Pécsi Tudományegyetem
Állam- és Jogtudományi Kar Doktori Iskola

Mezei Kitti

Büntetőjogi válaszok az informatikai kihívásokra

Doktori (PhD) értekezés

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

Pécs, 2019

TARTALOMJEGYZÉK

I. BEVEZETŐ GONDOLATOK

1. A témaválasztás indokolása, aktualitása[1]

Nem túlzás azt állítani, hogy az informatika és a technológiai fejlődés mindenkinek az életét érinti, és arra hatást gyakorol. Ez a dinamikus fejlődés a jogrendszert is folyamatos kihívások elé állítja. Éppen ezért az új technikai újítások esetén szükségessé válik, hogy az ezekkel kapcsolatban felmerülő jogi kérdésekre, problémákra reagálni tudjon. Ez különösen fontossá vált azért, mert az egyes társadalmi és gazdasági folyamatok is egyre inkább függnek az információs rendszerektől. Az információs társadalom egyik jellemzőjévé vált az infokommunikációs eszközök számának, sokféleségének és komplexitásának a növekedése. Az innováció egyre inkább az egyes gazdasági ágazatok működését, illetve a gazdasági szereplők versenyképességét határozza meg.

Azonban a gyors ütemű informatikai fejlődésnek az előnyei mellett megvannak a veszélyei is, hiszen a modern technológiák adta lehetőségeket a bűnelkövetők is kihasználják. Ennek köszönhetően jelentek meg nagy számban az informatikával összefüggő bűncselekmények, amelyek körét ma már rendkívül nehéz behatárolni, köszönhetően az új technológiák megjelenésének (pl. Internet of Things[2], mobilinformatikai eszközök), a megvalósítható funkciók bővülésének, illetve a hálózatok használatának az elterjedésének, amelyek magukkal hozzák az újabb elkövetési módokat, illetve büntetendő cselekmények körét (pl. „hacking", számítógépes vírusok, adatlopások).[3] Ma már szinte bármelyik hagyományos bűncselekmény elkövethető az új eszközök segítségével. Mindez a jogalkotást és a jogalkalmazást is kihívások elé állítja különösen a büntetőjogi szabályozásra tekintettel, illetve a minősítés kérdéseiben. A büntető igazságszolgáltatás hatékonyságának növelése napjainkban sürgetően veti fel e téma kutatásának az igényét. Ennek ellenére a hazai szakirodalom keveset foglalkozik a büntetőjog és az informatika összefüggéseivel, ezért a témát érintő tudományos kutatások hiánypótlónak tekinthetők.

---

[1] A doktori értekezés az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV és ÚNKP-17-3-I kódszámú Új Nemzeti Kiválóság Programjának támogatásával 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 bekapcsolható legyen a rendszerbe.

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

Az internetnek számos előnye van, amelyek egyben a használatával összefüggő visszaélések térnyerését, illetve a hatékonyabb bűnelkövetést is lehetővé teszik. Az internetre csatlakozott eszközök és felhasználók száma évről évre növekvő tendenciát mutat, így a kiterjedt online jelenlét az elkövetők számára még inkább lehetővé teszi a tömeges informatikai támadások kivitelezését. Az internet esetén egy egész világra kiterjedő hálózatról van szó, amely azonnali és valós idejű kapcsolatteremtésre ad lehetőséget, és a lényegét az elektronikus formában megjelenő adat adja („Big Data" jelenség)[4]. Az internet speciális, de egymással összefüggő tulajdonságokkal rendelkezik, amelyek megkönnyíthetik az elkövetést azonban már egy új színtéren:

Az internet globális jellege egy határon átívelő bűnözést tesz lehetővé. Az elkövetők a világ bármely pontján kereshetnek célpontokat, illetve sebezhetőségeket, és ehhez még arra sincs szükségük, hogy akár ugyanabban az országban tartózkodjanak a kiválasztott sértettel az elkövetéskor. Ennek köszönhetően a büntető eljárásjogban is összetett joghatósági és illetékességi kérdések megválaszolásra várnak a mai napig.

Az internet a „hálózatok hálózataként" egyben decentralizált és rugalmas hálózatok létrehozására nyújt lehetőséget, amelyek az elkövetők laza szerveződését segítik elő például az elkövetők számára egymás között a feladatoknak, a szakmai tudásuknak, jártasságuknak és a kifejlesztett technikai eszközeiknek a megosztását teszik lehetővé. Az internet egyben egy kommunikációs csatornaként is szolgál, amely a különböző bűncselekmények elkövetésében is fontos szerepet tölthet be.

Ennek köszönhetően napjainkra az informatikai bűnözés egy profit-orientált, szolgáltatás-alapú üzleti modellé nőtte ki magát, amelynek motorját az online feketegazdaság adja (pl. Darknet fórumok), ahol a különböző támadásokat elősegítő eszközök és egyéb illegális szolgáltatások is elérhetőek.

Az internet anonimitást biztosít, amelyet az elkövetők fokozhatnak a különböző titkosítást és magasabb fokú anonimitást biztosító eszközök bűnelkövetési célú felhasználásával (pl. TOR hálózat és a kriptovaluták használata). Azonban azok számára is relatív névtelenséget kínál, akik kevésbé jártasak az informatika világában, mert egy IP cím, e-mail cím, vagy ál-Facebook profil mögé rejtőznek és ezekben az esetekben is még nehéz lehet a konkrét személyek lenyomozása és azonosítása.

[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.

Mindemellett a sértettekkel egy távoli kapcsolatfelvételt garantál, ezáltal megszünteti azokat a szociális akadályokat, amelyekkel az elkövetőknek a valóságban, akár egy személyes találkozáskor kellene szembe nézniük, ezáltal ez is megkönnyíti számukra az elkövetést**.** Az ilyen típusú bűnözésre magas fokú látencia jellemző, mert a gyanútlan felhasználók sokszor nem is észlelik, hogy bűncselekmény sértettjévé váltak vagy egyszerűen a hatóságok felé nem jelentik (pl. bankkártya-visszaélések, pénzintézetek ellen intézett támadások) amely tovább nehezíti a felderítést.

További előnye az internetnek, hogy a segítségével könnyedén lehet végrehajtani adat vagy program manipulációt minimális költség mellett, mert az információk elektronikus megjelenítésnek köszönhetően lehetőség van az adatok másolására minőségi veszteség nélkül, valamint módosítására anélkül, hogy annak sokszor 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 az interneten keresztül és akár több millió rendszert megfertőzni egyidejűleg, vagy például egy botnet hálózat segítségével az elkövetők nagyszabású támadásokat tudnak végrehajtani, amely teljes rendszer leálláshoz vezethet.[5]

2017-ben az informatikai bűnözés által okozott kár 600 milliárd dollár értékben realizálódott a különböző sértetti körnél (pl. vállalatok, pénzintézetek, kormányzati szervek stb.) és a szakértők szerint ez 2021-re meg fog duplázódni, ami úgy gondolom, hogy rávilágít arra, hogy mekkora potenciált rejt magában a technológiák bűnelkövetési célú felhasználása az elkövetői oldalról, míg egyben mekkora kockázatot és veszélyt a sértetti oldalról.[6]

2. Az értekezés tárgya és szerkezete

A büntetőjog és az informatika összefüggéseinek vizsgálata a legtágabb értelemben olyan hatalmas területet ölelne fel, amely túlterjeszkedne egy doktori értekezés keretein, ezért a kutatás tárgykörének meghatározása során fontosnak tartottam, hogy ezt korlátok közé szorítsam. Egyrészt elsősorban a büntető anyagi jogi kérdésekkel foglalkozom, és csak érintőlegesen büntető eljárásjogi kérdésekkel. Másrészt az értekezés kizárólag az informatikai, valamint az információs rendszerek felhasználásával elkövetett gazdasági, anyagi haszonszerzésre irányuló bűncselekményekkel kapcsolatos szabályozási kérdésekre fókuszál.

[5] KOOPS, Bert-Jaap: The Internet and its Opportunities for Cybercrime. Tilburg School Legal Studies Paper Series No. 09/2011. 740-741. o.
[6] https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf [2018.05.23.]

Az értekezés célja a szabályozással kapcsolatos hiányosságokat feltárása és az erre vonatkozó javaslatok kidolgozása.

Az értekezés három nagy szerkezeti részre tagolódik. A bevezetést követő első nagy rész a történeti és fogalmi alapvetés, amely az informatikai bűnözés elleni fellépés nemzetközi dimenzióját vizsgálja, így különös tekintettel az Európai Unió és az Egyesült Államok szabályozási történetére. Emellett a fogalmi kérdések tisztására kerül sor, kiemelten az informatikai bűnözés meghatározására fókuszálva.

Ezt követően az egyes informatikai támadásokkal kapcsolatos büntetőjogi kihívásokat vizsgálom a tekintetben, hogy az Európai Unió, illetve a hazai és az Egyesült Államok szabályozása mennyiben tud ezekre reagálni, így a vonatkozó rendelkezések részletes elemzésére került sor. Ebben a fejezetben a büntető anyagi jogi szabályozás mellett a hazai új büntetőeljárásról szóló törvény elektronikus bizonyítékokkal összefüggő rendelkezéseire és az ezzel kapcsolatos uniós jogalkotási törekvések bemutatása is megvalósult.

Ezután az utolsó rész következik, amelyben az informatika és internet segítségével elkövetett „hagyományos" gazdasági bűncselekmények szabályozási kihívásainak elemzésére kerül sor, így a bankkártyákkal kapcsolatos visszaélésekre, a szervezett bűnözés megjelenésére az interneten és az ezzel összefüggő bűncselekményekre, így külön figyelmet fordítva a pénzmosásra az online térben, valamint a kriptovaluták büntető anyagi és eljárásjogi kihívásaira.

3. A szakirodalom és az alkalmazott módszertan áttekintése

Az alkalmazott kutatási módszerek bemutatása mellet fontos, hogy sor kerüljön a felhasznált szakirodalmi források rövid bemutatására. Az értekezés elkészítése során a témakör szempontjából releváns uniós, hazai és amerikai jogforrások kerültek felhasználására. A joganyag elemzése mellett az egyes részeknél hangsúlyt fektettem a vonatkozó joggyakorlat bemutatására, valamint az adott kérdésköröket tárgyaló, releváns magyar és nemzetközi jogirodalmat dolgoztam fel.

A téma sajátos jellegéből adódóan egy interdiszciplináris módszer alkalmazása vált szükségessé. A kutatás során még a normatív és dogmatikai módszer alkalmazására került sor, valamint a vizsgálat során az egyes részeknél a logikai és kritikai elemzésé is. Emellett hangsúlyt fektettem a komparatív módszerre különösen az uniós, hazai és amerikai szabályozás vonatkozásában, amely során érintettem az anyagi büntetőjogi rendelkezések hasonlóságait és különbözőségeit.

II. AZ INFORMATIKAI BŰNCSELEKMÉNYEK

1. Történeti áttekintés

1.1. Az informatikai bűnözés elleni fellépés európai dimenziói

1.1.1. OECD jelentés

Az első fontos nemzetközi jogi dokumentum a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) által kibocsátott 1986-os jelentés volt, amelyben iránymutatást kívántak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez, mellyel egyúttal a kodifikáció elősegítése volt a cél. A büntetendő cselekmények körét a következőképpen rendszerezte 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.

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

Az Európa Tanács a 1980-as évek második felében hozott létre egy szakértői bizottságot a számítógépes bűncselekményekkel kapcsolatos ismeretek összegyűjtésére és a veszélyek felmérésére. A bizottság kiemelt célja az 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 iránymutatásul szolgál a tagállamok jogalkotói

számára, amennyiben ilyen típusú bűncselekmény esetében új jogszabályokat hoznak, vagy a régiek kerülnek átalakításra, akkor abban az esetben kötelezve vannak arra, hogy az ajánlással összhangban járjanak el. Az ajánlás felhívja a figyelmet arra, hogy kizárólag egy egyetemes, kötelező erejű jogi dokumentum felel meg a célnak, hogy hatékonyan feltudjanak lépni ezzel 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.[7]

Henrik W. K. Kaspersen kiemelte, hogy az anyagi szabályozás mellett a büntetőeljárási jogi kérdésekkel is együttesen foglalkozni kell.[8] Ulrich Sieber is felhívta a figyelmet a határon átnyúló együttműködés fontosságára, különösen a különböző szervezetek közötti összehangolt tevékenységekre az informatikai bűnözés leküzdéséhez (pl. hiányozott eddig a kölcsönös bűnügyi jogsegély és a nemzetközi nyomozás megteremtésének az alapja).[9] A büntető eljárásjogi aggodalmakra válaszul megszületett az ET. 95. (13.) számú ajánlása, amely az információs technológiákkal kapcsolatos eljárási problémákra törekedett megoldást nyújtani, így például a házkutatás és lefoglalás; technikai megfigyelés; kötelezettség a nyomozó

[7] GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. A PIN kód megadása vagy biztonságosan az Internet? Pécsi Határőr Tudományos Közlemények XIII. 237-238. o.
[8] 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.
[9] SIEBER, Ulrich: Legal Aspects of Computer-related Crime in the Information Society: COMCRIME-Study. prepared for the European Commission, 1 January 1998.

hatóságokkal való együttműködésre; elektronikus bizonyítékok; titkosítás használata; statisztika és képzés; nemzetközi együttműködés során felmerülő kérdésekre ad választ.[10]

1.1.3. A Számítástechnikai Bűnözésről Szóló Egyezmény

2001 novemberében Budapesten írták alá az Európa Tanács által előkészített Számítástechnikai Bűnözésről Szóló Egyezményt (Convention on Cybercrime) (a továbbiakban: Budapesti Egyezmény). A Budapesti Egyezmény az Európa Tanács tagjain kívül más országok számára is nyitva áll aláírásra és ratifikálásra. Az eddigi ajánlásokhoz képest tovább lépést jelentett és újabb jogi normákat fogalmazott meg. A számítógépes technikai fogalmakat definiálja és ezáltal egységes értelmezést nyújt. A következő fogalmakat határozza meg: a számítógépes rendszer, számítógépes adat, internetes szolgáltató, illetve átmenő adat definícióját. Mind az anyagi és eljárásjogi szabályozást tartalmazza. Az anyagi jogban a bűncselekménytípusok köre kibővült és újabb jogsértési típusok jelennek meg (pl. eszközökkel való visszaélés, a gyermekpornográfiával kapcsolatos bűncselekmények). Az egyes bűncselekménytípusokat logikusan csoportokba rendezi.

Az egyezmény négy részre osztható fel:

- A büntető anyagi jogi részt tartalmazza (2 – 13. 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 nemzetközi együttműködésre vonatkozó irányelveket fogalmaz meg. Valamennyi aláíró fél részéről igényli a kölcsönös jogsegélynyújtást, illetve a „ lehető legszélesebb körben együttműködnek a számítástechnikai rendszerekkel és adatokkal kapcsolatos bűncselekményekre vonatkozó nyomozások és eljárások során, illetve bármely bűncselekményre vonatkozó elektronikus bizonyítékok összegyűjtése érdekében” (23 – 35. Cikk).
- A záró rendelkezésekben az egyezmény hatályára, a fenntartásokra, a módosításokra, a viták rendezésére és az egyezmény felmondására vonatkozó részekre térnek ki (36 - 48. Cikk).

Az egyezmény anyagi jogi szabályozás terén kimondja, hogy minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával

[10] SCHJOLBERG, Stein: The history of global harmonization on cybercrime legislation – the road to Geneva. 2008. 5. o.

