénye nélkül, csak példálózó jelleggel, hogy a szakirodalom szerint mely információk alkalmasak az adott személy azonosítására: vannak azok, 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), valamint azok is idetartoznak, amelyek különböző életeseményünkhöz köthetők, példaként említhetők a végzettségek, munkahelyek, házasságkötés, vezetői engedély, személyazonosító igazolvány, társadalombiztosítási azonosító jel, bankkártya és bankszámla adatok (biographical identity), végül az általunk választottak is, így a felhasználónevek, jelszavak és egyebek is (chosen identity).[228]

Az Európai Unióban, a 2019. május 25-étől alkalmazandó, Általános Adatvédelmi Rendelet (a továbbiakban: GDPR)[229] 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 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."[230] Ezt a fogalommeghatározást emelték be a hazai információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.). értelmező rendelkezéseibe is.[231]

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

[227] CLOUGH: i.m. 241. o.
[228] KOOPS, Bert-Jaap – LEENES, Ronald – MEINTS, Martin – VAN DER MEULEN, Nicole – JAQUET-CHIFFELLE, David-Olivier: A typology of identity-related crime. Conceptual, technical and legal issues. Information, Communication & Society Volume 12. No. 1. February 2009, 3-4. o.
[229] 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.
[230] 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 egy exempflikatív jellegű felsorolást alkalmaz, amely például érinti az elektronikus és telekommunikációs azonosításra szolgáló információkat is.
[231] Infotv. 3. § 1-3. pont

visszaélést és az egyéb csalás-jellegű magatartásokat is szankcióval fenyegeti a törvény.[235] A német büntető törvénykönyv is hasonló módon más tényállásokon belül szabályozzam így a már tárgyalt phishing (StGb. 202b. §), valamint számítógépes csalás (StGb. 263a. §), illetve a hagyományos csalás keretében (StGb. 263. §).[236] Ellenpéldaként említhető az amerikai szabályozás, amely már külön nevesíti a személyazonosság-lopást (identity theft).[237]

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 fogalmaknak a 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.[238] 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[239], 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 bűncselekménynek az elkövetési tárgya maga a személyes adat, míg az adat által azonosított vagy azonosítható természetes személy a bűncselekmény sértettjének tekinthető.[240]

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

---

[235] KORINEK (2013): i.m. 44. o.
[236] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019.
[237] 18 U.S.C. 1028. § (a)(7) bekezdése értelmében személyazonosság-lopást valósít meg, „aki tudatosan, jogosulatlanul, másnak a személyazonosságát igazoló azonosítót átad, birtokol vagy használ, azzal a szándékkal, hogy olyan jogtalan cselekményt kövessen el, vagy az elkövetéséhez segítséget nyújtson, illetve az elkövetésére felbujtson, amely a szövetségi jogot sérti, vagy az alkalmazandó tagállami vagy a helyi jog szerint bűntettnek minősül." Például a személyazonosság-lopást valósították meg a United States vs. Christian-ügyben, amikor a két terhelt magas beosztású katonatisztek nevét és társadalombiztosítási azonosítószámát szerezte meg egy nyilvános oldalról. Ezután egy vezető számítástechnikai cégtől hitelt, míg két pénzintézettől hitelkártyát igényeltek a sértettek nevében. Hasonló eset történt a United States vs. Wahl-ügy esetében, amely során a sértettek születési idejét és társadalombiztosítási azonosítószámait szerezték meg, majd autóvásárlásra kölcsönt vettek fel a nevükben, és a befolyt összegből saját vállalkozásukat finanszírozták. Lásd SZABÓ Imre: Internetes bűncselekmények, különös tekintettel az internetes csalásra. ELTE ÁJK, 2002. 18. o.
[238] HOLLÁN Miklós: A nemzeti büntetőjog kerettényállásai és az uniós jog. Miskolci Jogi Szemle 2018/2. 19-20 o.
[239] 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. HVG-Orac Lap- és Könyvkiadó Kft. Budapest, 2018. 271. o.
[240] 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. Complex, Budapest, 2013. 459. o.

okozásával vagy haszonszerzési célból követik el.[241] 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.[242] A jelentős érdeksérelem objektív jellegű fogalom, vagyis a passzív alany szubjektív értékítéletének nincs jelentősége az eredmény megállapításának szempontjából. A 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)[243], de anyagi jellegű vonzata is lehet.[244]

A Kúria elvi éllel mondta ki, hogy a jelentős érdeksérelem okozásával elkövetett személyes adattal visszaélés elkövetője nem csak az adatvédelmi jogszabályok fogalom meghatározásának megfelelő adatkezelő,[245] hanem bárki lehet.[246]

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 pedig 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.[247]

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 jelen van a használatukkor. Ha ezekhez a tárgyakhoz köthető

---

[241] 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.
[242] 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. ELTE-ÁJK, Budapest, 2017.
[243] BELOVICS: i.m. 273. o.
[244] HORVÁTH Tibor – KERESZTI Béla – MARÁZ Vilmosné – NAGY Ferenc - VIDA Mihály: A magyar büntetőjog különös része. Korona Kiadó. Budapest, 1999. 135. o.
[245] 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."
[246] 1/2012. számú BJE határozat
[247] PÉTERFALVI – ESZTERI: i.m. 411. o.

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 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 egy részletes személyiségprofil is alkotható.[249]

A személyes adattal való visszaélés tényállásával kapcsolatban egyes szerzők kritikaként fogalmazták meg, hogy nem nyújt megfelelő védelmet például a kiskorúak számára, a tömeges, valamint az érintett teljes személyiségét érintő profilozással szemben, és végül az ún. deepfake-jelenség esetén.[250]

A személyes adattal visszaélés bűncselekmény minősített esete valósul meg, ha az elkövetési tárgy különleges adat vagy bűnügyi személyes adat[251], valamint a másik esetkör valósul meg, amennyiben hivatalos személyként vagy közmegbízatás felhasználásával követik el.

A személyes adat mint elkövetési tárgy, azonban nem csak a személyes adattal való visszaélés során, hanem más bűncselekményekkel kapcsolatban is előfordulhat, így jellemzően a hivatali visszaélés (Btk. 305. §) és a tiltott adatszerzés (Btk. 422. §) esetén.

A joggyakorlatban a személyes adattal visszaélés és a hivatali visszaélés elhatárolásának kérdése a hivatalos személyek által hozzáférhető adatbázisokból harmadik személynek történő jogosulatlan adatszolgáltatásban nyilvánul meg a legtöbbször. Például a Kúria által elbírált konkrét ügyben a terhelt adóellenőrként gyakorolt közhatalmi jogosítványokat. A terhelt a célhoz kötöttség követelményét sértő módon, nem hivatali ügyben, hanem személyes ismeretség okán belépett és bent maradt a Nemzeti Adó- és Vámhivatal különböző adatbázisaiban, annak ellenére, hogy azok törvényes úton is hozzáférhetők. A Kúria megállapította, hogy a személyes szívességtétel okán az információs rendszerbe belépési jogosultság kereteinek túllépésével való belépés vagy bennmaradás – és az ezúton történő

[249] SZABÓ Endre Győző: II. Fejezet: Adatvédelem és technológia. KLEIN Tamás – TÓTH András (szerk.): Technológia jog, robotjog, cyberjog. Wolters Kluwer. Budapest, 2018. 33. o.

[250] A „deepfake" elkövetési forma esetében algoritmus segítségével képesek az adott személyről készült videófelvételben az arckép kicserélését egy másik személy arcképére, amely bárki számára megtévesztő lehet. Lásd MISKOLCZI Barna – SZATHMÁRY Zoltán: Büntetőjogi kérdések az információk korában. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2019. 140-141. o.

[251] 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 érdek-képviseleti 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."

adatszerzés – a hivatalos személy részéről hivatali visszaélést valósít meg, ha annak célja jogtalan előnyszerzés vagy hátrányokozás. Ez a bűncselekmény valósul meg akkor is, ha az adat jogosultsági feltételekhez kötötten bárki által megismerhető. Amennyiben a hivatalos személy személyes adattal visszaélésben megnyilvánuló jogtalan előnyszerzési vagy hátrányokozási célú magatartása egyszersmind haszonszerzésre is irányul – a specialitás elve alapján – e magatartásával a személyes adattal visszaélés bűncselekményét valósítja meg, méghozzá annak a Btk. 219. § (4) bekezdésében szabályozott minősített esetét.[252]

Összeségében elvi éllel rögzíthető, hogy a személyes adattal visszaélés bűncselekménye a haszonszerzés vagy a jelentős érdeksérelem megléte esetén, míg a hivatali visszaélés bűntette a hivatalos személy által a jogtalan adatkezeléssel szerzett jogtalan előny vagy okozott jogtalan hátrány esetén állapítható meg. A haszonszerzés célzata nélkül a rendőrség informatikai rendszeréből jogosulatlanul lekérdezett adatok más részére történő továbbadása nem a hivatali visszaélés bűntettét, hanem az információs rendszer megsértésének vétségét valósítja meg.[253]

Az elmúlt években pár nagyobb „adatlopás" ügy történt, amelyek között példaként említhető a Yahoo esete, mert az elkövetőknek már két alkalommal sikerült megszerezniük a vállalat felhasználóinak az adatait (felhasználóneveket, jelszavakat) célzott támadások következtében, amelyeket nyilvánosságra is hoztak. Ez az incidens 2013-ban egy milliárd, míg 2014-ben ezt félmilliárd felhasználót érintett.[254] 2018-ban pedig a Cambridge Analytica botrány felelősei a Facebook 87 millió felhasználójának adataival élhettek vissza, ebből 2,7 millió uniós állampolgár volt érintett.

A büntetőjogi rendelkezéseken kívül fontosnak tartom, hogy említést tegyek a személyes adatok védelmével kapcsolatban a GDPR-ról is, amely az adatbiztonság javítását segíti elő, azáltal, hogy egységes és egyértelmű adatvédelmi szabályokat nyújt az Unió egész területén.

A GDPR – uniós rendelet révén – közvetlenül és ágazatoktól függetlenül, széles körben alkalmazandó, míg a korábban már vizsgált NIS irányelvet át kell ültetniük a tagállamoknak a belső jogukba és csak meghatározott ágazatokra vonatkozik. Előbbi kizárólag a személyes adatok védelmét célozza és a szolgáltatók (adatkezelők) mellett az érintetteknek is jelentős szerepet biztosít, míg utóbbi a hálózatokra, infrastruktúrára koncentrál, így a szolgáltatókat célozza elsősorban a szabályozás. Mindkettő érinti az Unión kívül letelepedett, de az EU területére szolgáltatást nyújtó szolgáltatókat is. Magyarországon GDPR által nyitva hagyott egyes területek szabályozását az Infotv. átfogóan módosított változata biztosítja.

[252] BH 2015.11.296.
[253] Kúria Bfv. I. 1.357/2014/11.
[254] https://www.bbc.com/news/technology-47044652 [2019.03.05.]

A rendelet előírja, hogy személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Éppen ezért a GDPR bevezette az ún. „adatvédelmi incidens" fogalmát, amely lényegét tekintve a személyes adatok integritásának és bizalmas jellegének a sérülését jelenti. A pontos meghatározása pedig a következő: „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi." A tág definíció alapján tehát nagyon sokféle adatvédelmi incidens előfordulhat, ide tartozhat például egy személyes adatokat is tartalmazó laptop elvesztése, egy informatikai rendszer megtámadása, de akár egy rossz helyre küldött levél vagy e-mail is e körbe tartozik. Az adatvédelmi incidensek súlyos következményekkel (pl. személyazonosság-lopás, pénzügyi veszteség, egyéb gazdasági hátrány stb.) járhatnak az érintettekre nézve, ha megelőzni nem sikerül ezeket, fontos, hogy nagyon rövid határidőn belül intézkedések történjenek az incidensek következményeinek az elhárítása érdekében. Fontos fogalmi elem, hogy az adatvédelmi incidens a biztonság sérüléséből következzen, valamint kizárólag személyes adatot érinthet, így a know-how-hoz vagy üzleti titokhoz jogosulatlanul férnek hozzá, akkor nem minősül incidensnek. Tehát nem minden adatvédelmi jogsértés adatvédelmi incidens, de minden adatvédelmi incidens adatvédelmi jogsértés.[256] Az adatvédelmi incidenst haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő hetvenkét órán belül kell bejelenteni az illetékes felügyeleti hatóságnak.[257] Amennyiben ezt elmulasztják az érintett vállalkozások, akkor súlyos bírságokkal sújthatják őket. A GDPR egyik legjelentősebb újítása az egységes adatvédelmi bírság bevezetése minden tagállamban, amelynek mértéke mindenhol azonos, és jelentősen magasabb a korábbi bírságösszegekhez képest. A kiszabható bírságok 10 millió euróig, illetve vállalatok esetében a teljes világpiaci forgalom 2%-áig terjedhetnek, súlyosabb esetben ezek duplája jelenti a bírság legmagasabb összegét. A kettő közül a magasabb összeget kell kiszabni.[258]

[256] ÁRVAY Viktor: Az adatkezelő és adatfeldolgozó kötelezettségei. In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): Magyarázat a GDPR-ról. Wolters Kluwer Hungary Kft., 2018. 215. o.
[257] Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság jár el.
[258] SZABÓ Endre Győző: Az adatvédelmi bírságról – a GDPR szabályainak elemzése. Alkotmánybírósági Szemle 2018/2. 27. o.

Végül megemlíteném a 2006-ban elfogadott adatmegőrzési irányelvet[259] is, amelyet súlyos bűncselekmények, így különösen a szervezett bűnözés és a terrorizmus megelőzése érdekében az elektronikus hírközlő vagy nyilvános hírközlő hálózatok szolgáltatói részére adatmegőrzési kötelezettséget írt elő. 2014-ben azonban az Európai Unió Bírósága döntésében érvénytelennek nyilvánította az irányelvet, és ezt azzal indokolt, hogy a rendelkezései nem összeegyeztethetők az Európai Unió Alapjogi Chartájával, illetve a magánszféra védelméhez fűződő jog tiszteletben tartásának kötelezettségével. Az adatmegőrzési rendelkezések alapján őrzött adatok ugyanis pontos tájékoztatást adhatnak a felhasználók magánéletéről, mindennapi szokásaikról, kapcsolataikról. A Bíróság szerint az adatmegőrzés önmagában igazolható a súlyos bűncselekmények elleni fellépés és a közbiztonság megőrzésének szükségessége érdekében, de az irányelv elfogadásával átlépték az arányosság elvének határait. Nem biztosított megfelelő garanciarendszert, amely kizárná a visszaéléseket, például a személyes adatok engedély nélküli felhasználását, valamint nem rögzítette, hogy azokat kizárólag az Unió területén lehetne felhasználni.[260]

[259] Az Európai Parlament és Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. HL L 105/54. 2006.4.13.https://hpops.tk.mta.hu/blog/2014/05/az-alapjogi-chartaba-utkozik-az-adatmegorzesi-iranyelv

260 https://hpops.tk.mta.hu/blog/2014/05/az-alapjogi-chartaba-utkozik-az-adatmegorzesi-iranyelv [2019.05.21.]

6. Az előkészületi cselekmények sui generis bűncselekményként való szabályozása

A kiberbűnözés napjainkra egy szolgáltatás-alapú üzleti modellé vált, a különféle támadások indítására szolgáló eszközöket, programokat szolgáltatásként lehet igénybe venni vagy akár megvásárolni az ún. Darknet online feketepiacokon és fórumokon keresztül.[261] A kibertámadások végrehajtása egyszerűbbé vált azáltal, hogy könnyen hozzá lehet jutni a bűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár a már kész botnet infrastruktúrához, és ezért is fontos, hogy már az előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra.

Ennek megfelelően már a Budapesti Egyezmény szabályozta az eszközökkel való visszaélést (6. cikk), amelynek értelmében bűncselekménynek minősül a következő cselekmények jogosulatlan és szándékos elkövetése: az előállítása, az értékesítése, a felhasználás céljából való megszerzése, az ország területére való behozatala, a forgalomba hozatala vagy a más módon történő hozzáférhetővé tétele az elsődlegesen azon eszközöknek, ideértve a számítástechnikai programot, melyeket a 2-5. Cikkben meghatározott valamely bűncselekmény elkövetése érdekében hoztak létre vagy alakítottak át, vagy egy számítógépes jelszónak, egy belépési kódnak, illetőleg hasonló, a számítástechnikai rendszerbe vagy annak bármely részébe való belépést lehetővé tevő számítástechnikai adatnak, azzal a céllal, hogy azt a 2-5. Cikkekben foglalt valamely bűncselekmény elkövetésére használják fel. Továbbá az előbb említett dolgoknak a birtoklása a 2-5. Cikkben foglalt valamely bűncselekmény elkövetésére való felhasználás érdekében. A szerződő felek azonban a belső jogukban kiköthetik, hogy a büntetőjogi felelősséget meghatározott számú dolog birtoklása alapozza csak meg. Fontos, hogy csak a meghatározott célzat fennállása esetén büntetendők a felsorolt magatartások, valamint a szerződő felek kötelesek legalább a számítógépes jelszavak vagy belépési adatok értékesítését, a forgalomba hozatalát vagy a más módon történő hozzáférhetővé tételét kriminalizálni.[262]

A 2013-as irányelv a bűncselekmények elkövetéséhez használt eszközök (7. cikk) rendelkezése szerint a tagállamoknak meg kell hozni a szükséges intézkedéseket annak érdekében, hogy a következő eszközök jogosulatlan és bármely, a 3-6. cikkben említett bűncselekmény elkövetéséhez való felhasználásának szándékával való előállítása, árusítása, használatra történő beszerzése, behozatala, forgalomba hozatala vagy egyéb módon történő hozzáférhetővé tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön: az olyan

[261] Erről lásd részletesen „A szervezett bűnözés az interneten” című részt.
[262] COUNCIL OF EUROPE: i.m. 13. o.

számítógépes programok, amelyek elsősorban a 3–6. cikkben említett bármely bűncselekmény elkövetésére készültek vagy lettek átalakítva; vagy olyan számítógépes jelszavak, belépési kódok vagy hasonló adatok, amelyekkel egy információs rendszerhez vagy annak egy részéhez hozzá lehet férni.

Ennek megfelelően a Btk. 424. §-ban szabályozza az információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét, amely tényállásnál a törvény a szankcionálni kívánt előkészületi cselekményeket mint önálló, befejezett bűncselekmény elkövetési magatartásaként, sui generis módon határozza meg.[263] A bűncselekmény elkövetési tárgya az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §) vagy a tiltott adatszerzés [Btk. 422. § (1) bekezdés d) pont] vagy az információs rendszer vagy adat megsértésének (Btk. 423. §) elkövetéséhez szükséges, vagy azt megkönnyítő jelszó, számítástechnikai program, valamint az ezek készítésére vonatkozó gazdasági, műszaki, szervezési ismeret. A (3) bekezdés értelmező rendelkezése meghatározza, hogy a jelszó: „az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító".

A bűncselekmény elkövetési magatartásai két fordulatban kerülnek meghatározásra. Az a) pont szerinti fordulat elkövetési magatartásai a jelszó vagy számítástechnikai program készítése, átadása, hozzáférhetővé tétele, megszerzése vagy forgalomba hozatala. A készítés eredménye például a kész program. Az átadás történhet a birtokba adáson kívül, a rendelkezésre bocsátással, illetve a megfelelő ismeret átadásával. A hozzáférhető tételnek minősül minden olyan tevékenység vagy mulasztás, amelynek köszönhetően hozzáférhetővé válik a jelszó vagy program az arra nem jogosult részére. A megszerzés a rendelkezési lehetőség megteremtését foglalja magában. A forgalomba hozatal esetén az elkövető több személynek juttatja el a jelszót vagy a programot.

A b) pont szerinti fordulat elkövetési magatartása a jelszó vagy számítástechnikai program készítésére vonatkozó szervezési ismeret másnak a rendelkezésére bocsátása. A rendelkezésre bocsátás azt jelenti, hogy az érintett személy a tényállásba foglalt ismeret birtokába jut. Ezt kimeríti a tudomásszerzés, de előfordulhat az is, hogy az ismereteket valamely tárgy tartalmazza, és ezt bocsátják a rendelkezésére.[264]

---

[263] GÁL Andor: Az előkészületi cselekmények büntetendő nyilvánításának egyes típusairól. Magyar Rendészet 2018/3. 30. o.: Az előkészületi magatartás befejezett bűncselekményként történő szabályozása az alábbi jogkövetkezményeket eredményezi: az előkészülettől való önkéntes visszalépés mint büntethetőséget megszüntető ok nem alkalmazható, a bűncselekmény kísérleti stádiumban is megvalósulhat, valamint a bűncselekményhez kapcsolódhat felbujtás és bűnsegély.

[264] MOLNÁR (2018): i.m. 979-980. o.

A Btk. büntethetőséget megszüntető okot is meghatároz: nem büntethető az (1) bekezdés a) pontjában meghatározott bűncselekmény elkövetője, ha – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó, vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.[265]

A bűncselekmény rendbelisége ez esetben is az információs rendszerek számához igazodik. A tényállás mindkét fordulata csak szándékosan, méghozzá egyenes szándékkal követhető el és az elkövető szándéka arra kell, hogy irányuljon, hogy akár ő maga vagy tőle különböző személy az információs rendszer felhasználásával elkövetett csalást vagy a tiltott adatszerzést vagy az információs rendszer vagy adat megsértését elkövesse.[266] Aki a tárgyalt bűncselekmények elkövetése céljából jelszót vagy programot készít, átad, hozzáférhetővé tesz stb., a Btk. 424. §-ában írt vétséget valósítja meg. Azonban, ha a tettes ezeket az adatokat alkalmazva az információs rendszer felhasználásával elkövetett csalást megkíséreli vagy véghez is viszi, az említett előkészületi magatartás a tettesi cselekményhez nyújtott bűnsegélyként értékelendő.

6.1. Visszaélés számítógéphez való hozzáféréshez szükséges jelszavakkal és hasonló információkkal (Trafficking in passwords)

A CFAA 1030. § (a)(6) bekezdésének értelmében vétség miatt büntetendő, „aki tudatosan, megtévesztéssel (intent to defraud) a számítógéphez jogosulatlan hozzáférést biztosító jelszót vagy hasonló információt megszerez, azért, hogy másnak átadja, hozzáférhetővé tegye vagy forgalomba hozza (trafficking), ha ez

(A) hatással van az államközi vagy nemzetközi kereskedelemre, vagy

(B) olyan számítógéphez biztosít hozzáférést, amelyet az Egyesült Államok kormánya használ, vagy annak érdekében használnak.”

A trafficking tág fogalmat jelöl, mert megvalósul, ha az elkövető a számítógéphez való hozzáférést biztosító jelszót átadja, forgalomba hozza vagy egyéb módon hozzáférhetővé teszi másnak, vagy abból a célból szerzi meg, hogy azt másnak rendelkezésére bocsájtsa, de önmagában a birtoklás nem meríti ki ezt az esetet a célzat hiányában, valamint a személyes használat sem. A bűncselekmény megállapításához nincs szükség a haszonszerzési célból

[265] 2017. évi CXCVII. törvény 342. § 22. pont iktatta be
[266] MOLNÁR (2018): i.m. 946–954. o.

történő elkövetésre. A jelszavak és rosszindulatú programok készítése – az uniós és hazai gyakorlattól eltérően – azonban nem szerepel a szankcionált magatartások között. Továbbá a jogalkotó a tényállásban értékelte azt is, hogy az elkövető a jelszót valamilyen fondorlatos, megtévesztő módon szerzi meg (intent to defraud).[267]

A „jelszó" (password) fogalmát a CFAA nem határozza meg, mint például, ahogy ezt a magyar Btk. teszi. Megállapítandó azonban, hogy a jelszó egy tágabb fogalmi kört határoz meg, mert nem korlátozódik csak egy kifejezésre vagy kódra, hanem ez magában foglalhat akár egy leírást, útmutatást vagy egyéb módszert vagy ezek kombinációját is, a lényeg – és az ekként funkcionáló más információ esetén is –, hogy jogosulatlan hozzáférést biztosít a számítógéphez.[268] Nem egyértelmű ugyan, de a hasonló információ fogalmi körébe tartozik például egy kártékony program vagy kód is.[269]

A 1030. § (a)(6) bekezdés megsértéséért pénzbüntetés és/vagy egy évig terjedő szabadságvesztés, ha pedig korábban már elítélték a CFAA hatálya alá eső bűncselekményért, akkor tíz évig terjedő szabadságvesztés szabható ki.

Érdemes megemlíteni, hogy egy másik bűncselekménynél is jelentősége van a jelszavaknak, ugyanis a 1029. §-ben szabályozott hozzáférést biztosító eszközökkel való visszaélés (access device fraud) bűncselekményre tekintettel egyúttal hozzáférést biztosító eszközöknek (access device) is minősülnek. Ez a tényállás pedig lefedi a legtöbb phishing esetet például, ha az elkövető megtévesztő e-maileket küld azért, hogy megszerezze mások bankkártya vagy bankszámla adatait vagy jelszavait, vagy a már jogosulatlanul megszerzett banki adatok felhasználásával utalásokat végez. Az hozzáférést biztosító eszköz fogalma is rendkívül tág, mert magában foglal bármely számot, azonosítót vagy eszközt önmagában, vagy más eszközzel együttesen, amely(ek) pénz, áru, szolgáltatás vagy bármely értékkel bíró dolog megszerzésére, vagy (pénz)utalás kezdeményezésére használható(k).[270]

[267] U.S. DEPARTMENT OF JUSTICE (2015): i.m 27. o.
[268] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 49-51. o.
[269] WANG (2016): i.m. 131. o.
[270] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 96-97. o.

7. Az információs rendszer felhasználásával elkövetett zsarolás esetei

A számítógépes zsarolás egy hagyományos bűncselekmény modern változata, amely során gyakran az elkövetők az információs rendszerek, valamint a virtuális fizetőeszközök használatával fenyegetik a sértettet, hogy kárt okoznak neki, amennyiben a követelésüknek nem tesz eleget. Például azzal fenyegetnek, hogy betörnek az adott rendszerbe és titkosítják vagy törlik a tárolt adatokat (pl. zsarolóvírus használatával), vagy DDoS-támadással, valamint adatlopással vagy a már ellopott információnak a nyilvánosságra hozatalával fenyegetnek. Emellett a zsarolásnak egy új formája is megjelent, amely során az elkövetők Darknet fórumokon szereznek meg olyan adatbázisokat, amelyek nagyszámban tartalmaznak e-mail címeket, és ezekre elküldik azt az üzenetet, hogy kompromittáló kép- vagy videófelvétel van az érintett felhasználóról és amennyiben nem fizet, akkor közzéteszik a felvételt.

Egyre gyakoribb, hogy zsarolás során használják fel a DDoS-támadásokat. 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). 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 végett bitcoin formájában fizetséget kérnek a cégtől. Abban az esetben, 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. Azonban nem javasolt, hogy fizessenek a zsarolóknak, mert nincs garancia a fizetség esetén sem a további támadás elkerülésére. A DD4BC csapatnak a bevált módszere egyre elterjedtebbé vált és már „copycat" hacker csoportok is megjelentek.[271]

Europol továbbá figyelmeztet a zsarolás új formájára, amikor a kiszemelt sértettektől kompromittáló felvételeket szereznek meg például a közösségi médián keresztül a bizalmukba férkőzve majd a felvételek megosztásával fenyegetnek, amennyiben meghatározott összeget bitcoinban nem fizetnek. Ezeket gyakran önálló elkövetők követik el, de ezek az esetek egyre

[271] https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 [2017.09.18.]
http://neih.gov.hu/zsarolo-ddos [2017.09.21.]

növekvő számban bűnszervezetekhez is köthetők, akik „call center”-t működtetnek haszonszerzés céljából.[272]

7.1. A zsarolás hazai szabályozása a technológiai fejlődés tükrében

A hazai büntetőjog nem szabályozza külön a számítógépes zsarolást. Azonban az egyik legaktuálisabb kérdés a zsarolás és az informatikai bűncselekmények kapcsolatának a vizsgálata. Előfordulhat ugyanis, hogy az elkövetők jogosulatlanul belépnek a sértett számítógépébe a biztonsági intézkedések kijátszásával, például malware aktiválásával – gondoljunk csak a zsarolóvírusokra vagy trójaival megvalósuló hátsó ajtó nyitásra – és megszerzik az azon tárolt bizalmas, személyes adatokat, értékes gazdasági vagy üzleti titkokat, esetleg kompromittáló képeket. A 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 család, barátok részére elküldi a felvételt, amennyiben a sértett nem fizet egy meghatározott pénzösszeget a részére.

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 állt be, akkor a zsarolás kísérlete valósul meg.[273]

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.

[272] EUROPOL (2017): i.m. 35. o.
[273] AKÁCZ József: XXXV. A vagyon elleni erőszakos bűncselekmények. In: Kónya István (szerk): Magyar büntetőjog I-III. – Kommentár a gyakorlat számára. 3. kiadás HVG-ORAC Lap- és Könyvkiadó. Budapest, 2017.

7.2. A számítógépes zsarolás (Threatening to damage a computer) a CFAA-ban

A 1030. § (a)(7) bekezdés a számítógépes zsarolást szabályozza, amely szerint bűntett miatt büntetendő, „aki azzal a szándékkal zsarol meg mást, hogy tőle pénzt vagy egyéb értékkel bíró dolgot megszerezzen, és olyan tartalmú üzenetet továbbít az államközi vagy nemzetközi kereskedelmen keresztül, amelyben

(A) a védett számítógépben való károkozással fenyeget;

(B) a védett számítógépben tárolt információ jogosulatlan vagy jogosultságainak kereteit túllépve történő megszerzésével, vagy a megszerzett bizalmas információ nyilvánosságra hozatalával fenyeget; vagy

(C) pénzt vagy egyéb értékkel bíró dolgot követel, vagy kér a védett számítógépben való károkozással kapcsolatban, és az így okozott kár a zsarolást segíti elő.”

Az első fordulat miatti felelősségre vonáshoz nem szükséges, hogy az elkövető a zsarolás tárgyát képező pénzt vagy egyéb értékkel rendelkező dolgot megszerezze, valamint az sem, hogy az elkövető szándéka kiterjedjen arra, hogy a fenyegetését valóban megvalósítsa. Általánosságban a zsarolás során az elkövető a sértettet fenyegetéssel vagy erőszakkal kényszeríti. A fenyegetést nemzetközi vagy államközi kereskedelmen keresztül kell továbbítani, azonban nem szükséges, hogy ez elektronikus úton történjen, hanem megvalósulhat telefonhívás, e-mail formájában vagy egyéb üzenetváltási rendszeren keresztül.

A kár bekövetkeztéhez elegendő – a korábban már a 1030. § (a)(5) bekezdésnél említett módon –, ha az elkövető a tényállásszerű magatartásával a számítógép működését befolyásolja (pl. a rendszer működését megzavarja, a jogosult felhasználók nem tudnak hozzáférni a rendszerhez, adatokat vagy programokat töröl, vagy hozzáférhetetlenné tesz, a számítógépet lelassítja stb.). Ellenben nem minősül károkozással való fenyegetésnek, ha azzal fenyegetnek, hogy nyilvánosság előtt feltárják például az adott vállalat rendszerében található sebezhetőségeket vagy azt tényt, hogy a rendszert feltörték.

A 1030. § (a)(7)(B) bekezdése két fordulatot foglal magában. Az első esetben az elkövető azzal fenyeget, hogy bizalmas információkat szerez meg a sértettől, ha a követelésnek nem tesz eleget. A második fordulatban pedig azzal, hogy a megszerzett bizalmas információkat nyilvánosságra hozza. Ez azt jelenti, hogy az elkövető az első esetben még nem, míg a második esetben már rendelkezik az információkkal, ami a zsarolás alapját képezi.

A 1030. § (a)(7)(C) bekezdése szerint büntetendő, aki tartózkodik a kapcsolatfelvételtől egészen a károkozásig, majd miután hozzáfért a sértett számítógépéhez és például titkosítja az

adatokat rajta, akkor áll elő a követelésével, hogy pénzt kérjen a titkosítást feloldó kulcsért cserébe.

A számítógépes zsarolás öt évig terjedő szabadságvesztéssel büntetendő, amennyiben a törvény hatálya alá eső másik bűncselekmény miatt is elítélték korábban az elkövetőt, akkor tíz évig terjedő szabadságvesztés is kiszabható.[274]

[274] U.S. DEPARTMENT OF JUSTICE (2015): i.m. 52-54. o.

8. A tiltott adatszerzés nemzetközi, uniós és hazai szabályozása

A Budapesti Egyezményben szabályozott jogosulatlan kifürkészés (3. cikk) esetén büntetendő a számítástechnikai rendszeren belüli, az abból származó, illetőleg a rendszerbe irányuló számítástechnikai adatok nem nyilvános továbbítása során technikai eszközök felhasználásával történő jogosulatlan és szándékos kifürkészése, ideértve az ilyen számítástechnikai adatokat továbbító, a számítástechnikai rendszerből származó elektromágneses sugárzást. Azonban a szerződő felek kiköthetik, hogy a bűncselekményt tisztességtelen céllal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

A 2013-as irányelv a jogellenes adatszerzéssel (6. cikk) szembeni tagállami intézkedéseket tesz kötelezővé, amelynek értelmében az információs rendszeren belülre, kívülre vagy azon belül továbbított, nem nyilvános számítógépes adatok – többek között az információs rendszerekből érkező, ilyen adatokat hordozó elektromágneses sugárzás – technikai eszközökkel történő, szándékos és jogosulatlan megszerzése, legalább a súlyosabb esetekben bűncselekménynek minősüljön. Adatszerzés különösen a kommunikáció tartalmának lehallgatása, ellenőrzése vagy figyelemmel kísérése és az adattartalmak közvetlenül, az információs rendszerhez való hozzáférés és az információs rendszer használata által történő, vagy közvetetten, elektronikus megfigyelő vagy lehallgató eszközök révén történő megszerzése.

A bűncselekmény előzményének tekinthető az 1978. évi Btk.-ból ismert magántitok jogosulatlan megismerésének tényállása, azonban új elnevezést kapott és ki lett bővítve az elkövetési tárgyak köre a személyes adattal, a gazdasági és az üzleti titokkal. A Btk. miniszteri indokolása szerint a bűncselekmény áthelyezésének rendszertani oka van, hiszen ennek egyik elkövetési fordulatát is információs rendszer útján valósítják meg, és e magatartás szintén a Budapesti Egyezmény megsértését jelenti, így indokolt ezek egy fejezeten belüli elhelyezése.

A bűncselekmény első alapesetében az elkövető célja a személyes adat, a magántitok, a gazdasági titok vagy az üzleti titok jogosulatlan megismerése, így e bűncselekmény védett jogi tárgya az ezek védelméhez fűződő társadalmi érdek.

A személyes adat tekintetében a háttérjogszabály az Infotv., amely a GDPR-nak megfelelően határozza meg a 3. § 2. pontjában a személyes adat fogalmát: „az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés”.

A magántitok a fogalmát a Btk. nem határozza meg, de továbbra is irányadónak tekinthető az ítélkezési gyakorlat, miszerint magántitok minden olyan, csak szűk körben, illetve a beavatottak előtt ismert bizalmas tény, körülmény vagy adat, amelynek megőrzéséhez az érintett személynek méltányolható érdeke fűződik, illetve amelynek nyilvánosságra hozatala a sértettre nézve érdeksérelemmel jár.[275] A magántitok lehet dologi (tárgyiasult formában rögzített: leírt, lefényképezett, kép-, hang- vagy videóhangfelvételen rögzített) vagy eszmei jellegű (csak a beavatott tudatában rögzült). A tény, illetve az adat titokjellege viszonylagos, amelyet csak az elkövetés konkrét összefüggései alapján lehet megítélni. Ilyen adat lehet a passzív alany személyi, családi, vagyoni helyzete, egészségi állapota, vagy az egyéb személyes jellegű szokásaira vonatkozó ismeretek.[276]

A gazdasági titok egy gyűjtőfogalmat takar, amelyhez tartozik a banktitok[277], értékpapírtitok[278], biztosítási titok[279], valamint a pénztártitok[280], amelyek lényegüket tekintve a pénzügyi szektor titkainak csoportjába tartoznak. Az egyik kommentár a bűncselekmények

[275] BH 2004.170.

[276] HORVÁTH – KERESZTI – MARÁZ – NAGY - VIDA: i.m. 171-172. o.; Lásd ehhez bővebben még BÉRCES Viktor: A magántitok büntetőjogi védelmének értelmezési sémái. Jogtudományi Közlöny 2017/9. 394-407. o.

[277] A hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. (Hptv.) törvény 160. § (1) bekezdése szerint „banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyiintézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik."

[278] Az értékpapírtitok fogalmát két törvény is meghatározza: a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény (Bszt.) és a tőkepiacról szóló 2001. évi CXX. törvény (Tpt.) és fogalmai között csak annyi különbség van, mint amennyi a pénztártitok fogalmánál is látható volt: más szolgáltatói körre vonatkozik. A Bszt. meghatározása szerint „értékpapírtitok: minden olyan, az ügyfélről a befektetési vállalkozás, a multilaterális kereskedési rendszer működtetője és az árutőzsdei szolgáltató rendelkezésére álló adat, amely az ügyfél személyére, adataira, vagyoni helyzetére, üzleti befektetési tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, illetve a befektetési vállalkozással és árutőzsdei szolgáltatóval kötött szerződéseire, számlájának egyenlegére és forgalmára vonatkozik" míg ugyanez a Tpt. alapján a „befektetési alapkezelő, a kockázati tőkealap-kezelő, a tőzsde, központi értéktár, központi szerződő fél" rendelkezésére álló adatok stb. tekintetében áll fenn.

[279] A biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény szerint „minden olyan – minősített adatot nem tartalmazó –, a biztosító, a viszontbiztosító, a biztosításközvetítő rendelkezésére álló adat, amely a biztosító, a viszontbiztosító, a biztosításközvetítő ügyfeleinek – ideértve a károsultat is – személyi körülményeire, vagyoni helyzetére, illetve gazdálkodására vagy a biztosítóval, illetve a viszontbiztosítóval kötött szerződéseire vonatkozik.

[280] A magánnyugdíjról és a magánnyugdíjpénztárakról szóló 1997. évi LXXXII. törvény 78. § (2) bekezdése alapján pénztártitok „minden olyan, a pénztártagról a pénztár vagy a pénztári szolgáltató szervezet rendelkezésére álló, a tevékenysége folytán tudomására jutó tény, információ vagy adat, amely a pénztártag személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, tulajdonosi, üzleti kapcsolataira, valamint egyéni számláján nyilvántartott összegre, járulékbefizetéseire és a részére járó nyugdíjszolgáltatásra vonatkozik." A pénztártitok fogalma emellett egy másik törvényben, az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvényben is szerepel, eszerint: „pénztártitok minden olyan, a pénztártagról és a munkáltatói tagról a pénztár vagy a pénztári szolgáltató rendelkezésére álló, a tevékenysége folytán tudomására jutó tény, információ vagy adat, amely a pénztártag, a pénztártag kedvezményezettjének, örökösének, közeli hozzátartozójának személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, tulajdonosi, üzleti kapcsolataira, valamint egyéni számláján nyilvántartott összegre, illetve amely a munkáltatói tag, illetve a támogató adataira, vagyoni helyzetére, üzleti tevékenységére, tulajdonosi, üzleti kapcsolataira vonatkozik."

elhatárolása során megjegyzi, hogy „a gazdasági titok a magántitok speciális változata,”[281] más titokfajtáknál csoportosításra utaló megjegyzést azonban nem tesz.[282]

Az üzleti titok fogalmát korábban a Ptk., míg jelenleg az üzleti titok védelméről szóló 2018. évi LIV. törvény határozza meg, amelynek értelmében: „üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos - egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja. Emellett a védett ismeret is (know-how) üzleti titoknak minősül, amely az azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezési ismeret, megoldás, tapasztalat vagy ezek összeállítása.”

Szőke Gergely szerint érdemes arra is ügyelni, hogy ugyan a jogi személyek titkai kapcsán inkább az üzleti titok védelme tűnik elsősorban nyilvánvalónak - különösen az üzleti életben -, azonban semmi sem zárja ki, hogy a jogi személyeknek is legyen nem nevesített magántitkuk, aminek különösen akkor lehet jelentősége, ha az adott adat, információ, ismeret nem felel meg az üzleti titok fogalmának.[283]

A tiltott adatszerzés deliktumának az elkövetési magatartásai a d) pont szerint az elektronikus hírközlő hálózat vagy eszköz útján[284], illetve információs rendszeren folytatott kommunikáció tartalmát titokban való kifürkészése, és az észlelteket technikai eszközzel való rögzítése, valamint az e) pont szerint információs rendszerben kezelt adatokat titokban kifürkészése, és az észlelteket technikai eszközzel rögzítése, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

Az információs rendszerben kezelt adatokat titokban történő kifürkészése jogosulatlan belépéssel vagy bennmaradással valósulhat meg és önmagában is alkalmas lehet az információs rendszer vagy adat megsértése bűncselekmény Btk. 423. § (1) bekezdésében meghatározott

[281] HEGEDŰS István – JUHÁSZ Zsuzsanna – KARSAI Krisztina – KATONA Tibor – MEZŐLAKI Erik – SZOMORA Zsolt – TÖRŐ Sándor: Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez, Wolters Kluwer, Jogtár kommentár a 413. §-hoz

[282] SZŐKE Gergely László: Gondolatok a hazai titokvédelmi szabályozás rendszeréről. Jura 2018/2. 244. o.

[283] SZŐKE: i.m. 256. o.

[284] Az elektronikus hírközlésről szóló 2003. évi C. törvény 188. §-ának 19. pontja szerint az elektronikus hírközlő hálózat: átviteli rendszerek és - ahol ez értelmezhető - a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások - beleértve a nem aktív hálózati elemeket is -, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára. A törvény 188. §-ának 18. pontja szerint elektronikus hírközlő eszköz: az elektronikus hírközlő berendezések és a kapcsolódó eszközök összessége, ideértve az antennákat is.

fordulatának a megállapítására. Ez a magatartás ugyancsak a tiltott adatszerzés eszközcselekménye, mert arra az információs rendszerben kezelt adatok technikai eszközökkel történő rögzítése érdekében kerül sor.

Célzatos bűncselekmény, mert az elkövető cselekményének a magántitok, a gazdasági vagy az üzleti titok jogosulatlan megismerésére kell irányulnia.

A Kúria döntésében kimondta, hogy a sértett által másokkal folytatott telefonbeszélgetések rögzítése alkalmas arra, hogy a terhelt a sértett és más személyek magántitkainak a birtokába juthasson. Ez a megállapítás azonban azt jelenti, hogy a telefonbeszélgetések rögzítése során esetlegesen magántitkok, gazdasági vagy üzleti titkok is megismerhetők és rögzíthetők, ám ennek lehetőségéből mindössze a terhelt eshetőleges szándékára lehet következtetni, amely célzatos bűncselekmény esetében a bűnösség megállapításához nem elegendő.[285] Úgy vélem, hogy ez az információs rendszerre alkalmazva is hasonló eredményhez vezethet, itt különösen fontos vizsgálni az illető szándékát és az eset összes körülményét, hogy bizonyítást nyerjen, hogy a tényállásban kiemelten kezelt információk valamelyikének megismerésének céljából fürkészi ki és rögzíti.

Az elkövetési magatartásokkal kapcsolatban fontos kiemelni, hogy kizárólag a technikai eszközök alkalmazásával történő megfigyelés és rögzítés valósít meg bűncselekményt. Ennek az az indoka, hogy a technikai eszközök alkalmazása jelentős mértékben növeli az ilyen jellegű cselekmények társadalomra veszélyességét.[286] Amennyiben ennek a feltételnek nem felel meg az érintett magatartása például az elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított közleményt kifürkészi, de nem rögzíti, akkor a levéltitok megsértése miatt büntethető [Btk. 224. § (1) bekezdés b) pont], valamint egyéb esetekben az információs adat vagy rendszer megsértéséért.

Emellett érdemes foglalkozni röviden a Btk. 422. § b) pontjával is, amelynek értelmében, aki a meghatározott adatok vagy titkok megismerése céljából más lakásába, egyéb helyiségébe vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti az a tiltott adatszerzés bűncselekményét valósítja meg. Ebben az esetben problémát okozhat az elkövetés helye, hiszen kizárólag magánlakás, annak egyéb helyisége vagy azokhoz tartozó bekerített helyen valósulhat meg, vagyis nem csak a lakáson belül. A különböző optikai, elektronikai eszközökkel, kamerával, fényképezőgéppel vagy egyéb lehallgató eszközök felszerelésével egy repülő drón is alkalmas lehet ezen magatartás tanúsítására.

[285] Kúria Bfv. III. 1548/2014/7.
[286] MOLNÁR (2018): i.m. 966-967. o.

Az üzleti vagy gazdasági titkok esetében azonban felmerül a kérdés, hogy ezeket nem biztos, hogy egy magánlakásban, vagy udvaron figyelhet meg az ingatlan fölé berepülő drón. Éppen ezért Csák Zsolt álláspontja szerint itt már felmerül a jogi szabályozás igénye[287], hiszen a repülő drónok alkalmazására figyelemmel az elkövetés helyét ki kellene terjeszteni a gazdasági, ipari létesítményekre és azokhoz tartozó ingatlanokra, ahol nagyobb eséllyel valósulhat meg gazdasági, illetve üzleti titkok megismerése, megfigyelése.[288]

A tiltott adatszerzés minősített esetét valósítja meg és ezért súlyosabban büntetendő, egy évtől öt évig terjedő szabadságvesztéssel, aki hivatalos eljárás színlelésével, üzletszerűen, bűnszövetségben vagy jelentős érdeksérelmet okozva követi el a bűncselekményt.

[287] Lásd de lege feranda javaslatot ehhez NAGY Zoltán András: A jövő tegnap óta tart: A modern technikai-technológiai folyamatok kihívásai a jog területén. Belügyi Szemle 2018/10. 42-45. o.
[288] CSÁK Zsolt: A drónok kapcsán felmerülő egyes büntető és eljárási jogi kérdések. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019. 34. o.

III. A TECHNOLÓGIAI FEJLŐDÉS HATÁSA A GAZDASÁGI BŰNCSELEKMÉNYEKRE

1. A bankkártyákkal és a banki átutalásokkal kapcsolatos bűncselekmények

Az elmúlt időszakban a digitalizáció, a technológiai fejlődés jelentős változást eredményezett a gazdaság számos területén. A változások a pénzügyi innovációk megjelenése és elterjedése révén nem hagyták érintetlenül a pénzforgalmat és a pénzügyi infrastruktúrákat sem, amelyek egyben egyre inkább függenek az információs rendszerektől, és mindez jelentős hatást gyakorol a bankszektorra és annak versenyképességére. Az elektronikus pénzforgalmi szolgáltatások elérése és használata a fejlett társadalmakban alapvető igénnyé vált. Ennek köszönhetően készpénz használata fokozatosan szorul vissza világszerte, és az emberek többsége már bankkártyával fizet, valamint a vásárlásait és egyéb ügyleteit az interneten keresztül intézi.

A modern fizetési technológiák egyúttal az új típusú fizetési eszközök használatát termethetik meg. Egyetértek azzal a kriminológiai állásponttal, amely szerint abban az esetben, ha egy technikai eszköz bevezetésére sor kerül, akkor ez után szükségképpen számolni kell azon bűnelkövetők megjelenésével is, akik vissza kívánnak élni vele, és e cselekményük a társadalom védelme érdekében büntetőjogi reagálást igényel a jogalkotó részéről.[289] Ezt igazolja a bankkártya használat elterjedése is, mivel rövid időn belül megjelent az ezzel összefüggő bűnözés is, amely esetén egy szervezett, specializált és folyamatosan alkalmazkodó bűnelkövetésről van szó, és célja a bankszektor biztonsági intézkedéseinek kijátszása, valamint az új fizetési technológiák kihasználása. Jelen fejezetben a készpénz-helyettesítő fizetési eszközök közül, kiemelten a bankkártyával kapcsolatos kérdéseket vizsgáljam.