összhangban bűncselekménynek minősüljön 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).

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 csoportok 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).

2003-ban az egyezményt kiegészítették a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyvvel. A Budapesti Egyezmény azonban egyes számítástechnikai cselekmények szabályozását még nem tartalmazza mint például ilyen a személyazonosság-lopás, a gyermekekkel történő szexuális célú kapcsolattartás, illetve a kiberterrorizmus és a kéretlen levél (spam) problémájára sem tér ki. Magyarországon a 2004. évi LXXIX. törvénnyel hirdették ki az egyezményt, ezzel összhangban a régi 1978-as Büntető Törvénykönyvbe a 300/C. § szakaszba a számítástechnikai rendszer és adatok elleni bűncselekményt vezették be, valamint egyéb más törvényi tényállásokat kiegészítették a meghatározottak szerint, azonban ennek részletes bemutatására a későbbiekben kerül sor.[11]

Ugyanebben az évben az Európai Tanács 2001/413/IB kerethatározata került elfogadásra a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről.[12]

2002-ben került elfogadásra az Európai Parlament és a Tanács 2002/58/EK elektronikus hírközlési adatvédelmi irányelve, 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-k telepítésére vonatkoznak. Ez az irányelv 2009-ben egészült ki az ún. „süti"

[11] NAGY (2009): i.m. 40-56. o.

[12] 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 [2017.10.08.]

(cookie) irányelvvel, amely alapján a viselkedésalapú reklám célba juttatásához használt cookie-k kizárólag az érintettek hozzájárulását követően helyezhetők el a felhasználók számítógépein.[13]

Az Europol szervezetén belül 2002-ben hozták létre a Csúcstechnológiai Bűnözési Központot (High Tech Crime Centre).[14]

Az Európai Tanács 2004/97/EK határozattal létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA), amely az Unió, a tagállamok, a magánszektor és az európai polgárok szolgálatában álló hálózat- és információbiztonsági szakértői központ. Jelenleg az 526/2013/EU rendelet szabályozza a szervezet működését.[15]

1.1.4. A 2005/222/IB tanácsi kerethatározat

2005-ben pedig az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat elfogadására került sor,[16] amelynek a célja a számítógépes bűnözés elleni küzdelem és az információbiztonság előmozdítása volt. A transznacionális bűnözés ezen új formáját tekintve a kerethatározat fő célja az igazságügyi és egyéb illetékes hatóságok közötti együttműködés javítása az információs rendszerek elleni támadások területére vonatkozó büntetőjogi szabályok közelítése a következő területeken: információs rendszerekhez való jogsértő hozzáférés, rendszerekbe való jogsértő beavatkozás, adatokba való jogsértő beavatkozás. A kerethatározatnak megfelelően vette át a magyar szabályozás is az információs rendszer szóhasználatát az ilyen típusú bűncselekményeknél. Fogalommeghatározásokat is tartalmaz, amit a kerethatározatot felváltó új irányelv át is vesz, ezért annak a részletesebb szabályozására térek ki a későbbiekben, hiszen az teljes mértékben a kerethatározatra épül.

Az Európai Unióról szóló és az Európai Unió működéséről szóló szerződés 83. cikk (1) bekezdése pedig kimondja: „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

[13] http://adatvedelmiaudit.hu/2011/06/cookie-k-csak-hozzajarulassal/ [2017.09.21.]
[14] SZALÁRDI Gábor: A csúcstechnológiai bűnözés elleni küzdelem támogatása. Belügyi Szemle 2012/6. 98-99.o.
[15] https://europa.eu/european-union/about-eu/agencies/enisa_hu [2017.11.21.]
[16] http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32005F0222 [2017.11.21.]

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.

1.1.5. Az Európai Parlament és Tanács 2011/92/EU számú irányelve és a Számítástechnikai Bűnözés Elleni Európai Központ (EC3)

2011-ben az Európai Parlament és Tanács 2011/92/EU számmal irányelvet fogadott el a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről. Ezzel összefüggésben 2012-ben kezdetét vette egy nemzetközi összefogás „Globális szövetség a gyermekek online szexuális kizsákmányolása ellen", amelyhez az uniós országokon kívül más országok is csatlakoztak.

2013. január 11-től kezdte meg működését az 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. A központ a következő bűncselekményekre fókuszál: amelyeket szervezett bűnözői csoportok követnek el mint például az online csalás, illetve amelyek súlyos kárt okoznak az áldozataiknak, továbbá amelyek a kritikus (információs) infrastruktúrát érintenek.[17] Az EC3-n belül a Focal Point Terminal nyomoz a nemzetközi fizetési csalásokkal kapcsolatban, együttműködve az érintett intézményekkel, mint az Európai Központi Bank és a nemzeti bankok, 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 műveleteket mint például a botneteket. Az említett elemző rendszer a sandbox technológiára épül, amelyre a rendvédelmi szervek a további vizsgálatok elvégzése érdekében elektronikus úton töltik fel a felderített ügyek során felmerülő malware mintázatokat, valamint

[17] 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.

az ezekkel összefüggésben keletkezett adatokat, ami után az egység az általa tett megállapításokat egy részletes jelentésben küldi vissza (pl. a rosszindulatú program azonosítását).[18]

A Focal Point Twins pedig olyan esetekkel foglalkozik, amikor a gyermekek szexuális kizsákmányolásához és bántalmazásához kötődő eseteket vizsgálta (pl. szexuális zsarolás, ún. „grooming"[19]). Emellett áldozatazonosítási munkacsoport (Victim Identification Task Force) is működik, amelynek célja az ismeretlen áldozatokról meglévő anyagok elemzése.[20]

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 kapcsolat fenntartó hatóságokkal az EU-n kívül is, hogy koordinálják a nemzetközi választ az azonosított, magasfokú fenyegetésekre. A J-CAT 2014-ben indult köszönhetően az EC3, EUCTF, FBI és az Egyesült Királyság Nemzeti Bűnüldözési Ügynökség (NCA) közös együttműködésének (pl. sikeres akciójuk között említhető a DD4BC zsaroló bűnözői csoport tagjainak kézre kerítése).

Az EC3-nak stratégiai funkciója is van, egybegyűjti a szaktudást 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 lakosság tudatosságának növelése és a partnerségi kapcsolatok szélesítése a nemzetközi színtéren.[21]

---

[18] SZONGOTH Richárd – VETTER Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. Belügyi Szemle, 2018/7-8. 9. o.

[19] 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, ami 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.

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

[21] MEZEI Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. Jura 2018/1. 353. o.

Az EC3 szakértelme az igazságügyi informatika területén figyelemre méltó: saját igazságügyi informatikai laboratóriumot hozott létre, amely a legkorszerűbb segítséget nyújt, és emellett saját független technológiai kutatást és fejlesztést is végez.[22]

1.1.6. Az Európai Parlament és Tanács 2013/40/EU számú irányelve

2013 augusztusában az Európai Parlament és Tanács 2013/40/EU számmal irányelvet[23] fogadott az információs rendszerek elleni támadásokról, amely a 2005/222/IB 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. Számos új szabályt vezet be a számítástechnikai bűncselekmények büntetendőségének és szankciójának harmonizálására. Az új szabályok közé tartozik az ún. botnetek - számítógép-hálózatok távoli irányítására tervezett rosszindulatú számítástechnikai programok - törvényen kívül helyezése is. Felhívja a figyelmet arra, hogy valamennyi tagállamban hatékony fellépésre van szükség, ezért biztosítani kell, hogy ugyanaz a bűncselekmény valamennyi tagállamban büntetendő legyen és a bűnüldöző hatóságok számára biztosítani kell a fellépéshez szükséges, az egymás közötti együttműködést elősegítő eszközöket. Az irányelv a büntetőjogi rendszereknek az uniós országok közötti közelítését és az igazságügyi hatósági együttműködés bővítését sürgeti az alábbi területeken mint az információs rendszerekhez való jogellenes hozzáférés, információ rendszerekbe vagy adatokba való jogellenes beavatkozás, jogellenes adatszerzés.

A hatékony prevenció érdekében a hatóságoknak együtt kell működniük a magánszférával és a civil társadalommal (pl.: ez kiterjedhet a szolgáltatók általi a potenciális bizonyíték megőrzésére, együttműködési és partnerségi hálózat kiépítésére a szolgáltatókkal és a gyártókkal).

A jogi személyek felelősségét és a velük szemben alkalmazandó szankciókat a kerethatározathoz hasonlóan tartalmazza. Továbbá a joghatósági kérdésekre is választ ad. 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 operatív kapcsolattartó 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

[22] 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.
[23] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2013.218.01.0008.01.HUN [2017.09.20.]

milyen formában és várhatóan mikor teszi. Továbbá tagállamoknak biztosítani kell egy olyan rendszer meglétét, amely rögzíti, előállítja és rendelkezésre bocsátja ezekre a bűncselekményekre vonatkozó statisztikai adatokat. Az irányelvet a tagállamoknak 2015. szeptember 4-ig kellett implementálniuk a nemzeti jogukba.

1.1.7. A NIS irányelv

Végül érdemes szót ejteni a 2016-os hálózati és információs rendszerek biztonságáról szóló irányelvről, vagyis az úgynevezett NIS irányelvről, ami ugyan nem büntetőjogi tárgyú szabályozás, de fontos a téma szempontjából. Ez az első uniós szintű szabályozás az információbiztonság területén, mely kötelezően és geopolitikai alapon határoz meg szabályokat és kötelező együttműködést egyes intézmények számára. Korábban is megfigyelhető volt a tagállamok információbiztonsággal foglalkozó szervei közötti együttműködés, viszont ez önkéntesen és bizalmi alapon valósult meg. Az irányelv célja, hogy megfogalmazzon egy közös intézményt és eszköztárat a tagállamok számára, illetve egy európai szintű együttműködés alapjait fogalmazza meg. Ennek megfelelően elkülöníthetünk nemzeti szinten végrehajtandó és közösségi szinten végrehajtandó feladatokat. Az irányelv célja, hogy minden tagállam rendelkezzen minimális képességekkel, a szükséges intézményekkel, szabályokkal, valamint a hálózat- és információbiztonság magas szintjét biztosító nemzeti szintű stratégiával. Az irányelv előírásai szerint minden tagállamnak ki kell jelölnie egy vagy több (akár szektoronként egy-egy) számítógép-biztonsági eseményekre reagáló csoportot (továbbiakban: CSIRT), amely legalább az adott szektor incidenskezelésért felelős.

Az irányelv a hatályt tekintve két csoportra osztható. Elsőként definiálja az ún. alapvető szolgáltatásokat nyújtó szolgáltatók csoportját, melybe a digitális infrastruktúrák, energetika, közlekedés, banki szolgáltatások, pénzügyi szolgáltatások, egészségügyi szektor tartozik. A második alanyi kör a digitális szolgáltatásokat nyújtó szolgáltatók csoportja, melyek körébe pl. az online piactér, keresőmotorok, felhő szolgáltatók tartoznak. Az irányelv különböző kijelölési szabályokat, megfelelési kritériumokat, valamint incidens bejelentési kötelezettségeket fogalmaz meg az alapvető szolgáltatásokat nyújtó szolgáltatókra vonatkozóan csakúgy, mint a digitális szolgáltatást nyújtó szolgáltatókra.

A fent felsorolt szektorokban a tagállamoknak ki kell jelölniük a meghatározott szempontok figyelembevételével a hatály alá eső vállalatokat, cégeket. Ehhez szektoronként pontosítani, specializálni kell az irányelv rendelkezéseiben megfogalmazott kijelölés kritériumait.[24]

1.2. Az Egyesült Államok büntetőjogi szabályozása az informatikai bűncselekményekre vonatkozóan

1.2.1. A kezdeti szabályozási törekvések 1984-ig

Az első számítógépes 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 továbbiakban: CFAA). 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. Más jogtudósok úgy vélték, hogy a hagyományos elméletek nem nyújtanak segítséget a számítógépes bűnözéssel szemben, éppen ezért új törvények megalkotására van szükség, mert a korábbi szabályozás megalkotásakor még nem vették figyelembe az informatika felérékelődött szerepét a bűnelkövetésben és alkalmazásuk nem megfelelő a számítógépes bűncselekmények esetében. Például erre először az United States vs. Seidlitz ügy 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 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 az adatvédelmet is veszélyeztette. A kritikákat figyelembe véve végül nem fogadták el a törvényt.

[24] 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.

Azonban 1984-ben végül elfogadásra került a már említett CFAA, az első szövetségi törvény, amely kifejezetten a számítógépes bűncselekmények szabályozását célozta.[25] A CFAA kezdetben három bűncselekményt vezetett be.[26] Az első 1030.§ (a)(1) bekezdésben szabályozott bűncselekménynél a védett jogi tárgy a nemzetbiztonsági titok biztonságához fűződő érdek. Az említett bekezdés értelmében büntetendő az, aki a számítógéphez jogosulatlan hozzáfér abból a célból, hogy nemzetbiztonsági információhoz jusson hozzá azzal a szándékkal vagy okkal feltételezhető, hogy az Egyesült Államok ellen felhasználhatja azt és árthat vele. A második bűncselekmény a személyes pénzügyi információkat védi a 1030.§ (a)(2) bekezdésben, amely szerint büntetendő az, aki számítógéphez jogosulatlanul hozzáfér, hogy olyan információt szerezzen meg, amit pénzintézet pénzügyi nyilvántartása vagy fogyasztóvédelmi ügynökség adatállománya tartalmazza. A harmadik bűncselekmény az Egyesült Államok kormányzati számítógépeit védi. 1030.§ (a)(3) bekezdése értelmében büntetendő az, aki számítógéphez jogosulatlanul hozzáfér, azért hogy az Egyesült Államok kormányzati számítógépén tárolt információt használja, módosítsa, megsemmisítse, közzé tegye, amellyel a számítógép működését befolyásolja.[27]

Azonban a CFAA fő hiányossága volt kezdetben, hogy nem lehetett megfelelően alkalmazni, vagyis a gyakorlatban nem bizonyult hatékonynak, ezt jelzi, hogy a kihirdetésétől kezdve két évig nem indul 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 magánélethez fűződő jog és a szabadságjogok csorbítását. Ezt figyelembe véve a CFAA a védelmet kizárólag a pénzügyi nyilvántartások és fogyasztói információk, illetve a kormány tulajdonai számára biztosította, amelyekhez kormányzati vagy gazdasági érdek fűződött. Ennek fényében a magánszemélyekhez tartozó számítógépek, illetve amelyek nem a fent említett információkhoz kapcsolódnak azok kiesnek a törvény tárgyi hatálya alól, vagyis a személyi számítógépeken tárolt személyes információk vagy pénzügyi nyilvántartásokon kívül eső hitelkártyák nem voltak a CFAA által védve. Másodszor a törvény hiányossága, hogy nem tudott mit kezdeni azzal az esettel, ha a számítógéphez jogosultan férnek hozzá, de a jogosultságainak kereteit túllépve férnek hozzá az adott információhoz.[28]

[25] Az Egyesült Királyságban is hasonlóan külön törvényben, a „Computer Misuse Act 1990”-ben kerültek szabályozásra az informatikai bűncselekmények. Erről lásd részletesen: SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Királyságban. Belügyi Szemle 2015/9. 48-68. o.

[26] WANG, Qianyun: A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. 99-100. o.

[27] KERR, Orin: Vagueness Challenges to the Computer Fraud and Abuse Act. Minnesota Law Review 2010. 1564. o.

[28] WANG: i.m. 102-106. o.