Magyarországon a Magyar Nemzeti Bank 1992-ben tette lehetővé a bankkártyák használatát, amelyet hamarosan követett a büntetőjogi szabályozás is. Az 1994. évi IX törvény 26-27. §-ai alapján váltak büntetendővé az új eszközzel kapcsolatos visszaélések és a vonatkozó tényállások elnevezése akkoriban a bankkártya-hamisítás, valamint bankkártyával visszaélés volt. Ezt követően az uniós nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló kerethatározatnak eleget téve a tényállások módosítására és egységesítésére került sor. A 2003. évi II. törvény 25-28. §-ai a tényállások elnevezését

[289] AMBRUS István – DEÁK Zoltán: Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből. Belügyi Szemle 2011/2. 85. o.

módosította a következőkre: a készpénz-helyettesítő fizetési eszköz-hamisításra (Btk. 392. §) és a készpénz-helyettesítő fizetési eszközzel visszaélésre (Btk. 393. §). Emellett bevezetésre került az ezen eszközök hamisításának az elősegítése is (Btk. 394. §). Az 1978. évi Btk. a gazdasági bűncselekmények elnevezésű fejezetében, ezen belül is a pénzügyi bűncselekmények cím alatt szabályozta , míg később a Btk.-ban átkerültek a pénz- és bélyegforgalom biztonsága elleni bűncselekményekről szóló önálló fejezetbe.

Fontos foglalkozni továbbá a legújabb uniós szabályozással, ugyanis elfogadták a 2019/713 számú irányelvet (a továbbiakban: 2019-es irányelv)[290] a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelem elősegítése érdekében, amely felváltotta korábbi tanácsi kerethatározatot. Ennek bevezetése azzal magyarázható, hogy a meglévő szabályozást frissíteni és kiegészíteni kellett – különös tekintettel a számítógépes csalásra – e bűncselekményekkel kapcsolatos, a büntetésekre, a megelőzésre, a sértettek segítésére, valamint a határon átnyúló együttműködésre vonatkozó további rendelkezésekkel. Ezt indokolta továbbá az is, hogy az e területen az egyes tagállamoknak a büntetőjogi szabályozása hiányos, valamint a tényállások között jelentős eltérések voltak, és ezért vált szükségessé ezeknek a közelítése egymáshoz.

A 2019-es irányelv minimumszabályokat ír elő, ezért a tagállamok ennél szigorúbb büntetőjogi szabályokat is elfogadhatnak. Továbbá közös fogalommeghatározásokat is nyújt, amelyeknek ki kell terjedniük a készpénz-helyettesítő fizetési eszközök olyan új típusaira is, amelyek lehetővé teszik az elektronikus pénz és a virtuális fizetési eszközök átutalását. A 2. cikk a) pontja értelmében: „a készpénz-helyettesítő fizetési eszköz olyan immateriális vagy materiális védett készülék, tárgy vagy rögzített adat, vagy ezek kombinációja, ide nem értve a törvényes fizetőeszközöket, amely önállóan, illetve egy eljárás vagy eljárások alkalmazásával lehetővé teszi, hogy birtokosa vagy felhasználója pénzt vagy pénzbeli értéket utaljon át, többek között digitális csereeszközök révén”. Erre tekintettel büntetőjogi védelmet kizárólag az olyan fizetési eszközök kapnak, amelyek speciális védelmi jellemzőkkel vannak ellátva, tehát a 2. cikk b) pont szerint az utánzással vagy csalárd felhasználással szemben, például tervezés, kódolás vagy aláírás útján védett készüléknek, tárgynak vagy rögzített adatnak minősülnek. Ezáltal a gazdasági szereplőket is arra kívánják ösztönözni, hogy az általuk kibocsátott fizetési eszközöket megfelelő védelemmel lássák el.

[290] Az Európai Parlament és a Tanács (EU) 2019/713 irányelve (2019. április 17.) a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról. HL L123/18, 2019.5.10.

A készpénz-helyettesítő fizetési eszközök fogalmába bele kell foglalni, hogy a készpénz-helyettesítő fizetési eszköz több különböző, együttesen ható elemből állhat, például egy fizetési mobilalkalmazásból és egy ahhoz társuló engedélyezésből (pl. jelszó). A készpénz-helyettesítő fizetési eszközök fogalmát a 2019-es irányelv azzal az értelmezéssel alkalmazza, hogy az eszköz ténylegesen lehetővé teszi, hogy birtokosa vagy felhasználója pénzt vagy pénzbeli értéket utaljon át, vagy fizetési megbízást kezdeményezzen, tehát annyiban alkalmazandó, amennyiben az eszköz fizetési funkciójáról van szó. Így például egy fizetési mobilalkalmazásnak a hozzá tartozó szükséges engedélyezés nélküli, jogellenes megszerzése nem minősül készpénz-helyettesítő fizetési eszköz jogellenes megszerzésének, mivel ténylegesen nem teszi lehetővé felhasználója számára pénz vagy pénzbeli érték átutalását.

Mindezen kívül az egyik legnagyobb újdonság, hogy a 2019-es irányelv hatálya kiterjed a virtuális fizetési eszközök – azaz a kriptovaluták – átutalását lehetővé tevő digitális pénztárcákra is. A 2. cikk d) pontja szerint digitális csereeszköz az elektronikus pénz[292] és a virtuális fizetési eszköz, utóbbinak a fogalommeghatározását a korábban elfogadott 2018/843 számú irányelvből (a továbbiakban: ötödik pénzmosás elleni irányelv)[293] vették át, amit a későbbiekben elemzek a kriptovalutákkal kapcsolatos résznél. A „digitális csereeszközök" fogalommeghatározásával ennek az irányelvnek el kell ismernie, hogy a virtuális fizetési eszközök átutalására szolgáló digitális pénztárcák rendelkezhetnek – de nem szükségszerűen rendelkeznek – a fizetési eszközök sajátosságaival, és nem terjeszthetik ki a fizetési eszköz fogalommeghatározását. A fizetési azonosító adatok megszerzését célzó hamis számlák kiküldését jogellenes eltulajdonítási kísérletnek kell tekinteni.

A minimumszabályok a büntetendő cselekmények azon tényállási elemeit érintik, amelyek hozzájárulnak a készpénz-helyettesítő fizetési eszközök csalárd felhasználásához, vagy előkészítik azt. Ezért már önmagukban, a készpénz-helyettesítő fizetési eszköz tényleges csalárd felhasználása nélkül is bűncselekménynek kell tekinteni az olyan cselekményeket, mint például a fizetési eszközök csalás céljából történő gyűjtése, birtoklása és megosztása. Előbbire példaként az adathalászatot, a kártyaadat-lefölözést vagy a pénzforgalmi szolgáltatások igénybevevőinek hamis honlapokra való irányítását vagy átirányítását, míg utóbbira a hitel-,

[292] Az Európai Parlament és a Tanács 2009/110/EK irányelv 2. cikkének 2. pontjában meghatározott „elektronikus pénz": a kibocsátóval szembeni követelés által megtestesített, elektronikusan tárolt – ideértve a mágneses tárolást is – monetáris érték, amelyet pénzeszköz átvételével bocsátanak ki a 2007/64/EK irányelv 4. cikkének 5. pontjában meghatározott fizetési műveletek teljesítése céljából, és amelyet az elektronikuspénz-kibocsátón kívül más természetes vagy jogi személy is elfogad.

[293] Az Európai Parlament és a Tanács (EU) 2018/843 irányelve (2018. május 30.) a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról. HL L 156/43. 2018.6.19.

bankkártyaadatok interneten történő értékesítését említik. A 2019-es irányelv a 3-7. cikkben az alábbi bűncselekményeket szabályozza: a készpénz-helyettesítő fizetési eszközök csalárd felhasználását, mind a materiális és mind az immateriális eszközök csalárd felhasználásával kapcsolatos bűncselekményeket, az információs rendszerekkel kapcsolatos csalást, illetve ezen bűncselekmények elkövetéséhez használt eszközöket.

Felhívja a figyelmet még arra is, hogy a sértettek számára a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekmények súlyos gazdasági és nem gazdasági következményekkel járhatnak. Amennyiben az ilyen csalás személyazonosság-lopással jár, a következményeit gyakran súlyosbítja a jó hírnevet, a szakmai hírnevet vagy a magánszemély hitelminősítését érő kár és a súlyos érzelmi károsodás. A tagállamoknak segítő, támogató és védő intézkedéseket kell elfogadniuk az említett következmények enyhítése érdekében.

Megjegyzendő, hogy a hazai szabályozás már a Btk. hatályba lépése óta a 2019-es irányelvben rögzített bűncselekmények tényállási elemeivel szemben támasztott követelményeknek megfelel, ezért nincs szükség ezek módosítására sem, például tartalmazta már az információs rendszer felhasználásával elkövetett csalás tényállását, amely lefedi a 2013-as irányelvben említett információs rendszerekhez vagy rendszert érintő adat jogellenes beavatkozás deliktumainak az elkövetési magatartásaival megvalósuló immateriális készpénz-helyettesítő fizetési eszköz jogellenes megszerzését, illetve a jogosulatlan használatát is. Az uniós szabályozás ismertetését követően áttérek a készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények hazai és hatályos szabályozására és ezen belül is elsősorban a bankkártyákra fókuszálva.

A bankkártyákkal kapcsolatos visszaéléseknek két típusa különböztethető meg: az ún. card-present és a card-not-present csalás. Ezen csoportosítás mentén fogom ismertetni a szabályozást is.[294] A bankkártyákkal kapcsolatos bűncselekményeknek a jogi tárgya elsősorban a pénzforgalom zavartalan működéséhez fűződő társadalmi érdeknek a védelme. A card-present csalás esetén a bankkártya fizikailag jelen van, és ezt használják ki az elkövetők. A gyakori elkövetési módok között szerepelnek az ATM visszaélések, amelyek során a bankautomatákra ún. skimmer (miniatűr adatrögzítő) eszközöket telepítenek. Egyre többféle eszközzel találkozhatunk például 3D-nyomtatóval készített billentyűzettel, hamis ATM-nyílásokkal, billentyűzetre néző kamerákkal. Ezeken kívül arra is van példa, hogy közvetlenül az automatát fertőzik meg erre a célra kifejlesztett, rosszindulatú szoftverrel, és így gyűjtik a gyanútlan

[294] EUROPOL (2018): i.m. 40-45. o.

felhasználók bankkártya adatait (pl. az interneten már elérhetők kézikönyvek a különböző ATM automatákhoz, amelyek a kártékony programok telepítését megkönnyíthetik).[295]

Amennyiben a bankautomatákból sikeresen megszerezték az adatokat, akkor ezek segítségével klónkártyákat készíthetnek, amely további visszaélésre ad lehetőséget. A másik esetkör során az új és kényelmes fizetési megoldást nyújtó, PayPass-kártyával történő fizetést használják ki, aminél már az is elegendő, ha a kártyát odatartjuk a POS-terminálhoz, és a két eszköz rádiófrekvenciás jelek útján kommunikál egymással. A bűnelkövetők ezeket a rádiófrekvenciás jeleket képesek rögzíteni újabb skimmer eszközökkel, és az ilyen módon szerzett adatokkal interneten vásárolhatnak. Más módszerrel a PayPass-kártyát zsebtolvajlás útján szerzik meg és a használatából származó előny egyből hátrány lesz, hiszen a PayPass-kártyával fizetett tranzakciókat – a technológiából adódóan – nem kell jóváhagyni például PIN kóddal, így ez korlátlan visszaélésre ad lehetőséget, ha megszerzik a kártyát.[296]

Érdemes megemlíteni, hogy az ún. EMV (Europay Mastercard Visa) chipekkel ellátott kártyák a visszaélések elleni védelmet szolgálják, és bár az EU-n belül széles körben elterjedt ez a technológia, nemzetközi szinten a kártyák nagy része csak a mágnescsíkos megoldással rendelkezik. A bűnelkövetők a skimming technikát addig fogják hatékonyan kihasználni, amíg a mágnescsíkos kártyák használatát be nem tiltják teljesen.[297]

Az említett esetek a készpénz-helyettesítő fizetési eszköz hamisításának tényállását valósítják meg, amely három elkövetési magatartást tartalmaz. A klónkártyák létrehozása a hamis készpénz-helyettesítő fizetési eszköz készítésének felel meg. A klónozás eredményeként létrejön egy olyan eszköz, amely a lemásolt eszközhöz hasonló hozzáférést, rendelkezési lehetőséget biztosít a kártyabirtokos bankszámlájához, tehát ebben az esetben a létrehozott új kártyának az adott funkció betöltésére való alkalmasságán van a hangsúly.[298] Az ATM és PayPass visszaélések során az elektronikus készpénz-helyettesítő fizetési eszközökön tárolt adatok, vagy az ahhoz kapcsolódó biztonsági elemek technikai eszközzel történő rögzítése történik. A bűncselekmény kizárólag a felhasználás célzatával követhető el, egyenes szándékkal, azonban a felhasználást megszorítóan kell értelmezni, mert ez alatt a készpénz-helyettesítő fizetési funkció gyakorlását kell érteni. A bűncselekmény rendbelisége a készpénz-helyettesítő fizetési eszközök számához igazodik. Azonban, amíg az elkövető azonos

[295] CLOUGH: i.m. 226. o.
[296] MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós - Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017. 302. o.
[297] EUROPOL (2018): i.m. 40. o.
[298] MOLNÁR (2018): i.m. 763. o.

bankszámlaszerződés – vagyis azonos jogviszony – keretei között fejti ki a magatartásokat, akkor ez a természetes vagy a folytatólagos egység keretei között értékelendő. A hamisítás, a készítés, illetve a rögzítés befejeztével, azaz a már a további beavatkozás nélküli felhasználásra szánt eszköz előállításával a bűncselekmény befejezetté válik.[299]

Aki egy vagy több – ezáltal törvényi egységet létrehozva – olyan készpénz-helyettesítő fizetési eszközt, amely nem vagy nem kizárólag a sajátja, vagy amelynek a használatára nem vagy nem kizárólagosan jogosult, mástól, annak beleegyezése nélkül, jogtalanul elvesz vagy megszerez, az a készpénz-helyettesítő fizetési eszközzel visszaélés deliktumát valósítja meg. A szóban forgó bűncselekmény második elkövetési magatartását meríti ki, aki a hamis vagy meghamisított, illetve az előző pontban meghatározott módon elvett vagy megszerzett eszközt, vagy az elektronikus eszközön tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemeket átadja, megszerzi, az ország területére behozza, onnan kiviszi, vagy azon átszállítja. Ennek azért van jelentősége, mert sokszor a bankkártyáknak, valamint az adatoknak a megszerzésének a célja, hogy azokat különböző internetes Darknet fórumokon értékesítsék, amelyekre igen nagy kereslet van. Erre tekintettel az elektronikus adatok esetén az átadás és a megszerzés a tudomásra hozatallal, vagy más módon történő rendelkezésre bocsátással már tényállásszerű lehet, nem szükséges hozzá a birtokbavétel.[300] Az elvétel esetén pedig a bűncselekmény befejezetté válásához nincs szükség további elkövetési magatartásra, így a tartós birtokba helyezkedésre vagy annak szándékára, valamint pénzfelvétel megkísérlésére.[301] Ha a készpénz-helyettesítő fizetési eszközzel visszaélést bűnszövetségben vagy üzletszerűen követik, akkor a bűncselekmény minősített esete valósul meg és a büntetési tétel az alapesetben meghatározott egy évi szabadságvesztéshez képest három évre emelkedik. Bűnösséget tekintve, a bűncselekmény elkövethető egyenes, illetve eshetőleges szándékkal is. Nem valósul meg azonban bűncselekmény, ha az elkövető jogszerűen van az elkövetési tárgy birtokában, valamint a lejárt érvényességű bankkártya nem lehet az elkövetési tárgya.[302] A készpénz-helyettesítő fizetési eszközzel visszaélés immateriális bűncselekménynek minősül, a tényállás eredményt a korábbi szabályozástól eltérően már nem értékel. Amennyiben károkozás is történik, akkor az információs rendszer felhasználásával elkövetett csalás miatt vonható felelősségre az illető.

[299] MOLNÁR (2018): i.m. 764. o.
[300] MOLNÁR (2018): i.m. 766. o.
[301] BH 2017.177.
[302] BH 2009.349.

A következőkben a card-not-present csalás esetével foglalkozom. Ennek esetén a bankkártya fizikailag nincs jelen az elkövetéskor, így az offline fizetésnél használt védelmek sincsenek biztosítva, mint az aláírás, a PIN-kód és a chip technológia. Példaként említhetők a különböző internetes csalások, amelyek között gyakori elkövetési módszerként jelennek meg a megtévesztésen alapuló különféle adathalász technikák, ál-oldalak használatai, amelyekkel viszonylag alacsony kockázat mellett magas profitot lehet elérni. Ezeket a módszereket az internetes vásárlók megtévesztésére egyaránt használják.

A phishing továbbra is népszerű módja az érzékeny adatok – például jelszavak, bankkártyaszámok – megszerzésének, sőt ahogy már korábban említettem gyakran arra is használják, hogy kártékony programokat juttassanak el a magánkézben lévő eszközökre, valamint vállalati rendszerekre. A botnetek képesek nagy mennyiségű személyes vagy egyéb titkos adat megszerzésére. Általában jól ismert bankok, pénzintézetek – vagy cégek, szolgáltatók, sőt akár állami szervek – nevében küldenek e-mail üzeneteket, amelyekben azt kérik a felhasználótól, hogy lépjen be elektronikus úton fiókjába vagy a bankkártya adatait adja meg adategyeztetés céljából. A levél általában egy linket is tartalmaz, hogy az áldozat könnyebben eljuthasson a honlapra. Azonban ez nem a bank vagy cég valódi weboldalára mutat, hanem egy ahhoz kísértetiesen hasonlító – esetleg kívülről nem is megkülönböztethető – ál-honlapra, amely többnyire a botnet valamely tagján fut. Ez történhet még az ún. pharming adathalász módszerrel is, amely esetén ugyancsak egy csalárd módon felépített honlapot használ az elkövető az adatok megszerzésére, azonban ennél egy rosszindulatú szoftver vagy kémszoftver segítségével az eredeti lapról egy másik, hamisított weblapra téríti el a felhasználót. Ha a gyanútlan felhasználó ezeken keresztül bejelentkezik, akkor a felhasználói neve és jelszava máris az adathalászoknak az adatbázisába kerül. Ezt követően gyakran a bankszámlán található összegeket rövid időn belül más számlákra utalják tovább. A bankkártya adatok megadását követően pedig az elkövetők már rendelkezhetnek is ezekkel.

Másik módszer az ún. VoIP (Voice over IP), avagy vishing csalás, amikor IP-alapú telefont, hangüzenetküldő eszközt használnak, és az elkövetők arra vesznek rá mást, hogy adja meg személyes, pénzügyi vagy biztonsági adatait, vagy utaljon pénzt nekik (pl. megkérik arra, hogy adategyeztetési célból közölje a bankkártya adatait, mert letiltották azt és újra aktiválni kell).

Előbbi esetben, ha csak a belépési adatokat szerzik meg, akkor a már korábban részletesen vizsgált információs rendszer felhasználásával elkövetett csalás 375. § (1) bekezdése szerinti károkozó adatvisszaélés alakzata valósul meg, míg az utóbbi két esetben az (5) bekezdésben szabályozott elektronikus készpénz-helyettesítő fizetési eszközzel való visszaélés alakzata, amely esetén az elkövető a jogosulatlanul megszerzett ilyen eszköz felhasználásával okoz kárt.

A „jogosulatlan használatot” úgy kell érteni, hogy az valamely személy azon cselekményét jelenti, hogy a rá bízott elektronikus készpénz-helyettesítő fizetési eszközt jogosulatlanul és tudatosan saját vagy más személy javára használja fel. Ugyanez vonatkozik a hamis, hamisított bankkártyákra, valamint a jogalkotó büntetendővé tette az ilyen eszközökkel történő fizetés szándékos elfogadásával megvalósuló károkozásra is.

Ha a készpénz-helyettesítő fizetési eszköz jogosulatlan megszerzését követően annak jogtalan haszonszerzést célzó felhasználására is sor kerül, akkor nem a készpénz-helyettesítő fizetési eszközzel visszaélés, hanem – látszólagos anyagi halmazat folytán – csak az információs rendszer felhasználásával elkövetett csalás állapítható meg.[303] Ezzel szemben a készpénz-helyettesítő fizetési eszköz hamisítása nem szükségszerű eszközcselekménye a 375. § (5) bekezdésébe ütköző csalási cselekménynek, ezért egymással valóságos anyagi halmazatban állnak.[304]

Érdemes megjegyezni, hogy a pénzintézetek ért támadásokat magas látencia jellemzi, mert az ezek által okozott kár általában kisebb a jóhírnevükben bekövetkezhető hátrányokhoz képest. Ezért általában ellenérdekűek a nyomozó hatóságok törekvéseivel.[305] Az ügyfeleik kárát általában megtérítik, és ezáltal valóban ők lesznek a károsultak. Ezt a Legfelsőbb Bíróság is kimondta döntésében, hogy a bankkártya visszaélések tényleges károsultjai – és így a sértettjei – a bankkártyákat kibocsátó pénzintézetek.

A 2019-es irányelv is rögzíti, hogy számos esetben bűncselekmény áll olyan kiberbiztonsági események hátterében, amelyekről - a NIS irányelv értelmében - értesíteni kell a releváns illetékes nemzeti hatóságokat. Az ilyen események tekintetében fennállhat az a gyanú, hogy azok bűnügyi jellegűek, még ha esetleg az adott ügy szakaszban nincs is elegendő bizonyíték annak megállapításához, hogy bűncselekmény történt. Ebben az összefüggésben az alapvető szolgáltatásokat nyújtó érintett gazdasági szereplőket és digitális szolgáltatókat – amely körbe tartoznak például a pénzintézetek is – arra kell ösztönözni, hogy a NIS irányelvben előírt jelentéseket osszák meg a bűnüldöző hatóságokkal annak érdekében, hogy hatékonyan és átfogó módon lehessen reagálni az ilyen típusú visszaélésekre, valamint az elkövetők cselekményeikért való felelősségre vonását segítse. Ezenkívül a számítógép-biztonsági eseményekre reagáló csoportokat is be kell vonni a bűnüldöző hatóságok általi nyomozásokba, akik ezáltal tájékoztatást és szakértői segítséget tudnak nyújtani.

[303] BH 2015.244.
[304] MOLNÁR (2018): i.m. 765. o.
[305] NAGY Zoltán András: A számítógépes környezetben elkövetett bűncselekmények kriminológiai aspektusairól. In: Gál István – Nagy Zoltán András (szerk.): Az informatika és a büntetőjog. Pécs, 2006. 158. o.

Végül fontos még a fizetési csalásokról szólni, amelyek ugyan nem a bankkártyákkal, de a banki utalásokkal függnek össze. Az adathalászat körében előfordul az a módszer is, hogy megadott bankszámlaszámra kérnek meghatározott összegű utalást, például a szolgáltatónál vagy adóhatóságnál esedékes díjat, illetve tartozását egyenlítse ki az ügyfél.

Az egyik legveszélyesebb támadási forma a célzott adathalászat, amely hasonló elgondolás mentén működik, mint a hagyományos formája, de azzal a különbséggel, hogy nem tömegesen kerülnek kiküldésre a levelek, hanem célirányosan, meghatározott kisszámú személy részére. A leveleket mind tartalmilag, mind formailag is úgy hozzák létre, hogy azoknak az egyedi vonásaik ne keltsenek gyanút. A támadást mindig megelőzi a kiszemelt célpontoknak a tanulmányozása (pl. munkahelyüket, viselkedésüket, szervezeti struktúrát előzetesen felmérik). Gyakran az elkövetők a cég vezetőjének adják ki magukat – innen a CEO-csalás elnevezés is – és a pénzügyekért felelős személynek (pl. pénzügyi kontrollernek vagy könyvelőnek) e-mailt küldenek, amelyben kérik, hogy egy sürgős banki tranzakciót hajtson végre. Ezt pedig követhetik további levelek vagy akár telefonhívások, amelyekben megerősítik a tranzakció iránti igényt úgy, hogy a felek magukat például megbízható üzleti partnernek vagy ügyvédnek mutatják be. A kérés sokszor jól időzített, mert a hivatali órák végén történik, amikor már nehéz további megerősítést kérni. A másik eset, ha nyilvánosan bejelentett eseménykor kerül sor a támadásra (pl. vállalati fúziók esetén), amikor a szervezeten belül bizonytalanság állhat fenn. Az ún. whaling során pedig a célpontok a szervezet vezetői.[306] Ezek az említett esetek mind a hagyományos értelemben vett, Btk. 373. §-a szerinti csalásnak minősülnek.

Érdekességként megemlítem, azt a hasonló ügyet, amelyben a Készenléti Rendőrség irányítása alá tartozó Nemzeti Nyomozó Iroda rendelt el nyomozást. Az ügy azzal indult, hogy Robert Bosch Elektronikai Kft. feljelentést tett, mert ismeretlen személy vagy személyek a vállalat üzleti partnere, a KCE Singapore Ltd. képviselőjének nevében elektronikus levélben kérték a cég pénzügyi ügyintézőjét, hogy a felek között fennálló beszállítói szerződés alapján esedékes számlák ellenértékét a megszokottól eltérő számlaszámra utalják, mivel a cég folyamatban lévő auditálása miatt a számla kezelése bizonytalanná vált. Az ügyintéző a kérésnek megfelelően tíz utalást indított a megadott számlaszámra közel 2,2 millió dollár értékben. Az ügyben feltárták, hogy mindkét cégnek a rendszerét feltörték és onnan szerezték meg a szükséges adatokat, több postafiókot is lemásoltak, valamint a levelezésekhez is hozzáfértek. A megadott bankszámlaszámot egy Lengyelországban működő bank vezette és egy fiktív lengyel cég nevén volt, amelyet a jogsegélykérelemnek köszönhetően a hatóságok

[306] EUROPOL (2016): i.m. 32. o.

zároltak. Az e-mail nyomozás során tett elemzés nem vezetett eredményre, mert ezt olyan kanadai cégnél regisztrálták, amelynek a szerverszolgáltatója az Egyesült Államokban van bejegyezve. Az e-mail feladója közvetlenül nem volt azonosítható, mert az üzenet egy külső szerveren keresztül, átirányítás útján került a címzetthez. Lengyelországban és az Egyesült Királyságban is tettek feljelentést olyan csalások miatt, amelyek összefüggésbe hozhatók az érintett lengyel céggel.[307]

[307] Ez az átatuláshoz kapcsolódó csalás az angolszász rendvédelmi terminológiában „E-mail Business Compromise" elnevezéssel jelenik meg. Az említett esetről részletesen írt NAGY Tamás: Business E-mail Compromise, avagy az átutalásokhoz kapcsolódó csalások. Belügyi Szemle 2018/7-8. 66-82. o.; Az ilyen típusú támadások rendkívül nagy veszteséggel járnak, ezt erősíti meg az FBI jelentése is, amely szerint: 2016-ban 360 millió dollár értékű kárt okoztak, míg 2017-ben 675 millió dollár értékben. Lásd U.S. Department of Justice: Report of the Attorney General's Cyber Digital Task Force. Washington, 2018. 36. o.

2. A szervezett bűnözés az interneten

2.1. Bevezetés

Az internet vonzó környezetté vált a különböző profit-orientált bűnelkövetők számára. Különösen, azért mert átível a határokon, akár magas fokú anonimitást biztosít és arra sincs szükségük, hogy az egyes bűncselekmények elkövetésekor fizikailag jelen legyenek, ezért a kockázat minimalizálása mellett jelentős profitra tudnak szert tenni.[308] Ez még kedvezőbb számukra akkor, ha olyan országokból tudják működtetni a bűnözői infrastruktúrájukat, ahol nem biztosított a megfelelő jogszabályi háttér és technológiai kapacitás sem ahhoz, hogy hatékonyan feltudjanak lépni például a kiberbűncselekményekkel szemben.

A modern technológiákat kihasználó elkövetők által elkövetett bűncselekményeket két csoportra lehet osztani: egyrészt vannak az olyan büntetendő magatartások, amelyek korábban is léteztek, de a kapcsolattartási és más lehetőségek jobban elősegítik azok terjedését, így akár nagyságrendileg is növelve a társadalmi veszélyességüket. Ide sorolhatók mindenekelőtt a szervezett bűnözés hagyományos „üzletágai" (pl. kábítószer-kereskedelem). Másrészről vannak azok, amelyek a már említett módon a technikai vívmányok nélkül nem is léteznének, mint például a kiberbűncselekmények.[309]

Kétségtelen tény, hogy a hagyományos szervezett bűnözői csoportok számára is kedvezővé vált az ICT használata, azonban az kérdéses, hogy milyen mértékben terjed ki a tevékenységi körük például a kiberbűnözésre. Emellett jellemző rájuk, hogy már a feketegazdaságban[310] fejtik ki a különféle illegális tevékenységüket - amelyet a kereslet-kínálat törvénye határoz meg -, és ezt is megkönnyíti számukra, hogy a valós téren kívül már a digitális platformokon keresztül is folytathatják ezt. Nem véletlen, hogy a szervezett bűnözés motorját napjainkban már az illegális online kereskedelem jelenti. A szervezett bűnözés és a kiberbűnözéssel kapcsolatban két dolog megállapítására törekszem, hogy:

- az internet egy új színteret jelent-e a tradicionális szervezett bűnözői csoportok számára a különböző illegális tevékenységük folytatásához, valamint

[308] GYARAKI: i.m. 235. o.
[309] KORINEK László: A technika fejlődése és a bűnözés. In: Borbíró Andrea - Inzelt Éva - Kerezsi Klára - Lévay Miklós - Podoletz Léna (szerk.): A büntető hatalom korlátainak megtartása: A büntetés mint végső eszköz - Tanulmányok Gönczöl Katalin tiszteletére. ELTE Eötvös Kiadó. Budapest, 2014. 290. o.
[310] TÓTH Mihály: A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése. MTA Law Working Papers 2015/4. 5. o.: „A feketegazdaság - szűkebb, vagy tágabb értelemben - elsősorban a legális gazdasági szférán kívüli tevékenységre, a követhetetlenségre, ellenőrizhetetlenségre, (vagy konkrétabban az adózatlanságra) utal, és a gondok alapvető forrásának a láthatatlan jövedelmek képződését tartja."

- ez lehetőséget teremt-e az új típusú, „szervezett” kiberbűnözői csoportok működéséhez, amelyek kifejezetten a kiberbűncselekmények elkövetésére specializálódnak.

2.2. A szervezett bűnözés fogalma és a hazai szabályozása

A szervezett bűnözői csoportok működését és értékrendjét meghatározzák azok az adott országok, társadalmak, illetve kultúrák, amelyekben illegális tevékenységüket kifejtik, így különösen hatással van a szerveződésükre az adott földrajzi és politikai helyzet, a kriminális tradíció – mint az illegális igények – és a bűnüldözés felépítése, valamint annak hatékonysága.[311] A társadalmak Európa-szerte egyre inkább egymással összekapcsoltabbá, illetve nemzetközi jellegűvé váltak, ami ugyanígy a szervezett bűnözés működésére is jellemző, hogy összekapcsoltabbá és nemzetközileg aktívabbá vált mint valaha.

A szervezett bűnözői csoportok tevékenységi és működési köre („üzleti portfoliója”) egyre változatosabb, bár a kábítószer-kereskedelem továbbra is a legjövedelmezőbb tevékenységnek számít, emellett azonban jellemző, hogy foglalkoznak még fegyverkereskedelemmel, embercsempészéssel, termékhamisításokkal és a kiberbűnözéssel is, amelyeket járulékosan a pénzmosás követ.[312]

Jellemzően a nagyobb „tradicionális”, hierarchikus szervezett csoportok mellett a kisebb és lazább szerkezetű csoportok jelentek meg, amelyeket sok esetben megbízott, speciális szaktudással rendelkező személyek erősítenek ad hoc jelleggel. Az is előfordul, hogy az egyes csoportok csak rövid időre alakulnak egy meghatározott illegális tevékenység elvégzéséig. Az Europol jelentése szerint jelenleg 5000 szervezett bűnözői csoport működik nemzetközi szinten, míg 2013-ban csak 3600 ilyen csoportról számoltak be. A növekedés köszönhető a kisebb bűnözői csoportok megjelenésének, különösen az ún. bűnözői piacok (criminal market) népszerűségének, amelyeknek a működése és az alapjukat képező üzleti modell erősen függ az internettől. Ezen piacok fragmentáltsága, különösen a kiberbűnözéssel kapcsolatban figyelhető meg, mert ezeken növekvő számban önálló, illegális vállalkozást folytató elkövetők vannak jelen, vagy akár többen alkalmi jelleggel fognak össze. Ez a tevékenységi kör általában az illegális árucikkekkel való kereskedést, vagy különféle szolgáltatások nyújtását foglalja magában.[313]

---

[311] TÓTH Mihály – KŐHALMI László: A szervezett bűnözés. In: Borbíró Andrea - Gönczöl Katalin - Kerezsi Klára - Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016. 608. o.
[312] ABADINSKY, Howard: Organized crime. Ninth Edition, Wadsworth Cengage Learning, 2010. 203. o.
[313] EUROPOL: European Union Serious and Organised Crime Threat Assessment (SOCTA) – Crime in the age of technology. 2017. 14. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [2018.03.21.]

Korinek László szerint – kriminológiai aspektusból vizsgálva – a szervezett bűnözést a következő ismérvek határozzák meg:

- a hatályos jogszabályok szerint tiltott szükségletek kielégítésére irányul,
- a lehető legkisebb kockázatvállalás mellett a leggyorsabb és lehető legnagyobb profitra törekvés jellemzi,
- a bűnözői csoportokon belül szakosodás, specializáció figyelhető meg,
- a szervezett bűnöző tevékenységét foglalkozásként űzi,
- jellemző az erőszak a bűnözőtársulás tevékenysége során,
- megfigyelhető a legális és illegális tevékenységek egyidejű jelenléte,
- a tevékenység nemzetközi, határokon átnyúló jellegű.[314]

2000 óta a Palermói Egyezmény[315] határozza meg a nemzetközi fogalmát a szervezett bűnözői csoportnak, amely értelmében bizonyos ideig fennálló, három vagy több főből álló strukturált csoportról van szó, amely összehangoltan működik egy vagy több, az egyezményben meghatározott súlyos bűncselekmény elkövetése céljából, közvetlen vagy közvetett módon pénzügyi vagy más anyagi haszon megszerzésére törekedve. A strukturált csoport nem egyetlen bűncselekmény azonnali végrehajtására, valamint nem alkalomszerűen létrehozott csoport. Nem szükséges, hogy tagjai pontosan meghatározott szerepekkel rendelkezzenek vagy, hogy tagsága állandó legyen, illetve, hogy fejlett hierarchiával rendelkezzen. Az egyezmény definiálja továbbá a súlyos bűncselekményt is, melynek értelmében legalább négy év szabadságvesztéssel vagy súlyosabb büntetéssel büntethető bűncselekményt megvalósító magatartást jelenti.

Uniós szinten a tagállamok a büntető anyagi jogszabályainak harmonizálása érdekében egy kerethatározatot[316] fogadtak el, amely az egyezmény alapján rögzíti a bűnszervezet fogalmát mint „olyan, kettőnél több személyből álló, hosszabb időre létrejött szervezett csoport, amely összehangoltan működik, és amelynek célja az, hogy legalább négy évig terjedő szabadságvesztéssel vagy szabadságelvonással járó intézkedéssel vagy annál szigorúbb szankcióval büntetendő bűncselekményeket kövessen el közvetlen vagy közvetett pénzügyi vagy egyéb anyagi haszonszerzés érdekében.” A szervezett csoport nem lehet valamely bűncselekmény elkövetésére véletlenszerűen létrehozott, és nem szükségszerű, hogy a

[314] KORINEK László: A szervezett bűnözés lényegi elemei. In: Harmadik Magyar Jogászgyűlés – Magyar Jogász Egylet. Budapest, 1996. 65-72. o.
[315] Az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény, amelyet a 2006. évi CI. törvénnyel hirdetettek ki Magyarországon
[316] A Tanács 2008/841/IB kerethatározata (2008. október 24.) a szervezett bűnözés elleni küzdelemről. HL L 300/42. 2018.11.11.

tagoknak formálisan meghatározott szerepe legyen, állandó tagsági összetétellel, illetve kidolgozott szervezeti felépítéssel rendelkezzen.

A nemzetközi elvárásoknak megfelelően ezt a definíciót vette át Magyarország is. Ennek fényében a 2002 óta a Btk.) 459. § (1) bekezdés 1. pontja a következőképpen határozta meg a bűnszervezet fogalmát, „amely három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekmények elkövetése."

2019-ben azonban ennek a fogalomnak a szűkítésére került sor, amelyet a költségvetési törvény[317] módosított. Ennek következtében többletfeltételek fennállásának bizonyítása szükséges a bűnszervezet megállapításához, a továbbiakban már nem az „összehangoltan működő csoport", hanem kizárólag a „hierarchikusan szervezett, konspiratívan működő csoport" esetén van erre lehetőség.

Az említett bekezdés 2. pontjában foglalt értelmező rendelkezés a bűnszövetséget is definiálja, amely akkor létesül, „ha két vagy több személy bűncselekményeket szervezetten követ el, vagy ebben megállapodik, és legalább egy bűncselekmény elkövetését megkísérlik, de nem jön létre bűnszervezet." E fogalomnak a negatív eleme, hogy nem jöhet létre bűnszervezet.[318]

A következőkben részletesen áttekintem a bűnszervezet fogalmi ismérveit. Az eddigi szabályozás az "összehangolt működést" írta elő, amely tartalmát tekintve nem mást jelentett, mint a benne cselekvő személyek egymást erősítő hatása. Ezt azonban új törvényi kritériumoknak az együttes megléte váltja fel, így a hierarchikus felépítés és a konspiratív kapcsolatrendszer. Az alá-fölérendeltségnek a követelménye a bűnszervezet oldaláról vizsgálandó. A konspiráció jellemzője, hogy nem feltétele a bűnszervezetben cselekvők közvetlen kapcsolata, a más cselekvések, illetve a más cselekvők kilétének konkrét ismerete. A bűnszervezeten belüli személyes ismeretség valamennyi elkövetővel nem feltétele a megállapításának.[319] Hiszen a bűnszervezet létrejöhet úgyis, hogy a keretében bűncselekményeket irányító vagy vezető személy hangolja össze azoknak az elkövetőknek a magatartását, akik egymás tevékenységéről nem is tudnak.[320] A hierarchikus szervezetben a

[317] 2019. évi LXVI. törvény Magyarország 2020. évi központi költségvetésének megalapozásáról 107. §.
[318] Lásd bővebben GELLÉR - AMBRUS: i.m. 410-425. o.
[319] BH 2016.9.234.
[320] CSÁK Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018. 328-329. o.

bűnszervezet vezetője, amennyiben nem valósít meg tetteti magatartást, akkor felbujtóként tartozik felelősséggel a bűnszervezet tagjai által elkövetett bűncselekményekért.[321]

A bűnözői csoportok konspirációs szabályok szerint tevékenykednek. Ezért előfordulhat, hogy valaki úgy kapcsolódik be a csoport működésébe, hogy csak – eseti jelleggel – egyetlen cselekményt valósít meg tettesként vagy részesként, mégis a bűnszervezetben elkövetés megállapítható vele szemben, mert nem az alanyi bűnösség, hanem a bűnszervezet fogalmi elemei megállapításának kérdése a "hosszabb időre szervezett" kitétel, amely a több bűncselekmény rendszeres jellegű elkövetését jelenti, de a bűnszervezet oldalán kell fennállnia. Az elkövető tudatának továbbá nem arra kell kiterjednie, hogy egy bűnszervezet a törvényi előfeltételek szerint létrejött, hanem arra, hogy a bűnszervezet tárgyi sajátosságai ismeretében annak "működéséhez" csatlakozik, illetve annak keretében cselekszik. A Btk. rendelkezései nem tesznek különbséget a bűnszervezeten belüli cselekvés hiearchiája ("posztjai"), aktivitása, intenzitása szempontjából, ezek a büntetéskiszabás körében értékelendő körülmények.[322] A bűnszervezet megállapításához nem többletkövetelmény a bűnös profitszerzési célzat.[323]

A bűnszervezetben elkövetésre vont jogkövetkeztetésnek van helye – az egyéb törvényi feltételek megléte esetén –, ha az elkövetési magatartások egymást kiegészítő jellegűek, azok kapcsolódása a célzott és végrehajtott bűncselekményhez kölcsönös, az adott tényállásszerű elkövetési magatartás keretei közé illeszkedő cselekmény más személy előző cselekményéhez társul, avagy a célzott bűncselekmény megvalósulásához további láncolatos tevékenységet feltételez.[324] A bűnszervezet fogalmának utolsó objektív ismérve egy szervezeti célt határoz meg, amely szerint a bűnszervezet létének nem törvényi előfeltétele akár egyetlen bűncselekmény befejezett elkövetése vagy kísérlete sem. A Btk. nem sorolja fel, hogy milyen típusú bűncselekmények tartoznak ide csak annyit, hogy ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekményekről lehet szó. Ezzel kapcsolatban felmerül az a kérdés, hogy mindez azokra a bűnszervezetekre hogyan alkalmazható és miképpen minősíthető a szervezet működésébe becsatlakozó elkövetők magatartása, akik kihasználják az internet nyújtotta előnyöket és például az illegális tevékenységüket az online piacterekre kiterjesztve folytatják (pl. kábítószer-kereskedelem, gyermekpornográf tartalmak terjesztése stb.).

[321] EBH 2008.1849.
[322] 4/2005. számú BJE határozat; TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009. 148-151. o.
[323] BH 2008.139.
[324] BH 2018.4.106.

Mindezekre tekintettel azon az álláspontom vagyok, hogy amennyiben megvalósulnak a bűnszervezetnek a törvényi feltételei és az elkövető tudata át fogja azt, hogy bűnszervezethez kapcsolódva cselekszik – akár legyen szó csak egyszeri alkalomról –, akkor a bűnszervezetben történő elkövetés megállapítható, feltéve, ha az általa kapcsolódó bűncselekmény ötévi vagy súlyosabb szabadságvesztéssel büntetendő. Ugyanez vonatkozik a tetteseken kívül a részesekre is, tehát amennyiben a szükséges feltételek teljesülnek, akkor az esetükben is a bűnszervezetben elkövetésről van szó.[325] Ezt erősíti a Kúria egyik eseti döntése is, amelyben kimondta, hogy a bűnszervezettel kapcsolatban elsődlegesen mindig a bűncselekmény elkövetését kell vizsgálni, majd az alanyi oldalt, az elkövető tudattartalmát, hogy felismerte-e, hogy az elkövetési magatartását a bűnszervezet keretén belül valósította meg. A törvény a bűnszervezet külső, tárgyi jellegű ismérveit határozza meg, ezért fontos, hogy ez a kívülálló számára is felismerhető legyen.[326]

Mindezt figyelembe véve a tudattartalom vizsgálatának körültekintően kell történnie, és ezzel párhuzamosan vizsgálni kell a büntetőeljárás során feltárt bizonyítási eszközökből származó, és a bűnszervezet fennállásának megállapításához szükséges ismérvekre következtetést megalapozó bizonyítékokat, és erre nézve a tényállásban megállapítást kell tenni.[327]

Amennyiben nem éri el a meghatározott büntethetőséget az elkövető cselekménye, akkor súlyosító körülményként értékelhető és nem alkalmazhatók a bűnszervezeti elkövetéshez kapcsolódó jogkövetkezmények. Más kérdés, ha például az elkövető cselekményei több részcselekményből tevődnek össze, ugyanakkor a természetes egységbe vagy a folytatólagosság egységébe olvadnak, és amely a szervezetbe tartozó tag esetében eléri az ötévi fenyegetettséget, akkor a joggyakorlat ebben az esetben megfontolandónak tartja annak megállapítását, hogy a bűnszervezet törvényi feltételei fennállnak. Azonban a szakirodalombam eltérő álláspont is található, amely szerint a bűnszervezeti elkövetés célja bűncselekmények elkövetése, a többes szám pedig egység-többségtani szempontból bűncselekményi többségre, egy eljárásban történő elbírálás esetén pedig bűnhalmazat fennállására enged következtetni. A nyelvtani értelmezés alapján a bűnszervezet hatókörének kiterjesztése aggályos lehet. Hasonlóan alakul a törvényi egység más esetkörei vagy a látszólagos halmazat esetén.[328] Ez alapján legalább két bűncselekmény szükséges a

[325] BH 2010.11.472.
[326] BH 2016.9.234.
[327] BH 2014.131.
[328] AMBRUS István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014. 20. o.

bűnszervezeti fogalom teljességéhez, amelybe beleértendő a joggyakorlat szerint a ténylegesen elkövetett és tervezett cselekmény is. Érdemes ezzel kapcsolatban a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének deliktumával foglalkozni, mert a Btk. hatályba lépését követően már nem a sértettek számához igazodik, hanem törvényi egység jön létre[329], azaz a sértettek számától függetlenül egy rendbeli cselekmény megállapítására van lehetőség egyéb feltételek megvalósulása esetén. Az egyik eseti döntésben a törvényszék azt az álláspontot alakította ki a nyelvtani, szöveg hű értelmezést alkalmazva, miszerint egy rendbeli összefoglalt bűncselekmény esetén nem lehet bűncselekményekről beszélni, ami a bűnszervezet meglétének egyik ismérve.[330]

Összességében elmondható, hogy a bűnszervezet fogalmába korábban a bűnöző célzatú tartós struktúrák számos formája volt beilleszthető, amely alkalmas lehetett arra, hogy egyrészről kifejezze az alkalmi kisebb súlyú bűnszövetséghez viszonyított többletkriminalitást, másrészről magában foglalja a szervezettség súlyosabb formájában rejlő veszélyességet is. Ez azonban a módosítás következtében már szűkíti a kört, mert kizárólag a hierarchikus szervezettséggel rendelkező csoportok tartoznak ide.

A bűnszervezet keretében történő elkövetéshez bármely szándékos bűncselekmény esetén súlyos általános részi jogkövetkezmények[331] társulnak - mivel a hatályos szabályok szerint általános jellegű minősítő körülmény -, míg a bűnszövetség esetében a bűncselekmény súlya közömbös, de csak akkor állapítható meg, ha a Különös Részben minősítő körülményként szerepel.[332]

A Btk. 321.§ (1) bekezdése szerint bűnszervezetben részvétel bűntette miatt büntetendő, aki bűncselekmény bűnszervezetben történő elkövetésére felhív, ajánlkozik, vállalkozik, a közös

---

[329] OTT István: Dogmatikai kérdések a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye kapcsán. Magyar Jog 2016/12., 717-721. o.

[330] Balassagyarmati Törvényszék B.210/2014/127.

[331] Azzal szemben, aki a szándékos bűncselekményt bűnszervezetben követte el, a bűncselekmény büntetési tételének felső határa a kétszeresére emelkedik, de a huszonöt évet nem haladhatja meg. Halmazati büntetés esetén a 81. § (3) bekezdése szerinti büntetési tételt, tárgyalásról lemondás esetén a 83. § (1)–(2) bekezdése szerinti büntetési tételt kell alapul venni. [91. § (1) bek.];
Azzal szemben, aki a bűncselekményt bűnszervezetben követte el, mellékbüntetésként kitiltásnak is helye van. [91. § (2) bek.];
A kétévi vagy ennél hosszabb tartamú szabadságvesztést fegyházban kell végrehajtani [37. § (2) bek. bb) pont];
A feltételes szabadságra bocsátás kizárt [38. § (4) bek. c) pont];
A végleges hatályú foglalkozástól eltiltás alól a bíróság az eltiltottat nem mentesítheti, ha az eltiltás méltatlanság okán, véglegesen történt [Btk. 53. § (4) bek.];
A bűncselekmény eszközének és tárgyának elkobzása méltányosságból nem mellőzhető [73. § b) pont.];
A bűnszervezet ideje alatt szerzett vagyont az ellenkező bizonyításáig elkobzás alá eső vagyonnak kell tekinteni [74. § (4) bek. a) pont];
A büntetés végrehajtásának felfüggesztése kizárt [86. § (1) bek. b) pont];
A tevékeny megbánás (közvetítői eljárás) kizárt [29. § (3) bek. b) pont].

[332] TÓTH Mihály: A bűnszervezeti elkövetés szabályozásának kanyargós útja. Magyar Jog 2015/1. 5-6. o.

elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja, illetve a bűnszervezet tevékenységét egyéb módon támogatja. A tényállás kétfajta elkövetési magatartástípust rendel büntetni: egyrészt a sui generis előkészületi bűncselekményt, azzal, hogy bár eltérő sorrendben, de az előkészület fogalmát alkotó magatartásokat jelöl meg; másrészt sui generis bűnsegélyt azzal, hogy azt, aki - mint a bűnszervezeten kívülálló személy - a bűnszervezet tevékenységét támogatja büntetni rendeli. Az elkövetési magatartások a bűncselekmény bűnszervezetben történő elkövetéséhez kapcsolódnak és amennyiben, aki az előkészületi jellegű magatartását tovább folytatva saját maga is bekapcsolódik a szervezet tevékenységébe, és azt a magatartást, amelyre felhívott stb. megkísérli vagy annak megvalósításában tettesként közreműködik, értelemszerűen a bűnszervezetben elkövetett bűncselekmény tetteseként fog felelni. A Btk. Kommentárja azt rögzíti, hogy a bűnszervezet tevékenységének "egyéb módon támogatása" csak a szervezeten kívül álló személy részéről valósítható meg, és feltételezi a bűnszervezet létezését. E fordulat elkövetőinek a cselekménye nem közvetlenül a bűnszervezetben elkövetett bűncselekményhez, hanem magához a bűnszervezet működéséhez kapcsolódik és tisztában kell lenniük azzal, hogy akár anyagi vagy más természetű támogatással a súlyos bűncselekmények elkövetésére létrejött csoportosulás tevékenységét előmozdítják anélkül, hogy a bűnszervezetben elkövetett bármely bűncselekményhez segítséget nyújtanának.[333] Tóth Mihály vitathatónak tartja a lehetséges alanyok szűkítését, mert indokolatlanul privilegizált helyzetet teremt azoknak a csoport-tagoknak, akik a tudatos csatlakozáson kívül akár rendszeres finanszírozással vagy öt évet meg nem haladó büntethetőségű bűncselekményekkel támogatják a bűnös tevékenység előkészítését. Nem világos, hogy miért kellene a lehetséges alanyok körét tekintve különbséget tennünk pl. a bűncselekmény elkövetéséhez szükséges eszközök beszerzésében, rendelkezésre bocsátásában testet öltő magatartás és az anyagi eszközök rendelkezésre bocsátása, esetleg a tekintélyen, befolyáson alapuló pszichikai támogatás között.[334]

Ezzel szoros összefügésben érdemes arra kitérni, hogyha egy adott, kívülálló személyt (pl. informatikus szakembert) megbíznak az online bűnözői infrastruktúra kezelésére, annak biztosítására vagy egyéb tevékenységre (pl. rosszindulatú programok készítésére), ami kapcsolódik a szervezet működéséhez – sőt elősegíti azt –, akkor ez hogyan értékelhető. Amennyiben fennállnak a bűnszervezetnek a feltételei és az elkövető a folyamatosan végzett, de ötévi szabadságvesztéssel fenyegetettséget el nem érő cselekményei valós bűnszervezethez

[333] BELEGI József: A közbiztonság elleni bűncselekmények – Btk. XXX. fejezet. In: Kónya István (szerk.): Magyar büntetőjog I-III. – új Btk. – Kommentár a gyakorlat számára. 5. kiadás, HVG Orac Lapkiadó Kft. 2016.
[334] TÓTH (2015): i.m. 7. o.

kapcsolódnak és ezek a súlyos bűncselekmények megvalósulását biztosítják, akkor a bűnszervezetben részvétel bűntettét valósítja meg.

A kiberbűncselekmények vonatkozásában utalnék arra, hogy a 2013-as irányelv is kimondja, hogy helyénvaló súlyosabb szankciókat megállapítani, ha az információs rendszer elleni támadást bűnszervezetben követik el, valamint, ha jelentős számú információs rendszert érint.[335]

2.3. A kiberbűnözői csoportok tipológiája

A kiberbűnözői csoportok tipológiáját Michael McGuire vizsgálta átfogóan, aki a kutatása során az általa feltárt ügyek alapján arra a következtetésre jutott, hogy az informatikai bűnözéssel kapcsolatos esetek 80%-a valamilyen szervezett tevékenység eredménye. Ez azonban nem jelenti azt, hogy az elkövetők a tradicionális és hierarchikus szervezett bűnözői csoportokhoz tartoznának vagy kizárólag kiberbűncselekményeket követnének el. A tanulmányában arra hívja fel a figyelmet, hogy a hagyományos bűnszervezetek egyre inkább kiterjesztik a tevékenységüket az intertre, emellett újabb és kevésbé szoros kapcsolatot ápoló bűnözői csoportok jelennek meg. A bűnözői csoportok különböző szintű szervezettséget mutatnak, attól függően, hogy a tevékenységüket csak a virtuális térben fejtik ki, online eszközöket használnak, hogy lehetővé tegyék a bűncselekmények elkövetését a „való" világban, vagy ezek kombinációja jelenik meg online és offline is.

McGuire egy olyan tipológiát ajánl a kiberbűnözői csoportokkal kapcsolatban, amely hatféle csoport felépítését foglalja magában, kihangsúlyozva, hogy ezek az alapvető szervezeti minták gyakran keresztezik egymást és rendkívül rugalmasan alakulhatnak, akár megtévesztő módon. Felhívja a figyelmet arra is, hogy mindez a folyamatos technológiai fejlődésnek köszönhetően változni fog a jövőben. Három főcsoportot különböztet meg, amelyeket további két alcsoportokra bont a tagok között fennálló kapcsolat erőssége alapján. Az első főcsoport online működik és további két alcsoportra osztható, amelyek a következők: a swarm és a hub.

A swarm egy olyan csoport, amely valamely közös cél érdekében tevékenykedik, irányítás és szervezett működés nélkül. Általában az ideológiai vagy politikai indíttatású csoportok tartoznak ide, amelyek online fejtik ki a tevékenységüket, mint például az Anonymous hacktivista csoport is.

[335] NAGY Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról. http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf [2018.02.28.]

A hub csoportok szintén online működnek, de a swarmhoz képest szervezettebbnek és hierarchikusabbnak tekinthetők, mert „az egyszerű" tagok meghatározott „irányító, létrehozó" kulcstagok köré csoportosulnak. A tevékenységük széleskörű magában foglalhatja a crimeware[336] terjesztést, az adathalász támadásokat és a gyermekpornográfiát. McGuire szerint az online feketepiacok működése illeszkedik ebbe a modellbe.

A második főcsoportba tartoznak azok a hibrid csoportok, amelyek online és offline is jelen vannak. A clustered hybrid esetében egy kisszámú csoportról van szó, amely meghatározott és speciális tevékenységgel foglalkozik. A hub felépítéséhez hasonló, de a különbség az, hogy az online elkövetés mellett az offline is megjelenik, például bankkártyákat skimmelnek, majd az interneten árulják a megszerzett bankkártya adatokat.

Az extended hybrid csoportok kevésbé centralizáltak, általában többen társulnak és kisebb alcsoportokra osztható, de a különféle bűncselekmények elkövetéséhez megfelelő koordinációval rendelkeznek.

A harmadik főcsoport azokat a csoportokat foglalja magában, akik elsősorban offline fejtik ki a tevékenységüket, de egyúttal a modern technológiák és az internet nyújtotta előnyöket is kihasználják már. Hierarchies alatt azokat a tradicionális bűnözői csoportokat értjük, akik illegális tevékenységüket az interneten is kifejtik, ilyenek lehetnek a tradicionális maffia családok, akik például a prostitúcióhoz kapcsolódó tevékenységüket kiterjesztik a pornográf, különösen a gyermekpornográf weboldalakra, illetve online szerencsejáték oldalakat üzemelnek vagy a zsarolást kibertámadások felhasználásával követik el.[337] A nemzetközi szindikátusok is érintettek a kiberbűnözésben, mint például a Triádok vagy Yakuzák, akik szoftverkalózkodással, bankkártya hamisításokkal és csalásokkal is foglalkoznak.[338]

Az aggregate csoportok lazán szervezettek, ad hoc jelleggel működnek. Például mobiltelefonokat használnak a csoport tevékenységének a koordinálásához vagy a nyilvános zavargások szervezéséhez.[339]

A vizsgálatom tárgya szempontjából két csoportot érdemes kiemelni és részletesen ezek összehasonlításával foglalkozom:a hierarchies, azaz a tradicionálisan szervezett bűnözői csoportok és a hub mint az új típusú kiberbűnözői csoport.

---

[336] A crimeware olyan rosszindulatú programokat foglal magában, amikkel az elkövetők célja, hogy haszonra szert tegyenek, ezáltal a felhasználók pénzügyi jólétét vagy értékes információit veszélyeztetik (pl. a vírusok, a trójai vagy keylogger, amik a bűnözői csoportok számára lehetőséget teremtenek az adatok ellopásához, illetve azokkal való kereskedéshez).

[337] MCGUIRE, Michael: Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security. 2012.

[338] KIM-WANG, Raymond – Choo-GRABOSKY, Peter: Cybercrime. In: Paoli, Letizia: The Oxford Handbook of Organized Crime. Oxford University Press, 2014. 485. o.

[339] BROADHURST – GRABOSKY - ALAZAB-CHON: i.m. 7. o.

2.4. A tradicionális szervezett bűnözői csoportok és a kiberbűnözői csoportok összehasonlítása

A tradicionális szervezett bűnözői csoportok általában etnikailag homogének és hierarchikusan strukturáltak, valamint multifunkcionális és bürokratikus bűnözői szervezeteknek tekinthetők. Az összehasonlítás alapját képező másik új típusú csoportosulás pedig az ún. „szervezett" kiberbűnözői csoport, amelynek meghatározására Marie-Helen Malas tett kísérletet: „egy strukturált csoport, amely három vagy több tagból áll, amelynek célja egy vagy több súlyos kiberbűncselekmény anyagi haszonszerzési célú elkövetése az információs rendszerek, illetve az internet felhasználásával".[340]

A kiberbűnözői csoportok fejlődésük során soha nem mentek végbe olyan szintű szervezettségen, mint a hagyományos bűnszervezetek. Az egyéni és fragmentált bűnözői tevékenységek felől mozdultak el a modern vállalati üzleti modellek alkalmazása felé és általában a hierarchikus felépítés hiányzik belőlük. A rugalmas kapcsolatrendszer jellemző rájuk, tagjaik magasan képzett szakemberek és általában a speciális szakismeretüknek, tudásuknak megfelelő feladatot látnak el, amivel hozzájárulnak a különféle crimeware és azokhoz kapcsolódó szolgáltatások fejlesztéséhez.

Míg a tradicionális bűnszervezetek ismérve, hogy erőszakos módon törekednek arra, hogy fenntartsák a monopol helyzetüket a saját területük, illetve érdekeltségük alá vont javak felett. Ennek érdekében lépéseket tesznek, hogy ellenőrzésük alatt tarthassák az általuk dominált piacot. Ez a területi kontroll az interneten nyilván nem kivitelezhető a virtuális környezet sajátosságaiból adódóan, éppen ezért kedvező feltételeket biztosít azok számára is, akik amúgy az adott piacról kiszorulnának. A kontroll mechanizmus érvényesítése továbbá még nehezebbé vált azért, mert a tagok között nincs szükség személyes kapcsolattartásra – sőt általában kizárólag elektronikus csatornákon keresztül kommunikálnak egymással – és a csoport működéséhez nem kellenek a formális szervezeti keretek (pl. a klasszikus hierarchikus szervezeti struktúra nem megfelelő a kiberbűnelkövetők számára). A digitális környezetben működő új típusú bűnözés hasonlóságot mutat a modern vállalati világ vállalkozásaihoz. Erre vonható következtetés, különösen az általuk alkalmazott árazási stratégia, a szolgáltatás-alapú verseny, az innováció és az „ügyfélszolgálat" megjelenése miatt. A kiberbűnözői csoportok ereje a rendelkezésre álló szoftver fejlettségben rejlik, és nem a csoport tagjainak a számában. Az alkalmazott automatizált műveletek nem csak a bűncselekmények elkövetéséhez és az online feketepiacok létrejöttéhez járultak hozzá, hanem a szervezeti struktúrára nézve is

[340] MALAS, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017. 365 o.

meghatározó tényezővé váltak, mert az emberi tényező helyett a technológia került a középpontba.

A kiberbűnözőkre jellemző, hogy egyre nagyobb mértékben veszik át és másolják a legális vállalatok üzleti modelljeit. A 2000-es évek óta fejlesztenek ki olyan üzleti mintákat, amelyek az eBay, Yahoo, Google és az Amazon high-tech cégek által használtakhoz hasonló. A „kiberbűnözői iparágat" már a professzionalitás, kifinomultság határozza meg a különféle kibertámadások terén. Jelen van még specializáció, a munkamegosztás az elkövetők között, valamint jelentős szerepe van a kommercializációnak és az integrációnak is. Utóbbi azt jelenti, hogy az egyes jogsértéseket további jogsértés követi, mint például az adatlopás után eladható a megszerzett adat, majd azt csalásra használhatják fel.

Az vitatott, hogy az informatikai bűnözés által megteremtett üzleti modell és a legálisan működő vállalkozások között milyen eltérések mutatkoznak: míg utóbbi a vásárlók számára az értékteremtést célozza, addig a kiberbűnözés magában foglalja az áldozatok kijátszását a kreatív csalások révén és a kockázat minimalizálását. Azonban, ha az informatikai bűnözést olyan modellnek tekintjük, ami kapcsolatot teremt az illegális eszközök, szolgáltatások „beszállítója" és a vásárlók között, akik ezeket bűncselekmények elkövetésére használják fel az áldozatokkal szemben, akkor ez a különbség nem jelentős, hiszen ez a rendszer is arra összpontosul, hogy értéket teremtsen a „fogyasztói" részére, akik azonban jelen esetben a kiberbűncselekmények elkövetői lesznek.

Az innováció eredményeképpen a bűnözői ökoszisztémában is új minták jelentek meg - amit mindkettő csoport kihasznál - mint például az áruk elhelyezésével, alvállalkozásokkal és kapcsolatépítéssel kapcsolatban. Olyan üzleti modellt alkalmaznak (Criminal-to-Criminal), amely hasonlóságot mutat a jogszerűen működő vállalkozásokéhoz (Business-to-Business), azonban ennek középpontjában az egymás közötti illegális áruk adásvétele és a tiltott szolgáltatások nyújtása áll az informatikai hálózatokon keresztül.[341]

Az automatizáció jelentős szerepet játszik a C2C modellek fejlődésében, mert idő- és költséghatékonyabbá teszi a működésüket. Az automatizált bűnözői tevékenységek alapját a botnet-hálózatok képezik, és a használatuk révén akár nagyszabású támadásokat indíthatnak (pl. a már korábban ismertetett DDoS- támadást), különböző rosszindulatú programokat tudnak terjeszteni, vagy nagy mennyiségű személyes, illetve egyéb bizalmas adatokhoz is hozzájuthatnak a spamküldések és az adathalász technikák alkalmazásával.[342]

[341] TROPINA, Tatiana: The evolving structure of online criminality. eucrim 2012/4. 160-162. o.
[342] TROPINA (2012): i.m. 160. o.

2.5. Specializáció és munkamegosztás

A „kiberbűnözői iparág” széleskörű tevékenységi kört ölelhet fel, amelyben az elkövetők funkcionálisan specializálódnak az egyes feladatokra, tehát jelen van a munkamegosztás. Ez pedig a következőképpen alakulhat:

A programozók azok, akik a különböző rosszindulatú programokat írják meg és egyéb eszközöket rendelkezésre bocsátják, amelyek a bűncselekmények elkövetéséhez szükségesek.

A forgalmazók vagy eladók, akik kereskednek és eladják a lopott adatokat és szavatolják az árukat, amiket mások biztosítanak a számukra.

A technikusok, akik fenntartják a bűnözői infrastruktúrát, a technológiai támogatást biztosítják. mint például a szerverek és a titkosítás zavartalan működését. A gazdagép (host) az a hálózatra csatlakoztatott számítógép, amely az illegális tartalmakat biztosító szervereket és hálózatokat kezeli sokszor botnetek és proxy hálózatok révén.

A hackerek, akik a sebezhetőségeket keresik a rendszerekben, programokban, illetve hálózatokban azzal a céllal, hogy rendszergazda szintű jogosultságot vagy magasabb szintű hozzáférést szerezzenek.

A csalás specialisták pedig különböző social engineering, csalás sémát dolgoznak ki és alkalmazzák azokat, mint például a phishing és a spam küldés is ilyen.

A „pénztárosok” kezelik a bűnös eredetű pénzt és a hozzá tartozó fiókokat, és más bűnözők számára is biztosítják ezeket megfelelő díjazás fejében, továbbá általában ők felügyelik az önálló pénzfutárok (money mule) tevékenységét is.

A pénzfutárok segítenek a bűncselekményekből befolyt bevételeknek az átutalásában harmadik félnek, hogy az további utalással biztonságosan elhelyezze a pénzt. Vannak olyan személyek, akik az átutalásokért és a pénz tisztára mosásáért felelnek digitális valuták és különböző országok pénznemei közötti átváltásokkal.

Végül a végrehajtók azok, akik kiválasztják a célpontokat, toboroznak és kijelölik a tagokat az említett feladatokra, ezen felül pedig a bűncselekményekből származó bevételek elosztásáért felelnek.[343]

2.6. Az online feketepiacterek és fórumok

A kiberbűnözés egy profit-orientált, szolgáltatás-alapú üzleti modellé (Crime-as-a-Service) nőtte ki magát, amely által elérhetővé váltak olyan szolgáltatások a Surface Weben[344] vagy a

[343] https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom [2018.03.05.]
[344] A hagyományos böngészők használatával szabadon elérhető része az internetnek.

Darkneten, amelyekkel kiberbűncselekmények követhetők el. A Darknet egy elosztott, anonimitást biztosító, titkosított hálózat az internet rejtett részén, a Deep Weben belül. Rejtett, mert kizárólag speciális böngésző szoftverek használatával érhető el, mint például ilyen a TOR, I2P vagy Freenet, amelyek magas fokú titkosítással vannak ellátva. A bűnelkövetők kihasználják ezeket, mert a használatuk révén könnyedén eltudják rejteni a személyazonosságukat, vagy éppen az internetes adat forgalmukat és a szerverük helyét.

Ahogy korábban már említettem, ezt az üzleti modellt az önálló kiberbűnözőktől kezdve – akik számára az internet lehetővé teszi a szervezeti kerethez kötöttség nélküli tevékenység végzését – a szervezett kiberbűnözői üzleti társulások vagy akár a tradicionális szervezett bűnözői csoportok is alkalmazhatják. Utóbbiak, amennyiben nem rendelkeznek a szükséges technikai ismeretekkel és eszközökkel, akkor ők is megtudják vásárolni a fórumokon keresztül.

A különböző illegális online tevékenységek megjelenése egy egyre fejlettebb és önálló digitális feketegazdaságot hoztak létre. Ezen belül speciális weboldalakat üzemeltethetnek, ún. online feketepiactereket és fórumokat, amelyek arra használhatók, hogy ezeken keresztül tilalmazott árukkal kereskedjenek és szolgáltatásaikat hirdessék. Ezeket együttesen ún. „hidden services"-nek, azaz rejtett szolgáltatásoknak hívják.

A leghíresebb online feketepiacok a következők voltak: Silk Road[345], Alphabay[346] és Hansa, utóbbi kettő esetén a nemzetközi bűnügyi együttműködésnek köszönhető, hogy a működésüket sikerült leállítani. Mindez az FBI, a Kábítószer-Ellenes Hivatal (Drug Enforcement Agency, DEA), valamint a holland nemzeti rendőrség és az Europol közreműködésével valósult meg.[347]

Érdemes foglalkozni a piacterek és fórumoknak a működésével, mert ezeken gyakran egy merev és egyedülálló struktúra van jelen, ami a kijelölt szerepekkel, feladatmegosztással és az eltérő felelősséggel lehetővé teszi, hogy a tagok hatékonyan biztosítsák a fórum működésének a rendjét. Ezeket a fórumokat az adminisztrátorok irányítják, akik meghatározzák az adott fórum célját és a működéshez szükséges szabályokat. Az alfórumokat pedig moderátorok ellenőrzik, akik az általuk kiválasztott megbízható személyek, gyakran az alfórum témájában jártas szakemberek és ezért annak a tartalmát kezelik. A fórumokon találhatók nagyszámú

[345] 2011 és 2013 között a Silk Roadot Ross William Ulbricht alapította, és mint adminisztátor, Dread Pirate Roberts néven üzemeltette, akit kábítószer-kereskedelem bűnszervezetben történő elkövetéséért, informatikai bűncselekmények bűnsegédjeként, valamint pénzmosásért életfogytiglan szabadságvesztésre ítélték. Az oldal leállítását követően rövid időn belül útjára indult a Silk Road 2.0, és azóta is számos hasonló célból létrehozott online feketepiac található a Dark Weben belül. Lásd United States v. Ulbricht, 31 F. Supp. 3d 540, 569-70 (S.D.N.Y. 2014)

[346] Érdekesség, hogy az Alphabay több mint 200 000 felhasználóval, és ezek között 40 000 eladóval rendelkezett, emellett 250 000 listázott kábítószer és pszichoakítv anyag, valamint több mint 100 000 egyéb illegális termék volt elérhető. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down [2018.08.21.]

[347] U.S. DEPARTMENT OF JUSTICE (2018): i.m. 137-138. o.

eladók is, akik különféle szolgáltatásokat nyújtanak és a termékekkel kereskednek a fórum tagjaival. Az eladói státusz eléréséhez általában próbamintát kell a moderátorok számára nyújtani, akik értékelik azt, majd később a szolgáltatás vagy termék további folyamatos értékelést és pontozást kap a vásárlóktól. Az értékelést és visszajelzést biztosító rendszer hasonló a legális kereskedelmi oldalakéhoz azzal a kivétellel, hogy a bűnözők számára a magas értékelés, vagyis „a jó hírnév" elérése nem olyan egyszerű. Lényegében ezek az online fórumok biztosítják a szükséges logisztikát a felhasználók számára, és a lehetőséget, hogy kiberbűncselekmény elkövetéséhez szükséges ismereteket és eszközöket megszerezhessék.[348]

Az illegális árukkal való kereskedésnek a Darkneten keresztül számos előnye van mind az eladók, mind a vásárlók részéről is. A Peer-to-Peer (P2P) technológiára épülő platformoknak köszönhetően az eladók és a vásárlók is közvetlenül kapcsolatba tudnak lépni egymással, közvetítő nélkül. Mindezt anonim módon tudják intézni, mert egyik félnek sem kell személyes adatot megadnia. A tranzakciók lebonyolításához általában a nehezen lenyomozható kriptovalutákat használják. Az online feketepiacokon, illetve fórumokon jellemzően az alábbi áruk adásvétele zajlik: kábítószer, gyermekpornográf tartalmak, hamis és hamisított áruk, lőfegyverek és crimeware.

2.6.1. Kábítószer-kereskedelem

A kábítószer-kereskedelem továbbra is a legnagyobb illegális piacnak számít és egyre több hagyományos szervezett bűnözői csoport vesz részt a különféle kábítószerek előállításában, forgalmazásában és terjesztésében, amely során az internet nyújtotta előnyöket is kihasználják. A különböző feketepiacok fő profilját is a kábítószer adja, mint például ilyen híres online „bazár" volt a már említett Silk Road és az Alphabay is. Az egyes tanulmányok szerint az első nyolc Darknet piactérnek a havi bevétele 10,6 millió és 18,7 millió euró között mozog kábítószer-kereskedelemből.[349] A Btk. 176. § szerint büntetendő, aki kábítószert kínál, átad, forgalomba hoz, vagy azzal kereskedik, bűntett miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő. A kábítószer-kereskedelemen (Btk. 176. §) kívül szóba jöhetnek még a hazai szabályozás értelmében a következő bűncselekmények, amelyek tiltott szerekhez kapcsolódnak: a kábítószer készítésének elősegítése (Btk. 182. §), kábítószer-prekurzorral visszaélés (Btk. 183. §), új pszichoaktív anyaggal visszaélés (Btk. 184. §),

[348] EUROPOL: The Internet Organised Crime Assessment (IOCTA). 2014. 19-21. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014 [2018.03.25.]
[349] EUROPOL (2017): i.m. 49-50.

teljesítményfokozó szerrel visszaélés (Btk. 185. §), valamint a gyógyszerkészítmények esetén gyógyszerhamisítás (Btk. 185/A. §) is.

2.6.2. Gyermekpornográfia

A gyermekpornográf tartalmak készítése, illetve azzal való kereskedés jövedelmező üzletté vált, amit a szervezett bűnözői csoportok is felismertek és kihasználnak. A Darkneten keresztül hirdetik és terjesztik a tiltott pornográf tartalmakat vagy külön weboldalakat hoznak létre haszonszerzési céllal. Új trendként jelent meg, hogy a gyermekmolesztálást az interneten keresztül élőben közvetítik, vagyis „streamelik". Az online tevékenység célja egyben lehet az offline szexturizmus iránti igény felkeltése is. A Btk. 204. § (1) bekezdés a) - c) pontja értelmében, aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt megszerez vagy tart, készít, kínál, átad vagy hozzáférhetővé tesz, forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz az gyermekpornográfia bűntette miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő. Az online streamelés esetén pedig a 204. § (4) bekezdésének b) pontjáért felel, aki tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf műsorban szerepeltet, és egy évtől öt évig terjedő szabadságvesztéssel büntetendő.[350]

A gyermekpornográfia szabályozása nemzetközileg differenciált képet mutat, mert például egyes országokban a büntetendő magatartásnak tekintik már a „tudatos hozzáférést" is, amelynek célja, hogy azon személyek is felelősségre vonhatók legyenek, akik a gyermekpornográf anyagokhoz online férnek hozzá, annak letöltése nélkül. Például külön erre a célra létrehozott oldalakon keresztül nézik, és ezért nem lehet őket büntetni a megszerzése vagy birtoklása miatt. Ebben az esetben szükséges annak bizonyítása, hogy az elkövető szándékosan lépett be az adott oldalra, ahol a tiltott anyag elérhető és tudomása volt arról, hogy ilyen jellegű tartalom hozzáférhető ott. A szándékosságra lehet következtetni ugyanis abból, ha az elkövető ismétlődő jelleggel látogatja a weboldalt vagy fizet ezért a szolgáltatásért. Az egyes

[350] Ezzel kapcsolatban érdemes említést tenni a Kúria 2/2018. büntető jogegységi határozatáról, amelyben kimondja, hogy a 204. § (1) bekezdésében írt eseteiben nem eredményez halmazatot önmagában az, hogy az elkövetési magatartás – az azokon szereplő tizennyolcadik életévét be nem töltött személyek számától függetlenül – több pornográf felvételt érint. Ugyanakkor bűncselekményegységet csak az azonos törvényi tényállásba ütköző magatartások képeznek. E bűncselekmény tekintetében nem azonos, hanem külön-külön törvényi tényállást tartalmaznak a Btk. 204.§ (1) bekezdésének a), b) és c) pontjai. Amennyiben az elkövető ugyanazon felvétellel kapcsolatban különböző pontokban írt elkövetési magatartásokat valósít meg, egységesen a legsúlyosabb büntetési tétellel fenyegetett bűncselekmény valósul meg. Ha az elkövető különböző felvételekkel kapcsolatban valósítja meg a Btk. 204. § (1) bekezdésének különböző pontjaiba ütköző elkövetési magatartásokat, az azonos törvényhelyen belül egységként minősülő cselekmények egymással valóságos halmazatban állnak. A gyermekpornográfia Btk. 204. § (2) bekezdése szerinti minősített esetének rendbelisége a felvételeken szereplő, a törvényhelyben meghatározott feltételeknek megfelelő személyek számához igazodik.

országokban ez a jogsértés a birtokláson belül kerül szabályozásra (pl. Németországban), a magyar szabályozásnak azonban nem része. Ezzel összefüggésben megjegyzendő, hogy a cache-ben tárolt képek nem elegendők a felelősségre vonáshoz a birtoklásért, anélkül, hogy bizonyítást nyerne az, hogy az adott személynek tudomása lenne az elkövetett magatartásról.[351]

2.6.3. Hamis és hamisított termékekkel, lőfegyverekkel kereskedés

A hamis és hamisított termékek is népszerűek, amelyek széles skálája elérhető mind a Surface Weben és mind a Darkneten, így többek között ruházati termékek, ékszerek, „kalóz" szoftverek, előfizetések különböző TV és zenei platformokhoz, online videójáték fiókok, valamint a legkeresettebb termékek közé tartoznak a hamis pénzek és személyazonosító okmányok. Emellett a különböző lőfegyverek is a keresett áruk közé tartoznak. Ebben a körben felmerülhetnek az alábbi büntetendő magatartások: a szerzői jogi vagy szerzői joghoz kapcsolódó jogok megsértése (Btk. 385. §), a pénzhamisítás (Btk. 389. §), közokirat-hamisítás (Btk. 342. §), okirattal visszaélés (Btk. 346. §) és a lőfegyverrel vagy lőszerrel való visszaélés (Btk. 325. §).

2.6.4. Crime-as-a-Service üzleti modell

A Crime-as-a-Service üzleti modellt követve az online feketepiacokon különböző szolgáltatások érhetők el, így a következők:

Infrastruktúra mint szolgáltatás (Infrastructure-as-a-Service): az informatikai támadások végrehajtásához szükség van egy védett infrastruktúrára, ami biztosítja a biztonságot, anonimitást és ellenállást a bűnüldöző hatóságok beavatkozásai elől. A tárhelyszolgáltatók (hosting providers), különösen az ún. bulletproof hosting szolgáltatások népszerűek, mert lehetőséget biztosítanak arra, hogy a felhasználók szabadon feltöltsék a kívánt tartalmat anélkül, hogy azokat eltávolítanák, még akkor is, ha illegálisnak minősülnek. Éppen ezért kulcsfontosságú szerepük van az online feketepiacok esetében, mert biztonságos tárhelyet biztosítanak a crimeware-nak, az ellopott adatoknak és egyéb illegális tartalmaknak. A VPN, vagyis a virtuális magánhálózat és a proxy szolgáltatások pedig fontos szerepet játszanak az anonimitás biztosításában, ezáltal segítenek a bűnüldöző szervek kijátszásában.

Az adat a legkeresettebb áru manapság. Nagy mennyiségű személyes és pénzügyi adatok adásvétele zajlik a digitális feketegazdaságban.[352] Az adat befolyásolja az illegális piacok

[351] DORNFELD – MEZEI: i.m. 34. o.
[352] EUROPOL (2014): i.m. 19-21. o.

fejlődését: meghatározott bűnözői tevékenységeket fejlesztettek ki, illetve folyamatosan dolgoznak azon, hogy javítsák, jobbá tegyék ezeket, annak érdekében, hogy hatékonyan szerezzék, „lopják el" ezeket az érzékeny adatokat (pl. phishing, malware és egyéb eszközöket használnak a kereskedelmi, pénzügyi adatbázisokkal szembeni támadásokhoz).[353] A bankkártya és az online bankfiók adatok a legkeresettebbek. Így a következő bűncselekmények merülhetnek fel e körben: a készpénz-helyettesítő fizetési eszköz hamisítása (Btk. 392.§), továbbá a készpénz-helyettesítő fizetési eszközzel visszaélés (Btk. 393.§) és a készpénz-helyettesítő fizetési eszköz hamisításának elősegítése (Btk. 394. §), valamint az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §). Például hazai esetre is már sor került, amelyben a terheltet információs rendszer felhasználásával elkövetett csalás miatt állították bíróság elé, mert a Darknet fórumon keresztül kriptovaluáért vásárolta meg a sértett felhasználó nevét és jelszavát, amelyek felhasználásával egy ruházati termékeket árusító webáruház honlapján tudott a profiljába belépni, majd a fiókban rögzített bankkártya adatok jogosulatlan megadásával vásárolt. A sértett a banknak jelezte ezt, és ezért a jogtalanul lehívott összeg jóváírásra került, így a kára teljes mértékben megtérült.[354]

A pénzügyi adatokon kívül még elérhetőek lakcímek, telefonszámok, e-mail címek, e-pénztárcák, társadalombiztosítási azonosítók és egyéb online felhasználó fiókokhoz kapcsolódó adatok is.

Pay-per-install szolgáltatások népszerű módszerei a malware terjesztésnek, ami úgy működik, hogy akik a szolgáltatást nyújtják, azok terjesztik a rosszindulatú fájlokat, amiket pedig a szolgáltatást igénybe vevők biztosítanak a számukra és a letöltések száma utána fizetnek nekik. Az ilyen szolgáltatások országspecifikus forgalmat biztosíthatnak. Emellett hozzá lehet jutni a DDoS-támadások indítására szolgáló botnetekhez, illetve a létrehozásukra szolgáló eszközök, programokat lehet igénybe venni (DDoS-for-hire vagy DDoS-as-a-Service) – napi vagy havi díjjal átlagosan 5 $ és 1,000 $ közötti áron.[355] Hasonlóképpen a különböző rosszindulatú programok is megszerezhetők a szolgáltatások keretében, mint például a legkönnyebb pénzszerzési módot biztosító zsarolóvírusok (Ransomware-as-a-Service). A legnagyobb veszélyt pedig az egyedi hatású és célzott támadásokra kifejlesztett kártékony programok jelentik különösen, amelyek a kritikus infrastruktúrákat célozzák és ezek is már elérhetőek a feketepiacokon (pl. a Stuxnet ismertté válásával „közkinccsé vált", ezután annak

[353] TROPINA (2012): i.m. 162. o.
[354] http://ugyeszseg.hu/a-darknet-hasznalatanak-veszelye-birosag-ele-allitas/ [2019.03.15.]
[355] EUROPOL: (2014): i.m. 19-21. o.

elemei kikerültek a „szabadpiacra” és tovább fejlesztve már hasonló mechanizmusokat tartalmazó malware-ek is elérhetővé váltak, mint a DuQu).[356]

Ahogy korábban erre már felhívtam a figyelmet, a Criminal-as-a-Service üzleti modell, különösen azért veszélyes, mert könnyen hozzá lehet jutni a kiberbűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár kész bűnözői infrastruktúrához. Éppen ezért fontos, hogy már az előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra. Hiszen a szolgáltatás igénybevételével a hozzá nem értő felhasználók is olcsón, egyszerűen és gyorsan tudnak támadást indítani, sokszor csak egy egérkattintás az egész, sőt a végrehajtáshoz még technikai segítséget is kapnak. A megszerzett ismeretekkel kiberbűncselekményeket tudnak elkövetni, amit a Btk. a 423. §-ban az információs rendszer és adat megsértése bűncselekmény körében szabályoz.

Hacking mint szolgáltatás (Hacking-as-a-Service): Alap szinten ez magában foglalhatja az e-mail vagy közösségi oldalak fiókjainak a feltörését, vagy összetettebb támadásokat, mint például a gazdasági kémkedést vagy személyes adatok gyűjtését a meghatározott célponttól.

Fordításokhoz kapcsolódó szolgáltatások: A támadások sokszor országspecifikusak és előfordulhat, hogy az elkövető nem feltétlenül beszéli a célország nyelvét, ezért igénybe vehet szolgáltatást fordítóktól, akik helyesen megfogalmazott szövegeket nyújtanak, ezzel elősegítve a támadás sikerét, mert sok esetben éppen a nyelvtani pontatlanságok lehetnek árulkodó jelei a csalásnak.

Pénzmosás mint szolgáltatás (Money laundering-as-a-Service): A bűnözők nem csak saját maguk javára végeznek pénzmosást, hanem szolgáltatásként is elérhető az általuk meghatározott díj ellenében.[357] Azért, hogy „tiszta” profitra tegyenek szert az illegális tevékenységükből a „piszkos pénzek” tisztára mosásához különféle szolgáltatásokat vehetnek igénybe annak érdekében, hogy ezeket a legális gazdaságba vissza tudják forgatni.[358] Ezek a szolgáltatások magukban foglalják az online és offline megoldások kombinációit, amelyeknek a középpontjában általában a pénzfutárok, a money mule hálózatok állnak. A „money mule” elnevezéssel ismert új pénzmosási technika a pénzintézetekkel történő kapcsolatfelvételt iktatja ki és egy harmadik személy közreműködésével, akinek segítségével terítik, bújtatják a bűncselekményből eredő „piszkos pénzt”. Indokolt tehát a fokozott óvatosság, hiszen aki akár az igen vonzónak tűnő ajánlatot elfogadja, maga is érintetté válik a pénzmosás bűncselekmény

[356] NAGY Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula - Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII. 2012. 227-228. o.
[357] EUROPOL (2014): i.m. 19-21. o.
[358] TÓTH (2002): i.m. 375. o.

elkövetésében.[359]. Ezzel szoros összefügésben új trendként jelent meg, hogy a nagyobb összegek tisztára mosása úgy történik, hogy azt kisebb összegű tranzakciókra bontják (micro money laundering), amelynek előnye, hogy kevésbé feltűnő.[360]

[359] EUROPOL (2014): i.m. 19-21. o.
[360] MARAS (2017): i.m. 336. o.

3. A pénzmosás a technológiai fejlődés fényében

3.1. Általános bevezető

A pénzmosás is azon bűncselekménytípus, amelyet szervesen érint a technológiai fejlődés azáltal, hogy az elkövetését jelentősen megkönnyítheti. Gondoljunk csak a bankoknak az egyre bővülő online szolgáltatásaikra, amelyeken keresztül könnyedén tudunk rövid időn belül akár több utalást is végezni, mindezt anélkül, hogy személyesen kellene ezt megtennünk egy bankfiókban. Éppen ezért napjainkra a világ bankjainak döntő többsége internet alapúvá vált. Azonban ez mára azt is eredményezte, hogy ez az egyik legismertebb és leggyakoribb módja lett a digitális pénzmosásnak. Ezen kívül a szerencsejátékok és a kaszinók is már régóta a pénzmosás hatékony eszközei között sorakoznak fel. Ezek pedig elterjedtek a virtuális hálózatokon ugyanúgy, mint a valós térben, és így még inkább alkalmasabbá váltak az illegális bevételek tisztára mosására. Már nem példa nélküli az sem, hogy pénzmosásra használják a különböző online videójátékokat,[361] valamint az e-kereskedelemben is az egyes ügyletek e célt szolgálhatják.[362] A legnagyobb kihívást pedig a kriptovaluták használata jelenti, de az ezzel kapcsolatos kérdéseket a későbbiekben foglalkozom.[363]

A technológiai fejlődésnek a pénzmosásra gyakorolt jelentős hatására tekintettel Daniel Adeoyé Leslie már kísérletet tett arra, hogy az ún. kiberpénzmosás (cyberlaundering) fogalmát határozza meg, mely elnevezés a pénzmosás és a technológia kettősét foglalja magában. Véleménye szerint ez azt jelenti, ha számítógépet használnak a pénzmosáshoz, így például egy tranzakció lebonyolításához. Ebben az esetben a számítógép az elkövetés eszköze, míg a színteret ehhez az internet biztosítja.[364]

---

[361] A „Second Life" videójátékban például az US dollárhoz igazított Linden-dollárért virtuális földbirtok, más ingatlan licitálható, vásárolható, illetőleg eladható egy másik játékosnak. Ahogy a való életben, itt is dolgok, ingatlanok, ruhák és más napi tárgyak, háziállatok vásárolhatók, szerencsejátékok űzhetők. Népszerű, pénzfizetéses játék a World of Warcraft is, amelynek a játékon belüli fizetőeszköze a „Gold". Azok az online játékok, amelyekben két vagy több személy között pénzforgalom lehetséges, egyszersmind a pénzmosásra is alkalmassá válnak. Lásd NAGY Zoltán András – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog 2017/1. 29. o.

[362] Például a felhasználók egymás közötti kereskedelme nehezen ellenőrizhető (Customer-to-Customer), valamint az is előfordulhat, hogy az elkövetők olyan valós kereskedelmi tevékenységet nem végző álwebáruházakat nyitnak, amelyek keresztül fiktív ügyleteket bonyolítanak le. Lásd TROPINA, Tatiana: Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum 2014. 77. o.

[363] Lásd „A kriptovaluták büntető anyagi és eljárásjogi kihívásai" című részt.

[364] LESLIE, Daniel Adeoyé: Legal Principles for Combatting Cyberlaundering. Law, Governance and Technology Seriec Volume 19. Springer 2014. 55. o.: A besorolását tekintve a szerző három álláspontot is vizsgált. Az egyik elsősorban a kiberbűncselekmények egyik leágazásának tekinti, és a technikai tényezőre helyezi a fő hangsúlyt. A második a pénzmosás egyik új technikájaként kezeli. A harmadik állásfoglalás szerint egy teljesen új jelenségről van szó, amely ötvözi a kiberbűnözés és a pénzmosás bizonyos elemeit.

A virtuális térben végrehajtott pénzmosásnak is ugyanaz a célja, mint a valós térben, azaz jellemzően gazdasági tevékenységek alatt folytatott illegális pénzügyi művelet, amelynek célja, hogy a bűncselekménnyel szerzett vagyon eredete igazolhatóvá váljon, jogellenes voltától megszabaduljon, vagyis lehetetlenné tegye az illegálisan szerzett – valamely bűncselekményből származó – pénz eredetének az azonosíthatóságát és ezáltal azt legális forrásból származónak tüntesse fel. A pénzmosásnak három fázisa különíthető el a szakirodalom szerint, amelyek a következők: az elhelyezés, a bújtatás és az integrálás. E három mozzanat együtt jelenti a pénz legalizálásának a folyamatát, amely során az – esetleg már feltárt – alapbűncselekmény és annak haszna közötti kapcsolatot kívánják elrejteni.

Jelen fejezetben azonban elsősorban a pénzügyi műveletekkel, így különösen a banki utalásokkal szoros összefüggésben felmerülő kérdéseket vizsgálom a hazai szabályozásra és a joggyakorlatra tekintettel.[365]

3.2. A dinamikus és a saját pénzmosás

A pénzmosás törvényi tényállásának módosítására több alkalommal is sor került az évek során, amelyet különösen az uniós jogharmonizációs kötelezettség tett szükségessé. Alapjaiban a 2001. évi CXXI. törvény megalkotásával változtatták meg a tényállásra vonatkozó hazai büntetőjogi szabályozást. A legfontosabb változás, hogy a törvénymódosítás büntetni rendelte a saját bűncselekménnyel szerzett pénz tisztára mosását is, tehát ez időponttól nem csupán a más által elkövetett alapbűncselekményhez kapcsolódó pénzmosás minősül bűncselekménynek.

Vitathatatlan tény, hogy manapság a pénzmosás különféle pénzügyi műveletek láncolatát – átutalások, átváltások, befektetések – foglalja magában, amelynek célja a pénz bűnös eredetének, valamint azonosságának leplezése a tranzakciók követhetetlenné válásával és annak tisztára mosásával a pénzintézetek hálózatában.[366] A pénzmosással kapcsolatban a látencia kétszeresen is jelen van. Egyfelől sokszor az alapbűncselekmény nem jut a hatóságok tudomására, másfelől ugyan ismertté vált, jobb esetben fel is derített alapbűncselekmény elkövetését követően a pénzmosás marad rejtve.

A Btk. 399. §-ában szabályozott szándékos pénzmosás tényállása körében a törvényhozó egyértelműen elkülöníti egymástól a más által elkövetett büntetendő cselekményből származó

[365] Lásd NAGY – MEZEI (2017): i.m. 29. o.
[366] TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. Budapest: KJK Kerszöv 2002. 357. o.

dologra elkövetett pénzmosást [(1) és (2) bekezdés], valamint a saját maga által elkövetett büntetendő cselekményből származó dolog tisztára mosását [(3) bekezdés].

A Btk. 399. § (1) bekezdés a) pontjának második fordulata szerint büntetendő, aki más által elkövetett büntetendő cselekményből származó dologgal összefüggésben bármilyen pénzügyi tevékenységet végez, vagy pénzügyi szolgáltatást vesz igénybe[367] abból a célból, hogy aa) az ilyen dolog eredetét eltitkolja, elleplezze, vagy ab) a más által elkövetett büntetendő cselekmény elkövetőjével szemben a büntetőeljárást meghiúsítsa. A továbbiakban a saját pénzmosás deliktumával kapcsolatban a gyakorlatban felmerülő kérdéseket vizsgálom, így különös tekintettel az eredetleplezési célzatra.

A Btk. 399. § (3) bekezdésében szabályozott saját pénzmosásnak minősül az első elkövetési magatartása esetén az illegális forrásból származó pénznek a gazdasági tevékenység során történő felhasználása (pl. az elkövető vállalkozásba fekteti, elszámolási ügyleteket rendez vele). A gazdasági tevékenység fogalmát – eltérően az 1978. évi Btk.-tól [315. § (2) bekezdés[368]] – nem határozza meg a hatályos törvény, ezért ezt az ítélkezési gyakorlatnak kell kialakítania. A második elkövetési magatartás esetén a pénzzel összefüggésben végzett pénzügyi tevékenység vagy pénzügyi szolgáltatás igénybevételéről van szó (pl. banki átutalások, készpénzfelvétel stb.).

A saját pénzmosás megállapításához az eredetleplezési célzat mint a törvényi tényállás alanyi elemének fennállására is szükség van. Ezzel kapcsolatban érdemes vizsgálni a célzat fogalmát, amely alatt az elkövetőnek a törvényi tényállásban értékelt célját, azaz egy olyan eredményképzetet értünk, melynek megvalósítására az elkövető törekszik. Erről akkor beszélhetünk, ha a törvényhozó az elkövető által elérni kívánt célt kifejezetten megjelöli a törvényi tényállásban, mint ahogy ezt a pénzmosás esetében is teszi. Azonban a jogirodalom nem egységes a tekintetben, hogy a célzat a szándékhoz, valamint a bűnösséghez hogyan viszonyul.[369] Finkey Ferenc szerint a célzat csak azokra a cselekményekre bír jelentőséggel, amelyeknél azt a Btk. határozottan megemlíti, illetve tényállási elemként írja elő. A szándéktól a célzat mindig megkülönböztethető és meg is különböztetendő. Fogalmilag nem más mint az

[367] Btk. 401. § (2) bekezdés: A 399-400. § alkalmazásában pénzügyi tevékenységen, illetve pénzügyi szolgáltatás igénybevételén a pénzügyi szolgáltatási vagy kiegészítő pénzügyi szolgáltatási, befektetési szolgáltatási vagy befektetési szolgáltatási tevékenységet kiegészítő szolgáltatási, árutőzsdei szolgáltatási, befektetési alapkezelési, kockázati tőkealapkezelési, tőzsdei, központi értéktári vagy központi szerződő fél, vagy biztosítási, viszontbiztosítási vagy független biztosításközvetítői, illetve önkéntes kölcsönös biztosító pénztári, magán-nyugdíjpénztári vagy foglalkoztatói nyugdíj-szolgáltatási tevékenységet, illetve annak igénybevételét kell érteni.

[368] Az 1978. évi Btk. szabályozása értelmében gazdasági tevékenységnek minősül a bevétel elérése érdekében vagy azt eredményező módon saját kockázatra rendszeresen végzett termelő, kereskedelmi vagy szolgáltató tevékenység.

[369] FÖLDVÁRI József: Büntetőjog – Általános rész. Budapest, Osiris Kiadó, 2001. 128. o.

az intentio, aminek elérése végett a tettes a kérdéses cselekményt létesíti, vagy az a képzet, amit a tettes az adott szándékos cselekmény elkövetése által közvetlenül megvalósítani akar. A szándék - mint általánosabb fogalom - a célzatot átfogja, azonban nem nyeli el, mert a célzat abban mindig kimutatható.[370]

E kérdésben egyetértek Tóth álláspontjával, miszerint a célzat csak akkor róható fel az elkövetőnek, ha az annak érdekében végzett tevékenység alkalmas lehet az adott cél elérésére, a szándék realizálására, különben az alanyi oldal kiüresedik.[371] Ez alátámasztható a teleologikus értelmezéssel is: amennyiben a célzat elérésére nem alkalmas az adott cselekmény, akkor az a jogtárgysértésre is alkalmatlanná válik, ezért nem jön létre bűncselekmény.[372]

A pénzmosásnak ezen alakzata csak szándékosan követhető el, és a leplezésre irányuló sajátos célzat megfogalmazásából következően kizárólag egyenes szándékkal. Az elkövetőnek a pénzügyi vagy banki műveletek végzése során a dolog eredetének leplezése végett kell eljárnia, és ez jelenti a bűncselekmény célzatát. „A leplezés aktív magatartás, amellyel az elkövető az alapbűncselekményből származó dolog és az alapbűncselekmény közötti kapcsolatot igyekszik eltűntetni."[373] Mindebből az következik, hogy az elkövető az illegálisan szerzett pénzt legális forrásból származónak tünteti fel az eredet leplezése érdekében, és erre a célra vonható le következtetés minden olyan magatartásból, amely az illegális vagyon és az annak forrását képező bűncselekmény egymástól való eltávolítására irányul.