1.2.2. A CFAA első módosítása 1986-ban

1986-ot követően a CFAA kiterjesztésére és módosítására került sor, amelynek köszönhetően a gyakorlatban alkalmazhatóbbá vált. A törvényt ért kritikák miatt az első módosítás a szándékra vonatkozóan terjedt ki, a „tudatosan" (knowingly) fogalom használatot váltotta a „szándékosan" (intentionally) használata a 1030.§ (a)(2) és a (a)(3) bekezdésekben szabályozott bűncselekményeknél, illetve jogellenessé (actus reus[29] kiterjesztése) tették a jogosultság kereteinek túllépését is. A módosítás további három új tilalmat is kodifikált a 1030§ (a)(4)-(6) szakaszokban. Az 1030.§ (a)(4) bekezdés büntetendővé tette a számítógéphez való jogosulatlan hozzáférést csalási szándékkal; amely alapvetően, a hagyományos ún. „wire fraud", azaz vezetékes csalás elkövetése számítógéppel. 1030.§ (a)(5) bekezdés értelmében felelősségre vonható az, aki jogosulatlanul hozzáfér a számítógéphez és információt módosít, megrongál, megsemmisít és ezáltal 1,000$ vagy nagyobb veszteséget okoz, vagy egy vagy több személynek az orvosi vizsgálatát, diagnózisát, kezelését vagy gondozását akadályozza. 1030§ (a)(6) bekezdés a számítógépes jelszavakkal való kereskedést tiltja. Az 1030.§ (a)(4) és (5) bekezdés a szövetségi érdekű számítógépek (federal interest computers) védelmére korlátozódott, amelyek közé tartoznak azok a számítógépek az (A) pont szerint, amelyeket vagy az Egyesült Államok kormánya használatában vannak, vagy a pénzintézetek használják, vagy a (B) pont szerint egy több államot átívelő számítógépes hálózat részeként jelenik meg. Az (A) pont a korábbi szabályozást fedi le, míg a (B) pont új, bár korlátozott alapot jelentett, amely akkor alkalmazható, ha több államot érintő bűncselekményt követnek el államok közötti hálózaton. Ebben az időben azonban az internet használata még gyerekcipőben járt, így kevés bűncselekmény tartozott ebbe a körbe.

1.2.3. 1988 és 1990 közötti módosítások

1988-1990 közötti időszakban három módosítása volt a törvénynek, melyek szintén a CFAA hatályát tovább kiterjesztették és elsődlegesen a pénzügyi biztonság, illetve a különböző pénzintézetek védelmét volt hivatott megerősíteni. Az 1988-as módosítás a pénzintézet (financial institution) fogalmát bővítette azáltal, hogy valamennyi pénzintézetet a törvény hatálya alá vonta, nem csak kizárólag a hitelkártya kibocsátókat. A 1989-es módosítás pedig a bank kifejezés helyett az intézetet használja, amely világosan meghatározza, hogy azon intézetek tartoznak ide, amelyeknek a betétjei biztosítva vannak a Federal Savings and Loan

[29] Az angolszász jogrendszerekben az actus reus a bűnös tettet jelenti, míg a mens rea a bűnös tudatot.

Insurance Corporation által. Az 1990-es módosítás pedig további két ponttal bővítette a pénzintézet fogalmát.

1.2.4. A CFAA ötödik módosítása 1994-ben

A CFAA 1994-es módosítása révén bővült a bűnösség (mens rea) köre és büntetendővé vált a gondatlanságból történő elkövetése a 1030.§ (a)(5) bekezdésben szabályozott bűncselekménynek, amely szövegének a megfogalmazása is változott a korábbihoz képest. Ez az ún. vírus rendelkezés, amely alapján felelősségre vonható az, aki jogosulatlanul továbbít programot, információt, kódot vagy parancsot, különösen ez a számítógépes vírusokra vonatkozik, és ezáltal szándékosan kárt okoz, illetve amennyiben gondatlanságból okoz kárt, azt is büntetni rendeli másik pontban. A módosítás lehetővé tette a sértettek számára a polgári jogi kártérítési eljárás indítását az 1030.§-ban szabályozott bűncselekmények elkövetőivel szemben.

1.2.5. The National Information Infrastructure Protection Act 1996

Kezdetben a (a)(2) bekezdés csak azokat az eseteket rendelte büntetni, amikor olyan információt szereztek meg, ami a pénzintézet pénzügyi nyilvántartásában található vagy a fogyasztóról az információt a fogyasztóvédelmi szerv nyilvántartása tartalmazta. Az 1996-os módosítás révén azonban bármely információ megszerzése büntetendővé vált, amennyiben egynél több államot érintett.

A módosítás továbbá a 1030.§ (a)(7) bekezdésben új bűncselekményt vezetett be, büntetendővé tette a számítógépes zsarolást.

A sérelmek körét is bővítette a 1030.§ (c)(4) bekezdésben, hozzáadva a következő eseteket: „a fizikai sérelem bármely személynél következik be”, illetve „fenyegetés a közegészség és biztonság számára”.

Végül a módosítás érintette a „szövetségi érdekű számítógép” fogalmát, mert új elnevezés, a „védett számítógép” váltja fel: (A) „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 a 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”. Orin Kerr professzor kritikával illette a „védett számítógép” elnevezést, mert valamennyi számítógép, amely az

Internetre csatlakozik már államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve kommunikációra van használva, hiszen az Internet maga egy nemzetközi hálózat, amit ezekre a célokra használnak, tehát bármely Internetre csatlakoztatott számítógép lehet a CFAA-ban szabályozott bűncselekmény célpontja, így megfelelőbb lenne a „számítógép" elnevezés használata a „védett számítógép" helyett.[30]

1.2.6. USA PATRIOT Act 2001

2001-ben az Egyesült Államok aláírta és ratifikálta a Budapesti Egyezményt. Ugyanebben az évben a szeptember 11-ei terrortámadást követően az USA PATRIOT Act 2001 (a továbbiakban: PA 2001)[31] 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". A definíció kiterjesztésével a cél az volt, hogy a törvény hatálya alá tartozzanak azok a számítógépek is, amelyek az Egyesült Államokon kívül találhatók.

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

1.2.6. The Identity Theft and Enforcement and Restriction Act 2008

A törvény legújabb módosítására 2008-ban került sor, amely a 1030.§ szakasz hatályát terjesztette ki azáltal, hogy eltávolították az államközi vagy nemzetközi kommunikáció során történő elkövetési (interstate or foreign communication) kitételt mint követelményt a 1030.§ (a)(2)(C) pontban és a módosítást követően a következőképpen néz ki: bármely jogosulatlan hozzáférés bármely védett számítógéphez, amely bármely – államok közöttit vagy államon belülit – információt képes helyreállítani büntetendő. További újdonság, hogy bekerült az 5.000$ értékhatár, illetve bűntettként a tíz vagy több számítógépben okozott kár, amely a botnetek elleni harcot hívatott erősíteni.

[30] WANG: i.m. 108-111. o.
[31] 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 harmadik legjelentősebb változtatás a védett számítógép definíciójának (B) pontját érintette, amelyet a hatályos törvény is tartalmaz a (B) pont szerint: „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.[32]

Bűncselekmény	**Bekezdés**
Nemzetbiztonsági információ megszerzése	(a)(1)
Számítógéphez való hozzáférés és információszerzés	(a)(2)
Behatolás kormányzati számítógépbe	(a)(3)
Számítógépes csalás	(a)(4)
Számítógép vagy információban való károkozás	(a)(5)
Jelszavakkal kereskedés	(a)(6)
Számítógépes zsarolás	(a)(7)

1. táblázat: A hatályos CFAA-ban szabályozott bűncselekmények

[32] KERR (2010): i.m. 1568-1571. o.

2. Fogalmi alapvetés

2.1. Az 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" kifejezésből honosodott meg a kiberbűnözés szó, amelynek a használata napjainkban széles körben elterjedt. Az értekezésem során az informatikai bűnözés és kiberbűnözés (cybercrime[33]) mint szinonim fogalmakat fogom használni, mert ezeknek a használata – különösen a nemzetközi – szakirodalomban széleskörűen elfogadott. Azonban fontos megjegyezni, hogy nincs ezekre vonatkozóan egy általánosan elfogadott és egységes jogi definíció.

Kezdetben eltérő elnevezéseket is használtak, így a számítógépes bűnözést (computer crime), amely kizárólag a számítógépre helyezte a hangsúlyt, illetve internetes vagy virtuális bűnözést (internet crime[34] vagy virtual crime), amely kizárólag az internetre fókuszált, valamint csúcstechnológiás bűnözést (high-tech crime) és elektronikus vagy digitális bűnözést, azonban utóbbi elnevezések túl tág fogalmi keretet adnak.

David Wall az informatikai bűnözés „evolúciájáról" ír, amelyben megkülönbözteti a több generációs informatikai bűncselekményeket:

- az első generációs informatikai bűncselekmények még olyan hagyományos bűncselekmények, amelyekben a számítógépet használtak eszközül az elkövetéshez, valamint az interneten található információkat használták fel az elkövetéshez;
- a második generációs informatikai bűncselekmények a hibridek kategóriájába tartoznak, mert a hagyományos bűncselekmények elkövetéséhez már az internetet használták fel;
- a harmadik generációs, modern kori informatikai bűncselekmények, amelyek az internet nélkül nem léteznének.[35]

A Számítástechnikai Bűnözésről szóló Egyezmény (Convention on Cybercrime) ugyan a kiberbűnözés fogalmát nem határozza meg, de a bűncselekményeket a következőképpen csoportosítja:

[33] 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.
[34] Lásd JEWKEY, Yvonne – YAR, Majid (eds.): Handbook of Internet Crime. Willan Publishing, 2010.
[35] 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.

- 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).

Marije T. Britz a számítógépes bűncselekmény fogalmát általánosan határozza meg, amelybe beletartozik minden olyan bűncselekmény, amelyet számítógép használatával követnek el.[36] Hasonlóan értelmezi Eoghan Casey is, de pontos meghatározással nem szolgál, csak utal arra, hogy ebbe a kategóriába kizárólag azon bűncselekmények tartoznak, amelyekben a számítógép a bűncselekmény eszközként vagy tárgyaként jelenik meg.[37] Britz emellett még a számítógéppel kapcsolatos bűncselekmény (computer-related crime) fogalmát használja, amely szerinte a számítógéppel kapcsolatos minden olyan bűncselekmény, melyben a számítógép bármilyen módon, akár közvetetten is jelen van, tehát az már ebbe a kategóriába tartozik (pl. a zsarolás e-mailben történik).[38]

A szakirodalomban több szerző is, így Jonathan Clough[39], Peter Grabosky[40] és Susan W. Brenner[41] is az informatikai bűnözésre mint egy gyűjtőfogalomként tekint, amelynek azonban két fő kategóriája különböztethető meg: az egyik azon deliktumok csoportja, amelyeket kizárólag információs rendszerek (számítógépekkel, azok hálózatával vagy egyéb ICT eszköz használatával) követhetők el. Jellemzően ezeknek a bűncselekményeknek a tárgya az információs rendszer, tehát amikor a támadás ezek ellen irányul. 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 valósítanak meg mint például ilyen a csalás, zsarolás, gyermekpornográfia, szerzői jogi jogsértések, zaklatás stb., ez az ún. „cyber-enabled crime" esetköre, amikor az információs rendszer a bűncselekmény elkövetésének az eszköze.[42] Az Europol is éves jelentéseiben hasonlóan ezeket a fogalmakat használja, de részben eltérő elnevezéssel: a „cyber-dependent crime"-t, valamint a „cyber-facilitated crime"-t.

[36] BRITZ, Marija T.: Computer Forensics and Cyber Crime: An Introduction. Pearson. London, 2013. 6. o.
[37] CASEY, Eoghan: Digital Evidence and Computer Crime. Elsevier. Amsterdam, 2012. 37. o.
[38] BRITZ: i.m. 6. o.
[39] CLOUGH: i.m. 10-11. o.
[40] GRABOSKY, Peter: Cybercrime. Oxford University Press, 2016. 8-9. o.
[41] BRENNER, W. Susan: Cybercrime – Criminal Threaths From Cyberspace. Praeger, 2010. 39-47 o.
[42] CLOUGH: i.m. 10-11. o.

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

Ezen csoportosítást – vagy ezek változatait – használják az angolszász jogrendszerekben is, így az Egyesült Államokban[43], az Egyesült Királyságban[44] és Ausztráliában[45] is.

Alisdair A. Gillespie a kiberbűncselekményeket a következőképpen csoportosítja:

- a számítógépekkel szembeni bűncselekmények,
- vagyon elleni bűncselekmények,
- a tiltott tartalommal kapcsolatos bűncselekmények,
- valamint a személy elleni bűncselekmények.[46]

A hazai szakirodalomban - kezdetben Polt Péter, Pusztai László és Nagy Zoltán András[47] - Ulrich Sieber nyomán[48] 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.[49]

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. Nincs egyetértés arra vonatkozólag, hogy az egyes cselekmények mennyiben kapcsolódnak a számítástechnikai rendszerekhez és mennyiben az internethez, és 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

[43] COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION: The National Information Infrastructure Protection Act of 1996.
[44] MCGUIRE, Mike – DOWLING, Samantha: Cyber crime: A review of evidence, Summary, 2013. 5. o.
[45] ATTORNEY'S GENERAL'S DEPARTMENT (Australia): National plan to compay cybercrime. 2013. 4-5. o.
[46] GILLESPIE, A. Alisdair: Cybercrime – Key Issues and Debates. Routledge, 2016. 7-8. o.
[47] PUSZTAI László: Számítógép és bűnözés. In: Gödöny József (szerk.): Kriminológiai és Kriminalisztikai Tanulmányok 26. OKRI, Budapest, 1989. 85. o.
[48] SIEBER, Ulrich: A számítógépes bűnözés és más bűncselekmények az információtechnológia területén. Magyar Jog 1993/2. 105-109. o.
[49] NAGY Zoltán András: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda. Belügyi Szemle 1999/11. 16-27. o.

bűnözés a számítástechnikai rendszerek és hálózatok integritását sértik, míg az internetes bűnözés esetében az internet mint elkövetési színtér, médium jelenik meg".[50]

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.[51]

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".[52]

Mindezekre tekintettel megállapítható, hogy a kiberbűncselekmények körében beszélhetünk új típusú bűncselekményekről, amelyek kizárólag információs rendszer segítségével követhetők el, emellett ide tartoznak azok a régi, hagyományos bűncselekmények is, amelyek elkövethetők könnyebben az új elkövetési eszközök alkalmazásával.

A technológiai fejlődésnek köszönhető, hogy az egyes vagyon elleni, illetve gazdasági bűncselekmények is könnyedén elkövethetők a modern technológiák és az internet segítségével, ami miatt átfedések mutatkoznak az informatikai és gazdasági bűnözés között. Az üzleti vállalkozások és egyes gazdasági szektorok – gondoljunk csak a pénzintézetekre – egyre inkább függnek az információs rendszerektől, amelyeket az elkövetők is kihasználnak (pl. bankkártyával összefüggő visszaélések és a pénzmosás területén).[53]

Az értekezésnek az egyes fejezeteiben kizárólag a tisztán informatikai bűncselekményekkel és az egyes gazdasági bűncselekményeknek a részletes vizsgálatával foglalkozom, amelyeknél az információs rendszerek elkövetési eszközként való felhasználása egyre gyakoribb és ezért kihívások elé állítják a jogalkalmazókat.

---

[50] 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.

[51] SZATHMÁRY Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. Doktori Értekezés (PTE ÁJK) Budapest, 2012. 79-80. o.

[52] SZABÓ Imre: Informatikai bűncselekmények. In: Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve. Budapest, CompLex, 2008. 547. o.

[53] SMITH, Russel G. – GRABOSKY, Peter – URBAS, Gregor: Cyber Criminals on Trial. Cambridge University Press, 2004. 9-11. o.

2.2. Az alapvető fogalmak: a számítógép és az információs rendszer

Az informatikai bűncselekményekkel kapcsolatban fontos az alapvető fogalmaknak a tisztázása, így különösen a számítógépé, mely szónak a használata már mindennapossá vált, azonban a modern technológiák rendkívül gyors fejlődésének köszönhetően a definiálása egyre nagyobb kihívást jelent. Manapság már az okostelefonok rendelkeznek olyan processzorral mint a hagyományos asztali számítógépek, valamint egyre több háztartási gép és más „okos" eszközök is erős feldolgozási kapacitással bírnak. Például az elkövetők már könnyedén hozzáférhetnek különböző IoT eszközökhöz például routerekhez, biztonsági kamerákhoz és akár az okostelevíziókhoz, gépjárművekhez és egészségügyi berendezésekhez is.

A jogalkotók részéről két megközelítés figyelhető meg vagy nem határozzák meg a számítógép fogalmát (pl. az Egyesült Királyság, Ausztrália és Kanada), vagy egy átfogó definíciót alkalmaznak (pl. az Egyesült Államok).[54]

A Budapesti Egyezmény mindkét megközelítést tartalmazza, mert ugyan a számítógép fogalmát nem határozza meg, 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". Tehát ezt figyelembe véve 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. A hálózat pedig kettő vagy több számítástechnikai rendszer közötti kapcsolat, amely lehet vezetékes, vezeték nélküli vagy mindkettő, a lényeg, hogy információcserére kerüljön sor a hálózaton belül.[55]

Az információs rendszerek elleni támadásokról szóló irányelv már a kor kívánalmainak megfelelően az információs rendszer (information system) fogalmát használja és nem szűkíti le a fogalmi kört kizárólag a számítógépre. Az új meghatározás hátterében áll az, hogy a köznyelvi számítógép-fogalom az eszközöknek viszonylag szűk körére, a személyi számítógépekre értendő, ugyanakkor az informatikai bűncselekmények tárgyai, illetve eszközei lehetnek olyan új modern eszközök is mint a táblagépek, az okostelefonok, a nyomtatók vagy az

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

adattovábbítást és a kapcsolatfelvételt biztosító műszaki berendezések és ez a kör idővel még bővülni fog köszönhetően a gyorsütemű technológiai fejlődésnek.[56]

Az 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."

A CFAA 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 ilyen.

A kiberbűncselekmények jogi tárgya a védett számítógéphez integritásához fűződő érdek. A védett számítógép 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 ezekre a célokra használnak. Tehát ezt szem előtt tartva, bármely internetre csatlakoztatott számítógép

[56] 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.

lehet a CFAA-ban szabályozott bűncselekmény célpontja, így megfelelőbb lenne a „számítógép” elnevezés használata a „védett számítógép” helyett.[57]

[57] WANG: i.m. 72-73. o.; 108–111. o.

3. A jogosulatlan belépés, avagy a „hacking” a büntetőjogban

3.1. Általános bevezető

Az első magatartás, amivel részletesen foglalkozom az a jogosulatlan belépés vagy másnéven „hacking”, mely utóbbi elnevezést gyakran használatos. A „hacker” kifejezést általában azokra a személyekre használják, akik kiemelkedően magasfokú informatikai ismeretekkel és gyakorlattal rendelkeznek. Az egyik legnépszerűbb nézet szerint a hackerek között különbséget lehet tenni, hogy milyen szándékkal törik fel a rendszert. Ez alapján beszélhetünk az ún. „white hat” vagy fehér kalapos hackerekről, akik „jószándékkal” például az adott rendszer biztonságát és sebezhetőségét tesztelik. Emellett vannak az ún. „black hat” vagy fekete kalapos hackerek, illetve másnéven „crackerek”, akik azzal a céllal hatolnak be a rendszerbe, hogy kárt okozzanak, vagy értékes fájlokhoz jussanak hozzá és a felsorolást még lehetne folytatni. Végül az utolsó csoportba az ún. „grey hat” vagy szürke kalapos hackerek tartoznak, akik valahol az előző két csoport között helyezkednek el, de pontosan nehéz meghatározni és elhatárolni a tevékenységüket.

Ezen terminológiáknak a használata azonban vitatható. Például általában egyetértés van a tekintetben, hogy az etikus hackerek[58] tevékenysége a fehér kalapos csoportba tartozik, azonban éles vita tárgyát képezi az, hogy a tevékenységük mennyiben minősül jogosulatlannak vagy sem. Ezt tovább nehezíti, hogy nincs egy általánosan elfogadott szempontrendszer, ami alapján meghatározható, hogy ki tekinthető etikus hackernek. Ennek ellenére már megjelentek különböző információbiztonsági cégek a piacon, akik kifejezetten etikus hacker képzést kínálnak.

Ezekre tekintettel felmerül a kérdés, hogy egyáltalán a jogosultság hiánya esetén beszélhetünk-e etikus vagy „white hat hacking”-ről. Steven Furnell rámutat arra, hogy a „biztonság fejlesztése” érdekében végzett hacking megítélése esetén a főkérdés azaz, hogy mi történik a megszerzett információval. Amennyiben ezt a hacker diszkréten bejelenti a cégnek, akkor ez etikus hozzáállásnak tekinthető. Azonban, ha ettől eltérő módon – ami gyakori eset – a hacker a nagy nyilvánosság előtt tárja fel a biztonsági rést, akkor ez a részéről nehezen tekinthető etikusnak, különösen, mert ezzel felhívja figyelmet a rendszerben található hibára, de facto másokat felhív arra, hogy kihasználják a rendszer sebezhetőségét. Furnell szerint további kérdésként merül fel, hogy egy diszkrét bejelentés esetén is etikusnak tekinthető-e az,

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

hogy a rendszerbe valaki engedély nélkül belép, de mást valójában nem csinál. Álláspontja szerint a hacker jogosulatlanul hozzáférhet a rendszerhez anélkül, hogy bármit megváltoztatna vagy megzavarná a rendszer működését, de láthat olyan érzékeny információkat mint személyes adatot vagy üzletit titkot, amivel a sértett szempontjából hátrányt okozhat.[59]

Mindezek fényében a jogosulatlan belépések azon esetei, amelyek károkozási szándék nélkül történnek, azok jó példát szolgáltatnak a grey hat hacking-re. A fehér kalapos hacking pedig csak azokra az esetekre korlátozódik, amikor a hackerek valamilyen speciális vagy általános felhatalmazást kapnak erre vonatkozólag. Ezért mindenképpen fontos megkülönböztetni azokat, akik csak saját elhatározásból programhibákat keresnek, biztonsági intézkedéseket kijátszanak jogosultság hiányában, illetve azokat, akik erre jogosultak valamilyen formában (pl. az informatikai rendszer tulajdonosa megbízza őt a rendszer támadására és tesztelésére).

Mindezekre tekintettel a jogosulatlan belépés megvalósulhat már egyszerűen egy nem engedélyezett hozzáféréssel a rendszerhez vagy összetettebb módon is például, amikor az elkövetők egy számítástechnikai-hálózatot használnak fel arra, hogy távoli hozzáférést szerezzenek, mindez gyakran különböző joghatóság alá tartozó számítógépek közbeiktatásával történik. Ezek megvalósulhatnak felhasználó szintű műveletekkel, vagyis amikor az átlag felhasználónak megfelelő hozzáféréssel történik, vagy ún. „root level access", illetve „god level access" szintű hozzáféréssel, amikor ugyanazokkal a jogosultságokkal rendelkeznek mint a rendszergazda, és ezáltal lehetőségük van a rendszerben tárolt valamennyi fájl, adat megtekintéséhez és módosításához vagy program futtatásához. A szoftverek gyors ütemű fejlesztésének köszönhetően elkerülhetetlenek a programhibák, amiket az elkövetők sokszor kihasználnak mielőtt még ezeket a szoftverfejlesztők kijavítanák például különösen veszélyesek az ún. nulladik napi („zero-day") támadások, amelyek olyan, eddig nem ismert sebezhetőséget használnak ki, amiről még nem tudnak a programkészítők, valamint a felhasználóknak sincs tudomásuk róla.

Sokszor olvashatunk különböző esetekről, amikor felhasználói fiókokat (pl. e-mail, közösségi oldalak) törnek fel, azonban a jogosulatlan belépések többségének a célpontjai elsősorban a különböző nagyobb cégek vagy kormányzati szervek rendszerei és nem a magánszemélyeké.

Az elkövető célja továbbá az is lehet a több számítógéphez való jogosulatlanul belépéssel, hogy a közbeiktatásuk révén elrejtse a személyazonosságát és a bűncselekmény elkövetésének

[59] GILLESPIE: i.m. 44-45. o.

a helyét vagy más büntetendő cselekményeket így gyermekpornográfia tartalmakhoz való hozzáférését, spam küldést, amire különösen alkalmasak a nyilvános Wi-Fi hozzáférési pontok.[60]

Az információalapú társadalmakban a vállalatok számára az egyik a legnagyobb értékke 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).[61]

Az egyes hacking-jellegű cselekmények mögött tehát különböző motivációk húzódnak, de leggyakrabban a következők: hozzáférés az információhoz, az adat megváltoztatása, illetve törlése, valamint az információs rendszer használata.[62]

Az ilyen típusú támadásokat azonban leggyakrabban az szenzitív, értékes adatok jogosulatlan megszerzése vezérli. Az ellopott adatokkal a sértetteket zsarolhatják, különösen, ha szellemi tulajdon részét képezik. Más esetekben az adatokat (pl. e-mail címeket, felhasználói fiók adatokat) további csalás jellegű tevékenységekhez használják fel mint például adathalászathoz. A legtöbb esetben személyes adatokat szereznek meg, majd pénzügyi adatokat és egyészségügyi adatokat. Például jellemző az alábbi információk megszerzése: név és születési idő, telefonszámok, e-mail címek, felhasználói adatok[63], jelszavak és bankkártya adatok.

A Yahoo adatait – felhasználóneveket, jelszavakat – nem egyszer, hanem kétszer is sikerült megszerezniük az elkövetőknek. 2014 szeptemberében félmilliárd felhasználó adatai kerültek nyilvánosságra, míg előtte, 2013 augusztusában egymilliárd felhasználó adatai szivárogtak ki.[64]

A 2018-as Cambridge Analytica botrány felelősei a Facebook 87 millió felhasználójának adataival élhettek vissza, ebből 2,7 millió uniós állampolgár volt érintett.

Azonban a büntetőjogi rendelkezéseken kívül fontos említést tenni a személyes adatok védelmével kapcsolatban az EU Általános Adatvédelmi Rendeletéről (a továbbiakban:

[60] CLOUGH: i.m. 37. o.
[61] AMBRUS István – FARKAS Ádám: Whistleblowing és büntetőjog – szempontok a vállalati visszaélések megítéléséhez. Magyar Jog 2017/7-8. 442-443. o.
[62] CLOUGH: i.m. 33. o.
[63] http://www.europarl.europa.eu/news/hu/headlines/society/20180418STO02004/facebook-cambridge-analytica-botrany-zuckerberg-valaszoljon-az-europaiaknak [2018.07.21.]
[64] https://www.bbc.com/news/technology-47044652 [2019.03.05.]

GDPR)[65], amely nem csak az adatbiztonságot javítja, hanem egységes és egyértelmű szabályokat nyújt a cégek számára is az Unió egész területén.

A GDPR-t - uniós rendelet révén - a tagállamoknak közvetlenül alkalmazniuk kell. Magyarországon a nyitva hagyott egyes területek szabályozását az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotörvény.) átfogóan módosított változata biztosítja.

A GDPR 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.

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, így 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.[66] Az adatvédelmi incidenst haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő hetvenkét órán belül kell bejelenteni az illetékes felügyeleti hatóságnak.[67] Amennyiben ezt elmulasztják az érintett vállalkozások, akkor súlyos bírságokkal sújthatják őket. Például

[65] 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.
[66] 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.
[67] Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság jár el.

legfeljebb 20 millió euró összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeggel szankcionálhatóak. A kettő közül a magasabb összeget kell kiszabni.

3.2. A jogosulatlan belépés uniós szintű szabályozása

A Budapesti Egyezmény értelmében a jogosulatlan belépés bűncselekményét követi el az, 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 vagy fájl küldés, ellenben a bűncselekményt valósítja meg, aki olyan számítógépbe lép be, ami a nyilvános telekommunikációs hálózatra csatlakozik vagy ugyanazon hálózaton belül található, mint ilyen a helyi hálózat (LAN) vagy intranet egy szervezeten belül. E tekintetben a kommunikáció módja közömbös (pl. lehet az vezetékes vagy vezeték nélküli, illetve bluetooth stb.). A szerződő felek kiköthetik, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy számítástechnikai adatok megszerzésére irányuló, illetőleg más tisztességtelen céllal, avagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.[68]

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). Azonban nem büntetendő az, amikor a számítástechnikai rendszerhez ingyenes és nyilvános hozzáférés áll rendelkezésre.

Az információs rendszerek elleni támadásokról szóló irányelv értelmében jogosulatlannak minősül az 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.

[68] COUNCIL OF EUROPE: Explanatory Report to the Convention on Cybercrime. European Treaty Series – No. 185. 2001. 9-10. o.

Azonban az irányelv nem állapít meg büntetőjogi felelősséget abban az esetben, ha a bűncselekmény objektív kritériumai teljesülnek, de a cselekményt nem jogsértő szándékkal követték el, például ha az érintett személy nem tud arról, hogy az adott hozzáférés jogosulatlan, vagy ha az információs rendszerek tesztelésével vagy védelmével bízták meg (pl. ha egy társaság vagy egy forgalmazó kijelöl valakit a biztonsági rendszerének a tesztelésére). Az irányelvvel összefüggésben 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. Az irányelv 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 törvénykönyvekbe 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.[69] Rövid időn belül azonban egy új és önálló tényállás megalkotása vált szükségessé és így lett a számítógépes csalás a régi Btk. 300/C. §-ába 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. Újabb, jelentős változásokat az 1999. évi CXX. törvény hozott, mert a nagy nyilvánosság általános részi fogalmát kiterjesztette az elektronikusan rögzített információ távközlő hálózaton való közzétételére is.

[69] BH 1989/184.

Végül a Budapesti Egyezményben foglalt büntetőjogi rendelkezésekkel összhangban léptette életbe a számítástechnikai rendszer és adatok elleni bűncselekmény (régi Btk. 300/C. §), valamint a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása elnevezésű bűncselekményeknek a tényállását a 2001. évi CXXI. törvény, amely koncepcionálisan új szabályozást teremtett meg. Ezek a bűncselekmények azonban ekkor még a gazdasági bűncselekmények fejezetében (XVII. fejezet) kerültek szabályozásra, azonban ez a megoldás nem juttatta megfelelően kifejezésre a védendő értékek sokféleségét. A számítógépes csalás helyébe iktatott új tényállás – az új formában megjelenő számítógépes csalás mellett – 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.[70] Az értelmező rendelkezésben meghatározásra került a számítástechnikai rendszer fogalma is.