Megjegyzendő, hogy a törvényi tényállás célzatát megvalósító tényállási elem részben kétség kívül tudati jellegű, a pénzmosás tényállása azonban olyan speciális, hogy a bűncselekmény egyértelmű megállapíthatósága érdekében szükséges a célzatot megalapozó körülmények tényállásba foglalása is.[374] Ezzel szoros összefüggésben, hogy a Varsói Egyezmény[375] 9. cikk (2) bekezdés c) pontjában a pénzmosással kapcsolatos értelmező szabály kimondja, hogy: „…a bűncselekmények elemeként meghatározott tudomásra, szándékra, vagy célzatra objektív, ténybeli körülményekből lehet következtetni".

[370] FINKEY Ferenc: A szándék fogalma és ismérvei a büntetőjogban, különös tekintettel „a szándék hiánya miatt" történő felmentésre. Pesti Lloyd-Társulat Nyomdája. Budapest, 1899. 50. o.
[371] TÓTH Mihály: A látszólagos anyagi halmazat egyes kérdései – gyakorlatias nézőpontból. In: Koltay András – Molnár Gábor (szerk.): Bonus Iudex: Ünnepi kötet Varga Zoltán 70. születésnapja alkalmából. Budapest, Xenia Kúria – PPKE ÁJK, 2018. 424. o.
[372] A teleologikus értelmezés büntetőjogi alapkérdéseiről bővebben lásd SZOMORA Zsolt: A jogi tárgy funkciói és a jogtárgyharmonikus értelmezés. Bűnügyi Szemle 2009/2. 11–17. o.
[373] MOLNÁR (2009): 519. o.
[374] Debreceni Ítélőtábla Bf.II.390/2013/12.
[375] Az Európa Tanács pénzmosásról, a bűncselekményből származó jövedelmek felkutatásáról, lefoglalásáról és elkobzásáról, valamint a terrorizmus finanszírozásáról szóló, Varsóban, 2005. május 16-án kelt Egyezménye, amelyet a 2008. évi LXIII. törvény hirdetett ki Magyarországon

Az eredetleplezési célzat fennállásának megállapításához szükséges továbbá annak bizonyítása, hogy az elkövető tudata átfogja legalább azt, hogy a pénz bűnös eredetű és magatartásával a valós eredet elfedésének érdekében hajt végre pénzügyi tevékenységet.[376]

A bíróság továbbá egyik eseti döntésében meghatározta, hogy az eredetleplezési célzat fennállásának igazolásához fel kell tárni többek között a továbbított összeget megkapó személyek kilétét, a pénz további útját, valamint adatot arra vonatkozóan, hogy azt a legális gazdaságban felhasználták.[377]

Mindezek fényében fontos hangsúlyozni, hogy az eredetleplezési célzatot nem lehet kiterjesztően értelmezni, mert ez oda vezetne, hogy a pénzmosás megállapítására akkor is sor kerülhetne, ha egy vagyon elleni bűncselekmény során eltulajdonított készpénzt az elkövető például a későbbiekben külföldi fizetőeszközre váltja, mivel azt egy külföldi utazás során kívánja elkölteni. Ez a bíróság értelmezése szerint is ellentétes a jogalkotó eredeti szándékával.[378]

Az Országos Kriminológiai Intézet empirikus kutatása során a következő leggyakrabban előforduló alapbűncselekményeket határozta meg, amelyekhez jellemzően pénzmosás kapcsolódhat: a költségvetési csalás (adócsalás), a gazdasági tevékenység során elkövetett csalás, a sikkasztás, illetve a hűtlen kezelés.[379] Ezért különösképpen lényeges vizsgálni az egyes gazdasági vagy vagyon elleni bűncselekmények utócselekményeinek a célzatát, mert ezekben az esetekben felmerül, hogy az elkövető a tevékenységével magát a bűncselekményt próbálja leplezni, és nem az abból származó dolog eredetét, ezért e célzat hiánya esetén méltánytalan lenne pénzmosás miatt is felelősségre vonni az illetőt.

A saját pénzmosás deliktuma például „csak akkor tényállásszerű, ha az elkövető a dolgot az eredetének leplezése céljából használja fel gazdasági tevékenység során. […E…] célzat hiányában az is bűncselekménynek számítana, ha valaki a be nem fizetett adóját a saját neve alatt elhelyezné egy bankszámlán, mivel ezzel már bankműveletet végzett az adócsalásból származó pénzzel. Ekkor külön pénzmosás miatt büntetőeljárást indítani célszerűtlen (és méltánytalan) lenne”.[380]

A saját pénzmosással kapcsolatban fontos kiemelni, hogy csak azok a magatartások nyerhetnek önálló büntetőjogi értékelést, amelyek nem szükségszerű velejárói az

[376] Miskolci Törvényszék 11.B.986/2010/75.
[377] Fővárosi Törvényszék 2.B.282/2012/21.
[378] BH 2006.143; Heves Megyei Bíróság B.582/2010/199.
[379] KÁRMÁN Gabriella – MÉSZÁROS Ádám – TILKI Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3. 92. o.
[380] GÁL István László: A pénzmosás. Complex Kiadó, Budapest, 2004. 76. o.

alapbűncselekmény elkövetésének. A dologgal összefüggésben igénybe vett pénzügyi szolgáltatások – a kétszeres értékelés tilalmára is figyelemmel – csak abban az esetben valósítják meg a bűntettet, ha azok az eredetleplezési cél miatt túlmutatnak a bűncselekménnyel szerzett előny puszta realizálásán.[381]

A saját pénzmosás felveti a látszólagos anyagi halmazatot érintő büntetlen utócselekmény kérdéskörét is.[382] E kérdésben a BH 2004.7. mondta ki először, hogy a pénzmosás nem a csalás büntetlen utócselekménye, minthogy a törvény a pénzmosást kiemelte a lehetséges utócselekmények köréből. Azonban fontos leszögezni, hogy ezt a döntést sem lehet kiterjesztően értelmezni, mint ahogy ezt a gyakorlat sok esetben teszi és hivatkozik is rá. A konkrét ügyben a vádlottak a sértett társaságtól kicsalt és a bankszámlájukra érkező pénzt fiktív jogcímen – méghozzá a csalás tárgyát képező valójában nem is létező lízingtárgyak vételárának feltüntetésével – továbbutalták. A másodfokú bíróság megállapítása szerint számos körülmény utalt arra, hogy a vádlottak a pénz illegális eredetének leplezése és tényleges útjának elfedése érdekében a háttérben gazdasági ügyletek látszatát keltve további banki műveleteket végeztek. Az ügy jelentőségét tehát nem az jelenti, hogy a pénzmosást önálló bűncselekményként kell értékelni a jogalkotói döntés folytán és ezért nem lehet büntetlen utócselekmény. A bíróság valójában arra hívta fel a figyelmet, hogy a pénzösszegek továbbutalása már nem a csalással okozott kár realizálása érdekében történt, hanem az ily módon megszerzett pénz eredetének leplezése érdekében, amely alapján az alapbűncselekményként értékelendő csalás mellett járulékosan a pénzmosás is megvalósult.

Azonban egyre gyakoribb – köszönhetően ezen eseti döntés kiterjesztő értelmezésének is –, hogy az alapbűncselekményekből származó anyagi javaknak a bankszámlára helyezése, átváltása, bankszámlák közötti átutalása vagy felvétele – még akkor is, ha a pénz eredete, a pénzmozgás útja továbbra is könnyen nyomon követhető – már felveti a pénzmosás gyanúját, sőt akár a vád tárgyát képezheti és marasztaló ítélet alapját adhatja. Ezek a magatartások azonban az esetek többségében csak az alapbűncselekményekből származó haszon realizálását, vagy a bűncselekmények felderítésének elkerülését célozzák, nem a pénz eredetének leplezését, ezért ezek büntetlen utócselekményként értékelendők és nem pénzmosásként. Az utócselekmény büntetlen (önállótlan) abban az esetben, ha az elkövető részéről a jogszerű magatartás tanúsítása gyakorlatilag önfeljelentést jelentene, vagyis az utócselekmény

[381] SINKU Pál: A pénzmosás miatti bűnügyek gyakorlata – Az ügyészi jogalkalmazás tapasztalatai. In: Barabás A. Tünde – Vókó György (szerk.): A bonis bona discere – Ünnepi kötet Belovics Ervin 60. születésnapja alkalmából. Budapest, Xenia OKRI – PPKE ÁJK, 2017. 144. o.
[382] Lásd GÁL István László: Új magyar büntetőjog a XXI. században: szemelvények az új Btk. Különös részének újdonságaiból. Jogtudományi Közlöny 2015/7-8. 333-334. o.

tanúsításától való tartózkodás esetén leleplezné a korábban elkövetett bűncselekményét. Földvári József álláspontja szerint emberiességi szempontok miatt indokolt a halmazat látszólagossága, míg Nagy Ferenc a bűnösség egyik feltételének a hiányát jelöli meg, ami a bűncselekmény egyik fogalmi eleme, az elvárhatóság.[383]

Érdemes ehhez áttekinteni a bírói gyakorlaton keresztül azokat az eseteket, amelyek szintén rámutatnak arra, hogy a pénzmosás ennél többet jelent, mert a megállapításához nem elegendő csupán az, hogy pénzügyi tevékenységet végezzenek az alapbűncselekményből származó pénzzel, hanem annak meghatározott céllal kell történnie, méghozzá azzal, hogy a pénz eredetét leplezzék és azt utólag a legális gazdasági életbe visszaforgassák.

Az egyik eseti döntés is ezt hangsúlyozta, amelyben a vádlottat jogosulatlan pénzügyi tevékenység és pénzmosás bűntette miatt vonták felelősségre, mert engedély nélkül végzett pénzváltói tevékenységet. A bíróság kimondta, hogy a vádlott esetében nem állapítható meg az eredetleplezési célzat megléte a pénzek átváltásakor, mert az általa üzemeltetett pénzváltói tevékenységéről könyvelést vezetett, melyben megtalálhatóak voltak azok az adatok, amelyek a pénzváltói tevékenységéhez kapcsolódtak és nyomon követhetően rögzítették a pénzmozgás útját is. A vádlott a Kft. nevében történt valuta-átváltásokat igazoló bizonylatokat a könyvelőjének átadta, azokat nem kívánta elrejteni vagy eltitkolni.[384]

Szabó Imre álláspontja is ezt erősíti, amely szerint például, ha az elkövető elleplezi a személyazonosságát, annak elsődleges célja a büntetőjogi felelősségre vonás elkerülése, azonban, ha ezzel a pénz útjának a nyomon követését is akadályozza, akkor például a hamis adatokkal történő bankszámlanyitás az eredetleplezési szándék fennállását jelentheti. Nem vonható le azonban kétséget kizáró következtetés az eredetleplezési célra, ha például a hamis bankszámlát létrehozó személy a pénzt azonosítható bankszámlára utalja tovább, mert ilyenkor a pénz eredete és útja továbbra is nyomon követhető lesz.[385]

Egy másik ügyben a bíróság a csalásból származó pénzösszegek felhasználásának egyes eseteiben nem állapította meg a célzat fennállását, mert azok a gazdasági társaság hitelállományának a csökkentését és a fizetésképtelenség elkerülését célozták, azonban azoknál az átutalásoknál, amelyeknél a cél az volt, hogy a pénz a vádlottakhoz többszörösen közvetve jusson el, az eredetleplezési célzatot megállapíthatónak találta.[386]

[383] AMBRUS (2014): i.m. 281. o.
[384] BH 2006.143.
[385] SZABÓ Imre: A pénzmosás a bírói gyakorlat tükrében. Ügyészek Lapja 2017/1. 56. o.
[386] Fővárosi Törvényszék 12.B.1229/2011.

Az eredetleplezési célzat megállapításához segíthetnek a pénzügyi műveletek jogcímei. Példaként említhető az egyik eseti döntés, amely során a bíróság nem látta igazoltnak a célzat fennállását akkor, amikor a vádlott a számlájára átutalt, csalásból származó pénzösszeget különböző célokra fordította, így lányának bankszámlájára két alkalommal összesen 18 millió forintot utalt át, azonban az utaláskor nem jelölt meg jogcímet. A hamis jogcím hiányából kifolyólag a bíróság nem vont le következtetést arra vonatkozóan, hogy az elkövető szándékában állt a csalásból származó pénz eredetének leplezése. Ezzel szemben, ha valótlan jogcímet ad meg az elkövető annak érdekében, hogy a pénz bűnös eredetét elfedje, akkor már e célzatra vonható le következtetés.[387]

Álláspontom szerint, amennyiben a pénzügyi műveletek tételesen nyomon követhetők, átláthatók, a pénz útja pontosan – akár egy egyszerű banki megkeresés révén – feltárhatók, akkor alkalmatlanok a pénz eredetének a leplezésére.

Az eredetleplezési célzaton kívül indokolt foglalkozni a pénzmosás alapvető jellegével, mert nem egy sui generis, hanem járulékos bűncselekményről van szó. A bűnkapcsolat egy formája, így a megvalósulását feltételezi egy másik Btk. szerint büntetendő cselekmény, ami az alapbűncselekménynek minősül. A Btk. szabályozásában lényegi változás az alapbűncselekményeket érintette, mert az 1978. évi Btk. értelmében a szabadságvesztéssel büntetendő cselekményhez kapcsolódhatott pénzmosás, míg a Btk. ezek körét bővítette és elegendő, ha büntetendő cselekményhez kapcsolódik járulékos jelleggel.[388] Tehát a pénzmosás az alapbűncselekményből származó dologra elkövetett járulékos magatartásokat rendeli önállóan büntetni, ezért az elkövetése fogalmilag kizárt mindaddig, amíg az alapcselekmény – vagy az alapcselekményt alkotó, önálló büntetőjogi értékelésre is alkalmas részcselekmény – elkövetése nem fejeződött be. A leplezés végett kifejtett magatartások jogi minősítésekor ezért körültekintően vizsgálni kell, hogy azok az alapbűncselekmény tényállásának keretei között értékelendők, vagy önállóan pénzmosást valósítanak-e meg.

A pénzmosás tényállásszerűségének megállapításához kizárólag azt a körülményt kell vizsgálni, hogy az adott történeti tényállás a Btk. szerint valamely büntetendő cselekményét kimeríti-e. Az alapbűncselekmény a különös részi diszpozíciónak az objektív tényállási eleme.[389]

[387] Fővárosi Ítélőtábla 5.Bf.38/2010/38.
[388] SCHUBAUER László: A pénzmosás elleni küzdelem magyarországi büntetőjogi eszközrendszerének kialakulása, változásai és továbbfejlesztésének lehetőségei. In: Hollán Miklós – Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex. MTA TK JTI – OKRI. Budapest, 2017. 357-358. o.
[389] MOLNÁR (2018): i.m. 800. o.

A saját pénzmosás kivételt képez a tekintetben, hogy az a személy, aki az alapbűncselekményben bármilyen elkövetői minőségben részt vett, ugyanezen bűncselekményhez kapcsolódó bűnkapcsolati bűncselekményért fő szabály szerint nem marasztalható, de az az elkövető, aki a saját bűncselekményéből származó pénzét mossa tisztára, az felelősségre vonható ilyen módon.[390]

A saját pénzmosás az alapbűncselekmény hiányában nem valósulhat meg, csak akkor lehet tényállásszerű, ha az elkövető az általa elkövetett bűncselekményből származó dolog eredetét leplezi.

A Kúria fontos megállapítást tett friss határozatában, amikor elvi éllel mondta ki, hogy „az alapbűncselekmény és a pénzmosás esetében valóságos heterogén alaki halmazat általában nem jöhet létre, ami azt jelenti, hogy egy elkövetési magatartás (vagy magatartássorozat) egyidejűleg az alapbűncselekmény és a pénzmosás tényállását nem merítheti ki."[391]

A büntetőjogi szakirodalomban uralkodó álláspont, hogy a két cselekmény között csak valódi anyagi halmazat állapítható meg.[392] A pénzmosás az alapbűncselekményhez képest más társadalomra veszélyességgel, valamint önálló jogi tárggyal rendelkező bűncselekmény,[393] ezért a megállapításához szükséges, hogy az elkövető több cselekményével, több – az alapbűncselekményt és a pénzmosást kimerítő – bűncselekmény törvényi tényállási elemeit valósítsa meg.

A pénzmosás megállapításánál annak sincs jelentősége, hogy az alapcselekmény elkövetője büntethető-e, valamint, hogy az a magyar joghatóság alá tartozik-e vagy sem, ezért a külföldön elkövetett bűncselekmény is alapcselekménye lehet a pénzmosásnak, feltéve, ha az alapcselekmény mindkét országban tényállásszerű és büntetendő.[394]

A kétszeres értékelés tilalmának – mint egész anyagi büntetőjogot átfogó – alapelvnek (ne bis in idem) megfelelően ugyanazon cselekmény miatt nem lehet kétszer büntetőjogi hátránnyal súlytani az elkövetőt. A kétszeres értékelés tilalma tekinthető az egység-többség tan elvi alapjának is, amelynek értelmében az egy vagy több bűncselekmény megállapítása során egy

[390] GELLÉR – AMBRUS: i.m. 432. o.
[391] Bfv.I.830/2017/16.
[392] ELEK Balázs: A jogirodalom által közvetített jogtudomány és a büntető ítélkezés. In: Bódig Mátyás – Ződi Zsolt (szerk.): A jogtudomány helye, szerepe és haszna. Tudománymódszertani és tudományelméleti írások. Budapest, MTA TK JTI – Opten Informatikai Kft., 2016. 167. o.
[393] A pénzügyi szektor és a gazdaság egyéb szereplőinek a törvényes működéséhez fűződő érdek, valamint a szervezett bűnözés elleni fellépés eredményességéhez fűződő érdek.
[394] JACSÓ Judit: Pénzmosás. In: Görgényi Ilona – Gula József – Horváth Tibor – Jacsó Judit – Lévay Miklós – Sántha Ferenc – Váradi Erika: Magyar Büntetőjog - Különös Rész. Wolters Kluwer Complex Kiadó, Budapest, 2013. 621. o.

körülmény sem értékelhető kétszeresen, de semmi sem maradhat értékelés nélkül.[395] Ammenyiben egy adott tevékenység - vagy mulasztás - két vagy több bűncselekmény törvényi tényállásának eleme, az csak az egyik bűncselekmény megállapításánál lehet figyelembe venni.[396] A bűncselekmény minősítése során a bírói gyakorlatban is szerepet kaphat az azonos körülmény kétszeres büntetőjogi értékelésének a tilalma.[397]

A Kúria helyesen hívta fel a figyelmet erre, hogy az ügyészség ugyanazt az elkövetési magatartást a kétszeres értékelés tilalmába ütköző módon értékelte, amikor a vádlottak által végrehajtott banki átutalásokat a jogtalan elsajátítás részeként és egyúttal a pénzmosás deliktumaként is meghatározta. A vádlottak a hozzájuk került pénzösszegnek a továbbutalásával szereztek rendelkezési jogot a pénz felett, így valójában ezekkel a műveletekkel valósították meg az eltulajdonítást, amely a jogtalan elsajátítás bűncselekményének tényállási eleme és így ehhez nem kapcsolódhatott pénzmosás. A vádhatóság részéről, amit eredetleplezési célzatként is értékeltek, az valójában az alapbűncselekmény immanens részét képező pénzügyi műveletek sora volt.[398]

Érdemes megjegyezni, hogy a pénzmosás esetén a vagyonelkobzás elrendelése szintén a kétszeres értékelés tilalmába ütközhet, ha az alapbűncselekménynél már elrendelésre került.

Az ügyészség részéről megfigyelhető egy a halmazatot bővítő gyakorlat[399], amihez közvetett módon hozzájárulhat az, hogy pénzmosás miatti marasztoló ítéletre vagy akár csak büntetőeljárás indítására is alig került sor az elmúlt években, holott az alapbűncselekmények száma nem csökken éves szinten. Az ENyÜBS adatai alapján az elmúlt években a regisztrált pénzmosási ügyek száma a következőképpen alakult: 2016-ban 18, 2014-ben 21, 2015-ben 27, 2016-ban 67, 2017 pedig 90.

[395] BELOVICS Ervin – GELLÉR Balázs – NAGY Ferenc – TÓTH Mihály: Büntetőjog – Általános rész. HVG-Orac Lap- és Könyvkiadó Kft. Budapest, 2015. 76-77.
[396] GELLÉR Balázs: Gondolatok a kettős értékelés tilalmáról és a látszólagos alaki halmazat feloldására szolgáló elvekről. In: GÁL István László (szerk.): Tanulmányok Tóth Mihály professzor 60. születésnapja tiszteletére. PTE ÁJK. Pécs, 2011. 219-228. o.
[397] BH 2000.279.
[398] Lásd MEZEI Kitti: A Kúria harmadfokú végzése a jogtalan elsajátításról és a pénzmosásról. Jogesetek Magyarázata 2018/3-4. 21-28. o.
[399] „Az alapcselekmény konkrét tényállási elemeinek megállapítását lehetővé tevő bizonyítékok nélkül is pénzmosás gyanúját alapozhatja meg – és ezért nyomozás elrendelésének alapja lehet – az, ha a vagyon birtoklásának, kezelésének, megtalálásának körülményeiből annak bűnös eredetére lehet következtetni.” Lásd 2/217. (VII. 31.) LÜ h. körlevele a pénzmosás miatti bűnügyekben követendő ügyészi gyakorlat eljárásjogi szempontjairól.

3.3. A „money mule” felhasználásával elkövetett pénzmosás

A saját pénzmosáson kívül külön foglalkozom a Btk. 400. § (1) bekezdésében szabályozott gondatlan alakzattal is, amely az ún. „money mule” jelenséghez szorosan köthető, azaz a pénzfutárok felhasználásával elkövetett pénzmosáshoz kapcsolódik. Ez Európa-szerte ismert pénzmosási technika és gyakran alapbűncselekményként a kiberbűncselekmények jelennek meg. Például a már jól ismert adathalász technikát alkalmazva, ismeretlen személyek különböző bankok áloldalait készítik el, majd ezt követően megtévesztő elektronikus leveleket küldenek szét a banki ügyfeleknek. Ezzel a cél, hogy az oldalt meglátogassák és megadják a banki azonosítójukkal, számlaszámukkal és jelszavukkal. A megtévesztést követően az elkövetők a megszerzett adatok birtokában belépnek a sértettek fiókjába és banki tranzakciókat kezdeményeznek, és ezzel kárt okozva nekik. Ezt követően pedig a bűncselekményből származó pénz továbbutalásához, vagy felvételéhez money mule-okat szerveznek be. Ezeknek az általában pénzmosásként értékelt cselekményeknek a közös jellemzője továbbá, hogy az alapbűncselekmény elkövetésének és az eredetleplezés színhelyének az országa különböző.[401]

A pénzfutárokat általában megtévesztő módon, jogszerű tevékenység látszatát keltve toborozzák (pl. legálisnak tűnő és rendkívül kedvező állásajánlattal) az interneten keresztül (pl. e-mailben vagy közösségi oldalak használatával). Ezt követően vállalják, hogy különböző pénzösszegek fogadására pénzintézeteknél bankszámlát nyitnak, vagy a meglévő számlájukat használják, és az onnan felvett összegeket ismeretlen megbízójójuk számára továbbutalják vagy készpénzben átadják meghatározott, igen magas – általában 5-10%-os – jutalék ellenében. Tehát a magánszemélyek bankszámláira aprózzák fel a bűnös eredetű pénzt, amelyet majd a bankszámla tulajdonosok átutalnak az elkövetők számlájára, így legalizálják a „piszkos pénzt”. Általában a sok kicsi sokra megy elvet követve nem nagy összegek mozognak a bankszámlák között, így a tranzakciók nem feltűnőek és ezért a pénzmosási ellenőrzéseken sem akadnak fenn.[402]

Ezekben az esetekben általában csak a pénzfutár válik ismertté, aki a pénzmosás gondatlan alakzatának az elkövetője, míg a megbízó, a pénzmosás szándékos elkövetője ismeretlen marad.[403] A money mule tudattartalmának vizsgálata kiemelten fontos, mert ez lesz a minősítésnek az alapja. A dolog eredetét átfogó tudattartalomra az elkövetés körülményeiből, vagyis az elkövetési magatartás megvalósításával kapcsolatos ténymegállapításokból (pl. a

[401] SISÁK Attila: A pénzmosás elleni küzdelem tapasztalatai egy nyomozó hatóság gyakorlatában. Kriminológiai Közlemények 72. 91. o.
[402] TROPINA (2014): i.m. 75-76. o.
[403] KÁRMÁN – MÉSZÁROS – TILKI: i.m. 90. o.

bankszámlára érkező pénzösszegek nagyságrendjéből, a terhelt és megbízója között kapcsolatból[404]) kell levonni a megfelelő jogi következtetéseket. A gondatlan alakzat abban az esetben vizsgálandó, ha a terhelt ténybeli alapon és reálisan hihette, hogy az elkövetési tárgy legális forrásból származik.

A gondatlan pénzmosással kapcsolatban egy büntethetőséget megszüntető okot is meghatároz, melynek értelmében nem büntethető az, aki a hatóságnál önként feljelentést tesz, vagy ilyet kezdeményez, feltéve, hogy a cselekményt nem, vagy csak részben fedezték fel. A rendelkezés kriminálpolitikai indoka, hogy nagyobb érdek fűződik a még felderítetlen cselekmények leleplezéséhez, mint az elkövető megbüntetéséhez, a járulékos jelleg miatt pedig a pénzmosás leleplezése gyakran a még ismeretlen alapcselekmény felderítését és üldözését is segítheti. Fontos változás ugyanakkor, hogy míg a korábbi Btk. a szándékos és a gondatlan pénzmosás esetén egyaránt lehetővé tette a büntetőjogi felelősség alóli mentesülést, addig a hatályos Btk. kizárólag a gondatlan pénzmosás esetén tartja ezt fenn.[406]

[404] Fővárosi Törvényszék B.555/2015/15.

[406] JACSÓ Judit – UDVARHELYI Bence: A Bizottság új irányelvjavaslata a pénzmosás elleni büntetőjogi fellépésről az egyes tagállami szabályozás tükrében. Miskolci Jogi Szemle 2017/2. 51. o.

4. A kriptovaluták büntető anyagi és eljárásjogi kérdései

4.3. A kriptovalutákról általában

A blockchain technológia[407] megjelenésével párhuzamosan terjedt el a virtuális fizetési és értékképzési rendszerként működő kriptovalutáknak a használata. A bitcoin 2009-es bevezetése óta, a kriptovaluták témakörét különböző szakpolitikai döntéshozók vizsgálták eltérő megközelítést alkalmazva, azonban közös vonás, hogy valamennyien a virtuális fizetőeszközök egyik alcsoportjának sorolták be.[408] Nem tekinthetők pénznek, mert a pénzkibocsátás intézmény által, szigorúan szabályozott keretek között történik, ezzel szemben a kriptovaluták nem rendelkeznek központi kibocsátóval, hanem komplex matematikai feladatokat megoldó számítógépek hálózatának segítségével jönnek létre. Fizikai formában nem, csak digitálisan érhetők el, de törvényes fizetőeszközre át- és visszaválthatók, valamint egyes kriptovaluták nem hozhatók létre végtelen mennyiségben.

A kriptovaluták rendszere decentralizált, vagyis közvetítő közbeiktatása nélkül működik, ami azt jelenti, hogy az 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. Nincs mögötte aranyalap, valuta vagy egy állam gazdasága, a kriptovaluta

[407] 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: https://www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html

[408] Az Európai Központi Bank a virtuális fizetőeszközöket három csoportra osztotta: a zárt rendszerrel rendelkezőkre, amelyek nem válthatók át valódi pénzre ilyenek például a játékon belüliek (pl. World of Warcraft Gold); a félig nyitott rendszerűekre, és ezeket a virtuális fizetőeszközöket valódi pénzért lehet meghatározott árfolyamon, a fejlesztő által támogatott platformon keresztül vásárolni (pl. Facebook Credits), azonban visszaváltásra nincs lehetőség; végül a teljesen nyitottak azok, amelyek kétirányban támogatottak, vagyis az átváltási lehetőség oda-vissza biztosított. A kriptovaluták az utóbbi csoportba tartoznak. Lásd ehhez részletesen a következő: EUROPEAN CENTRAL BANK: Virtual Currency Schemes. Frankfurt, 2012. 13. o., https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf; valamint a Pénzügyi Akció Munkacsoport (Financial Action Task Force, FATF) hasonlóan átváltható és nem átváltható virtuális fizetőeszközöket különböztet meg. Lásd FATF: Virtual Currencies - Key definitions and Potential AML/CFT Risks. 2014. 4. o; Bővebben még: HOUBEN, Robby - SNYERS, Alexander: Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Union, 2018. 20-22. o., valamint http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf [2019.02.11.]

értékét kizárólag annak kereslete és kínálata határozza meg. A kriptovaluták alapját – mint ahogy az elnevezésük is utal rá –a kriptográfia jelenti, ami egyszerűen fogalmazva, egy az információ védelmét biztosító technika azáltal, hogy titkosítja, azaz olvashatatlan formátumra alakítja át azt, amit csak a titkosítást feloldó kulccsal rendelkező személy képes feloldani.

A bitcoin (BTC) az első blockchain alapú kriptovaluta. A bitcoin lényegét tekintve egy generált számítástechnikai adat, amely tranzakciók feldolgozása és jóváhagyása révén keletkezik, egy előre meghatározott rendben, algoritmus alapján. Ezt a folyamatot nevezzük bányászásnak. Az így keletkező virtuális "érméket" a rendszer elosztja a bányászok között, akik a rendelkezésük alatt álló számítógépekkel támogatják és üzemeltetik a hálózatot. A létrehozható érmék száma korlátozott, maximum 21 millió bitcoint bányászhatnak ki. A rendszer lényege miatt az újabb érmék előállítása egyre nagyobb és nagyobb erőforrásokat igényel.[410]A Bitcoin elnevezés egyben egy digitális fizetési rendszert is magában foglal[411], amelynek a kifejlesztése Satoshi Nakamoto nevéhez fűződik.[412] Kliensszoftvere ingyenes, nyílt forráskódú[413], a bitcoin tranzakciók nyilvánosan nyomon követhetőek – 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.[414] Ezek ezért az ún. pszeudoanonim tranzakciók.[415]

Digitális javaknál felmerül egy másik probléma, ami a fizikai formában létező eszközöknél nem. Egy adott pénzérme vagy bankjegy fizikailag csak egy valakinek a birtokában lehet, míg virtuális javakat korlátlan mennyiségben másolhatunk, így több, az eredetivel egyező másolatpéldány jöhet létre. Nyilvánvaló, hogy nem engedhető meg, hogy ugyanazt az érmét valaki több helyen is elköltse, és ezáltal egynél több személy birtokolja. Ennek megoldására a Bitcoin rendszerben a résztvevők csak azt a tranzakciót fogadják el érvényesként egy adott

[410] SZATHMÁRY Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11. 642. o.

[411] A Bitcoin elnevezés nagy kezdőbetűvel a rendszer üzemeltető blokklánhálózatra utal, míg a bitcoin szó a kis kezdőbetűvel a hálózaton elérhető kriptovalutára.

[412] A név valójában egy magát meg nem nevező programozót - vagy programozók csoportját - takar. Lásd: SATOSHI Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. White Paper, 2008.

[413] A „nyílt forráskód" azt jelenti, hogy a technológia és a szoftver beépített, tesztelhető és a felhasználók együttműködésén keresztül fejlesztik.

[414] Lásd https://blockchain.info/ oldalon a Bitcoin – és már Ether – tranzakciók nyomon követhetők.

[415] 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". Lásd ehhez SZÉKELY Iván: Privát szférát erősítő technológiák. Információs Társadalom 2008/1. 25. o.

érme elköltésére, amelyik időben előbb következett be, ezáltal kiküszöbölhető a „kétszeres elköltés problémája”.[416]

Az utaláshoz egy kulcspár szükséges, ami áll egy nyilvános kulcsból (public key), ez másnéven a Bitcoin-cím[417], ami hasonló a bankszámlacímhez és mindenki számára nyilvános, valamint egy privát kulcsból (private key)[418], ami jelszóként funkcionál és csak az adott felhasználó számára elérhető. A privát kulcs ismerete szükséges ahhoz, hogy az adott címhez kapcsolt bitcoin egységeink felett rendelkezhessünk és utalásokat végezzünk. A privát kulcsból kinyerhető a nyilvános kulcs, míg fordítva erre nincs lehetőség. A kulcspár segítségével utalhatunk a kliensprogramon keresztül, ami egy ún. virtuális pénztárca (wallet) is egyben, és ennek egyben a fő funkciója a privát kulcs létrehozatala és tárolása. A kriptovaluta tárcánk nem más, mint egy fájl a számítógépen, amelyet „wallet.dat" néven találhatunk meg.[419] Ennek védelme érdekében számos intézkedés tehető, így például a fájl titkosítható, biztonsági másolat készíthető róla, vagy akár online, jelszóval ellátott tárhelyen tárolható, akár a felhőben.[420] Különböző kriptovaluta tárca típusok használhatók, amelyek között vannak az internetre valamilyen formában csatlakozó ún. „forró tárcák” (hot wallet):

- Asztali vagy mobiltárca: a privát kulcsot a számítógépen (pl. Jaxx) vagy a mobiltelefonon tárolják.
- Web alapú pénztárca: egy szolgáltató online felületén érhető el (pl. Coinbase), azonban ebben az esetben nem mi rendelkezünk a privát kulcsunkkal és ez kockázatos, mert a pénztárca-szolgáltatók gyakran célpontjaivá válnak a kibertámadásoknak és további visszaélésekre adnak lehetőséget.

A másik típus az ún. hideg vagy offline tárolás, ami biztonságosabb megoldást nyújt:

- Hardveres pénztárca: hardverkulcs alkalmazását jelenti, amely egy speciális pendrive-hoz hasonló eszköz, a hardverbe épített elektronika tárolja a privát kulcsot (pl. Ledger Wallet, Trezor).
- Papír alapú tárca: a kulcspár papírra történő kinyomtatását jelenti (pl. QR-kódként).
- Agypénztárca (brain wallet): amikor a felhasználó megjegyzi a privát kulcsot.[421]

Érdemes ismertetni a kriptovaluták piacán jelenlévő kulcsszereplőket is:

---

[416] TÜZES Marcell: Bitcoin - A pénz új formája. Infokommunikáció és jog 2012/4. 156. o.
[417] 1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55
[418] 5JBvhsfA5JesmcVTGNrb3gkHGgv67hwY5hUws1Pmdj65jRM9nPF
[419] ESZTERI Dániel: Bitcoin - Az anarchisták pénze vagy a jövő fizetőeszköze? Infokommunikáció és Jog 2012/2. 71. o.
[420] SZATHMÁRY (2015): i.m. 642-643. o.
[421] SIMON Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK-MTA TK JTI. Budapest-Pécs, 2019. 175. o.

- a felhasználók: akik a kriptovalutával rendelkező természetes vagy jogi személyek;
- a bányászok: akik a tranzakciók jóváhagyásában vesznek részt – amihez a hálózatban résztvevők 51%-ra van szükség – és ezért cserébe a kibányászott kriptovalutából meghatározott egységet kapnak, valamint csekély tranzakciós díjba részesülnek;
- a kriptovaluta tőzsdék és átváltók (cryptocurrency exchanger): akik a felhasználók számára nyújthatnak különböző szolgáltatást, így – a hagyományos tőzsdékhez hasonló módon – a kriptovaluták eladását és vételét meghatározott árfolyam alapján[422] (kriptotőzsde mint a Coinbase) és/vagy a kriptovaluták fiat pénzre vagy másik (pl. Kraken) kriptovalutára történő átválással (pl. Binance) meghatározott díj ellenében (átváltó-szolgáltató), emellett a pénztárca szolgáltatóknak megfelelő funkciókkal is rendelkezhetnek (pl. Bitfinex). A rendelkezésre álló szolgáltatások típusa szolgáltatónként eltérhet. Általában minden kriptotőzsde egyben átváltó is, azonban nem minden átváltó kriptotőzsde.
- kereskededési platformok: amelyek színteret biztosítanak a felhasználók számára, hogy egymás között bonyolítsák le a kriptovaluta adásvételüket (pl. LocalBitcoins).
- letétkezelő pénztárca-szolgáltatók: akik a felhasználók virtuális pénztárcáinak, a kulcspároknak nyújtanak online tárolási lehetőséget.[423]

A bitcoinon kívül érdemes az egyéb kriptovalutákról, ún. altcoinokról[424] is említést tenni, amelyek más előnyös tulajdonságokkal rendelkeznek, és ezért egyre többen használják ezeket, mint például ilyen az Ether, Dash, Zcash és a Monero.

Ethereum (ETH) egy decentralizált platform, amely okosszerződéseket[425] futtat, éppen ezért az alkalmazásában sokkal nagyobb lehetőség rejlik. Az Ether a kriptovaluta. Az Ether kínálata növekszik és évente kerül korlátozásra. A kriptovaluta kereskedésen kívül az Ethert a fejlesztők is használják az Ethereum hálózaton történő szolgáltatások fizetéséhez. Az Etherum gyorsabb tranzakciókat biztosít: a bitcoin esetén 10 perc egy utalás, míg az Etherum használatakor 14 másodperc.[426]

[422] TÜZES: i.m. 157. o.
[423] HOUBEN - SNYERS: i.m. 25-27. o.
[424] Altcoinokon belül vannak, amelyek a Bitcoin nyílt forráskódját használják (pl. Litecoin) és vannak, amelyek a saját forráskódjukat és elosztott főkönyvüket (pl. Ethereum és a Ripple).
[425] Az okosszerződés egy olyan számítógépes protokoll, melyben egy digitális szerződés előre meghatározott feltételekkel teszi lehetővé a szerződő felek között a tranzakció megvalósulását. A szerződésben rögzített feltételek végrehajtásához nincs szükség harmadik félre. Lásd bővebben KŐLVART, Merit - POOLA, Margus - RULL, Addi: Smart Contracts. In: Kerikmäe, Tanel - Rull, Addi (eds.): The Future of Law and eTechnologies. Springer, 2016. 133-145. o.; valamint MIK, Eliza: Smart contracts: terminology, technical limitations and real world complexity. Law, Innovation and Technology 2017/2. 4-6. o.
[426] GIRASA, Rosario: Regulation of Cryptocurrencies and Blockchain Technology: National and International Perspectives. Palgrave Macmillan, 2018. 39-40. o.

A Dash (DASH) szintén bányászható és nyílt forráskódú kriptovaluta. A bitcoinhoz képest gyorsabb, 4 másodperc alatt végzi az utalásokat. Emellett lehetővé teszi a privát védelmet a blokkcsatornán, különösen a „PrivateSend" funkció választásával, ami az ún. „coin-mixing" szolgáltatás használatával történik, így a tranzakció során az adott felhasználó által küldött összeget összekeverik más felhasználókéval annak érdekében, hogy ne lehessen visszakövetni annak az eredeti forrását.[427]

A Zcash (ZEC) szintén egy decentralizált és nyílt forráskódú kriptovaluta, amely azonban már a teljesen nyílt tranzakciótörténetet biztosító típusokkal ellentétben lehetőséget ad a résztvevő feleknek, hogy a pénzügyi műveletek részleteit titkosítsák. A Zcash esetén is a tranzakciókkal kapcsolatos információk nyilvánosan hozzáférhetők a blokkcsatornán, de a feladók és a címzettek azonosítója, valamint a tranzakciók összege továbbra is rejtve maradhat. A kétféle cím – egy nyilvános cím és egy privát cím – közül maguk a felhasználók választhatnak, hogy elkívánják-e rejteni a tranzakciós adatokat vagy sem.

A Monero (XMR) ennél is nagyobb adatvédelmi biztonságot kínál, mivel beépített funkcióként az összes tranzakció teljesen rejtve van a kriptográfia mögött, ami egyaránt titkosítja a feladó és címzett feleket, valamint az átutalt összegeket.[428]

Mindezek alapján megállapítható, hogy az egyes kriptovaluták 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.

Az elmúlt években a bitcoin piaci részesedése a kriptovaluták között csökkent (2015-ben 80%, míg 2017-ben 35%), azonban még mindig első helyen szerepel a bűnelkövetők által használtak közül.[429]

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

[427] HOUBEN - SNYERS: i.m. 48-49. o.
[428] HOUBEN - SNYERS: i.m. 45-46. o.
[429] EUROPOL (2018): i.m. 58. o.

Problematikus, hogy a virtuális fizetőeszközöknek nincs egységes szabályozásuk, ezért jelenleg egy jogi „szürke zónát” képeznek. Vannak azonban országok, amelyek már állást foglaltak a kriptovalutákkal kapcsolatban. Az egyik legprogresszívebb szabályozással Japán rendelkezik, mert a kriptovalutákat fizetőeszközként fogadja el. Továbbá a kriptovaluta átváltó szolgáltatók tevékenysége is részletesen szabályozott. Például a működésük regisztrációhoz kötött és szigorú kiberbiztonsági, valamint pénzmosás és terrorizmus finanszírozása megelőzésének az értekében támasztott követelményeknek kell megfelelniük.[430] Németországban a Pénzügyminisztérium állásfoglalása alapján „elszámolási egységnek” minősülnek és szabadon lehet kereskedni velük. Az Egyesült Államokban szövetségi és tagállami szinten kerültek szabályozásra, azonban a különböző szabályozó szervek eltérően értékelik a jogi besorolásukat.[431]

A központi bankok általában egységes állásfoglalásokat fogalmaztak meg e kérdésben, így például az Európai Központi Bank és a Magyar Nemzeti Bank is már több ízben közleményt tett közzé, amelyekben felhívják a figyelmet arra, hogy a virtuális fizetőeszközök nem minősülnek törvényes fizetőeszköznek, illetve pénznek sem. Véleményük szerint a fizetésre alkalmas virtuális eszköz elnevezés lenne a helyes. Figyelmeztetnek, hogy ezen eszközök esetében hiányoznak a megfelelő felelősségi, garanciális és kárviselési szabályok is, amelyek például visszaélés, ellopás esetén védenék a fogyasztók érdekeit.[432]

Érdemes megemlíteni, hogy a hazai szakirodalomban Eszteri Dániel és Szathmáry Zoltán már részletesen vizsgálták a virtuális fizetőeszközök jogi státuszát a nemzeti jogban és megállapították, hogy nem tekinthetők a következőknek: pénznek, értékpapírnak, vagyoni értékű jognak, árucikknek, valamint szellemi terméknek.[433] Eszteri szerint a bitcoin-mennyiség feletti rendelkezési jogosultság a felhasználó vagyoni értékű jogként csak akkor tekinthető, ha az adott bitcoin-mennyiség egy konkrét szerződéses viszonyban jelenik meg. Azonban a bitcoin puszta létét a jelenlegi jogszabályi környezet nem tudja kezelni.[434]

[430] A módosított Payment Services Act No. 59. of 2009.
[431] BLEMUS, Stéphane: Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide. Corporate Finance and Capital Markets Law Review 2017/4.
[432] https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2016-evi-sajtokozlemenyek/fokozott-kockazatot-hordoznak-a-vilaghalon-elerheto-virtualis-fizetoeszkozok
[433] Lásd ESZTERI (2012): 71-78. o.; valamint SZATHMÁRY (2015): i.m. 643-644. o.
[434] ESZTERI Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és jog 2017/1. 30. o.

4.4. A kriptovaluták bűnelkövetési célú felhasználása

Az Europol az évente közzétett jelentéseiben felhívja a figyelmet a kriptovaluták bűnelkövetési célú felhasználására, és rámutat arra, hogy ez átlépett egy olyan értéket, ami a rendvédelmi szervek fokozott figyelmét teszi szükségessé.

A virtuális fizetőeszközökkel összefüggő bejelentések száma emelkedést mutat Magyarországon is. 2017-ben a Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda összesen 38 virtuális fizetőeszközökkel kapcsolatba hozható bejelentést kapott, ezen felül 3 tájékoztatást és 1 megkeresést fogadott külföldi pénzügyi információs egységektől. A bejelentések kétharmadában jellemzően megjelennek az ismertebb virtuális fizetőeszköz váltó platformok. 2017-ben 4 esetben került sor információtovábbításra, amelyek címzettjei 3 esetben valamely rendőrségi szerv, egy esetben a Terrorelhárítási Központ volt.[435]

A következő részben részletesen elemzem a kriptovalutákkal összefüggő egyes bűncselekményeket a hazai és uniós szabályozásra tekintettel.