Az informatikai bűncselekményeknek a külön törvényben történő szabályozási megoldástól eltérően az országok többsége a nemzeti büntető törvénykönyvébe szabályozza az új típusú bűncselekményeket vagy egy önálló fejezetben (pl. Franciaország) vagy a különös részben szétszórtan elhelyezett tényállásokkal (pl. Németország).

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.[71] Erre egészen az új Btk.-ig kellett várni, amely már az uniós irányelvnek megfelelően – eleget téve a jogharmonizációs kötelezettségnek – átalakította a kiberbűncselekményekre vonatkozó szabályozást mind elnevezésben és mind tartalmilag, mert külön a XLIII. fejezetbe kerültek a „A tiltott adatszerzés és információs rendszerek elleni bűncselekmények" címmel, illetve a korábbi „számítástechnikai rendszer" terminológia helyébe az „információs rendszer" lépett.

A Btk. a 423. §-ban szabályozza a tisztán informatikai bűncselekménynek minősülő információs rendszer vagy adat megsértését.

Az információs társadalom jellemző indikátora, az infokommunikációs eszközök általános elterjedtsége és használata, amely változásokat eredményezett szinte valamennyi társadalmi

[70] 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.
[71] NAGY (2009): i.m. 61. o.

viszony területén. Az informatikai környezet egyrészt a már létező társadalmi értékek új szféráját, másrész egészen új a büntetőjog által védett értékeket hozott létre.[72]

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.[73] 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.[74]

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 tehát ma is a rongálás törvényi tényállása látja el.[75]

A törvény három külön fordulattal határozza meg a bűncselekmény elkövetési magatartásait és valamennyi fordulatának az elkövetési tárgya az információs rendszer, amelynek a betöltött funkciója a meghatározó.[76] Információs rendszer minden olyan berendezés - vagy egymással kapcsolatban lévő ilyen berendezések összesége -, amely automatikusan végez adatfeldolgozást, azaz adatok bevitelét, kezelését, tárolását, továbbítását látja el.[77] 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.).[78]

A Btk. 423. § (1) bekezdése a hacking-jellegű cselekményeket hivatott szabályozni. E bekezdés értelmében büntetendő, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a

[72] SZATHMÁRY (2012): i.m. 16. o.
[73] 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.
[74] 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.
[75] 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.
[76] 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.
[77] Btk. 459.§ (1) bekezdés 15. pont
[78] MOLNÁR (2016): i.m. 946. o.

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 az ezen keresztül elérhető védett számítógépes hálózatra (pl. intézményi belső hálózat, ún. intranet vagy az internet részét képező hálózat mint ilyen egy banki hálózat stb.).

A bűncselekmény megállapításához szükséges, hogy az információs rendszer technikai intézkedésekkel biztosított védelemmel legyen ellátva és ez a védelem aktív legyen, azaz rendelkezzen például felhasználói azonosítóval és jelszóval, tűzfallal vagy egyéb védelemmel. Tehát nem jogosulatlan a belépés abban az esetben, ha az információs rendszer nem védett, illetve a védelem nincs aktiválva, mert ezek konjuktív feltételek.[79] Emellett meghatározásra került az elkövetési mód is, így a bűncselekmény megvalósul akkor, ha a belépés a védelmi intézkedés megsértésével vagy kijátszásával történik például a biztonsági rendszer hiányosságait kihasználva lép be jogosulatlanul vagy a jogosult jelszavával vagy belépési kódjával, amelynek megszerzési módja azonban közömbös (pl. megtévesztéssel, kifürkészéssel, kódtörő programmal, social engineering, vagyis pszichológiai manipulációval vagy a felhasználó hanyagsága folytán jut hozzá az elkövető).

A jogosulatlan belépés esetén a német büntető törvénykönyv (a továbbiakban: StGB) 202a. §-a is hasonlóan szabályozza a hacking magatartásokat és abban az esetben szankcionálja, ha a rendszer technikai védelemmel volt ellátva és ennek kijátszásával férnek hozzá.[80]

A kiberbiztonságban a leggyengébb láncszem az ember, mert sokszor a sikeres támadás a sértetti közrehatásnak köszönhető, ezért az elkövetők előnyben részesítik a social engineering támadásokat – mint például az adathalászatot (phishing) – a technikai-technológiai megoldások helyett. Kevin Mitnick szerint a pszichológiai manipuláció a technológiai akadályokat (pl. tűzfalat vagy egyéb védelmet) könnyedén megkerüli a manipuláció, befolyásolás és megtévesztés segítségével.[81]

[79] NAGY (2014): i.m. 594-595. o.

[80] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany

[81] 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."

Nem célzatos bűncselekmény, ezért nem feltétele az elkövetésnek az sem, hogy haszonszerzési, károkozási vagy egyéb hasonló célzattal történjen. Az sem feltétele, hogy az információs rendszerben tárolt adaton az elkövető később bármilyen műveletet végezzen, vagy a rendszer működését akadályozza. A jogosulatlan belépés után megvalósított további jogosulatlan műveletek – például adatok törlése – már a következő bekezdések egyik fordulatát valósítják meg, amelybe a jogosulatlan belépés vétsége beolvad a súlyosabb jogtárgysértésre figyelemmel.[82]

A jogosulatlan belépésnek egy tipikus esete az ún. „wardriving" vagy „wireless hacking", amikor a vezeték nélküli hálózatot használják jogosulatlanul. A Wi-Fi kapcsolatok kialakításának több formája van: vannak a nyilvános hálózatok, amelyekhez bárki szabadon csatlakozhat, mindenféle korlátozás nélkül. Nyilvános, de zárt hálózatok is lehetnek, amelyek esetében egy speciális szoftver gondoskodik arról, hogy a hálózatot egy kód ismeretében lehet használni korlátozott ideig. Emellett vannak privát hálózatok, amelyek esetében a hozzáférést titkosítás, 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 a számítógépes 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"[83], ha a hálózat aktív védelemmel van ellátva és ezt sérti meg, különben nem.[84]

A jogosulatlan belépéssel kapcsolatban érdemes az etikus hacking kérdését is vizsgálni, különösen, mert az elmúlt években pár hazai esetre is fény derült, amelyek éles vita tárgyát képezték.

Az első eset során egy 18 éves fiatal 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 nem került sor, mert az ügyészség megállapította, hogy a célja valóban a biztonsági rés feltárása és ennek közlése

[82] SZATHMÁRY Zoltán: A számítástechnikai bűncselekmények és rendszertani elhelyezésük. Jogtudományi Közlöny 2012/4. 173-174. o.
[83] Lásd BLUTMANN László - KARSAI Krisztina - KATONA Tibor: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? Bűnügyi Szemle, 2008/1. I. évfolyam 1. szám 42-49.o.
[84] NAGY (2009): i.m. 272-273. o.

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 minősült, ami büntethetőséget kizáró ok.[85]

A második esetben egy programozónak tanuló hallgató a Magyar Telekom oldalán található nyilvános dokumentumban talált információs alapján jutott hozzá egy rendszergazdai jelszóhoz, amellyel hozzá tudott férni a Telekom teljes belső hálózatához, amely biztonsági résről tájékoztatta a céget és ezt követően további, újabb sebezhetőséget találva lépett be a cég rendszerébe. Ezután a Telekom ismeretlen tettes ellen tett feljelentést. Az ügyészség vádat emelt az információs rendszer megsértéséért, és mivel a „meghackelt" szerver a hírközlő hálózat része volt, ezért a Btk. 459 § (1) bekezdés 21. pontja alapján közérdekű üzemnek minősül, így e bűncselekmény minősített esetéért.[86]

A bírónak a konkrét esetben joga van megvizsgálni, hogy a törvényi tényállást kimerítette-e az illető, valamint van-e olyan társadalmilag fontos és méltányolható érdek, ami miatt a cselekményének a jogellenessége hiányzik, 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 vizsgálat tárgyává teheti például azt is, hogy a terhelt eljárása tekinthető-e közérdekű bejelentésnek-e vagy sem.[87] 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 céljából realizálja magát az elkövetési magatartást. A közérdekű bejelentés javaslatot is tartalmazhat.[88]

Áttérve a jogosulatlan belépés második fordulatára, ami akkor valósul meg, ha az elkövető az engedélyezett belépést követően a jogosultságának terjedelmi vagy időbeli kereteit

[85] https://jogaszvilag.hu/napi/bkk-botrany-fellelegezhet-az-etikus-hacker/ [2017.11.21.]
[86] http://ugyeszseg.hu/valasz-a-tarsasag-a-szabadsagjogokert-tasz-etikus-hacker-ugyeben-tett-allitasaira/ [2019.02.05.]
[87] 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.]
[88] 2013. évi CLXV. törvény a panaszokról és a közérdekű bejelentésekről 1. § (3) bekezdése

meghaladja, illetve a jogosultságot más módon megsérti az információs rendszerben való bennmaradással szándékosan. E fordulat alaki bűncselekményt határoz meg.[89]

A bűncselekmény alanya az első fordulatban a belépésre jogosulatlan személy lehet, míg a második fordulat esetén a belépésre jogosult személy.

A Kúria kimondta, hogy a büntetőjog alapelveivel összhangban a jogosultság keretein való túllépés is akkor minősül bűncselekménynek, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik (pl. más jelszavának a felhasználásával), ugyanis akkor, ha valakinek van jogosultsága az információs rendszerbe történő belépéshez, akkor pusztán e jogosultság kereteinek túllépése nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván. Tehát önmagában a jogosultság kereteinek túllépésével való belépés vagy bennmaradás nem büntetendő, amennyiben nem valamely biztonsági intézkedés megsértésével valósul meg, vagy nem kapcsolódik össze semmilyen további 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.[90]

Ezzel kapcsolatban Parti Katalin azon a véleményen van, hogy önmagában a jogellenes belépéseket elegendő lenne szabálysértésként szankcionálni.[91]

Miután az I. r. vádlottat cselekményénél haszonszerzési célzat nem vezette és a személyes adattal visszaélve jelentős érdeksérelmet sem okozott, a III. tényállási pontban írt bűncselekményének minősítése is helyes. Ezért a másodfellebbezés e körben sem vezetett eredményre, ennélfogva ebben a vonatkozásban is a másodfokú bíróság ítélete helybenhagyásának van helye.

---

[89] 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.
[90] BH 2017.12.392.
[91] PARTI Katalin: Gondolatok a számítástechnikai adatok és rendszerek elleni bűncselekmények tényállásairól. Büntetőjogi Kodifikáció 2005/2. 38. o.

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 hozzáférhetőek. A Kúria megállapította, hogy a személyes szívességtétel okán az információs rendszerbe belépési jogosultság kereteinek túllépésével való belépés vagy bennmaradás - és az ezúton történő 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 jogtalan haszonszerzésre is irányul – a specialitás elve alapján – e magatartásával a személyes adattal visszaélés bűncselekményét valósítja meg, méghozzá annak a 219. § (4) bekezdésében szabályozott minősített esetét.[92]

Összeségében elmondható, hogy a személyes adattal visszaélés bűncselekménye a jogtalan haszonszerzés vagy a jelentős érdeksérelem megléte esetén[93], míg a hivatali visszaélés bűntette a jogtalan előny vagy jogtalan hátrány célzat fennállásakor állapítható meg.

Jogtalan 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.[94]

3.4. A jogosulatlan belépéssel összefüggő bűncselekmények köre 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)]. A törvény azonban a „jogosulatlan hozzáférés" (unauthorised access) fogalmát nem határozza meg. Annak ellenére, hogy elfogadott álláspont az, hogy a hozzáférés nem csak szigorúan véve a „belépést" foglalja magában, hanem többek között a számítógép használatát is.

A CFAA általában a „jogosulatlan hozzáférés" keretében azokat az eseteket szabályozza, amikor az elkövetők mint „külső" vagy „kívülálló" személyek („outsiders") követik el a bűncselekményeket mint például a hackerek, míg a „jogosultság kereteinek túllépésével"

[92] BH 2015.11.296.
[93] A különleges adatra vagy bűnügyi személyes adatra elkövetve a bűncselekmény minősített esete valósul meg.
[94] Kúria Bfv. I. 1.357/2014/11.

elkövetett magatartások esetén „belső” személyekről („insiders”) van szó mint például az alkalmazottakról. A megkülönböztetés alapját a rendszerhez való hozzáférési jogosultság jelenti. Azok a személyek, akik hozzáférési jogosultsággal rendelkeznek a számítógéphez, általában büntetőjogi felelősségre akkor vonhatók, ha szándékosan okoznak kárt, nem pedig gondatlanságból. Ezzel szemben a kívülállók akkor is büntethetők a szándékos károkozáson kívül, ha gondatlanságból okoznak kárt.[95]

Fontos, hogy a bűncselekményeket megalapozó hozzáférésnek jogosulatlannak kell lennie. Ennek alapját a Budapesti Egyezmény képezi, melynek értelmében ez azt jelenti, ha az adott magatartást a tulajdonos vagy egyéb jogosult engedélyezi, akkor nem valósul meg bűncselekmény a jogosulatlanság meglétének hiányában. A pontos terminológia különbözhet országonként, de a főbb jellemzők megegyeznek.

A hozzáférésnek a korlátozása vagy megtagadása két módon történhet: technikai védelem (code-based restriction) vagy szerződés (contract-based restriction) alapján.[96] 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, mely alapján a tulajdonos határozza meg a hozzáférés feltételeit, mely történhet formálisan vagy informálisan, valamint kifejezetten vagy hallgatólagosan. Például ilyen lehet a munkaszerződés, használati feltételeket tartalmazó szabályzat. A szerződéssel történő korlátozás nagymértékben attól függ, hogy a szerződési feltételek mennyiben vannak pontosan és részletesen meghatározva.

Orin Kerr azzal a hasonlattal él, hogy a kettő között a különbség úgy ragadható meg, hogy a kód-alapú korlátozás esetén olyan mintha 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”.[97]

További kérdéseket vet fel az is, ha egy alkalmazottat elbocsátanak – egyúttal a jogosultságát is megvonják -, és ezt követően fér hozzá a cég rendszeréhez. Például ez történt a United States vs. Shahulhameed ügy során, amikor a Toyota Motors elbocsátotta az informatikus

[95] U.S. DEPARTMENT OF JUSTICE: Computer Crime and Intellectual Property Section Criminal Division: Prosecuting Computer Crimes. 2014. 5-6 o.
[96] 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.
[97] KERR (2003): i.m. 1662-1663. o.

alkalmazottját, azonban még a céges 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.[98]

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.[99]

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 volt 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 stb.

A legvitatottabb kérdésként merül fel, hogy vajon az adott személy túllépi-e a jogosultságainak a keretét, ha nem megfelelő céllal fér hozzá a számítógéphez. Ez különösen három esetben gyakori, ha:

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

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

(2) 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 ha az érintett személy ugyan aláírt korábban egy titoktartási szerződést a sértettel, amelyben hozzájárult ahhoz, hogy nem használja fel a sértett információját személyes haszonszerzésre, azonban a megállapodás nem tiltotta meg

[98] KERR, Orin S.: Computer Crime Law. Fourth Edition. West Academic Punlishing 2018. 48-51. o.
[99] KERR (2018): i.m. 37. o.

kifejezetten, hogy hozzáférjen a sértett számítógépes rendszeréhez. Tehát korlátozva lett az információ személyes felhasználása, de az nem, hogy az illető jogosultsága nem terjed ki a számítógépen található adatok megszerzésére vagy módosítására.[100]

3.4.1. Nemzetbiztonsági információ megszerzése (Obtaining national security information)

1030.§ (a)(1) bekezdés értelmében nemzetbiztonsági információ megszerzésének bűntette miatt büntetendő, „aki tudatosan, jogosulatlanul hozzáfér a számítógéphez vagy jogosultságainak kereteit túllépi azzal a céllal, hogy nemzetbiztonsági információt megszerezzen, és okkal feltételezhető, hogy az információ arra használható, hogy az Egyesült Államoknak kárt okozzon vagy más idegen nemzetet előnyhöz juttasson és ezért szándékosan közli, átadja, továbbítja vagy ezekre kísérletet tesz rá, vagy visszatartja az információt."