4.4.1. Csalás

A kriptovaluták megvásárlására általában vagy egy másik ilyen eszközzel rendelkező felhasználótól, vagy egy erre szakosodott tőzsdén keresztül van lehetőség. Az előbbi esetet kihasználva jelent meg egy olyan csalás módszer 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. Azonban ezt követően a fizetési számlán csalás jellegű tevékenység miatt az átutalások törlését és az összegek visszautalását kérték. [436]

Érdemes említést tenni egy hazai esetről, amelyről részletesen Eszteri írt.[437] A konkrét eset történeti tényállása a következő: a sértett és az I. rendű vádlott az e-mail üzenetváltás útján megállapodtak abban, hogy a sértett tulajdonában lévő 15 egységnyi bitcoint eladja I. rendű vádlott részére, aki ennek ellenértékét, összesen 2,5 millió forintot a bitcoin átutalását követően készpénzben fogja kifizetni. I. és II. rendű vádlott a megbeszélt helyen találkoztak a sértettel, aki magával hozta a laptopját, amit használva a vádlottak előtt átutalt 15 egységnyi bitcoint az

[435] NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: Éves jelentés – 2017. év, 11. o.
[436] NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: i.m. 11. o.
[437] ESZTERI (2017): i.m. 25-31. o.

elsőrendű vádlott által megadott címre. A sikeres átutalást követően II. rendű vádlott azt állította, hogy az átutalt bitcoin-mennyiség ellenértékeként ígért készpénz a parkolóban leállított gépjárműben található, ezért a sértett a vádlottak kísértetében elindult a parkolóba. A vádlottak a sértett előtt haladtak, majd miután kiléptek az áruház kapuján, hirtelen egymásra nézve és ezzel egymásnak jelt adva a személygépkocsihoz futottak, amibe mindketten beszálltak, majd az ajtókat belülről magukra zárták. A sértett a vádlottak távozását úgy akarta megakadályozni, hogy a személygépkocsi elé állt és abba kapaszkodott, amikor elindultak a gépjárművel. A kiérkező rendőrök a vádlottakkal szemben intézkedést foganatosítottak, így őket igazoltatták. Először mindössze közúti veszélyeztetés és súlyos testi sértés kísérlete miatt, később a sértett vallomása alapján azonban már csalással gyanúsították meg a vádlottakat. Az ügy megítélése szempontjából fontos, hogy a vádlottakat először igazoltató járőrök láthatóan nem voltak tisztában az elkövetett bűncselekmény súlyával és helyes minősítésével, a vagyon elleni elemet meg sem említették a jelentésben. Ennek megfelelően a sértett kérése ellenére a vádlottak informatikai eszközeit sem foglalták le a helyszínen. Az ügyészség a vádlottakat a Btk. 373. § (1) bekezdésébe ütköző és (3) bekezdés a) pontja szerint minősülő nagyobb kárt okozó csalás bűntett elkövetésével vádolta meg, mint társtetteseket. A vádlottak a sértettet szándékegységben cselekedve jogtalan haszonszerzés végett tévedésbe ejtették, mert a kialkudott vételár nem is állt a rendelkezésükre, és annak átadása nem is állt szándékukban. A bűncselekmény elkövetésével 2,5 millió forint kárt okoztak a sértettnek, ami nem térült meg. A sértett az ügy kapcsán polgári jogi igényt terjesztett elő. A járásbíróság is először csak a közlekedési és testi épség elleni elemet vizsgálta, a bitcoin mint pénzben kifejezhető ellenértékkel bíró virtuális vagyonelem értékelésétől pedig kezdetben elzárkózott.[438]

Emellett érdemes felhívni a figyelmet a kriptovaluták világán belül az egyre népszerűbb és önálló területet felölelő elsődleges érmekibocsátásra avagy angolul az „Initial Coin Offering”-re (a továbbiakban: ICO). „Az elsődleges érmekibocsátás az a folyamat, amelynek során az új kriptopénzt első alkalommal kínálnak eladásra az alkotók. Fiat vagy valamely vezető kripropénz (általában bitcoin és etherum) ellenében vásárolhatunk belőle. Az árusítás azelőtt indul, hogy a kriptopénz bármely kriptotőzsdén vagy bármely váltó kínálatában megjelenne.”[439] Ez egy nyilvános forrásgyűjtési módot jelent, valamely ötlet vagy vállalkozás finanszírozásához, egy blokklánc hálózat támogatásán keresztül. Ennek során az ötletgazda ún. „coin”-t (önálló, saját blokklánccal rendelkező kriptovalutát) vagy „token”-t (más által

[438] ESZTERI (2017): i.m. 25-26. o.
[439] GYÖRFI András: Az ICO – Így indul útjára egy kriptopénz. In: Györgyi András – Léderer András – Paluska Ferenc – Pataki Gábor – Trinh Anh Tuan: Kriptopénz ABC. HVG Könyvek, Budapest, 2019. 102. o.

létrehozott platformon alapuló kriptovaluta)[440] bocsát ki és kínál eladásra a támogatók részére hivatalos fizetőeszközért, vagy gyakrabban kriptovalutáért cserébe, így az ötletgazda, vagyis az ICO kibocsátója az eladott kriptovalutákból szerez pénzt az ötletmegvalósításához. Ezek a kriptoeszközök például megtestesíthetnek egy jövőbeni áru vagy szolgáltatás igénybevételére jogosultságot, az esetek többségében azonban nem mutatható ki a megtestesített érték. Gyakoriak a visszaélések, ugyanis sok esetben az ICO-val összegyűjtött pénzből nem kezdik el megvalósítani a kitűzött célt, sőt ez nem is állt szándékukban, ezáltal a csalás tényállását valósítják meg.[441] Éppen ezért a jegybankok többsége is figyelmeztet, hogy rendkívül kockázatos és spekulatív befektetési formának számítanak. 2018 elején pedig a visszaélések magas száma miatt több vezető technológiai vállalat is, például a Google és a Facebook is betiltotta az ICO hirdetéseket.[442]

A kriptovalutákhoz hasonló módon országonként eltérő a szabályozásuk, eddig az ICO-kal szemben a leghatározottabb fellépés Kína részéről történt, mert a központi bank illegálisnak minősítette az ICO-n keresztüli tőkebevonást és ezek azonnali beszüntetését rendelte el.[443] Érdemes megemlíteni Máltát, mert egy hiánypótló törvénycsomagot adott ki, amelyben részletesen szabályozza a virtuális eszközöket, szem előtt tartva a befektetők védelmét.[444]

Mindezekre tekintettel megállapítható, hogy a kriptovalutával összefüggésben elkövetett vagyon elleni bűncselekmény minősítése, a Btk. 373. §-ban szabályozott, hagyományos értelemben vett csalásnak felelhet meg. Ezzel kapcsolatban fontos a kárnak – mint tényállási elemnek – a fogalmával is részletesen foglalkozni. Ahogy ezt korábban már vizsgáltam 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. Azonban a Btk. 76. § értelmező rendelkezése 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

[440] GYÖRFI: i.m. 108. o.
[441] Az Egyesült Államokban az FBI letartóztatta az AriseBank igazgatóját azért, mert a befektetőket tévedésbe ejtve megközelítőleg 4 millió dollár értékben kárt okozott nekik. A vád szerint az ICO során a vállalkozásához, amit „az első decentralizált banki platformként" olyan szolgáltatásokkal hirdetett, amelyekre vonatkozóan nem rendelkezett engedélyekkel. Továbbá a saját AriseCoin virtuális fizetőeszközének kibocsátásával gyűjtött pénzt, majd ezt az összeget magáncélra költötte el. Lásd: https://www.justice.gov/usao-ndtx/pr/cryptocurrency-ceo-indicted-after-defrauding-investors-4-million [2019.01.15.]
[442] GYÖRFI: i.m. 104. o.
[443] https://fintechzone.hu/kriptovalutak-legfrissebb-fejlemenyek/ [2019.01.31.]
[444] A csomag három törvényt tartalmaz az innovatív technológiai megoldásokról és szolgáltatásokról, a Máltai Digitális Innovációs Hatóságról és a virtuális pénzügyi eszközökről. Lásd BUJTÁR Zsolt: A kriptovaluták európai és máltai szabályozásának az összehasonlítása - A máltai sólyom szárnyalása. Európai Jog 2018/5. 12-13. o.

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.[445] 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.[446]

4.4.2. A pénzmosás és a terrorizmus finanszírozása

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 eredménye. Ezeknek a jellemzőknek a kihasználásával egyúttal a kriptovaluták új lehetőséget - mint egy adóparadicsomat - jelenthetnek az adófizetés kikerülésére is, mert az adócsalók könnyebben tudják a segítségükkel elrejteni azon jövedelmeket és bevételeket, amelyek után nem kívánnak adózni. Az adócsalást egyszerűbbé teszi az is, hogy általában a kriptovaluta felhasználóknak nincs jelentési kötelezettségük.[447]

A tranzakciók szolgálhatják a legális üzleti műveletek elszámolását, de az illegális tevékenységekét is. A bűncselekményből származó pénzek kriptovalutákra történő átváltása, majd különböző címekre való továbbbutalása alkalmas ezek tisztára mosására. A pénzmosás valamennyi fázisa a virtuális fizetőeszközök használata során is – a fiat pénzekhez hasonló módon – megvalósulhat. Az elhelyezést a kriptovaluták megkönnyítik, mert anonim módon jelentős számú pénztárcát lehet létrehozni költségmentesen vagy alacsony költség és kockázat mellett. A rétegzés (bújtatás) megvalósul a többszöri átutalásokkal különböző pénztárcák között és/vagy különböző kriptovaluták és fiat pénzek, vagy kriptovaluták és kriptovaluták közötti átváltásával. Az „atomic swap” technológiai fejlesztés pedig még inkább elősegítheti a kriptovalutákkal kapcsolatos visszaéléseket. Az integráció megtörténhet a virtuális fizetőeszközöknek az árukra és szolgáltatásokra való váltásával vagy közvetlenül, vagy pedig

[445] MOLNÁR (2009): i.m. 702. o.
[446] ESZTERI (2017): i.m. 30. o.
[447] U.S. DEPARTMENT OF JUSTICE (2018): i.m. 55. o.

közvetve, fiat pénz útján, amit elősegít egyrészt mindazon áruk és szolgáltatások egyre növekvő száma, amelyekért a kriptovalutákat fizetőeszközként elfogadják. A másik megoldás a kriptovalutákba történő befektetés. Az intézményi befektetők számára is egyre inkább vonzóbbá váltak a virtuális fizetőeszközök piaca, amelyre befektetési, valamint kereskedési (spekulációs) szándékkal lépnek be. Ez a lépés jelentős likviditást biztosít ezeknek a piacoknak. Hasonlóképp, az olyan ICO-k is alkalmasak a bűnös eredetű pénz legalizálására, amelyeknél gyenge az ügyfélellenőrzés és ezt a bűnelkövetők kihasználhatják, a virtuális fizetőeszköz portfóliójukat más tokenekké alakítják az ICO-n keresztüli jegyzésekkel. A végső cél ez utóbbi esetén az, hogy a kriptotőzsdére bevezetésre került tokenekből vagy más virtuális fizetőeszközökben lévő befektetéseket kivegyék.[448]

A kriptovaluták átváltásával kapcsolatban különböző szolgáltatások érhetők el, amelyek a tranzakciók nyomon követhetőségét megnehezíthetik, így ezek a következők:

A már említett virtuális pénzváltó platformok, amelyek a kriptovaluták és a törvényes fizetőeszközök közötti átváltást segítik (pl. Kraken, Coinbase, Bitstamp). Ezek az olyan online kriptotőzsde vagy váltó szolgáltatók, akik nyílt és átlátható módon működnek (pl. ügyfélazonosítással, részletes felhasználási feltételekkel rendelkeznek).

Ezen kívül vannak a Darknet fórumokon elérhető ún. „mixing" vagy „tumbling" szolgáltatások, amelyek vagy egy közös, nagyobb összeget tartalmazó címet bontanak fel kisebbekre vagy fordítva több, kisebb összeget egyesítenek egy közös címen.[449] A céljuk ezzel az, hogy a többlépcsős tranzakciók lebonyolítása révén az eredeti forrás és az új kriptovaluta cím közötti kapcsolatot rejtsék el annak érdekében, hogy azt ne tudják azonosítani. Gyakran ezek a szolgáltatók azzal reklámozzák magukat, hogy a tranzakciók előzményeit is törlik rövid időn belül.

ShapesShift a különböző kriptovaluták közötti átváltást biztosítja, amelynek használata már regisztrációhoz kötött.[450]

Atomic swap használatával harmadik fél közbeiktatása nélküli más kriptovalutára történő átváltásra van lehetőség okosszerződés révén.

---

[448] POSKRIAKOV, Fedor - CHIRIAEVA, Maria - CAVIN, Christophe: Cryptocurrency compliane and risks: a European KYC/AMLP perspective. In: Dewey, Josias (ed.): Blockchain & Cryptocurrency Regulation 2019. Global Legal Group, 2019. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/13-cryptocurrency-compliance-and-risks-a-european-kycaml-perspective

[449] ESZTERI (2017): i.m. 27. o.

[450] https://shapeshift.io/

2013 óta az Egyesült Államokban a kriptovalutákkal kapcsolatos szolgáltatást nyújtó vállalkozások gyakorlatilag azonos megítélés alá esnek a pénzügyi szolgáltatást nyújtó egyéb vállalkozásokkal.[451]

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[452] – 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. A 3. cikk 19. pont értelmében: „olyan digitális értékmegjelenítés, amelyet nem központi bank vagy közigazgatási szerv bocsát ki vagy garantál, nem feltétlenül kapcsolódik rendeleti pénzekhez, és nem rendelkezik rendeleti pénz vagy pénz jogi státuszával, de természetes vagy jogi személyek elfogadják csereértékként, valamint elektronikusan átutalható, tárolható és lehet vele elektronikusan kereskedni.” Emellett a virtuális fizetőeszközök nem tévesztendők össze az elektronikus pénzzel, a pénz átfogóbb fogalmával[453], az (EU) 2015/2366 irányelv 3. cikkének k) és l) pontjában meghatározottak szerint mentesített eszközökön tárolt monetáris értékkel, illetve a kizárólag egy adott játékkörnyezeten belül használható, játékalapú fizetőeszközökkel. Bár a virtuális fizetőeszközöket gyakran használják fizetőeszközként, azok más célokra is felhasználhatók és szélesebb körben alkalmazhatók, például csereeszközként, befektetési eszközként, értéktároló termékként vagy online kaszinókban. Az ötödik pénzmosás elleni irányelv célja a virtuális fizetőeszközök valamennyi lehetséges felhasználásának szabályozása.

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 3. cikk 19. pontja határozza meg, amely alapján: „olyan szervezet, amely ügyfelei nevében virtuális fizetőeszközök tartására, tárolására

[451] Lásd ehhez Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. 2013. https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[452] Az Europol jelentése szerint megfigyelhető a terrorizmus finanszírozás terén a kriptovaluták használata, azonban a felderített esetek száma alapján ez még nem számottevő. Lásd EUROPOL: European Union Terrorism Situation and Trend Report 2018. 12. o.

[453] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelv 4. cikkének 25. pontjában meghatározott „pénz”: bankjegyek és pénzérmék, számlapénz, vagy a 2009/110/EK irányelv 2. cikke 2. pontjában szereplő meghatározás szerinti elektronikus pénz.

és átutalására szolgáló kriptográfiai magánkulcsok megőrzésével kapcsolatos szolgáltatást nyújt".

Az új szabályozás lényegét tekintve abból indul ki, hogy a virtuális fizetőeszközök rendszere decentralizált, mert nincs központi felügyeleti szervük, ezért nem lehet kihez fordulni a tranzakciókkal kapcsolatos információkért. Azonban az ötödik pénzmosás elleni irányelvben szabályozott szolgáltatók segítségével a kriptográfiai kulcsok – vagyis a címek és privát kulcsok – a regisztrált ügyfelekhez tartoznak, akik ezáltal beazonosíthatók, és ezen szolgáltatók biztosíthatják a tranzakciókra vonatkozó további adatokat a hatóságok részére, azokban az esetekben, amikor a felhasználók igénybe vesznek ilyen jellegű szolgáltatásokat.

A cél ezáltal, hogy a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem érdekében az illetékes hatóságoknak képeseknek kell lenniük arra, hogy a kötelezett szolgáltatók révén nyomon kövessék a virtuális fizetőeszközök használatát. 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. A kötelezett szolgáltatóknak a lehető legtöbb adatot be kell gyűjteniük az ügyfeleikről annak érdekében, hogy tisztába legyenek azok tevékenységével, üzleti kapcsolataik jellegével, pénzügyi szokásaikkal. Az ügyfélmegismerés és a tranzakció monitoring együttesen biztosíthatja a rendszer átláthatóságát. Az átváltó és pénztárca-kezelő szolgáltatók esetében a következő intézkedések fontosak: az ügyfél azonosítása a felhasználói fiók nyitásakor, nyilvántartás vezetése és beszámolók készítése, gyanús tevékenységek jelentése, belső szabályozási rendszer kiépítése (pl. belső szabályzatok, képzések, compliance officer alkalmazása stb.).[454]

Az ötödik pénzmosás elleni 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. Azonban érdemes kitérni arra, hogy a virtuális fizetőeszközök egymás közötti átváltását biztosító szolgáltatókra, valamint a kriptotőzsdékre és a kereskedési platformokra nem terjed ki a hatálya.

[454] Érdekesség, hogy az Egyesült Államok adóhatósága, az Internal Revenue Service (IRS) és az Igazságügyi Minisztérium Adóosztálya egymással együttműködve kiadta és érvényesítette az első virtuális fizetőeszközzel kapcsolatos „John Doe" idézést a világ egyik legnagyobb kriptotőzsdéjével (Coinbase) szemben. Ennek eredményeképpen a szolgáltató köteles volt átadni a 20, 000 $ kereskedési forgalom feletti fiókokra vonatkozó ügyfél információkat. Ezek azért fontos, mert elősegítheti az ügyfelek azonosítását és a nyomozás eredményes lefolytatását. Lásd ehhez bővebben: United States v. Coinbase, Inc. et al., Order Regarding Petition to Enforce IRS Summons at 14 (Doc. 78), Case No. 3:17-cv-01431 (N.D. Cal.).

Megállapítandó, hogy ez nem oldja meg teljes mértékben a virtuális fizetőeszközökkel végrehajtott műveletek anonimitásával kapcsolatos problémákat, mivel a felhasználók az ilyen szolgáltatók igénybevétele nélkül is végezhetnek műveleteket, hiszen nem kell azokat szükségszerűen átváltani törvényes fizetőeszközre. Az anonimitással kapcsolatos kockázatok elleni küzdelem érdekében lehetővé kell tenni a nemzeti pénzügyi információs egységek számára az ahhoz szükséges információk begyűjtését, hogy a virtuális fizetőeszköz címét a virtuális fizetőeszköz tulajdonosának kilétével tudják társítani. Emellett tovább kell vizsgálni annak lehetőségét, hogy a felhasználók önkéntes önbevallás formájában nyilatkozatot tehessenek a kijelölt hatóságoknak.

Az ötödik pénzmosás elleni irányelv tagállamok kötelesek 2020. január 10-ig kell átültetni a nemzeti jogukba. A Bizottság 2022. január 11-ig, majd azt követően háromévente jelentést készít a végrehajtásáról, és benyújtja azt az Európai Parlamentnek és a Tanácsnak. Az első jelentéshez, amelyet 2022. január 11-ig tesznek közzé, szükség esetén megfelelő jogalkotási javaslatokat kell mellékelni, ideértve adott esetben a virtuális fizetőeszközökkel, a felhasználók kilétét és a pénztárcacímeket rögzítő, a pénzügyi információs egységek számára hozzáférhető központi adatbázis létrehozására és fenntartására vonatkozó felhatalmazásokkal, valamint a virtuális fizetőeszközök felhasználói számára kidolgozott nyilatkozatmintákkal, és a tagállami vagyon-visszaszerzési hivatalok közötti együttműködés javításával, valamint a 20. cikk b) pontjában említett intézkedések kockázatalapú alkalmazásával kapcsolatban.

Érdekességként megemlítendő, hogy korábban csak egyetlen alkalommal került sor uniós szintű döntésre a virtuális fizetőeszközökkel kapcsolatban. Ennek során az Európai Unió Bírósága foglalkozott a bitcoin jogi értékelésével, méghozzá egy adózás kapcsán előterjesztett előzetes döntéshozatali eljárásban. 2015-ben a Bíróság állást foglalt arról, hogy a bitcoinok nemzeti (hivatalos) devizára való váltása áfa köteles vagy áfamentes tevékenységnek minősüle. A Bíróság megállapította, hogy a hagyományos devizák bitcoinra való át- és visszaváltása ellenérték fejében teljesített szolgáltatásnyújtásnak minősülnek. Tekintettel arra, hogy a bitcoin virtuális devizának nincs más célja, mint az, hogy fizetőeszközként használják, és e tekintetben egyes gazdasági szereplők elfogadják azt, ezért a Bíróság úgy döntött, hogy indokolt az adómentesség alkalmazása a bitcoin és a hagyományos devizák átváltására irányuló szolgáltatás esetén is. Az ítélet következetesen a bitcoinra a „virtuális deviza” kifejezést használja és a Bíróság szerint a 2009/110/EK irányelvben meghatározott elektronikus pénztől

annyiban különbözik, hogy az összegeket nem hagyományos számítási egységben, hanem olyan virtuális egységben fejezi ki, mint a bitcoin.[455]

A következőkben a pénzmosás hazai szabályozását vizsgálom a kriptovalutákra tekintettel. Először a pénzmosás elkövetési tárgyával foglalkozom, amely a bűncselekményként büntetendő cselekményből származó dolog. A dolog fogalmát sem a Btk., sem a Ptk. külön nem definiálja, hanem a Strasbourgi Egyezménynek az értelmező rendelkezése határozza meg az 1. cikk b) pontjában, amely szerint a „dolog": bármilyen dolog lehet, legyen az megfogható vagy megfoghatatlan, ingó vagy ingatlan, illetve olyan jogi irat vagy okmány, amely az ilyen dolgokra vonatkozó jogosultságot, vagy ahhoz fűződő érdeket igazol. Ez a fogalommeghatározás a pénzmosás tényállásának alkalmazása során közvetlenül érvényesítendő. A Ptk. az 5:14. § (1) bekezdésében annyit rögzít, hogy a birtokba vehető testi tárgy tulajdonjog tárgya lehet. A Btk. a 402. § (1) bekezdésében foglalt értelmező rendelkezés értelmében a 399-400. § alkalmazásában dolgon a vagyoni jogosultságot megtestesítő olyan okiratot, dematerializált értékpapírt is érteni kell, amely a benne tanúsított vagyoni érték vagy jogosultság feletti rendelkezést önmagában, illetve dematerializált formában kibocsátott értékpapír esetén az értékpapírszámla jogosultjának biztosítja.

Szathmáry Zoltán a kriptovalutáknak számítástechnikai adatként való kezelését tartja elfogadhatónak – a megfelelő polgári jogi besorolás hiányában – a büntető anyagi és eljárásjogi szabályok szempontjából.[456] A kriptovaluta egy vagyoni értéket megtestesítő számítástechnikai adat, amelyet fizetésre használnak. Szathmáryval egyetértve, megítélésem szerint is a megoldást a dolog fogalmának kiterjesztése jelentené egy értelmező rendelkezés keretében. Javaslata szerint ez a következőképpen történne: „vagyoni értéket önmagában vagy feldolgozása révén biztosító, fizetésre használt elektronikus adat vagy adatok összessége, ideértve a fizetés elektronikus nyilvántartási egységét is."[457]

A másik kérdés az elkövetési magatartással függ össze, méghozzá a saját pénzmosás esetén, a dolog eredetének eltitkolása, elleplezése céljából a pénzügyi tevékenység végzése, vagy pénzügyi szolgáltatást igénybevételekor, amelyet a törvény a Btk. 402. § (2) bekezdésében foglalt értelmező rendelkezéssel határozza meg. Ez azért is fontos, mert az elkövetők gyakran különböző átváltó vagy pénztárca-kezelő szolgáltatókat vesznek igénybe, amelyeken keresztül utalásokat végeznek vagy átváltják a kriptovalutákat. Felmerül a kérdés, hogy ezen szolgáltatók tevékenysége pénzügyi szolgáltatási vagy kiegészítő pénzügyi szolgáltatási tevékenységnek

[455] C-264/14. sz. Skatteverket kontra David Hedquist ügy
[456] SZATHMÁRY (2015) i.m. 644. o.
[457] SZATHMÁRY (2015): i.m. 646. o.

minősül-e a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény értelmében. Jelenleg azonban még nem. Ehhez a háttérjogszabály módosítása szükséges, azonban ez nem a büntetőjog feladata. Ez rámutat arra, hogy nemcsak magát a kriptovalutát kell a jognak kezelnie, hanem a használatához köthető tevékenységeket, hasznosítási formáit is például a fizetési rendszer működtetést, kereskedési felület üzemeltetést, bányászatot, tárolást, vagy a kriptovaluta alapú származtatott termékeket. Ezek a tevékenységek jelenleg nem illeszthetők be maradéktalanul a pénzügyi jogi tárgyú törvényeink fogalmi rendszereibe, ezért azok módosítására, kiegészítésére lesz szükség.

Virtuális fizetőeszközök bevonásával olyan hagyományos és jól ismert pénzmosási módszerek is új színezetet kaphatnak, mint a money mule jelenség. Ebben az esetben az elkövetők magukat virtuális pénzváltó platformok képviselőjének kiadva munkaszerződést ajánlanak, amelynek keretében a megkeresett fél „munkája" annyi lenne, hogy saját fizetési számláján a pénzváltótól származó jelentősebb összegeket kell fogadnia, majd azt készpénzben felvenni, vagy a „munkáltató" által megadott fizetési számlákra továbbutalni – természetesen jutalékért cserébe. Aki ilyen jellegű ajánlatot elfogad, maga is érintetté válik a pénzmosás gondatlan alakzatának elkövetésében.[458]

4.4.3. Darknet piacterek és fórumok

A kriptovalutákkal használatának a megjelenése a Darknethez köthetők. A különböző online piactereken és fórumokon virtuális fizetőeszközként (pl. bitcoin, Ether, Monero, Zcash) alkalmazzák a tilalmazott árukkal való kereskedés során, valamint a szolgáltatások ellenében. Érdekesség, hogy a Silk Road leállításakor közel 30,000 bitcoin-egység került lefoglalásra, ami akkoriban közel 20 millió dollárt ért.

4.4.4. Zsarolás

A zsarolás hagyományos bűncselekménytípus, de amint korábban is felhívtam a figyelmet rá, hogy a technológiai fejlődésnek köszönhetően már az infokommunikációs technológia és a virtuális fizetési rendszerek felhasználásával is elkövethető. Általában az informatika környezetben e bűncselekmény az elkövetők részéről fenyegetéssel valósul meg például a DDoS-támadások indítását, vagy a zsarolóvírus által titkosított adatok törlését, vagy a

[458] NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: Éves jelentés - 2016. év, 15. o.

jogosulatlanul megszerzett személyes adatok nyilvánosságra hozatalát helyezik kilátásba, majd a „váltságdíjat” kriptovalutákban kérik.[459]

4.4.5. Az információs rendszer elleni bűncselekmények

A kriptovaluták népszerűsége egyúttal a bűnelkövetők számára új célpontokat szolgáltatott: a kriptovaluta felhasználókat, az átváltó és letétkezelő pénztárca-kezelő szolgáltatókat, valamint kriptotőzsdéket és egyéb befektetési szolgáltatókat. Akiket – a pénzintézetekhez és azok ügyfeleihez hasonló módon – adathalász kísérletekkel, rosszindulatú programok használatával, vagy hacking útján támadnak az értékes adatokért, így különösen a privát kulcsok és a pénztárca fájlok megszerzése érdekében.[460] A fizetésre használható, virtuális pénztárcák bármilyen eszközön vagy az online pénztárca-szolgáltatóknál tárolhatók, így – hasonlóan más digitálisan tárolt adatokhoz – a hozzátartozó kódok esetleges feltörésével, vagy azok megszerzésével a virtuális fizetőeszköz hozzáférhetővé, így ellophatóvá válik.

Ezekben az esetekben a digitális környezet elengedhetetlenül szükséges a kriptovalutákkal kapcsolatos visszaélések elkövetéséhez, így indokolt ezeket a virtuális „lopásokat” informatikai bűncselekményként értékelni.[461] Érdemes azonban megjegyezni, hogy a lopás tényállása megvalósulhat, amennyiben a kriptovalutát hardveres pénztárcán, azaz offline tárolják és azt veszik el.[462]

Ahogy korábban már említettem a 2019-es irányelv hatálya alá tartoznak a digitális pénztárcák is, ezáltal uniós szinten megjelent az a jogalkotói szándék, hogy megfelelő büntetőjogi védelmet nyújtsanak az ezekkel kapcsolatos – különösen a számítógépes csalás révén megvalósuló – büntetendő magatartások esetén, ugyanis a letétkezelő pénztárca-szolgáltatókkal és átváltókkal szemben elkövetett támadások gyakoriakká váltak (pl. Mt. Gox és Coincheck esete).[463]

Az információs rendszer elleni bűncselekmények elkövetési tárgyaként mint számítástechnikai adat jelenik meg a virtuális pénztárca. Mindezekre tekintettel a Btk. 375. §-

[459] Lásd MEZEI Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jogászegyleti Értekezések 9-10. Budapest, 2018. 169. o.
[460] EUROPOL (2018): i.m. 8. o.
[461] ESZTERI Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécs, 2015. 205. o.
[462] MISKOLCZI – SZATHMÁRY: i.m.163. o.
[463] A 2014-es Mt. Gox és a 2018-as Coincheck japán kriptotőzsdék támadása során az elkövetők több százmillió dollár értékben jutottak hozzá a kriptovalutákhoz, és ezek hatására szigorodott a japán szabályozás. Például fontos követelménnyé vált, hogy a regisztrált tőzsdék esetén az ügyfelek eszközei elkülönüljenek a tőzsdéétől. A Mt. Gox esetén a kettő még azonos volt. A jelenlegi szabályozásnak köszönhetően naponta kell ellenőrizniük, hogy rendelkeznek-e megfelelő fedezettel.

ába ütköző információs rendszer felhasználásával elkövetett csalást valósítja meg az az elkövető, aki a virtuális pénztárcához (wallet.dat fájlhoz), vagy az online pénztárca-szolgáltatónál tárolthoz fér hozzá egy kibertármadás következtében. Ebben az esetben az adott tárcához tartozó kriptovalutával is rendelkezni tud, így amennyiben pénzügyi műveletet – azaz a rendszerben módosítást – hajt végre, akkor ezzel kárt okoz. A károkozás hiányában viszont a 423. § szerinti információs rendszer vagy adat megsértésének deliktumáért vonható felelősségre az illető (pl. előfordul, hogy a szolgáltatóktól jogosulatlanul megszerzik a felhasználói adatokat, és azokat később használják fel vagy értékesítik). A másik egyre gyakoribb eset az ún. cryptojacking, ami olyan folyamatot takar, amelynek során a jogosult felhasználó engedélye nélkül az információs rendszernek a feldolgozási sebességét vagy sávszélességét használják célzottan kriptovaluta bányászatra (pl. ez történhet malware fertőzés révén, vagy a felhasználó által meglátogatott honlapba beépítve).[464]

A rosszindulatú programnak a készítője, illetve aki a jelszóként funkcionáló privát kulcsot átadja, hozzáférhetővé teszi, megszerzi, vagy forgalomba hozza, az a 424. § szerinti információs rendszer védelmét biztosító technikai intézkedés kijátszásáért felel.

4.4.6. Piramisjáték szervezése

Az egyes bűnelkövetői körök a virtuális fizetőeszközöket egyfajta hívószóként alkalmazzák, miközben tevékenységük nem más, mint a jól ismert, hagyományos piramisjáték. E szervezetek látszólag virtuális fizetőeszközökbe történő befektetést és irreálisan magas hozamokat ígérnek. Azonban, mint a piramisjátékok esetén, kézzelfogható, tényleges belső értéket hordozó termék vagy eszköz nem található, hátterében jellemzően pedig egy offshore cég áll.

Ehhez érdemes megemlíteni az ún. „OneCoin”-t, mely konstrukció látszólag valamiféle eszközbe történő befektetést tesz lehetővé, valójában azonban kereskedni kizárólag a tevékenységet szervező által üzemeltetett zárt és nem ellenőrizhető fórumon van mód, valamint az állítólagos virtuális fizetőeszköz értéke, árfolyama objektíven megállapíthatatlan. A rendszerbe magas hozamokat ígérve szerveznek az interneten keresztül új belépőket olyan módon, hogy utóbbiak befizetéseiből a korábban csatlakozottaknak – akiknek így erőteljes anyagi érdeke a marketing és a toborzás – jutalékot fizetnek.[465]

[464] EUROPOL (2018): i.m. 19. o.

[465] OneCoin értékesítésre Magyarországon is sor került, ezért az MNB Piacfelügyeleti munkacsoportja is folyamatosan megfigyelés alatt tartja ezt a sémát. Az MNB egyúttal közös fellépésről egyeztetett a Belügyminisztérium és a rendőrség különböző szerveivel, az adóhatósággal, illetve ügyészségi vezetőkkel. Lásd: https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2017-evi-sajtokozlemenyek/a-onecoin-elleni-fellepesrol-targyalt-a-piacfelugyeleti-munkacsoport [2019.01.15.]

Ez a Btk. 412. §-ban szabályozott piramisjáték szervezésének felel meg, amely szerint, aki mások pénzének előre meghatározott formában történő, és kockázati tényezőt is tartalmazó módon való összegyűjtésén és szétosztásán alapuló olyan játékot szervez, amelyben a láncszerűen bekapcsolódó résztvevők a láncban előttük álló résztvevők számára közvetlenül, vagy a szervező útján pénzfizetést vagy más szolgáltatást teljesítenek, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

4.5 A kriptovalutákkal kapcsolatos büntető eljárásjogi kihívások

A kriptovaluták egységes szabályozásának és jogi besorolásuknak a hiánya büntetőeljárásjogi szempontból is kihívást jelent, mivel felmerül a kérdés, hogy lefoglalás tárgyát képezhetik-e vagy sem. Az Egyesült Államokban és az Egyesült Királyságban is sor került a kriptovaluták lefoglalására[466], valamint Dél-Koreában a Legfelsőbb Bíróság először hozott a kriptovalutákkal kapcsolatban döntést, amelyben mérhető értékkel rendelkező eszközöknek tekinti ezeket, és mivel értékkel rendelkeznek, ezért lefoglalhatók.[467]

A Be. szabályozása szerint lefoglalni az ingó dolgot, a számlapénzt, az elektronikus pénzt vagy az elektronikus adatot lehet. A jövőben a decentralizált virtuális fizetőeszközök elektronikus adatként lefoglalás tárgyát képezhetik. A Be. 315. § (1) bekezdése értelmében az elektronikus adat lefoglalása történhet az elektronikus adatról való másolat készítésével, áthelyezésével, az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével, vagy ezek lefoglalásával. A 315. § (2) bekezdésének értelmében a fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, ha olyan műveletet végeznek, amely végül is a vagyoni érték feletti rendelkezési lehetőségét akadályozza meg. Ezzel kialakítva az ún. virtuális vagyontárgyak biztosításának a keretszabályát.[468]

A kriptovaluták esetében problémát jelent az, hogy a jogosult soha nincs fizikai birtokában a kriptovaluta-egységeinek. Mindenképpen a privát kulcsra van szükség ahhoz, hogy azokkal rendelkezni lehessen. Éppen ezért az áthelyezés, másolat készítés és az információs rendszerek vagy adathordozók lefoglalása sem vezethet feltétlenül eredményre, mert ugyan a pénztárca fájlt átmásolhatják vagy a lefoglalt eszközt (pl. hardver pénztárca) elvonhatják, fennállhat azonban annak a veszélye, hogy a jogosult előzőleg biztonsági másolatot készített róla, és akkor

[466] https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins; https://www.ccn.com/london-police-seize-500000-in-bitcoin-from-cyber-crime-wave-hacker/ [2019.01.21.]
[467] http://www.koreatimes.co.kr/www/biz/2018/05/488_249868.html [2019.01.21.]
[468] CZINE Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018. HVG-ORAC Jogkódex

továbbra is rendelkezhet a kriptovaluta egyenlege felett. A másik probléma, hogy a privát kulcs nélkül a hatóság nem tud hozzáférni a kriptovaluta-egységekhez, a gyanúsított pedig nem köteles ezeket átadni a nyomozó hatóság számára. Éppen ezért különösen nagy körültekintést igényel a nyomoknak (pl. a kinyomtatott privát kulcs vagy az információs rendszeren található pénztárca fájl) a felkutatása[469]. Mindez következik abból, hogy a büntetőeljárásban az önvádra kötelezés tilalma érvényesül, ami azt jelenti, hogy senki sem kötelezhető arra, hogy önmagát terhelő vallomást tegyen vagy önmaga ellen bizonyítékot szolgáltasson.

A megoldást azokban az esetekben, ha a hatóság hozzáfér a privát kulcshoz, az jelentené, hogy rendelkezzenek egy hatósági címmel, amelyre átkellene utalni a lefoglalás foganosítása során a kriptovalutákat, és Szathmáry ezt „kikényszerített tranzakciónak" nevezi.[470] Ezáltal tud teljes mértékben megvalósulni a vagyoni érték feletti rendelkezési lehetőségnek az akadályozása. Erre utal a 11/2003. (V. 8.) IM-BN-PM együttes rendeletnek a 67.§ (5) bekezdése, amelyben az elkobzás vagy vagyonelkobzás alá eső fizetésre használt elektronikus adat lefoglalását az új Be. 315. § (2) bekezdésében meghatározott művelet elvégzésével, a fizetésre használt elektronikus adat áthelyezésével vagy az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával kell végrehajtani, ha az adat vagyonelkobzás alá esik, és a zár alá vétel feltételei nem állnak fenn, vagy az nem lenne végrehajtható, illetve az adat elkobzás alá esik, és az elektronikus adat ideiglenes hozzáférhetetlenné tételének vagy az elektronikus adat ideiglenes eltávolításának a feltételei nem állnak fenn. Az Be. 315. § (2) bekezdésében meghatározott művelet elvégzése végrehajtható olyan művelettel is, amely alapján a fizetésre használt elektronikus adat értéke a bűnjelkezelő e célból rendszeresített számláján kerül jóváírásra. A fizetésre használt elektronikus adat vagyonelkobzás érdekében történő lefoglalását követően haladéktalanul fel kell hívni az érintettet, hogy a bűnjel előzetes értékesítése vagy megváltása kérdésében nyilatkozzon. Ha az érintett kéri a fizetésre használt elektronikus adat értékesítését, ez csak abban az esetben mellőzhető, ha arra a bizonyítás érdekében is szükség van. Amennyiben a fizetésre használt elektronikus adat lefoglalását a 67. § (5) bekezdésében meghatározott módon hajtják végre, és annak a bírósági bűnjelkezelő rendelkezésére bocsátása szükséges, azt az ügyészség vagy a nyomozó hatóság a bírósági bűnjelkezelő e célból rendszeresített számláján történő jóváírással teljesíti.

A hatósági felügyelet alatt álló kriptovalutáknak a biztosítása is fontos, különösen a hatósági visszaélések elkerülése érdekében. Például a nyomozók a Silk Road-ügy során lefoglalt bitcoin-

[469] Lásd a kriptovaluák lefoglalásának a lépéseit részletesen HALÁSZ Viktor: A Bitcoin működése és lefoglalása a büntetőeljárásban. Belügyi Szemle, 2017/7-8. 128-146. o.
[470] SZATHMÁRY (2015): i.m. 646. o.

egységeket lopták el a hatósági pénztárcából.[471] Éppen ezért a hatósági tárcának a legalkalmasabb az ún. „multisig" vagy „multisignature" tárca típus, amely csak akkor engedélyezi a kriptovaluták küldését, ha a meghatározott számú privát kulccsal igazolást kap, az előre megadott kulcsok közül. Ezt a rendszert bármilyen kombinációban ki lehet alakítani a felek megegyezése szerint.[472]

[471] https://www.ethnews.com/two-more-years-in-prison-for-ex-secret-service-agent-who-stole-government-seized-bitcoin [2019.01.12.]
[472] FURNEAUX, Nick: Investigating cryptocurrencies – Understanding, extracting and analyzing blockchain evidence. Wiley, 2018. 71. o.

IV. TECHNOLÓGIAI KIHÍVÁSOK A BÜNTETŐELJÁRÁS SORÁN

1. Az elektronikus bizonyíték fogalma

A technológiai fejlődés egyre inkább lehetővé teszi a személyazonosság hatékony elrejtését és ez sok esetben megnehezíti a nyomozást. Ugyanakkor az elkövetők már gyakran digitális nyomot hagynak maguk után, és éppen ezért az elektronikus bizonyítékok egyre fontosabbá válnak a büntetőeljárás során. Az új technológiai vívmányok az elkövetés eszközeként jelennek meg és mindez nem korlátozódik kizárólag az informatikai bűncselekményekre, hanem szinte bármely más deliktum is elkövethető ezek segítségével. A felvázolt esetekben a nyomozó hatóságnak az elektronikus adatokat kell felkutatniuk, ezért a büntetőeljárásban egyre nagyobb szerepet kap a digitális felderítés.[473] Ez a hazai nyomozások során is tetten érhető, ugyanis már az emberölés miatt induló bűnügyek gyanúsítottjainak is rutinszerűen vizsgálják át a számítógépeit és telefonjait közvetett bizonyítékok után kutatva.[474]

Először a fogalmi áttekintéssel foglalkozom. A szakirodalomban a digitális vagy elektronikus bizonyíték elnevezés jelenik meg, amelyek már a második generációs bizonyítékok körébe tartoznak.[475] Az elektronikus bizonyíték (electronic evidence) fogalma alatt legáltalánosabb értelemben értendő minden olyan bizonyító erejű információ és adat, amelyeket bináris formában tároltak vagy továbbítottak (pl. IP-címek, e-mailek, kép- és videófelvételek stb.).[476]

Casey szerint a digitális bizonyíték minden olyan adat, amely alátámaszthatja, hogy bűncselekmény valósult meg, vagy amely összekapcsolja a bűncselekményt annak elkövetőjével.[477]

Marie-Helen Keles szerint az elektronikus bizonyíték magában foglal bármely olyan információt, amely kinyerhető számítástechnikai rendszerekből vagy más digitális

[473] Lásd ehhez részletesen FENYVESI Csaba: Kriminalisztikai világtendenciák – Különös tekintettel a digitális felderítésre. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019. 64-82. o.
[474] ELEK Balázs: Informatikus szakértés a büntetőeljárásban. Belügyi Szemle 2014/7–8. 158. o.
[475] FENYVESI Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 438-440. o.
[476] SCIENTIFIC WORKING GROUPS ON DIGITAL EVIDENCE AND IMAGING TECHNOLOGY: Digital & Multimedia Evidence Glossary. 2016. 7. o.
[477] CASEY: i.m. 7. o.

eszközökből, amennyiben ez a bűncselekménnyel összefüggésbe hozható, akkor bizonyítékként felhasználható az eljárás során.[478]

Peszleg Tibor szerint a digitális bizonyíték: „olyan számítástechnikai eszközről beszerzett adat, amelyet a bűncselekménynél valamilyen formában számítástechnikai eszközök tároltak, vagy amelyek feldolgoztak információkat a bűncselekményekkel kapcsolatban."[479]

Valamennyi fogalomnál közös, hogy büntetőjogilag releváns információkra vonatkoznak és amelyeket információs rendszeren tárolnak, vagy továbbítanak.[480]

A Budapesti Egyezmény is foglalkozik az elektronikus bizonyítékokkal, így célja, hogy lehetővé tegye az elektronikus formában megjelenő bizonyítékok összegyűjtését mind az informatikai vagy számítástechnikai rendszer útján elkövetett, vagy bármely más bűncselekmény esetén (pl. keresési előzmények, üzenetváltás).[481]

Az elektronikus bizonyítékokkal kapcsolatban felmerül a kérdés, hogy mit tekintsünk a bizonyíték forrásának. Erre vonatkozóan két elmélet létezik: az egyik szerint a forrás minden esetben a tárgy például adathordozó, amely a bizonyítékot tartalmazó adatot tárolja, míg a másik elmélet alapján – amely főleg az angolszász jogterületen terjedt el – a forrás maga az adat.[482]

2. A hatályos büntető eljárásjogi szabályozás hazánkban

A Be. hatályba lépésével számos változást hozott a kényszerintézkedések rendszerében, amely alkalmasabbá tette a digitális kihívásoknak való megfelelésre.

Az egyik legfontosabb szabályozási lépés volt, hogy a bizonyítási eszközök közé a 165.§ f) pontba bekerült az elektronikus adat is. A törvény 205. § (1) bekezdése a fogalmát is meghatározza, amelynek értelmében: „elektronikus adat a 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." Ez a fogalom lényegét tekintve megegyezik a Btk. által a 425. § (5) bekezdésben meghatározott „adat" fogalmával. Érdemes megemlíteni, hogy a Budapesti Egyezmény is foglalkozik a számítástechnikai adattal és ennek három típusát különbözteti meg:

[478] KELES, Marie-Helen: Computer Forensics: Cybercriminals, Laws and Evidence. Second Edition, Jones & Bartlett Learning, 2015. 76-77. o.
[479] PESZLEG Tibor: Interneten, számítógépen történő nyomrögzítés. Ügyészek Lapja 2005/1. 25. o.
[480] SORBÁN Kinga: A digitális bizonyítékok a büntetőeljárásban. Belügyi Szemle 2016/11. 84. o.
[481] Budapesti Egyezmény Preambuluma és 14. cikk 2. bekezdés a) - c) pont
[482] SORBÁN (2016): i.m. 82-83. o.

a forgalmi adatot (traffic data)[483], a tartalomra vonatkozó adatot (content data)[484] és az előfizetőre vonatkozó adatot (subscriber data)[485]. Ezeknek a megkülönböztetésére azért van szükség, mert eltérő szenzitivitásúak, ekként a büntetőeljárás, a bizonyítás, a felderítés során a magánszférát érintő hatósági beavatkozások lehetőségét is differenciálni kell a szerint, hogy melyik adat megismerésére és meddig jogosult az eljáró hatóság.[486] A tipizálás jelentősége még a gyakorlati elérésükben, a lefoglalásuk módszerében, a bűnügyi jogsegélyt érintő kérdésekben ragadható meg.[487]

Ahol a Be. a tárgyi bizonyítási eszközt említ, azon - eltérő rendelkezések hiányában - az elektronikus adatot is érteni kell. Tárgyi bizonyítási eszköz minden olyan tárgy, amely a bizonyítandó tény bizonyítására alkalmas, így különösen az:

- amely a bűncselekmény elkövetésének vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza,
- amely a bűncselekmény elkövetése útján jött létre,
- amelyet a bűncselekmény elkövetéséhez eszközül használtak,
- vagy amelyre a bűncselekményt elkövették.[488]

A bizonyítási eszköz a bizonyíték hordozója, a bizonyíték pedig az információ, a büntető jogilag releváns tények, amelyhez az eszközből jutunk.

Peszleg hangsúlyozza, hogy akár más bizonyítási eszközöknél, így az elektronikus adatok esetében is fontos a törvényesség, szakszerűség és a zárt bizonyítási lánc megléte.[489]

---

[483] Budapesti Egyezmény 1. cikk d) pont „forgalmi adat”: minden olyan, a számítástechnikai rendszeren átmenő és a számítástechnikai rendszer mint a kommunikációs lánc egyik eleme által létrehozott kommunikációra vonatkozó adat, mely jelzi a kommunikáció eredetét, rendeltetési helyét, útvonalát, idejét, napját, terjedelmét és időtartamát vagy a szolgáltatás típusát. Ezen adatfogalomnak feleltethető meg a 180/2004. (V. 26.) Kormányrendelet 2. § e) pontjában meghatározott kísérő adat fogalma. Kísérő adat az elektronikus hírközlési szolgáltató hálózatában és azzal összefüggő informatikai rendszereiben az adott kommunikációval összefüggésben az adott szolgáltatás teljesítésével kapcsolatban keletkező, illetve az elektronikus hírközlési szolgáltató hálózatában rendelkezésre álló adat.

[484] A tartalomra vonatkozó adat a kommunikáció információtartalmát jelöli, azaz a kommunikációhoz kapcsolódó minden olyan adat, amely nem tartozik a forgalomra vonatkozó adatok körébe. Lásd SZABÓ Imre: A számítástechnikai adat mint elektronikus bizonyíték – A magyar szabályozás elemzése az Európa Tanács számítástechnikai bűnözésről szóló egyezménye alapján. Kriminológiai Tanulmányok 48. Budapest, 2011. 16. o.

[485] Budapesti Egyezmény 18. cikk 2. bekezdés a)-c) pont alapján „előfizetőre vonatkozó adat”: bármely olyan számítástechnikai adat formájában vagy más formában megjelenő, szolgáltató által birtokolt, a szolgáltatásaira előfizetőkkel kapcsolatos, a tartalomra vonatkozó vagy a forgalmi adatoktól eltérő információ, mely lehetővé teszi, hogy megállapítsák a következőket: az igénybe vett kommunikációs szolgáltatás típusát, az erre vonatkozóan tett technikai intézkedéseket, valamint a szolgáltatás időszakát; az előfizető személyazonosságát, postai vagy földrajzi címét, telefonszámát vagy más elérhetőségét, a fizetésre és a számlázásra vonatkozó adatokat, melyek szolgáltatási szerződés vagy megállapodás alapján állnak a szolgáltató rendelkezésére; minden más, a kommunikációs berendezés helyére vonatkozó, szolgáltatási szerződés vagy megállapodás alapján a szolgáltató rendelkezésére álló információt.

[486] SZABÓ (2011): i.m. 16. o.

[487] NAGY (2018): i.m. 759. o.

[488] Be. 204. § (1) bekezdés a) – d) pont

[489] PESZLEG (2005): i.m. 24. o.

Három alapvető kritériumnak kell megfelelni a nyomozás során: a bizonyíték beszerzésénél ne sérüljön vagy módosuljon az eredeti adat, bizonyítható legyen az egyezés az eredetivel, valamint a bizonyíték elemzése ne változtassa azt meg.[490]

2.1. Az elektronikus adattal összefüggő kényszerintézkedések

2.1.1. A kutatás

Az eddigi házkutatás elnevezést a Be. kutatásra változtatta meg, amely terminológia így igazodik a kényszerintézkedés tartalmához, amely alapján a tárgya nem csupán a helyiségek, illetve körül határolt helyek lehetnek, hanem ezek mellett a jármű, információs rendszer és az ilyen rendszer útján rögzített adatok is. A kutatás célja az eredményes büntetőeljárás lefolytatása érdekében a lakás, az egyéb helyiség, a bekerített hely vagy a jármű átkutatása, ha megalapozottan feltételezhető, hogy az bűncselekmény elkövetőjének az elfogására, bűncselekmény nyomainak a felderítésére, bizonyítási eszköz megtalálására, elkobozható, illetve vagyonelkobzás alá eső dolog megtalálására vagy információs rendszer, illetve adathordozó átvizsgálására vezet.

A kutatás fontos lépés a későbbi nyomozási cselekményekre nézve, mert ekkor számos kérés eldönthető például vizsgálni kell, hogy található a házban Wi-Fi és ez megfelelő jelszavas vagy egyéb védelemmel rendelkezik-e, mert ennek hiányában fennáll annak a lehetősége, hogy más kapcsolódott rá a vezeték nélküli hálózatra, és követte el az adott bűncselekményt.[491]

Emellett ilyenkor bevett gyakorlat, hogy az információs rendszerben olyan vizsgálatokat végeznek, amelyekre később nem biztos, hogy lehetőségük lesz például mert egy adatot felhőszolgáltatás igénybevételével tárolnak.[492]

A kutatást elrendelheti a bíróság, az ügyész és új szabályozási elemként már a nyomozó hatóság is. A védett helyiségek esetén mint a közjegyzői és ügyvédi iroda, a védett tevékenységgel összefüggő hivatásbeli titok megismerésére irányuló kutatást továbbra is csak a bíróság rendelheti el, azonban késedelmet nem tűrő esetekben lehetőség van az utólagos engedélyeztetésre. A védett helyiségek köréből kikerültek az egészségügyi intézmények. Ennek oka a törvény indokolása szerint az, hogy egészségügyi adatokat[493] már nem csak egészségügyi

[490] WANG, Shiuh-Jeng: Measures of retaining digital evidence to prosecute computer-based cyber-crimes. Computer Standars & Interfaces 29. 2007. 218. o.
[491] VADÁSZ: i.m. 30. o.
[492] DORNFELD László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2. 119-120. o.
[493] Az egészségügyi intézményekben dolgozókat az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény is titoktartásra kötelezi. E törvény az egészségügyi adat

intézmények kezelhetnek. Adatkéréssel az egészségügyi adatok továbbra is csak az ügyészség engedélyével szerezhetők be.

2.1.2. Az elektronikus adat lefoglalása

A Be. 151. § (1) bekezdése alapján a lefoglalás célja a bizonyítási eszköz, illetve az elkobozható dolog vagy a vagyonelkobzás alá eső vagyon biztosítása a büntetőeljárás eredményes lefolytatása érdekében. Lefoglalni a következőket lehet: az ingó dolgot, a számlapénzt, az elektronikus pénzt vagy az elektronikus adatot, utóbbinak a részletes szabályozásával foglalkozom. A lefoglalás az elektronikus adat feletti tulajdonjogot korlátozza, amelyet a bíróság, az ügyészség és a nyomozó hatóság is elrendelhet.

E jogintézmény kulcsfontosságú szerepet játszik az informatikai bűncselekmények felderítésében az elektronikus bizonyítékok megszerzésének és megőrzésének eszközeként.

A lefoglalás általános szabályai mellett a törvény külön szabályozza az elektronikus adat lefoglalását. Ezzel kapcsolatban régóta viták folynak arról, hogy pontosan mit is kellene az eljárás során lefoglalni, így a meghatározott adatok körét, vagy az adathordozót, vagy a teljes információs rendszert. A büntetőeljárásról szóló 1998. évi XIX. törvényben (a továbbiakban: régi Be.) az adat lefoglalását a 2013. évi CLXXXVI. törvény 21. §-a illesztette be a törvény szövegébe. Ezt megelőzően bevett gyakorlatként volt érvényben a számítógép egészének a lefoglalása (pl. sokszor a büntetőeljárás szempontjából lényegtelen hardvereszközökkel együtt, mint a monitor és a billentyűzet), később a merevlemezt vagy még azt sem, és csak másolatot készítettek róla, majd a módosítást követően csak az adatokat foglalták le.[494]

Az elektronikus adat lefoglalásának módjait a törvény a 315. § (1) bekezdésben felsorolással rögzíti, ami egyben a lefoglalás tekintetében a fokozatosság szabályait figyelembe véve sorrendet állít fel.[495] Az elektronikus adat lefoglalása történhet:

1. az elektronikus adatról való másolat készítésével,
2. az elektronikus adat áthelyezésével,
3. az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével,

---

fogalmát az alábbiak szerint rögzíti: "az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat; továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat (pl. magatartás, környezet, foglalkozás)".

[494] VADÁSZ: i.m. 20. o.

[495] CZINE Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018. HVG-ORAC Jogkódex

4. az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy
5. jogszabályban meghatározott más módon lehet végrehajtani.

Az első két esetben magát az adathordozó tartalmát, vagyis az adatokat foglalják le másolat készítésével vagy áthelyezéssel. A lefoglalás módszertani kérdéseivel nem foglalkozik a törvény, annak ellenére, hogy ennek komoly jelentősége van. A másolás történhet egyszer úgy, hogy a hatóság a rendszert a helyszínen átvizsgálja, és a relevánsnak ítélt adatokat hagyományos módon másolja át az információs rendszerről közvetlenül egy adathordozóra. Ennek alkalmazása azonban kihívás elé állítja mind a hitelesség, mind a teljesség kriminalisztikai elvének érvényesülését. A digitális bizonyíték akkor hiteles, ha a későbbiekben is pontosan meghatározható, hogy az adat mely rendszerről származik, illetve, hogy az elektronikus adat pontos és teljes mása került lefoglalásra, továbbá, hogy az adat a lefoglalása óta változatlan maradt. A hiteles adatokon végzett vizsgálatok bármikor megismételhetők, a vizsgálat eredménye reprodukálható.[496] Ezen alapelvek érvényesülését hivatott biztosítani a 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67. § (2) bekezdése, amely arról rendelkezik, hogy a lefoglalás kizárólag utólag meg nem változtatható adathordozóra történhet, amely a lefoglalás időpontjában adatokat nem tartalmazhat. A hatóság köteles a jegyzőkönyvben feltüntetni az átmásoláshoz használt adathordozó típusát, gyártási számát, illetve a rajta tárolt adat jellegét és tartalmát. Továbbá a rendelet rendelkezik arról, hogy az átmásolás során biztosítani kell, hogy az eredeti adatok ne változzanak meg, ami általában csak speciális írásvédő eszköz vagy szoftver segítségével valósítható meg. A teljesség elve azt jelenti, hogy minden bizonyítékot le kell foglalni. Amennyiben a lefoglalást végző személy nem rendelkezik kellő szakértelemmel, akkor fontos bizonyítékok veszhetnek el (pl. a metaadat[497], a cache tartalma[498] stb.), ezért indokolt esetben szaktanácsadót kell igénybe venni. Az adatok lefoglalására nyitva áll egy másik lehetőség is, mégpedig amikor a hatóság szakértő vagy szaktanácsadó bevonásával bitazonos, hash kulccsal ellátott tükörmásolatot készít a teljes adathordozóról, de ez hatékonyan csak kisebb mennyiségű adatállomány esetén alkalmazható.[499]

A teljes rendszer lefoglalásának a hátránya, hogy annak egyes hardver részei (pl. videókártya, alaplap, tápegység stb.) gyorsan amortizálódnak és az elhúzódó büntetőeljárás

[496] MATUS Márk: Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben. In. Bócz Endre (szerk.): Kriminalisztika. BM Duna Palota és Kiadó Budapest, 2004. 292. o.
[497] A metaadatok az elektronikusan elérhető adatoknak a leíró adatai, vagyis strukturált információk az adatokról.
[498] Cache (gyorsítótár): a számítástechnikában az átmeneti információtároló-elemeket jelenti, melyek célja az információ-hozzáférés gyorsítása.
[499] SORBÁN (2016): i.m. 89. o.

következtében a lefoglalás elszenvedőjét akár komoly anyagi kár is érheti ezáltal, vagy mindez akár egy vállalkozás működését is veszélyeztetheti. A lefoglalásnál a szükségtelen károkozás tilalmát, az arányosság és a fokozatosság elvét is figyelembe kell venni. Ennek megfelelően a Be. rögzíti, hogy különösen a vagyont érintő kényszerintézkedés megvalósítása során kerüljék, hogy az érintettnek vagy másnak indokolatlanul kárt okozzanak.[500] Továbbá csak a legszükségesebb mértékben és ideig valósuljon meg a kényszerítő eszköz alkalmazása, vagyis arányosságot követel meg,[501] valamint súlyosabb kényszerintézkedés csak akkor rendelhető el, ha enyhébb eszközzel a cél nem érhető el.[502] A kényszerintézkedést az érintett kíméletével kell végrehajtani.[503]

Parti Katalin véleménye szerint a teljes adathordozó lefoglalásának alapját nem képezheti csak az a tény, hogy a bűncselekmény elkövetésére utaló releváns adatokat tartalmaz. Ehhez szükséges, hogy a szerver üzemeltetője, tulajdonosa és a bűncselekmény közötti kapcsolat fennállása (pl. megállapítható a gyanúja annak, hogy bűncselekmény elkövetésére használták fel). Hiszen a szerver-gazda számára aránytalan veszteséggel is járhat, ha a teljes adatparkot lefoglalják, mert például nem végezheti tovább az üzleti tevékenységét.[504]

Mindemelett adatvédelmi problémák is felmerülhetnek, mert a lefoglalt számítógép olyan személyes adatokat is tartalmazhat, amelyek nincsenek összefüggésben a büntetőeljárással vagy több személy adatait is tartalmazhatja (pl. egy vállalati hálózat több számítógépének vagy szerverének lefoglalásakor).[505] A Be. a hatóságok számára kötelezettségként állapítja meg az érintett azon - a magánéletével összefüggő - személyes adatai védelmét, amely adatok a büntetőeljáráshoz nem kapcsolódnak, a bűncselekmények feltárása szempontjából irrelevánsak. A hatóságok kötelezettsége arra is kiterjed, hogy az érintett magánéletéhez kapcsolódó, de személyes adatnak nem minősülő egyéb körülményei se kerüljenek a nyilvánosság elé.[506] Ennél fogva, amennyiben lehetőség van a szelektálásra, akkor az ilyen jellegű adatokat már eleve ki kell vonni a lefoglalás köréből, ha pedig azok a rögzítést követően, vagyis utólag jutnak a hatóság tudomására, úgy a szükséges biztonsági intézkedések megtétele mellett, a törlésükről

[500] Be. 271. § (6) bekezdés
[501] Be. 271. § (1) bekezdés
[502] Be. 271. § (2) bekezdés
[503] Be. 271. § (3) bekezdés
[504] PARTI Katalin: Gondolatok a szerver-lefoglalásokról. Infokommunikáció es Jog 2004/3. 97-101. o.
[505] SORBÁN (2016): i.m. 89. o.
[506] Be. 271. § (5) bekezdés

kell gondoskodni. Ugyanez a kitétel vonatkozik a gazdálkodó szervek, intézmények és más szervezetek üzleti, bank vagy ezekkel egy tekintet alá eső titkot képező egyéb adataira is.[507]

A rendőrségről szóló 1994. évi XXXIV. törvény 90. § is rögzíti, hogy csak bűnüldözési célra lehet felhasználni az összegyűjtött és tárolt személyes adatokat, és e céllal csak azokat kezelhetik, amelyek tényleges veszély elhárításához, illetve meghatározott bűncselekmény megelőzéséhez, felderítéséhez, bizonyításához szükségesek.

Az adatvédelmi biztos állásfoglalásában felhívta a figyelmet arra, hogy az eljáráshoz nem szükséges személyes adatokhoz való hozzáférés csak észszerű időtartamra korlátozható, és egy félévig elhúzódó lefoglalás már ezen túl mutat.[508]

Érdekesség, hogy Németországban a Szövetségi Alkotmánybíróság új alapjogként az információs önrendelkezési jogból levezetve az információs rendszer bizalmasságához és integritásához való jogot állapította meg, mely védelem az információs rendszer egészére terjed ki.[509] Peszleg is hangsúlyozza az emberi méltóság, személyiségi és kegyeleti jogok tiszteletben tartását.[510]

Az adatvédelmi biztos beszámolója alapján ismertté vált rendőrségi gyakorlat szerint a személyes adatokhoz csak az igazságügyi informatikai szakértő[511], az ügy előadója és elöljárói férhetnek hozzá és olyan vizsgálati környezetben dolgoznak, ahonnan kizárják az illetékteleneket. A kialakított gyakorlat szerint ugyanakkor a személyes jellegű információkhoz csak az igazságügyi informatikai szakértő férhet hozzá. A rendőrség az igazságügyi informatikai szakértő szakvéleménye alapján határozza meg a bűnügyileg releváns információkat.[512] A Nemzeti Nyomozó Iroda gyakorlata alapján a lefoglalt rendszerről teljes másolatot készítenek, és ezt vizsgálják át az eljárás során, ami egyúttal korlátozza az adatokhoz hozzáférők körét.[513]

Az adathordozók lefoglalásakor a kiszereléshez mindig hozzáértő személy szükséges, mert előfordulhatnak inkompatibilitási problémák. Peszleg is rámutat arra, hogy vannak olyan eszközök, amelyek „olyan egységet képezhetnek, hogy ha megbontják őket, már nem

[507] LACZI Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. Magyar Jog 2001/12. 726-738. o.
[508] Az adatvédelmi biztos beszámolója, 2009. Forrás: hwww.naih.hu/files/Adatvedelmi-biztos-beszamoloja-2009.PDF
[509] MOHÁCSI Barbara: Bűnüldözési érdek contra emberi jogok - az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. Magyar Jog 2008/12. 827-832. o.
[510] PESZLEG: Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek lapja, 2010/2. 23. o.
[511] Lásd ehhez MÁTÉ István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. Doktori értekezés. Pécs, 2017.
[512] TRÓCSÁNYI Sára: Első oldal. Infokommunikáció és jog 2009/6. 1. o.
[513] DORNFELD (2018): i.m. 123. o.

lehetséges az eredeti adattartalom visszaállítása (pl. RAID tömbök[514] esetén)".[515] A merevlemeznek az eredeti hardver környezetből való eltávolítása esetén felmerül az a veszély, hogy a számítógépen futó programok egy része nem lesz elindítható és ezáltal az értékes információkat nem lehet utólag kinyerni.[516]

A törvényben a szükségesség-arányosság követelménye a 315. § (4) bekezdésében kiemelten jelenik meg, mert a jogalkotó rögzíti, hogy a büntetőeljárás szempontjából szükségtelen adathordozóra ne terjedjen ki a lefoglalás, amennyiben az mégis kiterjed, akkor a legrövidebb ideig érintse az ilyen adatot. Abban az esetben, ha a másolatkészítés nem veszélyezteti az eljárás érdekét, akkor másolatot kell készíteni az erre jogosult kérésére.

Emellett kimondja, hogy az elektronikus adatot tartalmazó információs rendszer vagy adathordozó akkor foglalható le, ha az elkobozható, illetve vagyonelkobzás alá esik, az tárgyi bizonyítási eszközként bír jelentőséggel, vagy a bizonyítás érdekében az abban tárolt, előre meg nem határozható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség.

Összességében hiányzik az elektronikus bizonyítékok lefoglalására vonatkozó átfogó és szakszerű útmutatás hazai viszonylatban, míg példaként említhető az Egyesült Államok, ahol az Igazságügyi Minisztérium részéről, valamint Európában az Európai Tanács és az ENISA által már vannak erre irányuló törekvések.[517]

2.1.3. Az elektronikus adat megőrzésére kötelezés

Az elektronikus adat megőrzésére kötelezés nem önálló kényszerintézkedésként, hanem a lefoglalás körében került szabályozásra. A kényszerintézkedés jellemzője, hogy lefoglalástól eltérően nem fosztja meg az adat birtokosát, feldolgozóját, illetve kezelőjét a birtoklás jogától. Legfeljebb három hónapig tarthat, míg a lefoglalásra vonatkozóan nincs időbeli korlát meghatározva. A célja az adatmegőrzés, a bűncselekmény felderítése, a bizonyítási eszközök biztosítása, valamint a gyanúsított kilétének, tartózkodási helyének a megállapítása. A kibertérben elkövetett bűncselekmények elkövetése esetén az adatveszítés, adatmegsemmisülés a bizonyítékok megsemmisülését is jelenti és ez az eljárás sikerét veszélyezteti. Ennek érdekében a hatóság – bíróság, ügyészség és nyomozó hatóság – elrendelheti az információs

[514] RAID: tárolási technológia, mely segítségével az adatok elosztása vagy replikálása több fizikailag független merevlemezen, egy logikai lemez létrehozásával lehetséges.
[515] PESZLEG (2010): i.m. 27. o.
[516] VADÁSZ: i.m. 19. o.
[517] U.S. DEPARTMENT OF JUSTICE: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Law. 2009.; COUNCIL OF EUROPE: Electronic evidence guide—A basic guide for police officers, prosecutors and judges. 2013.; valamint ENISA: Electronic evidence—a basic guide for first responders. 2014.

rendszer útján rögzített adatok változatlan megőrzését és biztonságos tárolását, ha szükséges, akkor más adatállománytól elkülönítve. Amennyiben ez jelentős akadályozást jelentene, akkor lehetőség van az adat biztosítására más rendszerre vagy adathordozóra történő átmásolással. A kötelezettnek biztosítani kell, hogy az elektronikus adatot ne változtassák meg, ne töröljék, ne semmisítsék meg, ne továbbítsák, ne készítsenek arról másolatot. Emellett azt is meg kell akadályoznia, hogy az elektronikus adathoz jogosulatlan személyek hozzáférjenek. Az elrendelő az érintett adatok változatlan fenntartása érdekében, azokat minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírással vagy elektronikus bélyegzővel láthatja el. Ha az adatok egy belső hálózaton (intranet) érhetők el, akkor a rendszergazdát kell kötelezni az adatok megőrzésére.[518]

2.1.4. Az elektronikus adat ideiglenes és végleges hozzáférhetetlenné tétele

A Be. a már meglévő elektronikus adat ideiglenes hozzáférhetetlenné tétele kényszerintézkedésnek a szabályozását is módosította, amelyet bíróság rendelhet el. A nemzeti jogba a kényszerintézkedés bevezetésére azért került sor, hogy a 2011/93/EU irányelvnek[519] a 25. cikkében szabályozott gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak elleni intézkedéseknek megfeleljen. Azonban a hazai szabályozás nem csak a gyermekek védelmében nyújt teret a bíróságnak az adathozzáférés korlátozására és törlésére, hanem valamennyi bűncselekmény kapcsán biztosítja az adattal való rendelkezés jogának korlátozhatóságát, bizonyos feltételek mellett az elektronikus adat ideiglenes vagy végleges hozzáférhetetlenné tételét is az elrendelhető jogkövetkezmények közé sorolva.[520]

E kényszerintézkedés alkalmazásának a célja, hogy az elektronikus hírközlő hálózat útján is közzétett adatok – amelyek bűncselekmény elkövetésével hozhatók kapcsolatba (pl. uszító, gyűlöletkeltő írások, pornográf felvételek stb.) – hozzáférhetővé tételének korlátozása, megakadályozása.

A törvény egyben a (2) bekezdésben rögzíti, hogy mely feltételek fennállása esetén van lehetőség a kényszerintézkedés alkalmazására, amelyre az érintett adatot kezelő

[518] CZINE Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018. HVG-ORAC Jogkódex

[519] Az Európai Parlament és a Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról

[520] GAIDERNÉ HARTMANN Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele - egy új intézmény első évei. Magyar Jog 2015/2. 106-107. o.

tárhelyszolgáltató, valamint tárhelyszolgáltatást is végző közvetítő szolgáltató kötelezhető[521], ha:

- az eljárás közvádra üldözendő bűncselekmény miatt indult (pl. gyermekpornográfia, szerzői jogot sértő bűncselekmények stb.),
- amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye,
- és a hozzáférhetetlenné tétel elrendelése a bűncselekmény megszakítása érdekében szükséges.

A Btk. 77. § (1) bekezdésében új intézkedésként került bevezetésre az elektronikus adat végleges hozzáférhetetlenné tétele, amelynek a) - c) pontjai szerint:

- hozzáférhetetlenné kell tenni azokat az adatokat, amelyeknek közzététele vagy hozzáférhetővé tétele bűncselekményt valósított meg;
- azokra az adatokra teszi kötelezővé az intézkedés alkalmazását, amelyeket a bűncselekmény elkövetéséhez eszközül használtak;
- a bűncselekmény eredményeképp létrejött adat hozzáférhetetlenné tételét írja elő.

Verebics János például négy főbűncselekmény csoportot különít el az ideiglenes hozzáférhetetlenné tétellel akadályozható magatartások körében:

- az információ közzétételével, megosztásával megvalósuló cselekményi kört (pl. gyermekpornográfia),
- az információ és az információtovábbítás biztonságát és hitelességét sértő bűncselekmények csoportját (pl. adat- és titokvédelmi, információ hitelessége elleni tényállások),
- a tiltott adatszerzés és az információs rendszer elleni bűncselekményeket,
- valamint a szellemi tulajdon sérelmét eredményező bűncselekményeket.[522]

[521] A közvetítő szolgáltatók fajtáit az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) határozza meg, amelynek 2. § l) pontja értelmében:
„Közvetítő szolgáltató: az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely
la) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);
lb) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);
lc) az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);
ld) információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);
le) alkalmazásszolgáltató."

[522] VEREBICS János: Az információs bűncselekmények és az elektronikus adat ideiglenes hozzáférhetetlenné tételének lehetősége az új Btk.-ban. Gazdaság és Jog 2013/2. 3-5. o.

A kényszerintézkedés iránti bírósági határozatnak a tartalmát külön jogszabály határozza meg, így a 11/2014. (XII. 13.) IM rendelet 142. § (1) bekezdése alapján ennek rögzítenie kell az alábbi elektronikus adat forrásának azonosítására szolgáló információkat:

a) IP-cím ipv4 vagy ipv6 szabvány[523] szerint és alhálózati maszk,

b) domain név,

c) URL cím,

d) portszám.[524]

Mindezekre tekintettel nem az adat, hanem annak hálózaton elfoglalt helye azonosítható, tehát az eltávolítani kívánt tartalom ismételt közzététele esetén a határozat végrehajtása nem terjeszthető ki az új megjelenést biztosító oldalra, hanem újabb bírói intézkedés válik szükségessé. Gaiderné Hartmann Tímea szerint ez kiküszöbölhető lenne, ha a bíróság határozatában nem az adatelérés útját, hanem az adattartalmat jelölné meg.[525]

A bíróság a kötelezett tárhelyszolgáltatót a nevének és címének, illetve elnevezésének és székhelyének, telephelyének vagy fióktelepének, a cégjegyzék- vagy egyéb nyilvántartási számának, továbbá a tárhelyszolgáltató képviseletére jogosult nevének és címének a feltüntetésével jelöli meg.

Az eltávolításra kötelezett szolgáltató köteles a határozat közlésétől számított egy munkanapon belül az adatot eltávolítani. Amennyiben ezt nem teljesíti, akkor rendbírsággal sújtható.

---

[523] Az internetszolgáltatók a hálózatra felcsatlakozó felhasználók számára IP-címet osztanak ki, amely alapján azonosítani lehet őket. A jelenleg használt IPv4 szabvány szerint a kioszthatő címek száma 4,3 milliárdra korlátozódik, ami a használatban lévő eszközök számát tekintve nem elegendő, ezért a szolgáltatók dinamikusan osztják ki az IP-címeket. Ez a gyakorlatban azt jelenti, hogy az IP-k eltérő időpontban eltérő felhasználókat jelölnek. A nyomozó hatóságnak ezért úgy kell kikérnie az adatokat az internetszolgáltatótól, hogy az a bűncselekmény elkövetésének időpontjára vonatkozzon. A problémára technikai megoldást kínál az IPv6-ra történő átállás, hiszen itt már 50 billiárd IP-cím válik kioszthatóvá. Ez a folyamat azonban a tervezettnél máris hosszabb időt vesz igénybe, és egyelőre bizonytalan az időpontja. Az átmeneti időszakban a két verzió párhuzamosan működik, ami további komplikációkat jelenthet a büntetőeljárások során. Lásd DORNFELD László: Az elektronikus bizonyítékszerzés egyes kérdései. Kriminológiai Közlemények 77. 2017. 246. o.

[524] A rendelet 141. § (3) bekezdése meghatározza a fogalmukat is, azonban e jelentések az átlag felhasználói szintű tudással rendelkező jogalkalmazók számára kevés támpontot adnak az egzakt, kellően pontos, így a végrehajtás alapjául szolgáló határozat meghozatalához:

„elektronikus adat” a hozzáférést biztosító elektronikus hírközlési szolgáltatók által az elektronikus hírközlő hálózat útján közzétett olyan adat, amely egyedi azonosítók, mint az IP és URL cím, domain név és portszám alapján beazonosítható;

„IP-cím”: egyedi hálózati azonosító, amely a hozzátartozó alhálózati maszkkal együtt meghatározza, hogy mely hálózati címen érhető el az elektronikus adat;

„domain név”: az internet egy meghatározott részét, tartományát egyedileg leíró megnevezés;

„URL cím”: egységes erőforrás azonosító, amely egyetlen címben foglalja össze az interneten megtalálható elektronikus adat azonosításához szükséges legfontosabb információkat, mint a protokoll, a domain név vagy IP-cím, a portszám és az elérési út a célszerveren;

„portszám”: a TCP/IP és az UDP, illetve SCTP protokollokban az adott célszerveren a logikai csatlakozást meghatározó jelzőszám.

[525] GAIDERNÉ HARTMANN: i.m. 115. o.

A kényszerintézkedésnek két megvalósulási formája van, amelyek részletesen szabályozva vannak: az egyik az elektronikus adat ideiglenes eltávolítása (Be. 336. §) és a másik az elektronikus adathoz való hozzáférés ideiglenes megakadályozása (Be. 337. §). A kényszerintézkedés tehát kétszintű: először a tárhelyszolgáltatót kell felszólítani a tartalom eltávolítására, és utóbbira, az ún. „blokkolásra”[526] akkor van lehetőség, ha az ideiglenes eltávolítás nem vezetett eredményre, mert az eltávolításra kötelezett nem azonosítható, vagy ez aránytalan nehézséggel járna, továbbá, ha az eltávolításra vonatkozóan a külföldi hatóság jogsegély iránti megkeresésétől nem várható eredmény vagy a megkeresés aránytalan nehézséggel járna. Mindezen előzetes eljárást mellőzve akkor alkalmazható, ha az érintett adattal összefüggő bűncselekmény jellege ezt indokolttá teszi.[527] A törvény által taxatíve felsorolt bűncselekmények esetében, ha a büntetőeljárás kábítószer-kereskedelem, kóros szenvedélykeltés, kábítószer készítésének elősegítése, kábítószer-perkurzorral visszaélés, új pszichoaktív anyaggal visszaélés, gyermekpornográfia, állam elleni bűncselekmény, terrorcselekmény, terrorizmus finanszírozása vagy háborús uszítás miatt van folyamatban, az elektronikus adathoz való hozzáférés ideiglenes megakadályozására kerülhet sor.

A kényszerintézkedés végrehajtásának az ellenőrzését a Nemzeti Média- és Hírközlési Hatóság látja el, valamint a blokkolt tartalmakról vezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisát (KEHTA), amely csak a hatóság és a szolgáltatók számára hozzáférhető.[528]

Emellett lehetőség van arra a kényszerintézkedés alkalmazása előtt, hogy az ügyészség vagy a nyomozó hatóság a szolgáltatókat felhívja az önkéntes eltávolításra, azonban ez nem kötelező rájuk nézve (Be. 338. §).

2.2. Az elektronikus bizonyítékok határon átnyúló megszerzése

Napjainkban a nyomozások több mint felében végeznek határokon átnyúló megkeresést egy másik tagállamban vagy az EU-n kívül székhellyel rendelkező szolgáltatók birtokában lévő elektronikus bizonyítékok beszerzése céljából. Jelenleg az ilyen adatok beszerzéséhez

[526] Parti Katalin részletesen foglalkozik az ún. tartalomszűréssel vagy másnéven internet-blokkolással, amely három szintre osztható - attól függően, hogy ki dönt a tartalom szűréséről -, így beszélhetünk az önszabályozás körébe tartozó felhasználói és intézményi szintről, továbbá az internetszolgáltató által megvalósulóról, végül az állami szabályozásról. Utóbbiba tartozik a tárgyalt kényszerintézkedés is. Lásd PARTI Katalin: "10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és jog 2010/38. 97-104. o.

[527] GAIDERNÉ HARTMANN: i.m. 111-112. o.

[528] DETREKŐI Zsuzsa: Blokkolás Magyarországon - hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig. Infokommunikáció és jog 2014/4. 184-186. o.

igazságügyi együttműködésre és kölcsönös jogsegélyre van szükség, azonban az eljárás jelenleg lassú és nehézkes. Ma az olyan bűncselekmények csaknem kétharmada esetén nem lehet megfelelően lefolytatni a nyomozást és a büntetőeljárást, ahol más országban tárolnak elektronikus bizonyítékokat. Ennek az a fő oka, hogy rendkívül időigényes az ilyen bizonyítékok begyűjtése, illetve széttagolt a jelenlegi jogi szabályozás kerete. E kérdéskörben már jelentős bírósági döntések is születtek, amelyek szintén rámutattak arra, hogy ez mennyi problémát hordoz magában.[529] Az Egyesült Államokban az önkéntes együttműködés működik a bűnüldöző hatóságok és a szolgáltatok között, ami alternatív módszert szolgál az elektronikus bizonyítékok beszerzéséhez. Ez a fajta kooperáció ugyan általában gyorsabb, mint az igazságügyi, azonban a szolgáltatók eltérő módon kezelik a megkereséseket és szabadon dönthetnek a kért adatok kiadásáról, ezért megállapíthatjuk, hogy az eljárásból hiányzik az átláthatóság, ami végül jogi bizonytalansághoz vezet. A felhasználók nagy mennyiségű adatot generálnak, amelyek általában a szolgáltatók birtokában vannak, ezért különösen fontos a megfelelő együttműködés alapjainak a megteremtése velük.

Az elektronikus bizonyítékok megszerzésének a gyorsítása és hatékonyabbá tételének érdekében az Európai Tanács elfogadta álláspontját a büntetőügybeli elektronikus bizonyítékokra vonatkozó közlésre és megőrzésre kötelező európai határozatokról szóló rendeletről, amit következő lépésként az Európai Parlament előtt tárgyalnak meg.

A rendeletben foglalt legfontosabb újítás, hogy létrehozzák a közlésre kötelező európai határozatot (European Production Order), amely lehetővé teszi, hogy valamely tagállam igazságügyi hatósága – az adatok helyétől függetlenül – közvetlenül igényeljen elektronikus bizonyítékot bármely, az Unióban szolgáltatásokat kínáló és más tagállamban letelepedett vagy képviselettel rendelkező szolgáltatótól. Aki köteles erre 10 napon belül, hitelesen megállapított veszélyhelyzet esetén pedig 6 órán belül válaszolni, így különösen az emberi életet vagy testi épséget, vagy kritikus infrastruktúra épségét veszélyeztető helyzet esetén. Ehhez képest a meglévő európai nyomozási határozat esetében 120 nap, míg a kölcsönös jogsegély eljárás esetén pedig 10 hónap a válaszadási határidő.

---

[529] Microsoft Corp. v. United States ügy még 2014-ben indult, mikor az amerikai hatóságok egy kábítószer-kereskedelemmel összefüggő ügyben végeztek nyomozást, és ennek keretében hozzáférést kértek egy Outlook.com-os postafiók tartalmához. A Microsoft azonban az adatokat az írországi adatközpontjában tárolta, ezért a vállalat azzal érvelt, hogy az adatokat csak a dublini bíróságon keresztül lehet kikérni. A Legfelsőbb Bíróság a vállalatnak adott igazat, de közben elfogadták a CLOUD törvényt és az alapján új parancsot bocsátottak ki, amely előírta az információk kiadását. Lásd részletesen: DASKAL, Jennifer: Microsoft Ireland, The CLOUD Act, and International Lawmaking 2.0. Stanford Law Review Online, 9. 2018 May.
Lásd a kritikai elemzését a Yahoo és Skype v. Belgium ügyeknek, amelyek során a kedvező bírósági döntésnek köszönhetően a rendvédelmi szervek hozzáférhettek a külföldi szolgáltatóktól az adatokhoz, akkor is, hogy csak a szolgáltatásuk volt elérhető az országban: FRANSSEN, Vanessa: The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level? European Data Protection Law Review 3, 2017. 534-538 o.

A rendelet meghatározza az elektronikus bizonyíték fogalmát. Ennek értelmében olyan bizonyítékról van szó, amely elektronikus formában van tárolva a szolgáltatónál vagy a szolgáltató nevében, és fontos követelmény, hogy a határozatok kibocsátásakor a szolgáltatónál rendelkezni kell vele, vagyis nem vonatkozhat a jövőben megszerzendő adatokra.[530] A szabályozás négy adatkategóriát határoz meg, amelyekre a határozatok kiterjedhetnek:

Előfizetői adat (subscriber data), amely az előfizető vagy ügyfél azonosítását szolgálja mint például ilyen a megadott név, születési idő, postacím, számlázási és fizetési adat, telefonszám vagy e-mail cím, valamint a szolgáltatás típusa és tartama, az általa használt vagy részére biztosított interfészeket azonosító adatokat, a szolgáltatás igénybevételének érvényesítésére vonatkozó adatokat, de ez alól kivételt képeznek a felhasználó által megadott vagy a kérésére létrehozott jelszavak, vagy egyéb hitelesítési eszközök.

Hozzáférési adat (access data), amely nem alkalmas a felhasználó azonosítására, azonban az első fontos lépést jelenti ehhez. Ez magában foglalja a felhasználói hozzáféréséi adatokat egy szolgáltatáshoz például a ki és bejelentkezéseket dátumát és idejét vagy a szolgáltató által kiosztott IP-címet. Az IP-címekről érdemes részletesen kitérni, mert lehetnek statikusak vagy dinamikusak. A statikus cím meghatározott felhasználó számára kerül kiosztásra, míg a dinamikus esetén fontos, hogy pontosan meg kell határozni, hogy milyen időintervallumra nézve szeretné leválogatni az adott IP-címhez tartozó felhasználói kört az arra jogosult szerv, mert lehetséges, hogy egyetlen címet két nap alatt harminc felhasználó használt. A szolgáltatónak ezért több felhasználóra nézve kell vizsgálnia a forgalmi adatot. Éppen ezért a dinamikus IP-cím és az előfizetői adat megismerése gyakran eltérő megítélés alá esik országonként.[531]

Mind az előfizetői, mind a hozzáférési adat esetében az egyik uniós országból az ügyész vagy bíró közvetlenül, míg a nyomozó hatóság csak valamelyik hozzájárulásával kérheti a másik országban található szolgáltatót vagy annak jogi képviselőjét, hogy biztosítsa a kért elektronikus bizonyítékot a részére.

Tranzakciós adat (transactional data), amely az olyan adatok csoportját tartalmazza, amelyek a szolgáltatással kapcsolatba hozhatók, így az üzenet forrását vagy célállomását, adat az eszköz helymeghatározására, dátumra, időre, időtartamra, méretre, adatútra, formátumra, a protokoll használatára és a tömörítés típusára vonatkozóan.

[530] TOSZA, Stanislaw: The European Commision's Proposal on Cross-Border Access to E-evidence. eucrim 4/2018 214. o.
[531] CYBERCRIME CONVENTION COMMITTEE: Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments. 2018. 4. o.

Tartalmi adat (content data), amely bármely digitális formában tárolt adat így például szövegek, hang-, kép- és videófelvételek stb.

Az előfizetői, hozzáférési és tranzakciós adatok egyben az ún. nem tartalmi adatok (non-content data).

Az előfizetői és hozzáférési adatok elsősorban a felhasználó azonosítását célozzák, míg a tranzakciók és tartalmi adatok már részletesebb képet adhatnak az adott személy tevékenységéről, ezért nagyobb védelem illeti ezeket.[532] Erre tekintettel az utóbbi két adatkategória esetében az egyik uniós országból kizárólag a bíróság közvetlenül, míg az ügyészség és nyomozó hatóság csak a bírói hozzájárulással – aki ellenőrzi a határozatot az ezzel kapcsolatos törvényességi, szükségességi és arányossági követelménynek való megfelelősséget – kérheti a szolgáltatót vagy annak jogi képviselőjét, hogy biztosítsa a kért elektronikus bizonyítékot a részére.[533] A tranzakciós vagy tartalmi adatok – esetében egyedi küszöbérték alkalmazása mellett – kizárólag olyan bűncselekményekkel összefüggésben kérhetők, amelyek büntetési tételének felső határa a kibocsátó államban legalább három év szabadságvesztés, illetve kiberbűnözéssel vagy terrorizmussal kapcsolatos bűncselekmények esetén.

Mindezekre tekintettel a megkeresett szolgáltató országának a hatósága csak akkor válik érintetté az ügyben, ha konkrét jogi probléma merül fel, vagy a határozatot végre kell hajtani, mert azt nem teljesíti a szolgáltató.

Az eljárás menete ugyanúgy alakul és ez a szabályozás alkalmazandó, ha az elektronikus bizonyíték nem uniós országban található. Amennyiben szolgáltató az európai felhasználókra vonatkozó adatokat az EU-n kívül például az Egyesült Államokban tárolja, akkor ugyanúgy köteles az adatokat a határozat értelmében az európai hatóság számára szolgáltatni.

Az elektronikus bizonyítékok egy egérkattintással könnyedén megváltoztathatók vagy törölhetők, ezért sor kerül egy másik fontos jogintézmény bevezetésére, hogy megakadályozzák ezt. Ez az ún. megőrzésre kötelező európai határozat (European Preservation Order). Ez az új eszköz lehetővé teszi, hogy valamely tagállam igazságügyi hatósága konkrét adatok megőrzésére kötelezzen bármely, az Unión belül szolgáltatásokat kínáló és egy másik tagállamban letelepedett vagy képviselettel rendelkező szolgáltatót, annak érdekében, hogy a hatóság ezt az információt később a rendelkezésre álló jogintézmények útján kikérhesse.

Az új határozatokat közvetlenül az EU területén működő szolgáltatóknak lehet címezni. Fontos további követelmény ehhez, hogy másik tagállamban kell letelepedniük vagy másik

[532] TOSZA: i.m. 214. o.
[533] http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm [2019.02.21.]

tagállamban rendelkezniük kell képviselettel. Önmagában az EU-n belüli szolgáltatás nyújtás nem elégséges, mert minden szolgáltató ennek következtében a rendelet hatálya alá tartozna.

A szolgáltató fogalmát is meghatározza a rendelet, amelynek értelmében lehet természetes vagy jogi személy és az általa nyújtott szolgáltatás a meghatározó, amik a következők lehetnek: elektronikus hírközlési szolgáltatás, az információs társadalommal összefüggő szolgáltatás, amelynek az adattárolás meghatározó eleme a felhasználó részére nyújtott szolgáltatásoknak, beleértve a közösségi oldalakat is (Twitter és Facebook), valamint az internet domain névvel és IP-címmel összefüggő szolgáltatás (mint például az IP-cím szolgáltatók, domain név nyilvántartások és nyilvántartók, valamint a kapcsolódó titkosítási és proxy szolgáltatók). Az első két kategória magában foglalja például a következőket Skype, WhatsApp, Amazon, Dropbox, eBay és az e-mail szolgáltatókat, míg utóbbi kettő az internet infrastruktúrával foglalkozó szolgáltatókat fedi le, akik olyan adatokkal rendelkeznek, amelyek hozzájárulhatnak az elkövetők azonosításához.[534]

A javaslat emellett erős biztosítékokat és jogorvoslatokat nyújt. Mindkét határozat kizárólag büntetőeljárás keretében bocsátható ki, és azokra valamennyi büntetőjogi eljárási biztosíték alkalmazandó (pl. védelemhez való jog és ügyirathoz való hozzáférés). Emellett az új szabályok garantálják az alapvető jogok védelmét, valamint a személyes adatok védelméhez való jogot (pl. tájékoztatást kapnak arról, hogy a személyes adatukat kikérték). A kért adatokat nem lehet a megszerzésük céljától eltérő célra felhasználni, kivéve a következő eseteket: a kibocsátó állam közbiztonságát vagy alapvető érdekeit érintő azonnali és súlyos fenyegetés megelőzése érdekében, vagy olyan eljárások céljára, amikor közlésre kötelező európai határozatot lehetett volna kibocsátani. Különböző biztosítékok és jogorvoslatok állnak a szolgáltatók, és azon személyek rendelkezésére, akiknek az adatait kikérik, így az a lehetőség, hogy a szolgáltató felülvizsgálatot kérhet, ha például a határozat nyilvánvalóan sérti az Európai Unió Alapjogi Chartáját.[535]

2018 áprilisában, az Európai Tanács javaslat csomagjának a részeként egy irányelv tervezet elfogadására is sor került, annak érdekében, hogy a rendelet hatékonyságát biztosítani tudják. Ennek az irányelvnek a célja, hogy meghatározza a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályozását. E szerint kötelezik a szolgáltatókat, hogy jelöljenek ki jogi

[534] FRANSSEN, Vanessa: The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement? European Law Blog October 2018, https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/ [2019.01.22.]
[535] http://europa.eu/rapid/press-release_IP-18-3343_hu.htm [2019.02.21.]

képviselőt az Unión belül annak biztosítása céljából, hogy azonos kötelezettségek vonatkozzanak minden szolgáltatóra, amely szolgáltatásokat nyújt az Európai Unión belül, még ha a székhelyük harmadik országban van is, kötelesek jogi képviselőt kijelölni az Unióban a tagállamok illetékes hatóságai által a büntetőeljárás során a bizonyítékok összegyűjtése céljából kibocsátott határozatok és végzések átvétele, az azoknak való megfelelés, és azok végrehajtása érdekében. A jogi képviselőnek azon tagállamok egyikében kell tartózkodnia, ahol a szolgáltató letelepedett vagy szolgáltatásokat nyújt.[536]

A határozatok kötelező erejűek lesznek a szolgáltatókra nézve, ami előre lépést jelent, mert jelenleg gyakran a szolgáltatók jóindulatától függ, hogy átadják-e a bűnüldöző hatóságoknak a szükséges bizonyítékokat vagy sem. Továbbá javítja a jogbiztonságot is a vállalkozások és szolgáltatók számára, mivel a jövőben az elektronikus bizonyítékok közlésének elrendelésére vonatkozó azonos szabályokat kell majd alkalmazni valamennyi szolgáltatóra nézve.[537]

Az új határozatok mellett továbbra is nyitva állnak a „hagyományos" jogintézmények, így az igazságügyi együttműködés és a kölcsönös jogsegély. A rendelet a szankciókra vonatkozóan nem határoz meg konkrétumot, amennyiben a szolgáltatók nem teljesítik a határozatokat, tehát ennek részletes kidolgozását a tagállamokra bízza.

További kérdést vet fel, hogy az Egyesült Államokban elfogadták a „Clarifying Lawful Overseas Use of Data" (CLOUD) törvényt, amely kimondja, hogy „az Egyesült Államokban székhellyel rendelkező szolgáltatónak meg kell őriznie és rendelkezésre kell bocsátania minden vezetékes és elektronikus tartalmat, amely egy ügyféllel vagy előfizetővel kapcsolatban keletkezett, amennyiben ezzel a szolgáltató rendelkezik, függetlenül attól, hogy az adott adatokat, információkat a szolgáltató az Egyesült Államok területén belül vagy azon kívül tárolja."[538]

Végül a felhő alapú technológiai megoldásokra (cloud computing) szeretném felhívni a figyelmet, amelyek különösen nagy kihívást jelentenek a nyomozó hatóságok számára. Ennek a leggyakoribb formája a nyilvános felhőszolgáltatás, amely igénybevételének az esetén a szolgáltatók a felhasználóknak csak az erőforráshoz, infrastruktúrához (pl. hálózatokat, szervereket) biztosítanak távoli hozzáférést az interneten keresztül. Ez általában egy decentralizált rendszer és világszerte elhelyezkedő több szerverre másolják a tartalmat, így ez

[536] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018PC0226 [2019.02.21.]
[537] BUONO, Laviero: The genesis of the European Union's new proposed legal instrument(s) on e-evidence – Towards the EU Production and Preservation Orders. Era Forum, 2018 September 1-6. o.
[538] DASKAL, Jennifer: Unpacking the CLOUD Act. eucrim 4/2018. 220-224. o., valamint ehhez lásd részletesen még SIRY, Lawrence: Cloudy days aheas: Cross-border evidence collection and its impact on the rights of EU citizens. New Journal of European Criminal Law Volume (10)(3). 2019. 227-250. o.

lehet a felhasználóhoz a legközelebbi, vagy amely kevésbé leterhelt hálózatra tudja irányítani. Ennek az előnye, hogy a felhasználóknak nem kell a saját gépükön tárolniuk az adataikat, hanem egy megosztott, távoli tárhelyre tölthetik fel, amelyhez bárhonnan hozzáférhetnek, azonban az adatok pontos helye nem határozható meg ebben az esetben, ami elvezet a „loss of (knowledge of) location" problémaköréhez. Ugyanis kérdésként felmerült, hogy a szerver melyik országban található, illetve az adott pillanatban melyik szerven érhető el az adat. Ez pedig azt jelenti a jelenlegi szabályozásra tekintettel, hogy nem tudják megállapítani, hogy melyik állam jogosult eljárni, hogy a kölcsönös jogsegély iránti megkeresést kezdeményezze, azonban az új rendelet immár ezt a problémát orvosolná.

Ezentúl a felhőszolgáltatások különböző szolgáltatási modellt is magukban foglalhatnak (pl. szoftver, platform, infrastruktúra), így az adott szolgáltató esetén nehéz megállapítani, hogy a hatóságnak milyen típusú adatra kell a közlésre kötelező határozatot kiállítania (előfizetői, hozzáférési, tranzakciós vagy tartalmi).[539]

2.3. A titkosítással kapcsolatos aktuális kérdések a büntetőeljárásban

A titkosításnak (encryption) – például jelszavas, kriptográfiai vagy egyéb titkosítást nyújtó szoftveres védelem – mindennapi használata elterjedt, ezért ezt már a bűnelkövetők is kihasználják. A különböző titkosítási megoldások a már bevett bűnüldöző technikák, módszerek alkalmazását is ellehetetlenítik. A privátszférát erősítő technológiákat[540] gyakran rendelkezésüktől ellentétesen alkalmazzák.[541]

A titkosított eszközökkel és az azokon tárolt adatokkal pedig sok esetben a probléma az, hogy a tartalmuk nem ismerhető meg a nyomozó hatóságok számára, így a bizonyítás során sem tudják felhasználni ezeket. Mindez következik abból, hogy a legtöbb ország büntető eljárásjogában – így hazánkban is – a terhelt együttműködésén, illetve a helyszínen fellelhető és beszerzett bizonyítási eszközökön múlik sokszor a nyomozás sikere, mert az önvádra kötelezés tilalma érvényesül a büntetőeljárás során. Ez azt jelenti, hogy senki sem kötelezhető

[539] KLEIJSSEN, Jan – PERRI, Pierluigi: Cybercrime, Evidence and Territoriality: Issues and Options. In: Kuijer M. – Werned, W. (eds.): Netherlands Yearbook of International Law 2016. 158-159. o.
[540] KISS Attila: A privátszférát erősítő technológiák. Infokommunikáció és Jog 2013/3. 113. o.: A "Privacy Enhancing Technologies" (PETs) kifejezésre nem található általánosan elfogadott meghatározás, leggyakrabban azonban az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőneve. A hazai dogmatika a következő terminológiákat alkalmazza: "magánszféravédő technológiák", "privátszférát erősítő technológiák", és "adatvédelmet elősegítő technikai intézkedések."
[541] MISKOLCZI – SZATHMÁRY: i.m. 177-178. o.

arra, hogy önmagára nézve terhelő vallomást tegyen, vagy önmaga ellen bizonyítékot szolgáltasson.[542]

Azonban erre már van ellenpélda is, mert pár ország engedi a titkosítás feloldására való kötelezést, így a francia büntető törvénykönyv három, illetve minősített esetként öt évig terjedő szabadságvesztéssel fenyegeti azt, aki megtagadja a titkosítás feloldáshoz szükséges jelszó, kód átadását a hatóságnak[543], míg az Egyesült Királyságban két évig[544], Belgiumban egy évig terjedő szabadságvesztéssel rendelik büntetni ezt.[545] Felmerül a kérdés, hogy a terhelt esetében ez nem jelenti-e az önvádra kötelezés tilalmának a megsértését. A francia Legfelsőbb Bíróság döntése értelmében ez a rendelkezés alkotmányosnak tekinthető, mert a gyanúsítottat nem kötelezik ezzel magára nézve terhelő vallomásnak a megtételére, valamint az adat már tárolva van valahol, ami a gyanúsított akaratától függetlenül létezik. Belgiumban a bíróságok ítéletei között eltérések mutatkoznak, vannak olyan esetek, amikor a tilalom megsértéseként értékelték, míg mások összeegyeztethetőnek tartották a tisztességes eljárással. Ez a kérdés rendkívül aktuális és vitatott mind a szakirodalomban, mind a gyakorlatban is, vélhetően idő kérdése, hogy valamelyik ügy eljut egészen Strasbourgig, az Emberi Jogok Európai Bíróságához.