Ezen bűncselekmény megvalósulásához bizonyítani kell azt, hogy az elkövető tudatosan jogosulatlanul vagy jogosultságainak keretei túllépve fért hozzá a számítógéphez. A jogosultság terjedelme ügyenként eltérhet. Azonban érdemes megemlíteni, hogy azok a számítógépek vagy számítógép-hálózatok, amelyek nemzetbiztonsági információt tárolnak általában titkosítottak, valamint rendelkeznek megfelelő védelemmel és a hozzáféréssel kapcsolatos belső szabályzattal, ezért önmagában az is elegendő lehet, ha ezeket az elkövető megsértette.

Bizonyítani kell emellett azt is, hogy a megszerzett információ felhasználható az Egyesült Államokkal szemben, ehhez elegendő annak a bizonyítása, hogy minősített vagy korlátozott (classified vagy restricted) nemzetbiztonsági információ volt a bűncselekmény elkövetés tárgya és az elkövetőnek tudomása volt erről.

Végül az 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.[101]

3.4.2. Számítógéphez való hozzáférés és információszerzés (Accessing a computer and obtaining information)

A 1030.§ (a)(2) bekezdése értelmében, „aki szándékosan, jogosulatlanul hozzáfér a számítógéphez vagy jogosultságainak kereteit túllépve információt megszerez:

[100] U.S. DEPARTMENT OF JUSTICE: i.m. 8-11. o.
[101] U.S. DEPARTMENT OF JUSTICE: i.m. 12-16. o.

(A) pénzintézet pénzügyi nyilvántartásából vagy fogyasztóvédelmi szervtől;

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

(C) védett számítógépről, akkor az a számítógéphez való hozzáférés és információszerzés vétsége miatt büntetendő.

Aki gazdasági előnyért, anyagi haszonszerzésért, vagy más bűncselekmény, tiltott cselekmény elősegítése érdekében követi el bűncselekményt vagy 5,000$ értéket meghaladó információt szerez meg bűntett miatt büntetendő."

A jogosulatlan belépések sérthetnek több pontot is, például egy szövetségi szerv számítógépébe „betörés" megsérti a (B) pontot és a (C) pontot is.

1030. § (a)(2) bekezdés szerinti alapesetben nincs egy monetáris küszöbérték meghatározva, mert 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 nyilvántartási rendszerből. Azonban, ha az 5,000$ értéket eléri, akkor vétség helyett bűntett miatt vonható felelősségre.

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 szükséges, és nem történhet tévedés, figyelmetlenség vagy gondatlanság következtében.

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 a középpontjában a számítógéppel való visszaélés, a jogosulatlan hozzáférés áll.

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 vagyonilletőségébe tartozó hivatal beletartozik.

A bűncselekményt a törvényhozó vétség miatt pénzbüntetéssel és/vagy egy évig terjedő szabadságvesztéssel rendeli büntetni. Amennyiben a minősített esetek közül legalább egy megvalósul, vagyis az elkövető gazdasági előnyért, anyagi haszonszerzésért, vagy más bűncselekmény, tiltott cselekmény elősegítése érdekében követi el bűncselekményt vagy

5,000$ értéket meghaladó információt szerez meg, akkor bűntett miatt pénzbüntetéssel és/vagy öt évig terjedő szabadságvesztéssel büntethető.[102]

3.4.3. Behatolás kormányzati számítógépbe (Tresspassing in a government computer)

Ez azt az esetkört hivatott szabályozni bűncselekményként, amikor kívülállók hatolnak be szövetségi kormányzati számítógépekbe, még akkor is, ha közben nem szerzik meg az információt. A 1030. § (a)(3) bekezdése szerint büntetendő, „aki szándékosan, jogosulatlanul hozzáfér bármely 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."

A bűncselekmény elkövetési tárgya kizárólag az ún. „nem nyilvános" (nonpublic) számítógép lehet, amely magában foglalja a kormányzati számítógépeket, de például azokat a kormányzati szervereket nem, amelyek (köz)szolgáltatást nyújtanak a lakosság számára (pl. ilyen a kormányzati webszerver). Ezenkívül a számítógép a kormány tulajdonát kell, hogy képezze vagy legalább a kormány használja, vagy az érdekében használják, erre jó példa az, ha az Egyesült Államok egy fiókkal rendelkezik egy magáncégnek a szerverén, akkor azt már az Egyesült Államok használja és a bűncselekmény elkövetésének a tárgyát képezheti, annak ellenére, hogy nem a saját tulajdona.

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

Mindezek alapján a bűncselekmény elkövetői csak a „kívülálló" személyek lehetnek az adott kormányzati szervre tekintettel. Ez abból következett, hogy a Kongresszus 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 az már e szakasz értelmében büntetendő.

A törvény e bűncselekmény elkövetőjét pénzbüntetéssel és egy évig terjedő szabadságvesztéssel rendeli büntetni. Amennyiben visszaeső és korábban már elítélték valamely 1030. §-ban szabályozott bűncselekményért, akkor a törvényi maximum tíz évig terjedő szabadságvesztésre emelkedik.

[102] U.S. DEPARTMENT OF JUSTICE: i.m. 16-22. o.

Az esetek többségében a büntetendő cselekmények vonatkozásában átfedés mutatkozik a 1030. § (a)(2) és (a)(3) bekezdések között, ezért általában a (a)(2) bekezdése miatt indulnak büntetőeljárások.[103]

[103] U.S. DEPARTMENT OF JUSTICE: 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[104] (pl. e-mail fiókhoz, más banki vagy egyéb fiókokhoz való hozzáféréshez, 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.[105]

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 használatos a Distributed Denial of Service (rövidítve: DDoS), vagyis az elosztott szolgáltatásmegtagadással járó támadás elnevezés. 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.[106]

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.[107]

A felhasználó tudta nélkül megfertőzött számítógépeket, amelyek távolról irányíthatók „zombi”-nak nevezik. Másik elnevezésük a robot és network szavak összevonásából eredő „botnet”, amely a több bot összekapcsolásával keletkezett hálózatot jelenti. A botnet irányítóját,

[104] NAGY (2009): i.m. 115. o.
[105] http://www.cert-hungary.hu/ddos [2017.09.21.]
[106] GYÁNYI Sándor: Az információs terrorizmus által alkalmazott támadási módszerek és a velük szemben alkalmazható védelem. PhD értekezés tervezet. Budapest, 2011. 88. o.
[107] 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, „botmaster”-nek, illetve több irányító esetén „botherder”-nek nevezik. A botnet hálózat tagjait a fertőzött zombi számítógépek alkotják. Azt a központi vezérlő eszközt, amely vezérli a botnet-akciókat „controller”-nek hívják. A controller általában az ún. „drop server”-re csatlakozik, amely a botnet által gyűjtött adatok tárolására szolgáló tárhelyet jelenti, ami hozzáférhető a botnet hálózat tagjai és a botmaster részére is. A botmaster és botnet közti kapcsolatot és az utasítások eljuttatását biztosító kommunikációs útvonal az ún. Command&Control (C&C) szerver.[108]

A botnetek a kiberbűnözői infrastruktúrának az alapját képezik, mérhetetlen erőforrást biztosítanak számukra a rendelkezésre álló számítógép kapacitás és sávszélesség tekintetében.[109] A botnetek a DDoS-támadások indításán kívül alkalmasak spamküldésre, adathalászatra, hálózat-figyelésre, billentyűzet-figyelésre, különböző rosszindulatú programok, ún. „malware”-k (pl. 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, melynek 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,[110] bár az Europol felhívja a figyelmet arra, hogy ezek a nagyszabású támadások már könnyen megvalósíthatók kisebb számú, de ellenállóbb botnetekkel is.[111] Kezdetben 100 Gbps támadások voltak megfigyelhetők, napjainkra a 300 Gbps-ot is meghaladja, sőt az Europol jelentése szerint 600 Gbps támadásra is sor került és 24 óránál tovább is tarthatnak.[112]

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 a számítógépes hálózatra történő csatlakozással már ki vannak téve a veszélynek, a kockázat pedig különösen megnövekedett az új mobilinformatikai és Internet of Things (IoT) eszközök elterjedésével,

---

[108] GYÁNYI (2011): i. m. 89. o.

[109] 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.]

[110] GYÁNYI Sándor: A botnetek, a túlterheléses támadások eszközei. Magyar Rendészet, 2013. Különszám, 24. o.

[111] EUROPEAN PARLIAMENT'S POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS: i.m. 36. o.

[112] EUROPOL: The Internet Organised Crime Assessment (IOCTA) 2016. 35. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 [2017.10.24.]

főleg azért, mert utóbbinak még nincs megfelelően biztosított informatikai védelme (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).[113]

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

A túlterheléses támadások mögött húzódó motivációk általában különböznek. A támadást indíthatják anyagi haszonszerzés céljából (pl. zsarolás során használják fel). Emellett történhet egyéb gazdasági vagy károkozási céllal 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 - így ezáltal 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 weboldal üzembentartója számára legyen szó kis- és középvállalkozásról vagy nagyobb cégről. A támadással járó pénzügyi veszteség esetenként különbözhet és nem kizárt, hogy az megtámadott vállalkozás működésére hosszútávon is hatással lehet. Ez megnyilvánulhat a kieső és pótolhatatlan bevételben, illetve akár presztízsveszteséget is okozhat, mivel az ügyfelek nem tudják elérni a támadással célzott cég honlapját, sem igénybe venni a cég által kínált szolgáltatást, ezért inkább a konkurens vállalkozásokat választják és lemorzsolódnak az adott cégtől (pl. a pénzügyi ágazaton belül, különösen az értéktőzsde, értékpapír kereskedés piacán ez pillanatok alatt súlyos és jelentős kárt okozhat).[114]

A túlterheléses támadások hátterében politikai vagy ideológiai indíttatás is állhat, amit az ún. hacktivizmus[115] 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 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 azaz

[113] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf [2017.11.05.]
[114] URCUYO, Michael S.: From Internet trolls to seasoned hackers: protecting our financial interests from Distributed-Denial-Of-Service attacks. Rutgers Computer & Technology Law Journal Vol. 42., 2016, 300–330. o.
[115] A hacktivizmus, avagy a „hactivism" elnevezés a „hacking" és az „activist" szavak összevonásából ered.

„defacement”-tel, információk jogosulatlan megszerzésével, illetve azok későbbi nyilvánosságra hozatalával, vagy egyéb virtuális szabotázs akciókkal).[116]

A túlterheléses támadások szolgálhatják a kiberhadviselést[117] 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[118] (pl. az Egyesült Államok Védelmi Minisztériuma 2010-ben létrehozta a katonai Kiberparancsnokságot, míg Kína és Oroszország tagadja, hogy rendelkeznének kiberhadsereggel[119]). 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 hatalmas küzdelem folyt. Azonban ezeknek a támadásoknak a forrása még mindig vita tárgyát képezi, bár a rendelkezésre álló bizonyítékok alapján Oroszországból érkezhettek, de egyértelműen a mai napig nem tudják megállapítani és a felelősségre vonást kezdeményezni.[120] 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 kereteket ad az informatikai hadviseléshez a nemzetközi jogban már meglévő rendelkezések megfelelő alkalmazásával.[121] Azonban ennek a részletes elemzése nem képezi az értekezés részét.

---

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

[117] Azt a jelenséget nevezzük kiberhadviselésnek, amikor egy állam egy másik állam ellen informatikai támadást indít, melynek célja az adott ország társadalmi és gazdasági működésének akadályozása vagy ellehetetlenítése. Ez általában egy átfogó támadássorozat, amelynek a kiterjedése és az okozott kár mértéke hatalmas és az egész ország működését veszélyeztetheti. 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.

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

[119] 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.

[120] 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.]

[121] 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.

4.2. A „malware” támadásokról általában

A támadások másik gyakori típusát a különféle ún. „malware'-k vagyis rosszindulatú programok képezik, amelyeket az elkövetők továbbíthatnak, 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 arra használják ezeket a kártevő programokat, hogy jogosulatlanul behatoljanak az információs rendszerekbe, vagy módosításokat végezzenek, kárt okozzanak az adatokban a felhasználó tudta és hozzájárulása nélkül, de egyre gyakoribb, hogy azzal a céllal használják fel ezeket, hogy bizalmas adatokhoz férjenek hozzá, amelyek elősegítik a további csalásokat vagy egyéb jogsértéseket (pl. zsarolás, személyazonosság-lopás stb.).[122]

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 függ, hogy milyen céllal készítik és telepítik azt. 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 használhatók 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) alkalmasak a billentyű leütések rögzítésére.

Az elkövetők gyakran számítógépes vírusokat és férgeket használnak. Előbbi képes önmagának a lemásolására és megfertőzni információs rendszereket, amelyhez szüksége van egy „hordozóra”, gazdagépre tehát lényegében úgy viselkedik mint egy biológiai vírus. A számítógépes férgek ezzel szemben önmagukat reprodukálják, a hálózatok hibáit, vagy hiányos biztonsági beállításokat használják fel, hogy terjeszkedjenek. Manapság a legveszélyesebb programok ebből a típusból kerülnek ki. Az önsokszorosításon kívül a férgek többféle dologra is programozhatóak. Egyik jellemző következményük, hogy hátsó ajtót (backdoor) nyitnak a rendszerekre, amin keresztül adatokat szereznek meg, illetve botnet hálózat részévé tehetik a megtámadott számítógépet.

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

A trójai programok ártalmatlannak tűnnek, - sőt sokszor más hasznos programnak álcázzák magukat, így a gyanútlan felhasználó saját maga tölti le ezeket - de rejtett káros tevékenységet végeznek anélkül, hogy önmagukat sokszorosítanák. A trójai is alkalmas lehet a hátsó ajtó létrehozására a megfertőzött rendszerben, amelynek köszönhetően a támadó átveheti az irányítást a rendszer felett (pl. akár a mikrofon és webkamera felett is).

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 (pl. pendrive) való rácsatlakozással, vagy az interneten, valamint más számítógép-hálózaton keresztül egy végrehajtható fájl segítségével. Gyakran e-mail mellékletként küldenek rosszindulatú programokat vagy weblap címet, 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 (pl. letöltés gombok).

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 teljesen elérhetetlenné téve azokat, majd rendkívül magas, akár milliós nagyságrendű váltságdíjat követelnek a helyreállító, titkosítást feloldó kódért cserébe. A szoftver fizetési határidőt is szabhat, melynek lejárta után akár végérvényesen elérhetetlenné teszik az adatokat. Az elkövetők kilétének megismerése szinte lehetetlen, mert általában a „váltságdíjat" a nehezen lenyomozható virtuális valutában, ún. kriptovalutában[123] – 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 vasútvállalat rendszerét blokkolta teljesen.[124] 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.

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

[124] 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.