Ezzel szoros összefüggésben érdemes említést tenni azokról az esetekről is, amikor a felhasználó olyan titkosítást használ, ami nem egy jelszó vagy kód, hanem biometrikus adat[546] (pl. ujjlenyomat, arcfelismerés, írisz), amely különösen megnehezítheti a nyomozó hatóságok helyzetét és az eljárás lefolytatását, mert egyre több eszköznél jelenik meg a digitális azonosításnak ezen formája például okostelefonoknál és laptopoknál már általánossá vált a használatuk és ezek köre folyamatosan bővül.

Az itt felvázolt problémát megoldva, példaként említendő Norvégia, mint első állam, amely a büntető eljárásjogában engedi a biometrikus titkosítás feloldását, vagyis a nyomozó hatóság jogosult elrendelni azt, hogy a terhelt a biometrikus azonosítással hozzáférést biztosítson az eszközökhöz vagy adatokhoz. Abban az esetben, ha ezt megtagadja, akkor – arányos mértékben – kényszert alkalmazhatnak vele szemben a védelem feloldásához (pl. az ujjnak a

[542] Be. 7. § (3) bekezdés
[543] Amennyiben kétséget kizáróan kiderül, hogy a kód átadása megakadályozta volna a bűncselekményt vagy ezáltal a bűncselekménnyel okozott hátrány vagy kár csökkenthető lett volna.
[544] KOOPS, Bert-Jaap – KOSTA, Eleni: Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". Computer Law & Security Review 2018/4. 894. o.
[545] DORNFELD (2017): i.m. 248. o.
[546] A biometrikus adat fogalmát a GDRP 4. cikk 14. pontja határozza meg, amely szerint „egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat." A jellemzője, hogy egyedi, megváltoztathatatlan, a többi személytől megkülönböztet. A biometrikus azonosításról bővebben lásd SZABÓ Endre Győző (2018a): i.m. 38-43. o.

lenyomatolvasóhoz való helyezésével).[547] A kényszer alkalmazásához azonban az ügyészség engedélyére van szükség, amennyiben a késedelem a nyomozást veszélyezteti, akkor a rendőrség mérlegelhet a helyszínen és dönthet erre vonatkozóan, amit később az ügyészségnek kell átadni.

Az Európai Emberi Jogok Bíróságának Saunders v. United Kingdom döntésében a gyanúsított önvádolás alóli mentességének és a hallgatás jogának a kérdéseit vizsgálta részletesen. A Bíróság kimondta, hogy ezen jogokat azonban nem lehet kiterjesztően értelmezni: a nyomozó hatóság megszerezhet a terhelttől – a kényszerítő erő elfogadható használatával – olyan tárgyakat és anyagokat, amelyek a terhelt akaratától függetlenül léteznek, ilyen például egy dokumentum, a lehelet, a vér és vizelet minta, valamint a testi szövetminta (pl. DNS teszt céljából). Mindezekre tekintettel a norvég jogalkotók azon az álláspontonvannak, hogy a kikényszerített biometrikus hitelesítés az önvádra kötelezés tilalmát nem sérti, mert a terhelttel szemben valamely testi jellemzőjét használják fel, ami a gyanúsított akaratától független, és nem kell maga ellen terhelő bizonyítékot szolgáltatnia. Ez azt a célt szolgálja, hogy a nyomozó hatóság olyan információkhoz férjen hozzá – a fizikai-technikai akadályt leküzdve –, amelyre már törvényes alapjuk van a lefoglalás körében. Ezzel szemben a terheltet nem kényszeríthetik a jelszó vagy kód megadására. Valószínű, hogy a bűnelkövetők a jelszavas védelmet fogják választani az ujjlenyomattal szemben, mert utóbbit kikényszerítheti a nyomozó hatóság, míg előbbit nem.[548]

A kommunikáció egyes elemeit figyelembe véve a titkosítás alkalmazása szempontjából három, egymást átfedő csoport állapítható meg: a közlés sértetlenségének biztosítása és a közlést létrehozó vagy küldő személyének hitelesítése, valamint a közlés tartalmának titkosítása, illetve a kommunikációs csatorna bizalmasságának biztosítása.[549]

A titkosításnak tehát különböző formái lehetnek: a szolgáltató titkosít központilag és rendelkezik a kriptográfiai kulcsokkal, valamint a másik eset, ha a szolgáltató az információ-, kommunikáció átvitelt titkosítja, vagy az alkalmazásszolgáltató a végpontok közötti titkosítást alkalmaz a kommunikációhoz (pl. Skype), végül az utolsó eset, amikor a felhasználók által használt végpontok közötti titkosítás jelenik meg (végpontok közötti titkosítás). Az első két esetben a szolgáltató a titkosítás feloldását tudja biztosítani, ezért általában az ehhez kapcsolódó szabályozás jelen van az egyes államok jogrendszerében és a nyomozó hatóság kérheti a

[547] KOOPS – KOSTA: i.m. 894-895. o.
[548] BRUCE, Ingvild: Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure. Digital Evidence and Electronic Sigranute Law Review 2017/14. 26-30. o.
[549] SZÁDECZKY Tamás – SZŐKE Gergely László – ZÁMBÓ Alexandra Erzsébet: Titkosítás és jog – Gondolatok a titkosításhoz kapcsolódó jogi szabályozásról. Infokommunikációs jog 2017/1. 4. o.

dekódolást. Ezzel szemben az utolsó két eset problematikus, mert a szolgáltatók nem rendelkeznek a végpontok közötti titkosítás feloldásához szükséges kulcsokkal.[550]

A titkosítással kapcsolatban érdemes a Be. vonatkozó rendelkezését is vizsgálni, amely a büntetőeljárás során a bíróság, az ügyészség és az ügyészség engedélyével a nyomozó hatóság adatszolgáltatást kérhet az elektronikus hírközlési szolgáltatótól[551], amely vonatkozhat az elektronikus adat vagy irat továbbítására is. Az együttműködési kötelezettség körébe tartozik a szolgáltató titkosításfeloldó kötelezettsége is, amennyiben a titkosítást a szolgáltató végezte és nem maga a felhasználó [Be. 264. § (2) bekezdés]. „A rejtjelezett vagy más módon megismerhetetlenné tett adatot az adatkérés keretében megkeresett szervezet köteles az átadás vagy a közlés előtt eredeti állapotába visszaállítani, illetve az adatszolgáltatást kérő szerv számára az adat tartalmát megismerhetővé tenni" [Be. 264. § (3) bekezdés]. A felhasználó által titkosított kommunikáció dekódolására azonban a szolgáltató nem kötelezhető.[552]

Emellett az Ekertv. 3/B. §-a[553] annak az alkalmazásszolgáltatónak[554] a kötelezettségét határozza meg, aki az információs társadalommal összefüggő olyan szolgáltatást nyújt, amely a szolgáltatást igénybe vevők között titkosított kommunikációt biztosít és ezt olyan módon teszi, hogy a kommunikáció tartalma vagy a kommunikációs csatorna felépítésével kapcsolatos funkciók nem kizárólag a felhasználó végberendezésén valósulnak meg. Ezen szolgáltatók ugyanis kötelesek a titkosított kommunikációt biztosító alkalmazás igénybevételével továbbított küldemények, közlések tartalmát a külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén átadni, valamint a titkosított kommunikációt biztosító alkalmazás igénybevételével kapcsolatosan keletkező vagy kezelt - a 13/B. § (2) bekezdése szerinti - metaadatokat a 13/B. § alapján egy évig megőrizni és megkeresés esetén azokat szintén átadni.

---

[550] KOOPS – KOSTA: i.m. 891. o.

[551] Az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) értelmező rendelkezései alapján (Eht. 188. § 13. pont) az elektronikus hírközlési szolgáltatás fő ismérve, hogy teljesen vagy nagyrészt jeleknek elektronikus hírközlési hálózaton való átviteléből, és ahol értelmezhető, irányításával jár. Eszerint van átfedés a közvetítő és az elektronikus hírközlési szolgáltatók között: az egyszerű adatátvitelt és hozzáférést biztosító közvetítő szolgáltatók, tehát az internetszolgáltatók elektronikus hírközlési szolgáltatónak is minősülnek. Lásd SORBÁN Kinga: Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában – Felelősségek és kötelezettségek. In Medias Res 2019/1. 86. o.

[552] PARTI Katalin: Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntetőeljárás során a gyakorlat tükrében. Belügyi Szemle 2018/10. 30-31. o.

[553] Ekertv. 2. § m) pont: „Alkalmazásszolgáltató: az a természetes, illetve jogi személy vagy jogi személyiséggel nem rendelkező más szervezet, aki, vagy amely elektronikus hírközlő hálózat felhasználásával valamilyen szoftverhez vagy hardverhez való hozzáférést, szoftveres alkalmazást, valamint kapcsolódó szolgáltatásokat biztosít specifikus szoftveren vagy webes felületen több felhasználó számára, időben korlátozott vagy korlátlan módon, havi- vagy használat alapú ellenszolgáltatás fejében vagy ingyenes formában."

[554] 2016. július 17-től hatályos módosítását a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló 2016. évi LXIX. törvény iktatta be.

Felmerülhet bennünk az a kérdés, hogy ezen jogi eszközök kimerülése esetén milyen módon tud fellépni a hatóság a bizonyítékok megszerzése érdekében. Ez pedig az ún. „hatósági hacking" problémaköréhez vezet („police hacking", „government hacking" vagy „legal hacking"), amely alatt olyan nyílt vagy leplezett tevékenységet értünk, amelynek lényege, hogy a kommunikációban részt vevő felek akarata ellenére vagy tudta nélkül történik a kommunikáció tartalmának vagy a titkosított adatoknak a megismerése, technikai beavatkozással. Technikai értelemben erre számos módszer érhető el, például a brute force technikával a titkosítás feltörése, vagy az információs rendszert érintő sebezhetőségi pontok megszerzése, gyűjtése, visszatartása, majd felhasználása, valamint kombinált leplezett eszközök alkalmazása pl. kémprogramok felhasználásával. A kérdés az, hogy ezek közül melyek illeszthetők be a jelenlegi eljárásjogi eszközrendszerbe, és amelyek nem, azok miként képezhetők le jogi keretek között.[555] Például további kérdést von maga után, hogy joghatósági problémát jelenthet-e, ha nem tudják, hogy az elkövető által használt eszköz melyik államban található.[556]

A hazai Be. a 232. § (1) bekezdésében szabályozza a vonatkozó információs rendszer titkos megfigyelését, a bírói engedélyhez kötött leplezett eszközök alkalmazása körében, garanciális feltételekkel biztosított. Az erre feljogosított szerv adatokat titokban megismerhet, az észlelteket technikai eszközzel rögzítheti. Ennek érdekében az ehhez szükséges elektronikus adat az információs rendszerben, illetve a szükséges technikai eszköz - a nyilvános vagy a közönség részére nyitva álló hely kivételével - lakásban, egyéb helyiségben, bekerített helyen, illetve - a közösségi közlekedési eszköz kivételével - járműben, továbbá az érintett személy használatában lévő tárgyban elhelyezhető.

Érdekes szabályozási példaként említhető a sokak által vitatott és bírált holland törvény, amely a legszélesebb körben határozza meg, hogy milyen célból és módszerekkel alkalmazható a hatósági hacking, így a meghatározott típusú adatok gyűjtése érdekében (pl. a felhasználó azonosításához vagy helymeghatározásához szükséges adatok megszerzése), távoli hozzáférés biztosítása a tárolt adatokhoz, a számítógép használatának a valós idejű, távoli megfigyelése (pl. keylogger alkalmazása, képernyőkép vagy videó), elektronikus és szóbeli

[555] MISKOLCZI – SZATHMÁRY: i.m. 179-180. o.

[556] Erre a probléma felvetésre reagálva Ahmed Ghappour szerint például a Dark Weben, ha az adott állam bűnüldöző szerve hatósági hacking technikát alkalmaz, akkor ezzel megsértheti a másik állam szuverenitását. Lásd bővebben erről GHAPPOUR, Ahmed: Searching Places Unknows: Law Enforcement Jurisdiction on the Dark Web. Stanford Law Review Stanford Law Review Volume 69. April 2017. 1075-1136. o.; Ezzel ellentétes álláspontot képvisel Orin Kerr és Sean D. Murphy, akik szerint ez nem jelenthet problémát és az ilyen nyomozások során a nemzetközi együttműködés érvényesül. Lásd KERR, Orin – MURPHY, Sean D.: Government Hacking to Ligh The Dark Web: What Risks to International Relations and International Law? Stanford Law Review Volume 70. July 2017. 58-69. o.

kommunikációnak a lehallgatása (pl. e-mail, chat, Skype-beszélgetés, FaceTiming, kikerülve a végpontok közötti titkosításból adódó problémát), vizuális megfigyelés (pl. webkamera bekapcsolásával), valamint az illegális adatok törlése is megengedett távoli hozzáféréssel.[557]

Az Egyesült Államokban az ún. „Network Investigative Technique" (NITs) terminológiát használják erre. A Dark Weben, illetve valamennyi esetben, amikor az elkövetők a TOR hálózat vagy proxyk mögé rejtőznek, akkor a bűnüldöző hatóságok nem tudják a bűncselekmény elkövetésére használt eszköznek a pontos helyét meghatározni vagy az elkövetőt azonosítani, ekkor a legjobb esélyük erre az, ha a célszemély rendszerére sikerül eljuttatni a hatósági (kém)programot, például pszichológiai manipulációval. Amennyiben ennek a telepítése megtörténik, akkor értékes információkhoz juthatnak hozzá, mint például az eszköz valós IP-címéhez, amely segítséget nyújthat a felhasználó azonosításához.[558]

Végül említést teszek a példaértékű Silk Road nyomozásról, mert ez bemutatta, hogy a nyomozati módszerek különböző kombinációjának segítségével a nyomozó hatóságok meg tudnak birkózni az anonimitást és titkosítást biztosító technológiák által okozott nehézségekkel. Az online feketepiac a TOR használata révén rejtve volt, ezért nem tudták meghatározni a szervernek és az adminisztrátornak a pontos elhelyezkedését. Azonban a hét lépcsős nyomozati módszerrel sikerült felkutatni a „Dread Pirate Roberts" név mögött rejtőző Ross Ulbricht adminisztrátort a következőképpen:

- a nyilvánosan elérhető online adatok[559] gyűjtésével (pl. „rossulbricht@gmail.com" e-mail címet szerezték meg egy korai Silk Road reklámból, amit még saját maga tett közzé),
- az elektronikus bizonyítékok közlésére kötelező határozatokat bocsátottak ki a szolgáltatóknak, így a Googlenak, WordPressnek, PayPalnek és egy online fórumnak,
- emellett fedett beszélgetést folytattak Ross Ulbrichttel a TorChaten keresztül,
- kábítószer álvásárlásokat intéztek a piactérről,
- hacking technikák alkalmazásával távoli hozzáférést szereztek a szerverhez,
- egy sikeres kölcsönös jogsegély iránti megkeresést követően Izlandon lefoglalták a webszervert egy adatközpontban és az azon tárolt elektronikus bizonyítékokat felkutatták.

[557] SKORVANEK, Ivan – KOOPS, Bert-Jaap – CLAYTON NEWELL, Cryce – ROBERTS, Andrew: „My computer is my castle": New privacy frameworks to regulate police hacking. TILT Law & Technology, Working Paper Series February 2019. 10-12. o.
[558] KERR – MURPHY: i.m. 59. o.
[559] A Budapesti Egyezmény 32. Cikk a) pontja rögzíti, hogy az egyik szerződő fél a másiknak az engedélye nélkül a nyilvánosság számára elérhető módon (nyílt forrású) tárolt számítástechnikai adathoz hozzáférhet, függetlenül az adat földrajzi elhelyezkedésétől.

Végül a bűnüldöző hatóságnak sikerült meghatározni Ross Ulbricht tartózkodási helyét, akit ezután meg tudtak figyelni, valamint az online tevékenységét is nyomon követték a Silk Roadon. Ennek eredményeképpen képesek voltak meghatározni azt az időpontot is, hogy várhatóan mikor fogja bekapcsolni a számítógépét és adminisztrátorként bejelentkezni. 2013 októberében az FBI letartóztatta őt, és egyúttal lefoglalta a számítógépét egy San Franciscó-i könyvtárban, amely a szerverrel együtt elegendő bizonyítékot szolgáltatott ahhoz, hogy elítéljék kábítószer-kereskedelem és pénzmosás miatt.[560]

[560] OERLEMANS, Jan-Jaap: Investigating Cybercrime. Amsterdam University Press. 2017. 42-43. o.

2.4. A joghatóság és a kiadatás kérdése a kiberbűncselekmények esetén

Az államok joghatóságukat általában a földrajzilag meghatározott területi határokra korlátozzák, ami azt jelenti, hogy az adott állam szuverenitása alá tartozik az a bűncselekmény, amelyet a területén követtek el, vagyis az elkövetési magatartást az adott állam területén valósították meg vagy az eredmény az adott állam területén következett be.

Azonban a kiberbűnözés sajátossága, hogy határokon átível, ezért sokszor nehéz eldönteni, hogy mely állam területén követték el az adott informatikai bűncselekményt, gyakran előfordul, hogy az elkövető és a sértett különböző országokban tartózkodik, továbbá a bűncselekmény által érintett információs eszköz vagy adat harmadik országban található. Tovább bonyolíthatja a helyzetet, amennyiben az elkövető valamelyik harmadik ország közbeiktatásával követi el a bűncselekményt. Mindez a gyakorlatban joghatósági összeütközésekhez és párhuzamos eljárások megindításához vezethet.[561]

A szakirodalom a negatív és pozitív joghatósági összeütközést különböztet meg, de utóbbi jellemző a kiberbűncselekményeknél. A negatív esetén egyik állam se képes vagy hajlandó eljárni, míg a pozitív esetén több állam is a saját büntetőhatalmának érvényesítésére tart igényt ugyanarra a bűncselekményre nézve. Erre példaként említendő eset, ha egy holland állampolgár Belgiumban használ számítógépet ahhoz, hogy egy az amerikai Utah államban található számítógépbe lépjen be jogosulatlanul. Erre tekintettel ezek az államok joghatóságukat állapíthatják meg, sőt akár más állam is, amelyen keresztül az adatátvitel történt. Emellett a vírus fertőzések esetén is felmerülő probléma, mert a bűncselekményeknek az eredménye általában több országot is érint. [562]

Michal N. Schmitt szerint bármelyik ország, amelyből az elkövető működteti a bűnözői infrastruktúrát joghatóságot élvez, mert az elkövető és az elkövetéshez használt eszköz is az adott állam területén található. A tényleges fizikai jelenlét szükséges és elégséges a területi elv szerinti joghatósághoz, azonban az ún. „meghamisított" jelenlét ennek nem felel meg. A német szabályozás szerint például az az állam jogosult joghatóságra, amelynek területén az adott személy fizikailag jelen van az adatok internetre történő feltöltésekor, így ez meghatározza az ún. „Handlungsort"-ot.

A területi elv alkalmazásának az alkalmatlansága alapvetően az informatikai bűncselekmények jellegével magyarázható, pontosan azzal, hogy technikai nehézségeket okoz

[561] DORNFELD (2017): i.m. 243. o.
[562] BRENNER, Susan W. – KOOPS, Bert-Jaap: Approaches to Cybercrime Jurisdiction. J. High Tech. L. 1. 2004. 40-41. o.

az ilyen típusú bűncselekmények elkövetőinek a nyomon követése, a bűncselekmény elkövetési helyének a meghatározása. Az elkövetők számára rendelkezésre állnak különböző módszerek és programok, hogy elrejtsék helyzetüket és személyazonosságukat, így földrajzilag azonosíthatatlannak mutatkoznak például az ún. IP-cím hamisítás (spoofing) révén, valamint a proxy szerverek vagy VPN (Virtual Private Networks) használatával. Mindkettő lehetővé teszi, hogy úgy tüntessék fel mintha egy másik helyről kapcsolódnának az internetre, az IP-címet elrejtve, azonban előbbi esetén nincs titkosítva a forgalom, míg utóbbi nagyobb biztonságot nyújtva titkosítja is azt. Ezért a digitális elkövetés helyszíne sokszor egyáltalán nincs fizikai közelségben sem az elkövető tényleges tartózkodási helyével. Az egyik legnagyobb problémát az anonimitás jelenti, mert a földrajzi helymeghatározást, a kibertámadás forrásának megállapítását nagy mértékben megnehezíti, amelyet szintén számos program használata nyújthat így említve párat például a TOR, Anonymouse, The Cloak és a különböző e-mail titkosítást biztosító szoftverek.[563]

További problémát jelenthet, amennyiben botnet infrastruktúrát, azaz zombigépeket használnak fel a bűncselekmény elkövetéséhez, mert ezek gyakran különböző országokban találhatóak. A „zombi" hálózatok irányító központjait különböző államok területein szórják szét és szükség esetén percek alatt, más esetekben néhány perces rendszerességgel változtatják a „digitális székhelyüket".[564]

Susan W. Brenner felhívja a figyelmet területi elvnek a kiterjesztésére az informatikai bűncselekmények vonatkozásában. Véleménye szerint, ha az elkövető részben vagy egészben az adott ország területén követte el a bűncselekményt akkor például a joghatóságát érvényesítheti az az állam, amelynek a területén tartózkodik az elkövetéskor az elkövető és a sértett is, vagy, ha az elkövető vagy a sértett van jelen az elkövetéskor az adott ország területén, vagy a bűncselekmény elkövetésének bármely mozzanatát, részét az adott ország területén követték el. Emellett az országok fenntarthatják joghatóságukat saját állampolgáruk esetén, ha külföldön tartózkodva követne el kiberbűncselekményt.[565]

Emellett érdemes említést tenni arról az esetről, amikor a bűncselekmény tényállási elemei nem egyetlen, hanem több állam területén valósulnak meg. Itt utalnék a jogirodalomban elfogadott cselekményegység elméletre, amelynek lényege szerint, a materiális bűncselekmény

[563] MAILLART, Jean-Baptiste: The limits of subjective territorial jurisdiction in the context of cybercrime. ERA Forum 2018 September. 4-5 o.
[564] PRÉCSÉNYI Zoltán: A számítástechnikai ipar és a kiberbűnözés elleni küzdelem: Lehetőségek és korlátok. Magyar Rendészet 2013. különszám 167-178. o.
[565] BRENNER, Susan W.: Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law. 2001. 18. o.

belföldön elkövetettnek tekintendő, ha a nemzeti büntetőtörvény szempontjából jelentős bármelyik mozzanata, így akár az elkövetési magatartás (magatartáselmélet), vagy akár az eredmény belföldön valósul meg (eredményelmélet).[566]

A Budapesti Egyezményben is elsősorban a területi elv jelenik meg, másodsorban a személyi elv (22. Cikk). Erre tekintettel az egyezményben foglalt bűncselekmények esetén az az állam állapíthatja meg a joghatóságát: amelynek a területén; vagy a lobogóját viselő hajónak fedélzetén, a lajstromozott repülőgépének fedélzetén követték el a bűncselekményt, vagy amelyet az állampolgára követett el, ha a bűncselekmény az elkövetés helyének joga szerint büntetendő, vagy ha a bűncselekmény nem tartozik egyetlen állam joghatósága alá sem.

Utóbbi három esetben a szerződő felek fenntarthatják maguknak azt a jogot, hogy a joghatóságra vonatkozó szabályokat vagy azok bármely részét nem, vagy csak meghatározott esetben, illetve feltételek között alkalmazzák, valamint az egyezmény nem zárja ki azt sem, hogy belső joguk szerint meghatározott büntetőjogi joghatóságának gyakorlását.

Amennyiben több állam joghatósága is kiterjed az informatikai bűncselekményre, akkor az érintettek, amennyiben az célszerűnek mutatkozik, tárgyalást folytatnak annak érdekében, hogy eldöntsék, melyik fél képes megfelelőbben lefolytatni az eljárást.

Ugyanezt követi a 2013-as irányelv is uniós szinten. A tagállamok megállapítják joghatóságukat a kiberbűncselekmények tekintetében, amennyiben a bűncselekményt egészben vagy részben a területükön követték el, vagy egy állampolgáruk követte el, legalább azokban az esetekben, ha a cselekmény az elkövetés helyén bűncselekménynek minősül.

A területi elv szerinti joghatóság megállapításakor a tagállamok biztosítják, hogy joghatósággal rendelkezzenek abban az esetben, ha az elkövető a bűncselekmény elkövetésekor fizikailag jelen van a területükön, függetlenül attól, hogy a bűncselekmény a területükön található információs rendszer ellen irányul-e, vagy a bűncselekmény a területükön található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e a területükön.

A tagállamoknak tájékoztatniuk kell a Bizottságot, ha úgy döntenek, hogy a területükön kívül elkövetett bűncselekményekre vonatkozóan további joghatóságot állapítanak meg, többek között amennyiben az elkövető szokásos tartózkodási helye a területükön van, vagy a bűncselekményt a területükön letelepedett jogi személy javára követték el.

Az megállapítható, hogy a joghatóság terén mindenképpen paradigmaváltásra van szükség.

[566] SZABÓ Imre: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6. 48. o.

Emellett fontos említést tenni arról, hogy a joghatóság megállapításán kívül komoly problémát jelenthet még a kiadatás kérdése, mert gyakran előfordul, hogy az egyes országok nem hajlandóak kiadni az állampolgárukat semmilyen körülmények között sem, vagy más ország állampolgára esetén, a területükön elkövetett bűncselekményének gyanúsítottját. Ezt általában az államok egymás közötti két- vagy többoldalú kiadatási egyezményekkel biztosítják.[567]

A Budapesti Egyezmény is érinti a kiadatásra vonatkozó alapelveket (24. Cikk), amely szerint akkor kerülhet sor az egyezményben szabályozott bűncselekményekre vonatkozóan kiadatásra, ha mindkét érdekelt fél szabályozása szerint legalább egy év vagy ennél súlyosabb szabadságvesztéssel büntetendők. Amennyiben két vagy több fél között alkalmazható, egységes vagy viszonossági jogszabályon alapuló megállapodás, illetve kiadatási szerződés - beleértve az Európai Kiadatási Egyezményt - alapján más minimális büntetés kerül alkalmazásra, az ilyen megállapodásban vagy szerződésben meghatározott minimális büntetést kell alkalmazni. A szerződő feleknek az informatikai bűncselekményeket kiadatás alapjául szolgáló bűncselekményként kell elismerniük. A kiadatásnak a megkeresett állam belső jogában vagy a hatályban lévő kiadatási szerződésekben meghatározott feltételeknek kell megfelelnie, ideértve azokat az okokat is, melyek alapján megtagadhatja a kiadatási kérelem teljesítését. Végül az egyezmény az aut dedere aut judicare, azaz a kiadatás vagy elbírálás elvét alkalmazza. Ez az jelenti, hogy abban az esetben, ha a kiadni kért személy állampolgársága alapján tagadják meg a kiadatást, vagy azért, mert a megkeresett állam saját joghatósága alá tartozónak ítéli a bűncselekményt, akkor a megkeresett ország, a megkereső félnek az erre vonatkozó kérelme alapján a saját hatáskörrel rendelkező hatóságai elé terjeszti az ügyet a büntetőeljárás lefolytatása érdekében, és megfelelő időn belül beszámol az ügy kimeneteléről.

[567] GRABOSKY: i.m. 104. o.

V. ÖSSZEFOGLALÁS

Összeségében elmondható, hogy mind a nemzetközi színtéren, mind az Egyesült Államokban egészen az 1970-es évekig nyúlnak vissza a kiberbűnözéssel kapcsolatos kezdeti törekvések. Közös vonásuk, hogy a meglévő, hagyományos bűncselekményekre vonatkozó szabályozás helyett, elkezdték a speciális és önálló anyagi büntetőjogi rendelkezések megalkotását az új típusú informatikai bűncselekmények vonatkozásában. Az Európa Tanács több évtizedes munkájának eredményére 2001-ig, a Budapesti Egyezmény elfogadásáig kellett várni. Ez az első olyan kötelező erejű, multilateriális és a mai napig legjelentősebb jogi dokumentum, amely a kiberbűnözés elleni küzdelem alapjait teremtette meg. Az aláírásához csatlakozó országok számára keretet biztosít a nemzetközi együttműködéshez, továbbá olyan államok előtt is nyitva áll, amelyek nem tagjai az Európa Tanácsnak, így többek között az Egyesült Államok is ratifikálta. A Budapesti Egyezmény elősegíti az informatikai bűnözés elleni küzdelmet nemzetközi, uniós és az egyes országok regionális szintjén, különösen a közös büntető anyagi és eljárásjogi szabályokkal, valamint a technikai jellegű fogalmak világos meghatározásával.

A másik nagy előrelépést uniós szinten a 2013-as irányelv jelentette, amely az információs rendszerek elleni támadásokkal szemben lép fel a szükséges minimumszabályok megalkotásával. Felismerték, hogy rendkívül fontos a harmonizált és egységes szabályozás megteremtése mind büntető anyagi, mind eljárásjogi tekintetben, ami azért is kihangsúlyozandó, mert egy határokon átívelő bűnözésről van szó, és az elkövetők kihasználhatják a különböző országok jogrendszerének a szabályozási hiányosságait, differenciáltságát.

Az egyes országok általában különböző szabályozási megoldást választanak a kiberbűncselekmények körében. Jellemző, hogy vagy egy külön törvényben szabályozzák ezen deliktumokat, vagy a nemzeti büntető törvénykönyvükbe önálló fejezetbe iktatják a vonatkozó rendelkezéseket, vagy a különös részben helyezik el szétszórtan a tényállásokat.

Az Egyesült Államok az előbbi megoldást alkalmazva, szövetségi szinten, először 1984-ben, az uniós törekvéseket megelőzve szabályozta az informatikai bűncselekményeket, méghozzá egy külön törvénykönyvben. Ahhoz, hogy a CFAA lépést tudjon tartani a technológiai innovációval már nyolc alkalommal módosították 1986 és 2008 között. A változtatások közös céljaként felismerhető, hogy a törvény hatályát minél szélesebb körben igyekeztek kiterjeszteni. Például a szövetségi érdekű számítógép szűk fogalmától eljutottak a tágabb értelemben vett számítógép meghatározáshoz, amelynek hatálya alá tartozik lényegében majdnem valamennyi,

a világ bármely részén használt, akár egy háztartási eszközként funkcionáló számítógép is. Továbbá a büntetendő cselekmények körét is fokozatosan bővítették, így jutottak el a hatályos szabályozás szerinti hét informatikai bűncselekményhez.

Az első kutatási kérdésemmel kapcsolatban azt vizsgáltam, hogy a jelenlegi szabályozási környezet nemzetközi, uniós és hazai szinten, valamint az Egyesült Államokban mennyiben alkalmas a kiberbűnözés elleni fellépésre. Ezzel összefüggésben a következőkre jutottam:

A Budapesti Egyezmény elfogadása óta eltelt időben a technológiai fejlődés a megállapodás egyes rendelkezéseit már meghaladta, ezért szükségessé vált, hogy további jegyzőkönyvvel egészítsék ki, amely orvosolná ezeket a szabályozási hiányosságokat.

A 2013-as irányelv már az új kihívásokra részben reagált azzal, hogy az információs rendszerek elleni támadásokkal kapcsolatos büntetőjogi szabályait az újabb veszélyforrások figyelembevételével határozta meg (pl. büntetendő és szigorúbb büntetés alkalmazását teszi lehetővé a botnetekkel végrehajtott vagy a kritikus infrastruktúrák ellen irányuló kibertámadások esetén, valamint a személyazonosság-lopást is említi).

Magyarországon az elmúlt években az informatikai bűncselekmények szabályozása a nemzetközi és uniós elvárásoknak megfelelően alakult. A Btk. hatályba lépésével már annak önálló fejezetébe lettek illesztve, ami mindenképpen egy üdvözítő megoldás és haladás az új védendő társadalmi értékek elismerése felé. Nóvumként jelent meg az információs rendszer felhasználásával elkövetett csalás (Btk. 375. §) tényállása, amely a vagyon elleni bűncselekmények között kapott helyet, amelyet a jogalkotó az eltérő jogtárgy védelemmel indokolt.

Az értekezésemben vizsgáltam a leggyakrabban előforduló informatikai támadásokat, így kiemelten a jogosulatlan belépést, DDoS-támadásokat és a rosszindulatú programokkal kapcsolatos büntetőjogi szabályozási és minősítési kérdéseket. Mindezek alapján úgy gondolom, hogy a magyar szabályozás jelenleg alkalmas arra, hogy az informatikai környezetben elkövetett büntetendő magatartások széleskörét lefedje az információs rendszer elleni bűncselekmények körében, így az információs rendszer vagy adat megsértése (Btk. 423. §) és ezen rendszer védelmét biztosító technikai intézkedés kijátszása (Btk. 424. §) tényállásaiban.

A jogalkotó azonban egyes kérdésekben adós maradt, például nem határozza meg pontosan az előbbi bűncselekmény minősített eseténél [Btk. 423. § (3) bekezdés], hogy mi tekinthető jelentős számú információs rendszernek, tehát a jogalkalmazókra hárul ez a feladat, hogy egy erre vonatkozó gyakorlatot dolgozzanak ki. A joggyakorlat részben egyes kérdéseket

megválaszolt, ugyanis a hacking rendelkezés második fordulatánál [Btk. 323. § (1) bekezdés] a Kúria elvi éllel mondta ki, hogy a jogosultság keretein való túllépés is akkor minősül bűncselekménynek – az első fordulat szerinti jogosulatlan belépéshez hasonlóan –, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik.

A másik felmerült problémakör az etikus hackinghez kapcsolódik, amely sokszor éles vita tárgyát képezi, és visszavezethető arra, hogy hiányzik a megfelelő szabályozása és gyakorlata. A szakirodalmi álláspont szerint az információs rendszer tulajdonosa vagy egyéb jogosultja által más számára engedélyezett biztonsági tesztelés, illetve támadás tartozik ebbe a tevékenységi körbe. Erre utal rendelkezéseiben a Budapesti Egyezmény és a 2013-as irányelv is, amelyek szerint a büntetendő cselekményt jogosulatlanul kell elkövetni, ami azt jelenti, hogy ez a rendszer jogosultjának az engedélye nélkül történik. Ez különösen akkor vitatott, ha a hacker valamilyen sebezhetőségre hívja fel a figyelmet, különösen, ha a nagy nyilvánosság felé is közvetíti. A konkrét ügy során ezért a bíróságnak vizsgálnia kell az eset összes körülményére tekintettel a következőket: a hacker cselekménye mennyiben veszélyes a társadalomra, milyen szándék húzódott e magatartása mögött, valamint közérdekű bejelentésnek tekinthető-e az eljárása a megtámadott fél felé.

A hazai és amerikai szabályozást összevetve megállapítható, hogy utóbbi részletesebben szabályozza az egyes informatikai bűncselekményeket. Példaként említhető, hogy a jogosulatlan hozzáféréssel kapcsolatban több tényállást alkottak, valamint a DDoS-támadásra és a számítógépes vírusokra vonatkozó rendelkezéseknek hat minősített esete van, sőt külön számítógépes csalás és zsarolás deliktuma is rendelkezésre áll. Esetenként a kiszabható büntetések is sokkal szigorúbbak, ha például az elkövetőt korábban elítélték már informatikai bűncselekmény elkövetéséért, akkor akár tíz vagy húsz évig terjedő szabadságvesztést is megállapíthat a bíróság, továbbá az esetjoga is sokkal gazdagabb. A különbségek is tetten érhetők, azonban ez részben betudható annak, hogy a CFAA alapját az angolszász jogrendszer képezi. Az amerikai szabályozás egyes tényállásoknál a felelősség alapján differenciál, amely érintheti az elkövetési magatartáshoz (tudatos vagy szándékos elkövetés) vagy az eredményhez kapcsolódó felelősséget (szándékosan vagy gondatlanságból vagy hanyagságból történő károkozás), míg a Btk. kizárólag a szándékos elkövetést rendeli büntetni. További különbség, hogy az amerikai jog a védett számítógéphez való hozzáférés korlátozásának két típusát határozza meg: a technikai védelem (code-based) és a szerződés (contract-based) alapján. A magyar szabályozás azonban megköveteli a technikai intézkedés megsértését vagy kijátszását a tényállásszerűséghez, valamint a 2013-as irányelv is rögzíti, hogy például felhasználói

szabályzat vagy szolgáltatási feltételek révén korlátozó szerződéses kötelezettségek vagy megállapodások nem vonhatnak maguk után büntetőjogi felelősséget. Hasonló elkövetői kör büntethető mindkét törvény alkalmazásában, így aki a hozzáférési jogosultsággal nem rendelkező („kívülálló") személy vagy jogosultsággal rendelkező, de ennek kereteit túllépő („bennfentes") személy.

A CFAA legnagyobb hiányossága abban ragadható meg, hogy az egyes alapvető fogalmakat nem tisztázza, így többek között „a jogosulatlan hozzáférést" (unauthorized access), valamint a számítógépes adatot, avagy a CFAA-ban használt elnevezés alapján „az információt" (information) és a hozzáférést biztosító jelszavat, valamint a programokat sem. Következésképp, ezeknek az értelmezése a jogalkalmazókra hárul, különösen a precedensek megteremtésével. Ezzel szemben a hazai szabályozás e tekintetben jobban alkalmazható, mert ezen fogalommeghatározások elérhetők a Btk. rendelkezései között. A CFAA esetében látszik, hogy védendő jogi tárgyként elsősorban a védett számítógép áll a középpontban, amelyet alátámaszt az is, hogy a fogalmának tisztázása több évtizedes folyamat eredménye. Ezzel szemben a magyar tényállások fordulatai az információs rendszert, valamint a számítógépes adatot egyaránt védik. Mindkét szabályozás reagál arra, hogy a támadások indítására szolgáló eszközöket, programokat már akár szolgáltatásként is igénybe lehet venni vagy akár megvásárolni az interneten keresztül. Ez a kibertámadások végrehajtását rendkívül megkönnyíti, hiszen könnyen hozzá lehet jutni a bűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár a már kész botnet infrastruktúrához, és ezért is fontos, hogy már az előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra.

A második kutatási kérdésemben arra kerestem a választ, hogy képes-e hazai büntetőjogi szabályozás és jogalkalmazás reagálni, alkalmazkodni a technológiai fejlődés következtében bekövetkezett változásokra az egyes gazdasági bűncselekmények esetén. Ezzel kapcsolatban az alábbi következtetésekre jutatottam:

Az új fizetési eszközök használatának elterjedésével egyidejűleg megjelennek azok a bűnelkövetők, akik vissza kívánnak élni velük, ezzel párhuzamosan pedig új elkövetési módok megjelenésével is számolni kell. Éppen ezért fogadták el a 2019-es irányelvet, amelynek célja a minimumszabályok meghatározása volt az immateriális és materiális, speciális védelemmel ellátott készpénz-helyettesítő eszközök védelme érdekében. A szabályozás újdonsága abban ragadható meg, hogy már a hatálya alá tartoznak a fizetésre használt virtuális fizetőeszközök, vagyis a kriptovaluták, valamint a mobilalkalmazások a hozzátartozó jelszóval együttesen, amennyiben alkalmasak fizetési utalások lebonyolítására. A Btk. hatályba lépése óta megfelel

az irányelvben rögzített bűncselekmények tényállási elemeivel szemben támasztott követelményeknek, ezért ezek módosítására nincs szükség. Mindezek alapján a hazai szabályozási környezet megfelelő, és úgy vélem, hogy elsősorban a jogalkalmazók számára jelent kihívást az új elkövetési módoknak a nyomon követése, továbbá az egyes elkövetési magatartások minősítése okozhat problémát a gyakorlatban. Ezért is törekedtem arra, hogy részletesen ismertessem a bankkártyákkal és különböző banki átutalásokkal kapcsolatos visszaéléseket, amelyek a kiberbűnözés egyik kiemelt részterületeként értékelhetők. A card-present csalás terén az elkövetők az ún. skimminget és újabb technikákat alkalmaznak annak érdekében, hogy a fizikailag hozzáférhető bankkártya adatokat minél könnyebben megszerezzék. Ennél azonban nagyobb számban vannak jelen az internet használatához köthető card-not-present csalások, amelyek során az adathalászok egyre kifinomultabb technikák alkalmazásával szerzik meg a gyanútlan felhasználók adatait. Ezek egyaránt különösen nagy kihívást jelentenek nem csak a nyomozó hatóságok, hanem a pénzintézetek számára is.

A bűnelkövetők gyorsan átveszik és integrálják az új technológiákat a különböző bűncselekmények elkövetésekor és olyan üzleti modelleket alkalmaznak, amelyeknek az alapját egyre inkább az internet használata jelenti. A hagyományos szervezett bűnözői csoportok is felismerték az internet használatában rejlő lehetőségeket. Megfigyelhető az informatikai újítások kihasználása, amely magában foglalja például az illegális online kereskedelmet és a titkosított kommunikációs csatornák használatát.

Megállapítható, hogy az új technológiai vívmányok lényeges és maradandó hatással vannak a bűnözés természetére. Már a hagyományos szervezett bűnözés is kihasználja az internet nyújtotta előnyöket, például az illegális kereskedelmi tevékenységüket a magas fokú anonimitást biztosító Darknet piactereken és fórumokon folytatják (pl. kábítószer-kereskedelem, gyermekpornográfia). Mellettük megjelentek olyan kiberbűnözői csoportok is, amelyek sajátos üzleti modellt alkalmaznak (Criminal-to-Criminal), amelynek keretében az informatikai bűncselekmények elkövetéséhez szükséges eszközöket és szolgáltatásokat nyújtanak. Ezen kívül akár szaktudásukkal segíthetik a bűnszervezeteket egyes súlyos bűncselekmények elkövetésében, valamint az informatikai infrastruktúrájuk fenntartásában. Előbbi esetben éppen ezért, akár a hazai szabályozás szerinti bűnszervezetben elkövetett bűncselekmény jogkövetkezményei miatt is felelősségre lehet vonni az illetőt, míg utóbbi esetben a bűnszervezetben részvétel miatt. 2019-ben a bűnszervezet büntetőjogi fogalma szűkült, mert már további többletkövetelménnyé vált annak bizonyítása is, hogy a csoport hierarchikusan szervezett és konspiratívan működik. A kiberbűnözői csoportok azonban természetüknél fogva nehezen illeszthetők be a szervezett bűnözés hierarchikus, homogén

struktúrájába. Összeségében elmondható, hogy az internet új színtérként szolgál mind a régi szervezett, és mind az új típusú bűnözésnek, illetve mindkettő egymás mellett tud működni anélkül, hogy egymást kizárnák, amely az online tér speciális jellegének köszönhető.

Manapság a pénzmosás különböző – akár már online – pénzügyi műveletek láncolatát foglalja magában, célja a pénz bűnös eredetének elrejtése és tisztára mosása a pénzintézetek hálózatában. A gyakorlatban a saját pénzmosással kapcsolatban, különösen az eredetleplezési célzatra tekintettel merülnek fel kérdések. Az egyes tranzakciók ugyan felvethetik a pénzmosás gyanúját, de a saját pénzmosás deliktumának megállapításához szükséges eredetleplezési célzatot nem lehet kiterjesztően értelmezni. Ennek következtében kiemelten fontos az utócselekmények célzatának a körültekintő vizsgálata, például egy adott pénzösszeg banki továbbutalása az alapbűncselekményből származó haszon realizálását szolgálja-e, vagy magát az alapbűncselekmény leplezését. Az elkövetőnek ez esetben mi a magatartásával célja, hogy a büntetőjogi felelősségre vonást elkerülje, vagy valóban a pénz bűnös eredetét és annak további útját kívánja leplezni. Továbbá vizsgálandó, hogy ezek a műveletek mennyiben alkalmasak a leplezési cél eléréséhez, ugyanis, ha ezek tételesen nyomon követhetőek, illetve átláthatók, akkor alkalmatlanok a jogtárgysértésre, ezért nem jön létre bűncselekmény. A Kúria döntésében elvi éllel mondta ki, hogy egy adott elkövetési magatartás (vagy magatartássorozat) egyidejűleg az alapbűncselekmény és a pénzmosás tényállását nem merítheti ki. Ez azért is kizárt, mert a kétszeres értékelés tilalmába ütközne, ennek ellenére az ügyészségnél megfigyelhető egy a halmazatot bővítő gyakorlat. Ezen kívül a legnagyobb kihívást a pénzmosás terén a pénzfutárok (money mule) alkalmazása jelenti. Egyre gyakrabban az interneten keresztül jogszerű tevékenység látszatát keltve toboroznak, szerveznek be embereket, hogy a bűncselekményekből származó pénzek továbbutalását vagy felvételét végezzék. A különböző bankszámlákra felaprózott kisebb pénzösszegek nem feltűnők, így a pénzmosás ellenőrzéseken sem akadnak fent, ezért igencsak nehéz a felderítésük. A pénzfutárok tudattartamának a vizsgálata kiemelten fontos, mert ez lesz az elkövetési magatartásuk minősítésének az alapja.

Napjainkban már a kriptovalutákkal összefüggésben elkövetett bűncselekmények is egyre nagyobb számban fordulnak elő (pl. csalás, informatikai bűncselekmények, zsarolás, illegális ügyletek során fizetőeszközként jelenik meg), amelyek esetében nem is a bűncselekmény helyes minősítése okozhat problémát a gyakorlatban, hanem az, hogy az elkövetés tárgyát hogyan sorolhatjuk be jogi szempontból, és annak értékét hogyan határozzuk meg. A felderítésük nehézsége pedig a technológiai korlátokból adódik, abból, hogy decentralizált rendszerrel rendelkeznek. Az Unióban felismerték, hogy a kriptovaluták használata és a különböző átváltó, valamint pénztárcaszolgáltatók szolgáltatásainak az igénybevétele

pénzmosási és terrorizmus finanszírozási kockázatot hordoz magában. Ezért az ötödik pénzmosás elleni irányelvnek a hatályát már e szolgáltatókra is kiterjesztették, és nekik is meg kell felelni a szigorúbb pénzmosás elleni, avagy „ismerd meg az ügyfeled" szabályoknak. Azonban a kriptovaluták egymás közötti átváltását biztosító szolgáltatókra, valamint a kriptotőzsdékre és a kereskedési platformokra nem alkalmazható az új szabályozás. Továbbá az ilyen szolgáltatások igénybevétele nélkül is van lehetőség a kriptovalutákkal kapcsolatos műveletek végzésére. Újdonságként említhető, hogy az irányelv először határozta meg a virtuális fizetőeszközök fogalmát. A hazai szabályozás vizsgálata során megállapítható, hogy különösen a pénzmosás hazai tényállása világít rá arra, hogy jelenleg e deliktum elkövetési tárgyának, a bűncselekményből származó „dolognak" a fogalmát ki kellene terjeszteni a kriptovalutákra is egy értelmező rendelkezés keretében. Továbbá a jognak nem csak a kriptovalutát, hanem a vele kapcsolatba hozható tevékenységi kört is szabályoznia kell, például az átváltó-, befektetési és pénztárcaszolgáltatókét a pénzügyi vagy kiegészítő pénzügyi szolgáltatások keretében, amelyhez a háttérjogszabály módosítása szükséges, tehát ez elsődlegesen nem a büntetőjog feladata.

A harmadik kérdésem arra vonatkozott, hogy alkalmasak-e az uniós és a hazai törekvések a büntetőeljárás során felmerülő technológiai kihívásokkal kapcsolatos aktuális szabályozási kérdések megoldására, különös tekintettel az elektronikus bizonyítékokra. Ezzel kapcsolatban az alábbi megállapításokat tettem:

Az elektronikus bizonyítékok szerepe egyre inkább felértékelődött a büntetőeljárásban. Ennek megfelelően a Be. is már a kor kívánalmainak megfelelő rendelkezéseket tartalmaz, így a korábbi szabályozáshoz képest előre lépés, hogy külön nevesíti a bizonyítási eszközök között az elektronikus adatot, valamint részletesen szabályozza a rá épülő kényszerintézkedéseket. Azonban a lefoglalás módszertani kérdéseivel nem foglalkozik, annak ellenére, hogy komoly jelentősége van, ezért ennek menetére vonatkozóan hiányzik még egy világos, a gyakorlatban alkalmazható útmutatás. Az új szabályozás előremutató, mert már olyan kérdésekkel is foglalkozik, mint a virtuális vagyontárgyak lefoglalása (pl. a fizetésre használt kriptovaluták). Ugyanakkor ezek még nem nyújtanak megoldást a felmerülő problémákra, mert a hatóságokat több tényező is hátráltathatja a nyomozás során, például az az informatikai eszközöknél használt titkosítást biztosító technológiai védelem (pl. privát kulcs ismeretének hiánya, jelszóval vagy biometrikus azonosítóval védett eszközök és az önvádra kötelezés tilalmának az esete). Emellett amiatt, hogy a jogosult soha nincs fizikai birtokában a kriptovalutáknak, még ha a lefoglalás önmagában sikeres is, akkor sem feltétlenül elégséges, mert rövid időn belül

ezek továbbbutalhatóak, amennyiben a terhelt rendelkezik a pénztárca fájlról biztonsági másolattal. Éppen ezért ennek biztosítására kikényszerített tranzakció alkalmazására lenne szükség.