Részben ennek a támadásnak köszönhető, hogy Kalifornia állam büntető törvénykönyvébe önálló bűncselekményként jelent meg a ransomware felhasználása.[125]

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, és bankkártya használata nélkül több millió dollárhoz jussanak.[126]

További kiberbiztonsági kockázatot 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 ezzel a céllal fejlesztették ki – és, ezáltal Irán atomprogramját lényegében megbénították, mert több év kellett ahhoz, hogy egy atomfegyver előállításához szükséges dúsított uránt legyártsanak. Ma már tudjuk, a Stuxnet csak az első ilyen eszköz volt a sorban, testvérei a Duqu, a Gauss vagy a Flamer bizonyítják ezt.[127]

4.2.1. A célzott támadások

Szükséges külön kitérni az egyik legveszélyesebb támadási formára az ún. „Advanced Persistent Threat", avagy APT támadásokra. Ezeket a magyar szakterminológia gyakran célzott támadásokként nevezi, mert nem véletlenszerű célpontokat, hanem tudatosan kiválasztott rendszereket (pl. államigazgatási, védelmi vagy pénzügyi szervezeteket, így bankokat, tőzsdei cégeket) támadnak. Ezek általában támadások sorozatát foglalja magába. Ezek a támadások nagyon jól előkészítettek és nagyon sokáig fennállnak észrevétlenül.[128]

Az utóbbi évek egyik legnagyobb APT-alapú támadássorozata az ún. „Carbanak" volt[129], amely során az elkövetők kifinomult módszerekkel megközelítőleg 1 milliárd dollárt szereztek meg közel 30 országból, több mint 100 különböző pénzintézettől és hónapokig észrevétlenül tudtak maradni a rendszereken belül. A nemzetközi bűnügyi együttműködésnek köszönhető, hogy a támadásra fény derült, mindez a rendvédelmi szervek és a magánszféra – a Kaspersky Lab, az Interpol és az Europol – közös munkájának az eredménye.

---

[125] https://www.bleepingcomputer.com/news/government/new-california-law-makes-ransomware-a-standalone-crime/ [2017.05.21.]
[126] https://www.theguardian.com/technology/2014/oct/08/cash-machine-atm-malware-tyupkin [2017.05.23.]
[127] 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.
[128] KOVÁCS László: A kibertér védelme. Dialog Campus Kiadó. Budapest, 2018. 151-153. o.
[129] 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

Az APT támadások életciklusa és eljárási módja (modus operandi) általában social engineering, főleg ún. „spear phishing" támadásokkal kezdődik, így ebben az esetben is a támadás a banki alkalmazottaknak küldött célzott adathalász e-maileken keresztül indult. 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 rendszerekhez való hozzáféréshez, valamint távoli hozzáférést biztosító szoftver telepítésére, amelynek köszönhetően az alkalmazottak képernyő aktivitását is megfigyelték, sőt ezt videón rögzítették is. A támadás összetettségére utal, hogy az elkövetők különböző módszereket alkalmaztak a jogtalan haszonszerzés érdekében:

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.

Emellett 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 az automatáknál vártak és elhoztak.[130]

4.3. A DDoS-támadásokat és vírusokat érintő rendelkezések az Európai Unióban

A Budapesti Egyezmény számítástechnikai adat megsértését (4. cikk) is szabályozza, amely 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.

Emellett a számítástechnikai rendszer megsértése (5. cikk) miatt büntetendő, aki a számítástechnikai rendszer működését a számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével, jogosulatlanul és szándékosan, jelentős mértékűen akadályozza.

[130] EUROPOL (2018): i.m. 23. o.

Az akadályozásnak jelentős mértékűnek kell lennie, azonban, hogy mi minősül ennek, azt a szerződő felek határozhatják meg szabadon. 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 lelassítják a működést vagy programok, amelyek óriási mennyiségű e-mailt küldenek a címzettnek annak érdekében, hogy akadályozza a kommunikációt).[131]

Az információs rendszerek elleni támadásokról szóló irányelv a rendszert érintő jogellenes beavatkozást (4. cikk) is meghatározza, 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.

Az irányelv az adatot érintő jogellenes beavatkozást (5. cikk) is 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 jogosulatlan hozzáférhetetlenné tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön.

Az irányelv először hívta fel a figyelmet a botnetekre mint veszélyforrásokra, mert felismerték, hogy általuk egyre veszélyesebb, ismétlődő és átfogó támadásokat tudnak végrehajtani, melyek gyakran kulcsfontosságú információs rendszereket (pl. kritikus infrastruktúrákat) érintenek. Az irányelv először állapít meg büntetőjogi szankciót a botnetek létrehozására, amelyek 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 egy bűncselekményt – az irányelv meghatározása szerint – bűnszervezetben követtek el, illetve az súlyos kárt vagy alapvető érdeksérelmet okozott. Büntetendő és súlyosabb szankció megállapításának van helye, ha a támadás átfogó, azaz jelentős számú információs rendszert érint vagy súlyos kárt okoz, ideértve azokat a

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

támadásokat is, amelyek célja egy botnet létrehozása, vagy amelyeket botnet révén hajtanak végre, és ezáltal súlyos kárt okoznak. Helyénvaló arra az esetre is súlyosabb szankciókat megállapítani, ha a támadás valamely tagállam vagy az Unió kritikus infrastruktúrája[132] ellen irányul. Ez azért indokolt, mert a kritikus infrastruktúrák egyes elemeinek működése, illetve együttműködése oly mértékben függnek az információs rendszerektől, hogy azok összeomlása vagy megsemmisülése súlyos következményekkel járhat nem csak az adott infrastruktúrára nézve, hanem más kritikus infrastruktúrákra nézve 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.).[133] Ezek védelme különösen fontos, mert a támadások érinthetik például az erőművek, vízellátó vagy újrahasznosító ún. SCADA rendszereit, vagyis az ipari vezérlő rendszereket.[134] Érdemes felhívni a figyelmet arra is, hogy az uniós rendvédelmi szervekhez bejelentett, kritikus infrastruktúrákat érintő támadások között a DDoS-támadások dominálnak és egyre gyakoribbak a célzott támadások.[135]

A számítástechnikai bűnözésre alkalmazott integrált megközelítés egy másik fontos eleme a személyazonosság-lopás és a személyazonossághoz kapcsolódó egyéb bűncselekmények elleni hatékony fellépés. Magyarországon ma még a személyazonosság-lopás önálló bűncselekményként nem jelent meg, de ez nem jelenti azt, hogy büntetlenül maradna ez a magatartás, mert a személyes adatokkal való visszaélést szankcióval fenyegeti a törvény. 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.[136] A német StGB. is más tényállások keretén szabályozza így a már tárgyalt phishing, valamint számítógépes csalás vagy a hagyományos csalás keretében (263. §).[137] Példaként említhető azonban az amerikai

[132] 2008/114/EK tanácsi irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. HL L 345, 23/12/2008, 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."

[133] MUHA Lajos: a Magyar Köztársaság kritikus információs infrastruktúrájának védelme. PhD értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007, 36-37. http://real-phd.mtak.hu/74/1/1228916.pdf [2017.12.19.]

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

[135] EUROPOL (2017): i.m. 26.

[136] KORINEK László: Tendenciák korunk bűnözésében, bűnüldözésében. MTA székfoglaló előadás, 2013. 44. o.

[137] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019.

szabályozás, amely önállóan nevesíti a személyazonosság-lopást (identity theft). Általában az egyes országok a másnak a személyazonossággal összefüggő információjának a jogosulatlan megszerzését, az azzal való kereskedést, vagy a hamis személyazonosságra vonatkozó információ létrehozását rendelik büntetni.[138]

Mindezekre tekintettel az irányelv 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 támadásokat 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 megfelelően figyelembe kell venni ezt. A tagállamoknak gondoskodniuk kell arról, hogy a bírók az elkövető elítélésekor figyelembe vehessék e súlyosító körülményeket. Továbbra is a bírók mérlegelési jogkörébe tartozik, hogy e körülményeket a konkrét esetek egyéb tényállási elemeivel együtt miként értékelik.

A tagállamoknak szankciókat kell megállapítaniuk az információs rendszerek elleni támadások esetére. E szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük, és szabadságvesztést és/vagy pénzbüntetést is magukban kell foglalniuk.

4.4. A DDoS-támadásról és vírusokról szóló rendelkezések hazai szabályozása

Az információs rendszerekben különböző módon tudnak kárt okozni: 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

[138] CLOUGH: i.m. 241. o.

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 a tényállásszerű eredmény, az akadályozás bekövetkezésével válik befejezetté a bűncselekmény. A bűncselekmény e fordulatát nem csak az adatok bevitelére, megváltoztatására, törlésére és egyéb műveletek végzésére jogosulatlan személy, hanem arra jogosult személy is elkövetheti, azonban ehhez feltétel, hogy a beavatkozást szándékosan nem a jogosultsága keretei között, nem a rendeltetésének megfelelően, hanem a reá vonatkozó rendelkezések megsértésével végezze.[139] A jogosulatlan akadályozásra a leggyakoribb esetként a DDoS-támadások említhetők. A honlaprongálás (defacement) is e fordulat szerint minősül, amikor 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, így ha az elkövető az információs rendszer adatfeldolgozás eredményét a vírusok becsempészésével tudatosan befolyásolja, hogy ezáltal a programok működésre képtelenné váljanak, akkor is megvalósítja ezt a fordulatot.[140]

A (2) bekezdés b) pontja szerint büntetendő, 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. E § alkalmazásában adat: „információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”

Érdemes közelebbről vizsgálni az elkövetési tárgyat az informatikai bűncselekmények tekintetében. 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

[139] MOLNÁR (2018): i.m. 948. o.
[140] BH 1999.145.

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 valóságban létező, tehát kézzel nem fogható elkövetési tárgyakat is mint a számítástechnikai adatot.[141]

A büntetendő cselekmény elkövetési magatartása 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.[142]

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.[143]

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.[144]

---

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

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

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.[145] 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.[146] A másik minősített eset esetén 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 az uniós irányelv szerint alkalmazott kritikus infrastruktúra fogalma[147] 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.

[145] MOLNÁR (2018): i.m. 950. o.
[146] NAGY (2014): i.m. 598. o.
[147] 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”.

Külön érdekesség, hogy a magyarországi botnetfertőzöttségre figyelmeztető 2015-ös Symantec-tanulmány szerint Magyarország a botnetvírussal 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.[148] 2016-ban pedig a magyar kormányzati informatikai rendszert és oldalakat is sorozatos DDoS-támadás érte, aminek köszönhetően több óráig nem voltak elérhetőek a különböző szolgáltatások.[149]

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.[150] Folytatólagosan elkövetett információs rendszer vagy adat megsértésének bűncselekménye állapítható meg, ha az elkövető egységes akaratelhatározásból az azonos helyzetből (hozzáférésből) fakadó lehetőséget kihasználva, azonos számítástechnikai rendszer sérelmével, különböző alkalmakkal követi el a vizsgált bűncselekményt.[151]

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.[152]

---

[148] Internet Security Threat Report. 2015/20.
https://www.symantec.com/content/en/us/enterprise/other_resources/
21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf [2017. 09. 05.]
[149] Lásd a Belügyminisztérium által közzétett jelentést: http://www.kormany.hu/hu/belugyminiszterium/hirek/
senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast [2017. 09. 09.]
[150] MOLNÁR (2016): i.m. 950-951. o.
[151] Legfelsőbb Bíróság Bf. II. 74/2008/5.
[152] MOLNÁR (2016): i.m. 951. o.

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, feltéve, ha a bűncselekményt egyenes szándékkal, magatartásának előre látott következményeit kívánva hajtja végre.[153]

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.[154]

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.[155]

A német StGB 303b. §-ában a számítógépes szabotázsként szankcionálja a DDoS-támadást, különböző rosszindulatú programmal megvalósuló támadást, valamint adatmanipulációt kimerítő magatartásokat, így az 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

[153] Legf. Bír. Bfv. II. 74/2008/5.
[154] EBH 2009.2033. II.; BH 2009.264. II.
[155] Szegedi Ítélőtábla Bf.I. 180/2006/3.

évig terjedő szabadságvesztéssel vagy pénzbüntetéssel büntethető. A kísérlet is büntetendő. Amennyiben ez más üzleti vállalkozásának, vállalatának vagy közműnek az adatfeldolgozó rendszerével szemben követi el, akkor a büntetés öt évig terjedő szabadságvesztés is lehet. 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 infrastruktúrát érint, akkor hat hónaptól tíz évig terjedő szabadságvesztés is kiszabható vele szemben.[156]

Az információs rendszerben végzett műveletekkel jogtalan haszonszerzés nélkül is kárt tudnak okozni, ezért úgy gondolom, hogy - mind az amerikai és a német szabályozásra is figyelemmel - indokolt lenne ennek egy külön fordulatba történő szabályozása az információs rendszer vagy adat elleni bűncselekménynél.

Az informatikai környezetben elkövetett bűncselekmények esetén 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.[157] További példaként említhető, azaz eset, amikor az elkövető akár egy önvezető járművet is az elkövetés eszközeként használhat, amennyiben a hacertámadás 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.[158] Emellett az élet kioltására alkalmasak lehetnek a hadászati céllal kifejlesztett drónok is, amelyek már arcfelismerő szoftverrel rendelkeznek, így könnyedén beprogramozhatóak 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 szerezni a felhasználókról, vagy akár gondoljunk egy okosotthonra, amelyet ugyanúgy érhet egy informatikai támadás mint bármely más informatikai eszközt, és ennek következében az elkövető áttudja venni az irányítást felette és különböző parancsokat

[156] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019.
[157] 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.
[158] AMBRUS István: Az autonóm járművek és a büntetőjogi felelősségre vonás akadályai. In: Mezei Kitti – Nagy Zoltán András (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK. Pécs, 2019. 10-11.o.

küldeni ezáltal alkalmas lehet a sértett megfigyelésére vagy akár az otthonába történő be vagy onnan a kizárására.[159] Az autólopás is új szintre lépett a technológiai újításoknak köszönhetően, mert már az sem példa nélküli, hogy nagy értékű autókat lopnak el úgy, hogy a kulcs nélküli indítórendszerüknek a védelmét már különféle jeltovábbító eszközökkel kijátsszák.[160]

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 a jogalkotó ezt az egyes bűncselekmények (pl. csalás, zsarolás esetén) minősített eseteként szabályozza.[161]

4.5. A számítógépben vagy információban történő károkozás (Damaging a computer or information) a CFAA-ban

A CFAA 1030. § (a)(5) bekezdésében kerül szabályozásra. „Az (A) pontban büntetendő vétségként, aki tudatosan továbbít programot, információt, kódot vagy parancsot, ezáltal szándékosan, jogosulatlanul kárt okoz a védett számítógépben.

A (B) pont büntetni rendeli szintén vétségként azt, aki szándékosan, jogosulatlanul hozzáfér a védett számítógéphez és gondatlanságból kárt okoz.

A (C) pontja szerint büntetendő, aki szándékosan, jogosulatlanul hozzáfér a védett számítógéphez és ezzel a tevékenységével kárt és veszteséget okoz.

Amennyiben az (A) és (B) pontban szabályozott bűncselekményeket úgy követik el, hogy az alábbi minősített eseteket valósítják meg, akkor bűntettként büntetendők:

(1) legalább az 5,000$ értékű veszteség egy év alatt;
(2) az egészségügyi ellátást akadályozza;
(3) valakinél fizikai sérelem következzen be;
(4) fenyegetést jelentsen a közegészségre és közbiztonságra nézve;
(5) az igazságszolgáltatásban, a honvédelemben, a nemzetbiztonságban használt számítógép sérelmére kövessék el;
(6) károkozás 10 vagy több védett számítógép sérelmére egy év alatt.”