A bűnügyi nyomozások során további nehézséget okoz, hogy az elektronikus bizonyítékok gyakran más országokban találhatók, ezért ezek beszerzéséhez igazságügyi együttműködésre és kölcsönös jogsegélyre van szükség. Ezen eljárások azonban rendkívül lassúak, éppen ezért ezt a régóta fennálló problémát egy új rendelet elfogadásával kívánnák orvosolni uniós szinten, amely az elektronikus bizonyítékok határon átnyúló megszerzésének gyorsítását és hatékonyabbá tételét szolgálná. Ehhez két új eszközt szeretnének bevezetni: a közlésre kötelező és a megőrzésre kötelező európai határozatot, amelyek segítségével a hatóságok közvetlenül a szolgáltatókat tudják megkeresni és kötelezni az elektronikus bizonyítékok átadására vagy megőrzésére. A rendelet részben a Budapesti Egyezmény által is meghatározott adatkategóriákat szabályozza (előfizetői, hozzáférési, tranzakciós és tartalmi), amelyek eltérő szenzitivitásúak, ezért az egyes adattípusoknál az igazságügyi hatóságoknak a beavatkozási lehetősége is differenciáltan jelenik meg. Továbbá a jelenlegi szabályozási környezet nem tud mit kezdeni a felhőszolgáltatókkal, ugyanis sok esetben nem tudják megállapítani, hogy a szolgáltató által tárolt adat egyáltalán hol található az adott pillanatban, így azt sem, hogy melyik állam jogosult eljárni. Azonban az új rendelet részben ezt a kérdéskört is orvosolná azzal, hogy közvetlenül meg lehet a szolgáltatókat keresni, egy másik állam közreműködése nélkül.

Mindezzel szoros összefüggésben jelentős eljárásjogi problémaként merül fel a joghatóság kérdése, amely a kiberbűnözés sajátosságában, a határon átnyúló vagy transznacionális jellegében keresendő. Ez azt jelenti, hogy gyakran az elkövető és a sértett különböző országokban tartózkodik, valamint harmadik országban található információs rendszer közbeiktatásával követik el a bűncselekményt. A bűnelkövetők által használt anonimitást biztosító technológiák a helyzetet bonyolítják, mert könnyedén eltudják rejteni és személyazonosságukat, így földrajzilag azonosíthatatlannak mutatkozhatnak. Az államok a joghatóságuk meghatározásakor elsősorban a hagyományos területi elvet követik, azonban a felvázolt esetek is rávilágítanak arra, hogy ez nem alkalmazható kielégítően a kiberbűncselekmények esetében, ezért e téren mindenképpen paradigmaváltásra van szükség. Amennyiben a joghatóság megállapítása megtörténik, és az eljárás sikeresen zárul, akkor a kiadatás még mindig további problémát jelenthet.

Vitathatatlan tény, hogy a kiberbűnözés negatív hatást gyakorol a társadalomra. Fontos belátni, hogy ez egy olyan komplex problémakör, amellyel szemben egy többlépcsős

stratégiának az alkalmazása indokolt. A büntetőjog csak ultima ratio megoldás lehet, a hatékony fellépéshez ezen kívüli eszközökre is szükség van. Például uniós szinten két fontos jogi eszköz áll még rendelkezésre: a GDPR az adatvédelmi incidensek haladéktalan jelentésére kötelezi a vállalkozásokat az egész EU területén, amennyiben ezt elmulasztják, akkor súlyos bírságokkal sújthatják őket. A NIS irányelv pedig az alapvető szolgáltatásokat nyújtó szereplőknek állapít meg kötelezettségeket az információ- és hálózatbiztonság fenntartása érdekében, valamint e szolgáltatóknak a kiberbiztonsági eseményekről a nemzeti hatóságokat is értesíteniük kell.

A fokozott nemzetközi együttműködés és kapcsolattartás elősegítése is lényeges elem, különösen a magánszektor és a bűnüldöző hatóságok, illetve az egyes nyomozó hatóságok között, mivel az eddigi tapasztalat is azt mutatja, hogy a sikeres felderítéshez és a hatékony nyomozás lefolytatásához mindez nélkülözhetetlen.

Továbbá kiemelt jelentősége van a prevenciónak, különösen a felhasználókhoz igazított oktatásnak, ismeretterjesztésnek, mert sokszor az informatikai bűncselekmények elkerülhetők lennének, ha körültekintőbben járnának el, és ezáltal kiküszöbölhető lenne a sértetti közrehatás, amely jelentősen megkönnyíti az elkövetők helyzetét. Elsődlegesen nem a felelősség keresése a cél, hanem a károk, negatív következmények lehetőség szerinti elkerülése vagy legalább azok mérséklése. Ez pedig nem a büntetőjog feladata.[568]

De lege ferenda javaslatok

Az információs rendszerben végzett műveletekkel jelentős kárt tudnak okozni, ezért indokoltnak tartom az információs rendszer vagy adatmegsértés tényállásának egy külön fordulatban történő szabályozását. A károkozást a jogalkotó az információs rendszer felhasználásával elkövetett csalásnál értékeli csak, azonban e bűncselekménynél a jogtalan haszonszerzés célzat megléte is szükséges a tényállásszerűséghez. Ezzel szoros összefüggésben véleményem szerint a jelenlegi szabályozási rendszerben a büntetőjog kár fogalma helyett a vagyoni hátrány alkalmazása megfelelőbb lenne mindkét bűncselekmény esetén, mivel utóbbi a vagyonban bekövetkezett értékcsökkenésen kívül magában foglalja az elmaradt vagyoni előnyt is. Azonban ez sem jelent teljes megoldást, mivel az elkövetési magatartással összefüggésben a kár sokszor ténylegesen nem következik be, de felmerülhetnek az információs rendszert ért támadást követően a helyreállítással kapcsolatos kiadások, költségek. Javaslom ezért a kár vagy vagyoni hátrány büntetőjogi fogalmának a kiterjesztését egy értelmező

[568] KORINEK (2013): i.m. 51. o.

rendelkezéssel, amely magában foglalná a vagyoni hátrányok kiküszöböléséhez szükséges költségeket is.

A Btk. közérdekű üzem és a 2013-as irányelv szerint alkalmazott kritikus infrastruktúra fogalma nem fedi egymást, így a cselekmény minősítése vitatott lehet, különösen a szociális jólét, a közegészség intézményei ellen intézett támadások esetében, ezért a meghatározások közelítését javaslom.

Amennyiben az adott bűncselekmény elkövetésekor az információs rendszer mint elkövetési eszköz kerül alkalmazásra, akkor ez jelentős mértékben növeli az ilyen jellegű cselekmények veszélyességét a társadalomra nézve. Ezért javaslom, hogy a jogalkotó ezt az egyes bűncselekmények tényállásában minősített esetként szabályozza, például az általam vizsgált csalás és zsarolás tényállásainál.

Javaslatok a jogalkalmazó számára

Fontos, hogy a jogalkalmazók (bíróság, ügyészség, nyomozó hatóság) számára is biztosítva legyen a modern technológiákkal összefüggő jogi kihívásokat érintő, speciális oktatás, amely során megismerik a legújabb informatikai trendeket, elkövetési módokat és naprakész tudásra, ismeretekre tehetnek szert. Örvendetes, hogy erre vonatkozóan már megfigyelhetők európai és hazai törekvések is, például az Európai Jogi Akadémia (Academy of European Law) rendszeresen szervez képzéseket, szemináriumokat kifejezetten az igazságügyi szervek dolgozóinak. Magyarországon az Országos Bírósági Hivatal a kiberbűnözéssel kapcsolatos bírósági hálózat felállításáról döntött, valamint az ügyészség is létrehozta a Számítógépes Bűnözéssel Foglalkozó Országos Ügyészségi Hálózatot. Erre vonatkozó képzések jelentek már meg mind a bíróság, mind az ügyészség rendszerén belül.[569] Továbbá javaslom, hogy a jövő jogalkalmazói, a joghallgatók is már megismerjék és foglalkozzanak az új technológiák jogi vetületeivel az egyetemi oktatás keretében. Éppen ezért fontosnak tartom, hogy az e témakörbe tartozó kutatási eredmények szervesen beépüljenek az oktatásba is.

[569] Lásd BUONO, Laviero: Updating and diversifying the training offer for EU legal practitioners to meet the challenges posed by the new technologies. ERA Forum 2017. 1-6. o.; LAJTÁR: i.m. 51. o. https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja

FELHASZNÁLT IRODALOM

2/217. (VII. 31.) LÜ h. körlevele a pénzmosás miatti bűnügyekben követendő ügyészi gyakorlat eljárásjogi szempontjairól.

ABADINSKY, Howard: Organized crime. Ninth Edition, Wadsworth Cengage Learning, 2010.

AKÁCZ József: XXXV. A vagyon elleni erőszakos bűncselekmények. In: Kónya István (szerk): Magyar büntetőjog I-III. – Kommentár a gyakorlat számára. 3. kiadás HVG-ORAC Lap- és Könyvkiadó. Budapest, 2017.

AMBRUS István – DEÁK Zoltán: Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből. Belügyi Szemle 2011/2.

AMBRUS István – FARKAS Ádám: Whistleblowing és büntetőjog – szempontok a vállalati visszaélések megítéléséhez. Magyar Jog 2017/7-8.

AMBRUS István: Az autonóm járművek és a büntetőjogi felelősségre vonás akadályai. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019.

AMBRUS István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014.

András – MEZEI Kitti: A zsarolóvírus és botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Szent Lászlótól a modernkori magyar rendészettudományig. Pécs, 2017.

APPAZOV, Artur: Legal aspects of cybersecurity. University of Copenhagen, Faculty of Law, 2014. 21–22. http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf [2017.10.21.]

Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. 2013. https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

ÁRVAY Viktor: Az adatkezelő és adatfeldolgozó kötelezettségei. In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): Magyarázat a GDPR-ról. Wolters Kluwer Hungary Kft., 2018.

ATTORNEY'S GENERAL'S DEPARTMENT (Australia): National plan to compay cybercrime. 2013.

Az adatvédelmi biztos beszámolója, 2009. Forrás: hwww.naih.hu/files/Adatvedelmi-biztos-beszamoloja-2009.PDF

BELEGI József: A közbiztonság elleni bűncselekmények – Btk. XXX. fejezet. In: Kónya István (szerk.): Magyar büntetőjog I-III. – új Btk. – Kommentár a gyakorlat számára. 5. kiadás, HVG Orac Lapkiadó Kft. 2016.

BELOVICS Ervin – GELLÉR Balázs – NAGY Ferenc – TÓTH Mihály: Büntetőjog – Általános rész. HVG-Orac Lap- és Könyvkiadó Kft. Budapest, 2015.

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. HVG-Orac Lap- és Könyvkiadó Kft. Budapest, 2018.

BÉRCES Viktor: A magántitok büntetőjogi védelmének értelmezési sémái. Jogtudományi Közlöny 2017/9.

BERKI Gábor: Kiberháborúk, kiberkonfliktusok. In: Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – Pintér István: Műhelytanulmányok – A virtuális tér geopolitikája. Geopolitikai Tanács Közhasznú Alapítvány. Budapest, 2016.

BLEMUS, Stéphane: Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide. Corporate Finance and Capital Markets Law Review 2017/4.

BLUTMANN László - KARSAI Krisztina - KATONA Tibor: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? Bűnügyi Szemle, 2008/1.

BRENNER, Susan W. – KOOPS, Bert-Jaap: Approaches to Cybercrime Jurisdiction. J. High Tech. L. 1. 2004.

BRENNER, Susan W.: Cybercrime and the law: Challenges, issues and outcomes. Northeastern University Press, 2012.

BRENNER, Susan W.: Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law. 2001.

BRENNER, Susan W.: Cybercrime, Cyberterrorism and Cyberwarfare. Relations internationales 77(3).

BRENNER, W. Susan: Cybercrime – Criminal Threaths From Cyberspace. Praeger, 2010.

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

BRUCE, Ingvild: Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure. Digital Evidence and Electronic Sigranute Law Review 2017/14.

BUJTÁR Zsolt: A kriptovaluták európai és máltai szabályozásának az összehasonlítása - A máltai sólyom szárnyalása. Európai Jog 2018/5.

BUONO, Laviero: The genesis of the European Union's new proposed legal instrument(s) on e-evidence – Towards the EU Production and Preservation Orders. Era Forum, 2018 September

BUONO, Laviero: Updating and diversifying the training offer for EU legal practitioners to meet the challenges posed by the new technologies. ERA Forum 2017.

CASEY, Eoghan: Digital Evidence and Computer Crime. Elsevier. Amsterdam, 2012.

CHEN, Thomas M. – JARVIS, Lee - MACDONALD, Stuart: Cyberterrorism – Understanding, Assessment, and Response, Springer, New York, 2014.

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION: The National Information Infrastructure Protection Act of 1996.

COUNCIL OF EUROPE: Explanatory Report to the Convention on Cybercrime. European Treaty Series – No. 185. 2001.

CYBERCRIME CONVENTION COMMITTEE: Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments. 2018.

CZINE Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018. HVG-ORAC Jogkódex

CSÁK Zsolt: A drónok kapcsán felmerülő egyes büntető és eljárási jogi kérdések. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019.

CSÁK Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018.

DASKAL, Jennifer: Microsoft Ireland, The CLOUD Act, and International Lawmaking 2.0. Stanford Law Review Online, 9. 2018 May.

DASKAL, Jennifer: Unpacking the CLOUD Act. eucrim 4/2018.

DEÁK Zoltán: A kár büntetőjogi fogalmáról - megjegyzések egy eseti döntés margójára. Magyar Jog 2012/6.

DETREKŐI Zsuzsa: Blokkolás Magyarországon - hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig. Infokommunikáció és jog 2014/4.

DORNFELD László – MEZEI Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog, 2017/1.

DORNFELD László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2.

DORNFELD László: Az elektronikus bizonyítékszerzés egyes kérdései. Kriminológiai Közlemények 77. 2017.

DORNFELD László: Kiberterrorizmus – A jövő terrorizmusa? In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019.

ELEK Balázs: A jogirodalom által közvetített jogtudomány és a büntető ítélkezés. In: Bódig Mátyás – Ződi Zsolt (szerk.): A jogtudomány helye, szerepe és haszna. Tudománymódszertani és tudományelméleti írások. Budapest, MTA TK JTI – Opten Informatikai Kft., 2016.

ELEK Balázs: Informatikus szakértés a büntetőeljárásban. Belügyi Szemle 2014/7–8.

ESZTERI Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécs, 2015.

ESZTERI Dániel: Bitcoin - Az anarchisták pénze vagy a jövő fizetőeszköze? Infokommunikáció és Jog 2012/2.

ESZTERI Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és jog 2017/1.

EUROPEAN CENTRAL BANK: Virtual Currency Schemes. Frankfurt, 2012.

EUROPEAN PARLIAMENT'S POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS: Cybersecurity in the European Union and Beyond: Exploring the Threaths and Policy Responses. 2015. https://www.interpol.int/Crimes/Cybercrime [2019.04.30.]

EUROPEAN PARLIAMENT'S POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS: Cybersecurity in the European Union and Beyond: Exploring the Threaths and

Policy Responses. 2015. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf

EUROPOL: European Union Serious and Organised Crime Threat Assessment (SOCTA) – Crime in the age of technology. 2017. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

EUROPOL: European Union Terrorism Situation and Trend Report 2018.

EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2018. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

EUROPOL: The Internet Organised Crime Assessment (IOCTA) 2016. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

Europol: The Internet Organised Crime Assessment (IOCTA). 2014. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014

FENYVESI Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8.

FENYVESI Csaba: Kriminalisztikai világtendenciák – Különös tekintettel a digitális felderítésre. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. MTA Társadalomtudományi Kutatóközpont - PTE ÁJK. Budapest-Pécs, 2019.

FINANCIAL ACTION TASK FORCE: Virtual Currencies - Key definitions and Potential AML/CFT Risks. 2014. 4. o; Bővebben még: HOUBEN, Robby - SNYERS, Alexander: Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Union, 2018.

FINKEY Ferenc: A szándék fogalma és ismérvei a büntetőjogban, különös tekintettel „a szándék hiánya miatt" történő felmentésre. Pesti Lloyd-Társulat Nyomdája. Budapest, 1899.

FÖLDVÁRI József: Büntetőjog – Általános rész. Budapest, Osiris Kiadó, 2001.

FRANSSEN, Vanessa: The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level? European Data Protection Law Review 3, 2017.

FRANSSEN, Vanessa: The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement? European Law Blog October 2018, https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/ [2019.01.22.]

FURNEAUX, Nick: Investigating cryptocurrencies – Understanding, extracting and analyzing blockchain evidence. Wiley, 2018.

FURNELL, Steven: Hackers, viruses and malicious software. In: Jewkes, Yvonne – Yar, Majid: Handbook of Internet Crime. Willan Publishing, 2010.

GAIDERNÉ HARTMANN Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele - egy új intézmény első évei. Magyar Jog 2015/2.

GÁL Andor: Az előkészületi cselekmények büntetendő nyilvánításának egyes típusairól. Magyar Rendészet 2018/3.

GÁL István László: A pénzmosás. Complex Kiadó, Budapest, 2004.

GÁL István László: Új magyar büntetőjog a XXI. században: szemelvények az új Btk. Különös részének újdonságaiból. Jogtudományi Közlöny 2015/7-8.

GELLÉR Balázs - AMBRUS István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017.

GELLÉR Balázs: Gondolatok a kettős értékelés tilalmáról és a látszólagos alaki halmazat feloldására szolgáló elvekről. In: GÁL István László (szerk.): Tanulmányok Tóth Mihály professzor 60. születésnapja tiszteletére. PTE ÁJK. Pécs, 2011.

GHAPPOUR, Ahmed: Searching Places Unknows: Law Enforcement Jurisdiction on the Dark Web. Stanford Law Review Stanford Law Review Volume 69. April 2017.

GILLESPIE, A. Alisdair: Cybercrime – Key Issues and Debates. Routledge, 2016.

GIRASA, Rosario: Regulation of Cryptocurrencies and Blockchain Technology: National and International Perspectives. Palgrave Macmillan, 2018.

GRABOSKY, Peter: Cybercrime. Oxford University Press, 2016.

GYÁNYI Sándor: A botnetek, a túlterheléses támadások eszközei. Magyar Rendészet, 2013. Különszám

GYÁNYI Sándor: Az információs terrorizmus által alkalmazott támadási módszerek és a velük szemben alkalmazható védelem. PhD értekezés tervezet. Budapest, 2011.

GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN kód megadása vagy biztonságosan az Internet? Pécsi Határőr Tudományos Közlemények XIII.

GYÖRFI András: Az ICO – Így indul útjára egy kriptopénz. In: Györgyi András – Léderer András – Paluska Ferenc – Pataki Gábor – Trinh Anh Tuan: Kriptopénz ABC. HVG Könyvek, Budapest, 2019.

HALÁSZ Viktor: A Bitcoin működése és lefoglalása a büntetőeljárásban. Belügyi Szemle, 2017/7-8.

HEGEDŰS István – JUHÁSZ Zsuzsanna – KARSAI Krisztina – KATONA Tibor – MEZŐLAKI Erik – SZOMORA Zsolt – TÖRŐ Sándor: Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez, Wolters Kluwer Jogtár Kommentár

HOLLÁN Miklós: A nemzeti büntetőjog kerettényállásai és az uniós jog. Miskolci Jogi Szemle 2018/2.

HOLLÁN Miklós: A szolgáltatások megfizetés szándéka nélküli igénybevétele és a büntetőjog – Dogmatikai és jogpolitikai vizsgálódás egy empirikus kutatás hajnalán. Magyar Jog 2019/4.

HOLT, Bossler – BOSSLER, Adam M. – SEIGFRIED-SPELLAR, Kathryn C.: Cybercrime and digital forensics: An introduction. Routledge, 2018.

HORVÁTH Tibor – KERESZTI Béla – MARÁZ Vilmosné – NAGY Ferenc - VIDA Mihály: A magyar büntetőjog különös része. Korona Kiadó. Budapest, 1999.

Internet Security Threat Report. 2015/20.

JACSÓ Judit – UDVARHELYI Bence: A Bizottság új irányelvjavaslata a pénzmosás elleni büntetőjogi fellépésről az egyes tagállami szabályozás tükrében. Miskolci Jogi Szemle 2017/2.

JACSÓ Judit: Pénzmosás. In: Görgényi Ilona – Gula József – Horváth Tibor – Jacsó Judit – Lévay Miklós – Sántha Ferenc – Váradi Erika: Magyar Büntetőjog - Különös Rész. Wolters Kluwer Complex Kiadó, Budapest, 2013.

JEWKEY, Yvonne – YAR, Majid (eds.): Handbook of Internet Crime. Willan Publishing, 2010.

JOUGLEUX, Philippe – SYNODINOU, Tatiana-Eleni – MITROU, Lilia: Chapter 2: Criminalization of Attacks against Information Systems. In: Iglezakis, Ioannis (ed.): The Legal Regulation of Cyber Attacks. Wolters Kluwer, 2019.

KÁRMÁN Gabriella – MÉSZÁROS Ádám – TILKI Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3.

KARSAI Krisztina: Az alapelvek rendszere az európi büntetőjogban. MTA doktori értekezés. Szeged, 2015.

KARSAI Krisztina: XLIII. fejezet Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz. Complex Kiadó. Budapest, 2013.

KASPERSEN, Henrik W.K.: Implementation of Recommendation No. R (89) 9 on Computer-related Crime. Strasbourg, March 1997, Doc. CDPC (97) 5 and PC-CY (97) 5.

KELES, Marie-Helen: Computer Forensics: Cybercriminals, Laws and Evidence. Second Edition, Jones & Bartlett Learning, 2015.

KEMENES István: A kárfogalom a polgári jogi és a büntetőjogi kapcsolódási pontjai. Magyar Jog 2018/9.

KERR Orin S.: Computer Crime Law. Fourth Edition. West Academic Punlishing 2018.

KERR, Orin – MURPHY, Sean D.: Government Hacking to Ligh The Dark Web: What Risks to International Relations and International Law? Stanford Law Review Volume 70. July 2017.

KERR, Orin S.: Computer Crime Law. Fourth Edition. West Academic Publishing 2018.

KERR, Orin S.: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes. 78 N.Y.U. L. Rev. 1596 (2003).

KERR, Orin S.: Norms of computer trespass. Columbia Law Review Volume 116. 2016.

KERR, Orin: Vagueness Challenges to the Computer Fraud and Abuse Act. Minnesota Law Review 2010.

KIM-WANG, Raymond – Choo-GRABOSKY, Peter: Cybercrime. In: Paoli, Letizia: The Oxford Handbook of Organized Crime. Oxford University Press, 2014.

KISS Attila: A privátszférát erősítő technológiák. Infokommunikáció és Jog 2013/3.

KLEIJSSEN, Jan – PERRI, Pierluigi: Cybercrime, Evidence and Territoriality: Issues and Options. In: Kuijer M. – Werned, W. (eds.): Netherlands Yearbook of International Law 2016.

KONDOROSI András: Az információs rendszer felhasználásával elkövetett csalás. Infokommunikáció és jog 2014/2.

KOOPS, Bert-Jaap – KOSTA, Eleni: Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark". Computer Law & Security Review 2018/4.

KOOPS, Bert-Jaap – LEENES, Ronald – MEINTS, Martin – VAN DER MEULEN, Nicole – JAQUET-CHIFFELLE, David-Olivier: A typology of identity-related crime. Conceptual, technical and legal issues. Information, Communication & Society Volume 12. No. 1. February 2009.

KOOPS, Bert-Jaap – LEENES, Ronald: ID Theft, ID Fraud and/or ID-related Crime. Definitions matter. Datenschutz und Datensickerheit 2006 (9).

KOOPS, Bert-Jaap: The Internet and its Opportunities for Cybercrime. Tilburg School Legal Studies Paper Series No. 2011/9.

KORINEK László: A szervezett bűnözés lényegi elemei. In: Harmadik Magyar Jogászgyűlés – Magyar Jogász Egylet. Budapest, 1996.

KORINEK László: A technika fejlődése és a bűnözés. In: Borbíró Andrea - Inzelt Éva - Kerezsi Klára - Lévay Miklós - Podoletz Léna (szerk.): A büntető hatalom korlátainak megtartása: A büntetés mint végső eszköz - Tanulmányok Gönczöl Katalin tiszteletére. ELTE Eötvös Kiadó. Budapest, 2014.

KORINEK László: Tendenciák korunk bűnözésében, bűnüldözésében. MTA székfoglaló előadás, 2013.

KOVÁCS László – KRASZNAY Csaba: „Mert az övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-s amerikai elnökválasztás során. Nemzet és Biztonság 2017/3.

KOVÁCS László: A kibertér védelme. Dialog Campus Kiadó. Budapest, 2018.

KOVÁCS Mihály: A számítástechnikai rendszer és adatok elleni bűncselekmények a városi ügyészség gyakorlatában. Ügyészek Lapja 2011/5.

KŐLVART, Merit - POOLA, Margus - RULL, Addi: Smart Contracts. In: Kerikmäe, Tanel - Rull, Addi (eds.): The Future of Law and eTechnologies. Springer, 2016. 133-145. o.; valamint MIK, Eliza: Smart contracts: terminology, technical limitations and real world complexity. Law, Innovation and Technology 2017/2.

LACZI Beáta: A számítógép és a büntetőjog. Magyar Jog 2001/3.

LACZI Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. Magyar Jog 2001/12.

LAJTÁR István: A kiberbűnözésről. Ügyészek Lapja 2019/1.

LESLIE, Daniel Adeoyé: Legal Principles for Combatting Cyberlaundering. Law, Governance and Technology Seriec Volume 19. Springer 2014.

MAILLART, Jean-Baptiste: The limits of subjective territorial jurisdiction in the context of cybercrime. ERA Forum 2018 September.

MALAS, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017.

MÁTÉ István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. Doktori értekezés. Pécs, 2017.

MATUS Márk: Kutatás, lefoglalás, bűnjelkezelés számítástechnikai környezetben. In. Bócz Endre (szerk.): Kriminalisztika. BM Duna Palota és Kiadó Budapest, 2004.

MCAFEE: Economics Impact of Cybercrime – No Slowing Down Report February 2018.

MCGUIRE, Michael: Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security. 2012.

MCGUIRE, Mike – DOWLING, Samantha: Cyber crime: A review of evidence, Summary, 2013.

MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós - Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017.

MEZEI Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jogászegyleti Értekezések 9-10. Budapest, 2018.

MEZEI Kitti: A Kúria harmadfokú végzése a jogtalan elsajátításról és a pénzmosásról. Jogesetek Magyarázata 2018/3-4.

MEZEI Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. Jura 2018/1.

MISKOLCZI Barna – SZATHMÁRY Zoltán: Büntetőjogi kérdések az információk korában. HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2019.

MOHÁCSI Barbara: Bűnüldözési érdek contra emberi jogok - az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. Magyar Jog 2008/12.

MOLNÁR Gábor Miklós: XL. fejezet – A pénzmosás. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (szerk.): Büntetőjog II. – Különös Rész. HVG-Orac Lap- és Könyvkiadó Kft. Budapest, 2018.

MOLNÁR Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Kónya Sándor (szerk.): Magyar Büntetőjog - Kommentár a gyakorlat számára (Harmadik kiadás). HVG-ORAC Budapest, 2016.

MOLNÁR Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Kónya Sándor (szerk.): Magyar Büntetőjog - Kommentár a gyakorlat számára (Harmadik kiadás). HVG-ORAC Budapest, 2018.

MUHA Lajos: a Magyar Köztársaság kritikus információs infrastruktúrájának védelme. PhD értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest, 2007.

NAGY Tamás: Business E-mail Compromise, avagy az átutalásokhoz kapcsolódó csalások. Belügyi Szemle 2018/7-8.

NAGY Zoltán András – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog 2017/1.

NAGY Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról.
http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf

NAGY Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: Homoki-Nagy Mária - Karsai Krisztina - Fantoly Zsanett - Juhász Zsuzsanna - Szomora Zsolt - Gál Andor (szerk.): Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Szeged, 2018.

NAGY Zoltán András: A jövő tegnap óta tart: A modern technikai-technológiai folyamatok kihívásai a jog területén. Belügyi Szemle 2018/10.

NAGY Zoltán András: A kiberháború új dimenzió – a veszélyeztetett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). Pécsi Határőr Tudományos Közlemények XIII., 2012.

NAGY Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula - Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII. 2012.

NAGY Zoltán András: A sértett szerepe néhány kibertérben elkövetett bűncselekményben – alkalmazott viktimológia. In: Finszter Géza – Kőhalmi László – Végh Zsuzsanna (szerk.): Egy jobb világot hátrahagyni… Tanulmányok Korinek László professzor tiszteletére. PTE ÁJK. Pécs, 2016.

NAGY Zoltán András: A számítógépes környezetben elkövetett bűncselekmények kriminológiai aspektusairól. In: Gál István – Nagy Zoltán András (szerk.): Az informatika és a büntetőjog. Pécs, 2006.

NAGY Zoltán András: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda. Belügyi Szemle 1999/11.

NAGY Zoltán András: Bűncselekmények számítógépes környezetben. Ad librum Kft. Budapest, 2009.

NAGY Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! Magyar Jog 2016/1.

NAGY Zoltán András: XLIII. fejezet tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Tóth Mihály – Nagy Zoltán András (szerk.): Magyar Büntetőjog: Különös rész. Osiris Kiadó, Budapest 2014. TÓTH Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In: Gál István László – Nagy Zoltán András (szerk.): Informatika és büntetőjog. PTE ÁJK. Pécs, 2006.

NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: Éves jelentés – 2017. év

NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: Éves jelentés - 2016. év

NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany

OECD Policy Guidance on Online Identity Theft, 2008.

OERLEMANS, Jan-Jaap: Investigating Cybercrime. Amsterdam University Press. 2017.

OTT István: Dogmatikai kérdések a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye kapcsán. Magyar Jog 2016/12.

PARTI Katalin – KISS Anna: A számítástechnikai bűnözésről akkor és most. In: Bárd Petra – Hack Péter – Holé Katalin: Pusztai László emlékére. OKRI. Budapest, 2014.

PARTI Katalin – KISS Tibor: Az informatikai bűnözés. In: Borbíró Andrea - Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft. 2017.

PARTI Katalin: Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntetőeljárás során a gyakorlat tükrében. Belügyi Szemle 2018/10.

PARTI Katalin: Gondolatok a számítástechnikai adatok és rendszerek elleni bűncselekmények tényállásairól. Büntetőjogi Kodifikáció 2005/2.

PARTI Katalin: Gondolatok a szerver-lefoglalásokról. Infokommunikáció es Jog 2004/3.

PARTI Katalin: "10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és jog 2010/38.

PESZLEG Tibor: Interneten, számítógépen történő nyomrögzítés. Ügyészek Lapja 2005/1.

PESZLEG: Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek lapja, 2010/2.

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. ELTE-ÁJK, Budapest, 2017.

POSKRIAKOV, Fedor - CHIRIAEVA, Maria - CAVIN, Christophe: Cryptocurrency compliane and risks: a European KYC/AMLP perspective. In: Dewey, Josias (ed.): Blockchain & Cryptocurrency Regulation 2019. Global Legal Group, 2019. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/13-cryptocurrency-compliance-and-risks-a-european-kycaml-perspective

PRÉCSÉNYI Zoltán: A számítástechnikai ipar és a kiberbűnözés elleni küzdelem: Lehetőségek és korlátok. Magyar Rendészet 2013. különszám

PUSZTAI László: Számítógép és bűnözés. In: Gödöny József (szerk.): Kriminológiai és Kriminalisztikai Tanulmányok 26. OKRI, Budapest, 1989.

SATOSHI Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. White Paper, 2008.

SCHJOLBERG, Stein: The history of cybercrime 1976-2014. Cybercrime Research Institute, 2014.

SCHJOLBERG, Stein: The history of global harmonization on cybercrime legislation – the road to Geneva. 2008. https://cybercrimelaw.net/documents/cybercrime_history.pdf

SCHMITT, Michael N. – VIHUL L, Liis (eds.): Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

SCHUBAUER László: A pénzmosás elleni küzdelem magyarországi büntetőjogi eszközrendszerének kialakulása, változásai és továbbfejlesztésének lehetőségei. In: Hollán Miklós – Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex. MTA TK JTI – OKRI. Budapest, 2017.

SCIENTIFIC WORKING GROUPS ON DIGITAL EVIDENCE AND IMAGING TECHNOLOGY: Digital & Multimedia Evidence Glossary. 2016.

SIEBER, Ulrich: A számítógépes bűnözés és más bűncselekmények az információtechnológia területén. Magyar Jog 1993/2.

SIEBER, Ulrich: Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study. prepared for the European Commission, 1 January 1998.

SIMON Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK-MTA TK JTI. Budapest-Pécs, 2019.

SINKU Pál: A pénzmosás miatti bűnügyek gyakorlata – Az ügyészi jogalkalmazás tapasztalatai. In: Barabás A. Tünde – Vókó György (szerk.): A bonis bona discere – Ünnepi kötet Belovics Ervin 60. születésnapja alkalmából. Budapest, Xenia OKRI – PPKE ÁJK, 2017.

SIRY, Lawrence: Cloudy days aheas: Cross-border evidence collection and its impact on the rights of EU citizencz. New Journal of European Criminal Law Volume (10)(3). 2019.

SISÁK Attila: A pénzmosás elleni küzdelem tapasztalatai egy nyomozó hatóság gyakorlatában. Kriminológiai Közlemények 72.

SKORVANEK, Ivan – KOOPS, Bert-Jaap – CLAYTON NEWELL, Cryce – ROBERTS, Andrew: „My computer is my castle": New privacy frameworks to regulate police hacking. TILT Law & Technology, Working Paper Series February 2019.

SORBÁN Kinga: A digitális bizonyítékok a büntetőeljárásban. Belügyi Szemle 2016/11.

SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban. Themis 2016/1.

SORBÁN Kinga: Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában – Felelősségek és kötelezettségek. In Medias Res 2019/1.

SORBÁN Kinga: Vírusok és zombik a büntetőjogban - Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. In Medias Res 2018/2.

STEPHENSON, Peter – GILBERt, Keith: Investigating computer-related crime. CRC Press, 2013.

SZABÓ Endre Győző: Az adatvédelmi bírságról – a GDPR szabályainak elemzése. Alkotmánybírósági Szemle 2018/2.

SZABÓ Endre Győző: II. Fejezet: Adatvédelem és technológia. KLEIN Tamás – TÓTH András (szerk.): Technológia jog, robotjog, cyberjog. Wolters Kluwer. Budapest, 2018.

SZABÓ Imre: A pénzmosás a bírói gyakorlat tükrében. Ügyészek Lapja 2017/1.

SZABÓ Imre: A számítástechnikai adat mint elektronikus bizonyíték – A magyar szabályozás elemzése az Európa Tanács számítástechnikai bűnözésről szóló egyezménye alapján. Kriminológiai Tanulmányok 48. Budapest, 2011.

SZABÓ Imre: Az informatikai terrorizmus veszélyei. Belügyi Szemle 2011/2.

SZABÓ Imre: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6.

SZABÓ Imre: Informatikai bűncselekmények. In: Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve. Budapest, Complex, 2008.

SZABÓ Imre: Internetes bűncselekmények, különös tekintettel az internetes csalásra. ELTE ÁJK, 2002.

SZÁDECZKY Tamás – SZŐKE Gergely László – ZÁMBÓ Alexandra Erzsébet: Titkosítás és jog – Gondolatok a titkosításhoz kapcsolódó jogi szabályozásról. Infokommunikációs jog 2017/1.

SZALÁRDI Gábor: A csúcstechnológiai bűnözés elleni küzdelem támogatása. Belügyi Szemle 2012/6.

SZATHMÁRY Zoltán: A számítástechnikai bűncselekmények és rendszertani elhelyezésük. Jogtudományi Közlöny 2012/4.

SZATHMÁRY Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11.

SZATHMÁRY Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. Doktori Értekezés (PTE ÁJK) Budapest, 2012.

SZÉKELY Iván: Privát szférát erősítő technológiák. Információs Társadalom 2008/1.

SZOMORA Zsolt: A jogi tárgy funkciói és a jogtárgyharmonikus értelmezés. Bűnügyi Szemle 2009/2.

SZOMORA Zsolt: Btk. XXI. Fejezet. In: Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz. Complex, Budapest, 2013.

SZOMORA Zsolt: XXXV. A vagyon elleni bűncselekmények. In: Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz. Complex Kiadó. Budapest, 2013.

SZONGOTH Richárd – VETTER Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. Belügyi Szemle, 2018/7-8. 9. o., valamint BUONO, Laviero: Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, Volume 4. No. 3. 2012.

SZŐKE Gergely László: Gondolatok a hazai titokvédelmi szabályozás rendszeréről. Jura 2018/2.

TOSZA, Stanislaw: The European Commision's Proposal on Cross-Border Access to E-evidence. eucrim 4/2018

TÓTH András: Hálózati és információs rendszerek biztonsága európai szabályozásának alapjai. Infokommunikáció és jog 2017/1.

TÓTH Mihály – KŐHALMI László: A szervezett bűnözés. In: Borbíró Andrea - Gönczöl Katalin - Kerezsi Klára - Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016.

TÓTH Mihály: A bűnszervezeti elkövetés szabályozásának kanyargós útja. Magyar Jog 2015/1.

TÓTH Mihály: A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése. MTA Law Working Papers 2015/4.

TÓTH Mihály: A látszólagos anyagi halmazat egyes kérdései – gyakorlatias nézőpontból. In: Koltay András – Molnár Gábor (szerk.): Bonus Iudex: Ünnepi kötet Varga Zoltán 70. születésnapja alkalmából. Budapest, Xenia Kúria – PPKE ÁJK, 2018.

TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.

TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. Budapest: KJK Kerszöv 2002.

TRÓCSÁNYI Sára: Első oldal. Infokommunikáció és jog 2009/6.

TROPINA, Tatiana: Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum 2014.

TROPINA, Tatiana: Public-Private Collaboration: Cybercrime, Cybersecurity and National Security. In: Tropina, Tatiana – Callanan, Cormac (eds.): Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer, 2015.

TROPINA, Tatiana: The evolving structure of online criminality. eucrim 2012/4.

TÜZES Marcell: Bitcoin - A pénz új formája. Infokommunikáció és jog 2012/4.

U.S. DEPARTMENT OF JUSTICE: Computer Crime and Intellectual Property Section Criminal Division: Prosecuting Computer Crimes. 2015.

U.S. Department of Justice: Report of the Attorney General's Cyber Digital Task Force. Washington, 2018. 36. o.

U.S. DEPARTMENT OF JUSTICE: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Law. 2009.; COUNCIL OF EUROPE: Electronic evidence guide—A basic guide for police officers, prosecutors and judges. 2013.; valamint ENISA: Electronic evidence—a basic guide for first responders. 2014.

U.S. DEPARTMENT OF JUSTICE: The National Information Infrastructure Protection Act of 1996, Legislative Analysis. 1996.

UNITED NATIONS OFFICE ON DRUGS AND CRIME: Handbook on Indentity-related crime. Vienna, 2011.

URCUYO, Michael S.: From Internet trolls to seasoned hackers: protecting our financial interests from Distributed-Denial-Of-Service attacks. Rutgers Computer & Technology Law Journal Volume 42. 2016.

VADÁSZ Viktor: A számítógép demisztifikálása. Ügyészek Lapja 2010/2.

VARGA Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In Medias Res 2019/1.

VEREBICS János: Az információs bűncselekmények és az elektronikus adat ideiglenes hozzáférhetetlenné tételének lehetősége az új Btk.-ban. Gazdaság és Jog 2013/2.

WALL, David: Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. International Review of Law, Computers and Technology 2008/1-2.

WANG, Qianyun: A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. Erasmus University of Rotterdam. Rotterdam, 2016.

WANG, Shiuh-Jeng: Measures of retaining digital evidence to prosecute computer-based cyber-crimes. Computer Standars & Interfaces 29. 2007.

ZŐDI Zsolt: Jog és jogtudomány a Big Data korában. Állam- és Jogtudomány 2017/1. 2/217.
(VII. 31.) LÜ h. körlevele a pénzmosás miatti bűnügyekben követendő ügyészi gyakorlat eljárásjogi szempontjairól.

Hivatkozott bírósági döntések jegyzéke

2/2018. büntető jogegységi határozat

4/2005. számú BJE határozat

Balassagyarmati Törvényszék B.210/2014/127.

Bfv.I.830/2017/16.

BH 1989/184.

BH 1999/145.

BH 2000.279.

BH 2004.170.

BH 2006.143

BH 2006.143.

BH 2008.139.

BH 2009.264. I.

BH 2009.264. II.

BH 2009.349.

BH 2010.11.472.

BH 2014.131.

BH 2015.11.296.

BH 2015.244.

BH 2016.9.234.

BH 2016.9.234.

BH 2017.12.392.

BH 2017.177.

BH 2017.8.252.

BH 2018.4.106.

C-264/14. sz. Skatteverket kontra David Hedquist ügy

Debreceni Ítélőtábla Bf.II.390/2013/12.

EBH 2008.1849.

EBH 2009.2033. I.

EBH 2009.2033. II.

Fővárosi Ítélőtábla 5.Bf.38/2010/38.

Fővárosi Törvényszék 12.B.1229/2011.

Fővárosi Törvényszék 2.B.282/2012/21.

Fővárosi Törvényszék B.555/2015/15.

Fővárosi Törvényszék B.687/2012/11.

Heves Megyei Bíróság B.582/2010/199.

Kúria Bfv. I. 1.357/2014/11.

Kúria Bfv. III. 1548/2014/7.

Legfelsőbb Bíróság Bf. II. 74/2008/5.

Legfelsőbb Bíróság Bfv. II. 74/2008/5.

Miskolci Törvényszék 11.B.986/2010/75.

Szegedi Ítélőtábla Bf. I. 180/2006/3.

United States v. Coinbase, Inc. et al., Order Regarding Petition to Enforce IRS Summons at 14 (Doc. 78), Case No. 3:17-cv-01431 (N.D. Cal.).

United States v. Ulbricht, 31 F. Supp. 3d 540, 569-70 (S.D.N.Y. 2014)

Felhasznált internetes források

http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf

https://europa.eu/european-union/about-eu/agencies/enisa_hu

http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32005F0222

http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2013.218.01.0008.01.HUN

http://www.europarl.europa.eu/news/hu/headlines/society/20180418STO02004/facebook-cambridge-analytica-botrany-zuckerberg-valaszoljon-az-europaiaknak

https://www.bbc.com/news/technology-47044652

https://jogaszvilag.hu/napi/bkk-botrany-fellelegezhet-az-etikus-hacker/

http://ugyeszseg.hu/valasz-a-tarsasag-a-szabadsagjogokert-tasz-etikus-hacker-ugyeben-tett-allitasaira/

http://www.cert-hungary.hu/ddos

http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

https://www.bleepingcomputer.com/news/government/new-california-law-makes-ransomware-a-standalone-crime/

https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

http://real-phd.mtak.hu/74/1/1228916.pdf

https://www.symantec.com/content/en/us/enterprise/other_resources/

21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

http://www.kormany.hu/hu/belugyminiszterium/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast

https://www.dailymail.co.uk/news/fb-5472209/How-thieves-steal-car-without-keys-The.html

https://www.selectagents.gov/resources/USApatriotAct.pdf

https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629

http://neih.gov.hu/zsarolo-ddos

http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm

http://europa.eu/rapid/press-release_IP-18-3343_hu.htm

https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018PC0226

https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014

https://www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html

http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2016-evi-sajtokozlemenyek/fokozott-kockazatot-hordoznak-a-vilaghalon-elerheto-virtualis-fizetoeszkozok

https://www.justice.gov/usao-ndtx/pr/cryptocurrency-ceo-indicted-after-defrauding-investors-4-million
https://fintechzone.hu/kriptovalutak-legfrissebb-fejlemenyek/

https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/13-cryptocurrency-compliance-and-risks-a-european-kycaml-perspective

https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2017-evi-sajtokozlemenyek/a-onecoin-elleni-fellepesrol-targyalt-a-piacfelugyeleti-munkacsoport

https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins

https://www.ccn.com/london-police-seize-500000-in-bitcoin-from-cyber-crime-wave-hacker/

http://www.koreatimes.co.kr/www/biz/2018/05/488_249868.html

https://www.ethnews.com/two-more-years-in-prison-for-ex-secret-service-agent-who-stole-government-seized-bitcoin

http://adatvedelmiaudit.hu/2011/06/cookie-k-csak-hozzajarulassal/

https://www.theguardian.com/technology/2014/oct/08/cash-machine-atm-malware-tyupkin

https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

https://qubit.hu/2019/02/04/torvenyt-sertett-az-etikus-hacker-de-ha-nem-jelent-veszelyt-a-tarsadalomra-a-birosagnak-fel-kell-mentenie

http://adatvedelmiaudit.hu/2011/06/cookie-k-csak-hozzajarulassal/

http://europa.eu/rapid/press-release_IP-18-3343_hu.htm

http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm

http://neih.gov.hu/zsarolo-ddos

http://ugyeszseg.hu/a-darknet-hasznalatanak-veszelye-birosag-ele-allitas/

http://ugyeszseg.hu/valasz-a-tarsasag-a-szabadsagjogokert-tasz-etikus-hacker-ugyeben-tett-allitasaira/

http://www.cert-hungary.hu/ddos

http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

http://www.europarl.europa.eu/news/hu/headlines/society/20180418STO02004/facebook-cambridge-analytica-botrany-zuckerberg-valaszoljon-az-europaiaknak [2018.07.21.]

http://www.koreatimes.co.kr/www/biz/2018/05/488_249868.html [2019.01.21.]

http://www.kormany.hu/hu/belugyminiszterium/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast [2017. 09. 09.]

https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja

https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018PC0226

https://fintechzone.hu/kriptovalutak-legfrissebb-fejlemenyek/

https://hpops.tk.mta.hu/blog/2014/05/az-alapjogi-chartaba-utkozik-az-adatmegorzesi-iranyelv

https://jogaszvilag.hu/napi/bkk-botrany-fellelegezhet-az-etikus-hacker/

https://qubit.hu/2019/02/04/torvenyt-sertett-az-etikus-hacker-de-ha-nem-jelent-veszelyt-a-tarsadalomra-a-birosagnak-fel-kell-mentenie

https://www.bbc.com/news/technology-47044652

https://www.bleepingcomputer.com/news/government/new-california-law-makes-ransomware-a-standalone-crime/

https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629

https://www.ccn.com/london-police-seize-500000-in-bitcoin-from-cyber-crime-wave-hacker/

https://www.dailymail.co.uk/news/fb-5472209/How-thieves-steal-car-without-keys-The.html

https://www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html

https://www.ethnews.com/two-more-years-in-prison-for-ex-secret-service-agent-who-stole-government-seized-bitcoin

https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014

https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down
https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

https://www.justice.gov/usao-ndtx/pr/cryptocurrency-ceo-indicted-after-defrauding-investors-4-million

https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-forfeiture-48-million-sale-silk-road-bitcoins

https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2016-evi-sajtokozlemenyek/fokozott-kockazatot-hordoznak-a-vilaghalon-elerheto-virtualis-fizetoeszkozok

https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2017-evi-sajtokozlemenyek/a-onecoin-elleni-fellepesrol-targyalt-a-piacfelugyeleti-munkacsoport

https://www.selectagents.gov/resources/USApatriotAct.pdf

https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

https://www.techopedia.com/definition/2410/hacktivism

https://www.theguardian.com/technology/2014/oct/08/cash-machine-atm-malware-tyupkin