A 1030. § (a)(5)(A) pontban szabályozott számítógépben vagy információban való károkozás vétsége, mely szerint büntetendő az, „aki tudatosan olyan programot, információt, kódot vagy parancsot továbbít, amellyel szándékosan és jogosulatlanul kárt okoz egy védett

[159] SCHJOLBERG, Stein: The history of cybercrime 1976-2014. Cybercrime Research Institute, 2014. 148-149. o.
[160] https://www.dailymail.co.uk/news/fb-5472209/How-thieves-steal-car-without-keys-The.html [2019.01.21.]
[161] VADÁSZ Viktor: A számítógép demisztikálása. Ügyészek Lapja 2010/2. 16. o.

számítógépben". A (B) pont büntetni rendeli szintén vétségként azt, „aki szándékosan, jogosulatlanul hozzáfér a védett számítógéphez és gondatlanságból kárt okoz". A (C) pontja szerint büntetendő, „aki szándékosan, jogosulatlanul hozzáfér a védett számítógéphez és ezzel a tevékenységével kárt és veszteséget okoz". A három szabályozott pont között a CFAA a károkozáshoz és a sértett számítógépéhez való hozzáféréshez kapcsolódó bűnösség és elkövetési magatartás alapján differenciál. Az (A) pont megtiltja, hogy bárki szándékosan (intentionally) és tudatos továbbítással kárt okozzon a védett számítógépben, míg a (B) pont azt, hogy jogosulatlanul hozzáférve, gondatlanságból („recklessly", ami a magyar büntetőjog-tudományban használatos tudatos gondatlansághoz hasonló fogalom) kárt okozzon, a (C) pont szerint pedig büntetendő az a felhasználó, aki gondatlanságból („negligently", ami leginkább a hanyag gondatlansághoz közelít) és jogosulatlanul hozzáférve kárt és veszteséget okoz. Az utóbbi két pontban meghatározott esetekben tehát, a szándékos és jogosulatlan hozzáférés a feltétel, amely alapján felelősségre vonható az elkövető, ha jogosulatlanul hatol be a számítógépbe, még akkor is, ha nem terjedt ki a szándéka a károkozásra. Ezzel ellentétben az (A) pontban szabályozott esetben csak a tudatos továbbítás és a szándékos károkozás a feltétele a bűncselekmény megvalósulásának, ami történhet a számítógéphez való hozzáférése nélkül is, például amikor a támadó elárasztja az egyik weboldalt olyan mennyiségű adatcsomaggal a DDoS-támadás révén, melynek eredményeképpen a honlap hozzáférhetetlen lesz, akkor a károkozás szándékos, azonban az elkövető a támadás során nem fér hozzá a honlaphoz. A 1030.§ (a)(5)(A) bekezdés szerint felelősségre vonható az, aki a DDoS-támadást végrehajtja, illetve az is, aki a rosszindulatú programot ilyen céllal felhasználja vagy továbbítja. Ez következik abból, hogy a DDoS-támadás általában magában foglalja a káros kód továbbítását, 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.[162] A bűncselekmény elkövetési tárgya a védett számítógép, amelynek fogalmát korábban már ismertettem.

Problémát jelent, hogy nincs egy kiforrott esetjogi háttere az ilyen típusú ügyeknek, ami abból is következik, hogy nehéz azonosítani és bíróság elé állítani az elkövetőket. Elsősorban nem a CFAA nyújt az ügyészek számára segítséget arra vonatkozólag, hogy hogyan folytassák le a túlterheléses támadás miatt elrendelt eljárást, hanem igazi útmutatást az Igazságügyi Minisztérium kézikönyve adhat. A 1030.§ (a)(5)(A) alapján az eljárás megindításához kettő feltétel megléte szükséges: a továbbítás, illetve a kár. A bűntettet megalapozó eljáráshoz még

[162] BRENNER, Susan W.: Cybercrime and the law: Challenges, issues and outcomes. Northeastern University Press, 2012. 49. o.

egy feltétel szükséges: a törvényben felsorolt minősített esetek közül legalább egynek meg kell valósulnia.

Az említett szakasz megtiltja a tudatos DDoS-támadás végrehajtását károkozási célzattal a védett számítógéppel szemben. A törvény szövegben szereplő „program, információ, kód vagy parancs" továbbítása tágan magában foglalja azokat az eseteket, amikor a továbbítás képes a számítógép működését befolyásolni. Ez magában foglalja a szoftver kódokat (pl. férget vagy vírust), parancsokat (pl. információ törlésére irányulót), és a hálózati adatcsomagokat, amelyek elárasztják a hálózatot vagy a rendszer sebezhetőségeit használják ki mint a DDoS-támadások. Az eljárás során bizonyítani kell, hogy a vádlott a továbbításért felelős személlyel megegyezik és fontos, hogy a továbbítás tényét is bizonyítsák, 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 megsértse ezt a rendelkezést (pl. az elkövető káros kódot helyezett el egy programba, ami a munkáltatója rendszerében futott és egy idő után aktiválta magát, további káros kódokat töltött le, és ennek következtében a többi alkalmazott által használt gépek is használhatatlanná váltak). A következő feltétel, hogy az elkövető kárt okozzon a számítógépben, ami magában foglalja az információ vagy számítógép hozzáférhetetlenné tételét. A kár fogalma 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 lelassulást 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. Kár következik be, amikor 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 rendszer naplófájljaihoz vagy a bank adatbázisában módosítanak az egyenlegen). Ugyanúgy kár keletkezik, ha a számítógép működését változtatják meg (pl. keylogger telepítése az otthoni számítógépre) vagy, ha az információt vagy a számítógépet elérhetetlenné teszik. Emellett 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.[163]

[163] CLOUGH: i.m. 130. o.

Kárként értékelhető az is, ha az elkövető megváltoztatja a biztonsági szoftvert (pl. vírusirtót), aminek következtében az nem észleli a behatolást a rendszerbe.[164]

Végül ahhoz, hogy bűntett megállapítására kerüljön sor a 1030.§ (a)(5)(A) pontja értelmében, legalább egy minősített esetnek meg kell valósulnia a törvényben felsoroltak közül:

- legalább 5,000$ értékű veszteség egy év alatt;
- az egészségügyi ellátás akadályozása;
- fizikai sérülés okozása;
- fenyegetést jelent a közegészségre és közbiztonságra nézve;
- az Egyesült Államok kormánya által vagy érdekében, az igazságszolgáltatásban, a honvédelemben, vagy a nemzetbiztonságban használt számítógép sérelmére elkövetés;
- károkozás tíz vagy több védett számítógép sérelmére egy év alatt.

A CFAA tágan definiálja a veszteség fogalmát: „bármely kiadás a sértett részéről, ami magában foglalja a jogsértésre adott válaszokat, kárfelmérést, illetve azt az adatot, programot, rendszert vagy információt, amely a jogsértést megelőző állapotra történő helyreállításával kapcsolatos költségként felmerül és bármely bevétel kiesést, költséget, vagy egyéb károsszeget, amely a szolgáltatás szünetelésével összefüggésben keletkezett”. Ezt a legegyszerűbb bizonyítani, mert általában azt a pénzösszeget jelenti, amitől elesik az áldozat a szolgáltatás szüneteléséből adódóan. Amennyiben a leállás minél hosszabb ideig tart, annál nagyobb veszteség keletkezik. A bíróságok egy része azonban a cég jó hírnevét kizárta a veszteségi körből, de például a helyreállítással megbízott, illetve a leállás miatt a munkájukat végezni nem tudó alkalmazottak munkadíját vagy munkabérét, a weboldalon elszalasztott hirdetési és értékesítési bevételek is ide tartozhatnak. Azonban a korábbinál jobb és biztonságosabb rendszer felállításának érdekében tett intézkedések már nem. A sértett lehet természetes vagy jogi személy.

A CFAA azokkal a támadásokkal szemben is véd, amelyek akadályozzák „egy vagy több személynek az orvosi vizsgálatát, diagnózisát, kezelését vagy gondozását”. Azonban a sérelemnek nem kell jóvátehetetlennek vagy jelentősnek lennie, illetve pénzügyi veszteségnek sem kell bekövetkeznie. Ez a pont erős védelmet nyújt a kórházak, klinikák és más egészségügyi intézmények rendszerei és a bennük tárolt érzékeny adatok részére. A bizonyítékokkal elegendő annak az alátámasztása, hogy az elkövető tevékenysége legalább egy betegnek az egészségügyi nyilvántartását potenciálisan érintette.

[164] U.S. DEPARTMENT OF JUSTICE: i.m. 35–49. o.

A harmadik pont 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 pont esetében elegendő, ha a közegészség és közbiztonság veszélybe kerül a DDoS-támadással, például a forgalmi jelzőlámpák működésének leállása következik be - a közlekedési infrastruktúra elleni túlterheléses támadásnak köszönhetően -, azonban az nem jár fizikai sérüléssel, de az elkövető felelősségre vonható már azért, mert potenciális veszélyhelyzetet idézett elő. Ez a pont elsősorban a kritikus infrastruktúrák[165] (pl. energia-, közlekedési-, egészségügyi- és pénzügyi ágazat) elleni támadásokkal szemben lép fel, amelyek igen jelentős kárt tudnak okozni.

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. ide tartozik a bíróságok, ügyészségek számítógépes rendszere, valamint a katonai, 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 sor kerüljön a sikertelen támadás esetén is (pl. ebben az esetben egy DDoS-támadásnál nem szükséges, hogy a tényleges kár bekövetkezzen).

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. Ez a rendelkezés akkor alkalmazható, amikor az elkövetés botnethez köthető vagy más körülmények merülnek fel, de 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 teljes veszteség meghaladta az 5,000 $-t.

A CFAA 1030.§ (b) bekezdése értelmében büntetendő a 1030.§ (a) bekezdéseiben szabályozott bűncselekményeknek a kísérlete és az elkövetésben való megállapodása (előkészületi cselekménye) is.

Aki tudatosan továbbít programot, információt, kódot vagy parancsot és szándékosan kárt okoz a védett számítógépben, de nem eredményezi a korábban felsorolt hat sérelem közül

[165] 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 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.]

egyiket sem, az vétséget követ el és egy évig terjedő szabadságvesztéssel és/vagy pénzbüntetéssel büntetendő. A visszaeső tíz évig terjedő szabadságvesztéssel büntethető.

Amennyiben a tudatos továbbítás és szándékos károkozáson felül megvalósul a hat minősített eset közül legalább az egyik, akkor az elkövető bűntett miatt tíz évig terjedő szabadságvesztéssel és/vagy pénzbüntetéssel büntetendő.

Húsz évig terjedő szabadságvesztéssel büntethető pedig az, aki a 1030. § (a)(5)(A) pont megsértésével bűntettet követ el és elítélik a CFAA hatálya alá tartozó más bűncselekmény elkövetéséért is.

2002-ben a Kongresszus további rendelkezést vezetett be és a büntetési tételt megemelte, ha súlyos fizikai sérülés következik be eredményként. Amennyiben az elkövető szándékosan kárt okoz a védett számítógépben és megkíséreli vagy tudatosan, vagy gondatlanságból súlyos fizikai sérülést okoz, akkor a maximum szabadságvesztés húsz évre emelkedik. Végül, életfogytig tartó szabadságvesztést szabhat ki a bíróság akkor, ha az elkövető tudatosan vagy gondatlanságból halált okoz vagy megkíséreli.[166]

[166] URCUYO: i.m. 300–330. o.; U.S. DEPARTMENT OF JUSTICE: i.m. 35–49. o.

5. A számítógépes csalás

5.1. A számítógépes csalás uniós és hazai szabályozása

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

a) a másnak jogosulatlanul és szándékosan történő vagyoni károkozás, 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 számítógépes csalás a régi Btk.-ban még a számítástechnikai rendszer és adatok elleni bűncselekmény (300/C. §) keretében került szabályozásra, amely tartalmilag megfelelt a nemzetközi elvárásoknak.[167] Az új Btk.-ban azonban szétválasztásra került, és az eltérő jogtárgy védelem alapján, külön tényállásként az információs rendszer felhasználásával elkövetett csalás elnevezéssel nóvumként jelent meg a 375. §-ban a vagyon elleni bűncselekmények között. A javaslat indokolása 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. 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.[168]

Az információs rendszerek sokrétű funkciójából következik, hogy az e rendszerek ellen intézett támadások más társadalmi viszonyt is sérthetnek, így ezen bűncselekmények kettő - vagy akár több - jogtárggyal is jellemezhetők mint az információs rendszer felhasználásával elkövetett csalás is, mert az információs rendszerek integritása, biztonsága mellett a vagyoni viszonyokat is sérti.[169]

---

[167] „ (3) Aki jogtalan haszonszerzés végett
a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl vagy hozzáférhetetlenné tesz, vagy
b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza,
és ezzel kárt okoz, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő."

[168] A Btk. javaslatának 375. §-ához fűzött indokolás

[169] NAGY (2009): i.m. 60. o.

A 375. § (1) bekezdésében szabályozott károkozó adatvisszaélési alakzat szerint, aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt 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. Tehát az elkövetési magatartás megvalósul a már korábban az információs rendszer vagy adat elleni bűncselekménynél részletesen elemzett cselekményekkel.

Azonban e bűncselekmény eredmény-bűncselekmény, ezért akkor valósul meg, ha az elkövető magatartását jogtalan haszonszerzés céljából fejti ki, amelynek eredményeként kár[170] 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 azzal a céllal, hogy jogtalan haszonhoz jussanak. Például jellemző, hogy az elkövető pénzügyi rendszerhez fér hozzá és bankszámla egyenleggel vagy hitelkerettel manipulál. A bíróság egyik ügyben azért marasztalta az elkövetőt, mert a számítástechnikai rendszerbe vitt be olyan adatokat, amelyek nem voltak valósak, és amelyeket a rendszerbe nem volt jogosult bevinni. 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, amivel az volt a célja, hogy a jogtalan haszonszerzés érdekében véghez vitt magatartására ne derüljön fény, így végső soron a törlés célzata is a jogtalan haszonszerzés volt.[171]

Másik döntésben kimondták, 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.[172]

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

---

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

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 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.[173]

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[174] 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.[175]

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 esetben a bíróság számítógépes csalás bűntettében mondta ki a vádlott bűnösségét, aki a károsult gazdálkodó szervezet alkalmazásban állt mint informatikus szakértő és feladata volt a cég átfogó számítástechnikai rendszerének kidolgozása, alkalmazása. A vádlott 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

---

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

[174] Btk. 459.§ (6) bekezdés: E törvény 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.

[175] SZOMORA: i.m. 789. o.

működését lehetetlenné teszi. Minderről a vádlott munkáltatóját nem tájékoztatta. A gazdálkodó szervezet azonnali hatállyal megszüntette a vádlott foglalkoztatását. Ezt követően a vádlott által készített programok részben megsemmisítették önmagukat, részben működésképtelenné váltak, 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 vádlott 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.[176]

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 pénzösszegeknél.

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 információk értékének, valamint a bűncselekmény stádiumának a meghatározása.[177]

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 fejezetben 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. Tehát a kérdés, hogy az elkövető csak felhasználta-e az információs rendszerben rejlő lehetőséget és úgy követte el a bűncselekményt,

[176] BH 1999/145.
[177] LACZI Beáta: A számítógép és a büntetőjog. Magyar Jog 2001/3. 137-152. o.

hogy azt annak segítségével kívánta eltitkolni, vagy már a bűncselekmény elkövetése érdekében manipulálta az adatokat.[178] 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.[179]

A német StGB. 202b. §-a a phishing elnevezésű tényállással rendeli büntetni azokat a magatartásokat, amelyekkel technikai eszközök révén jogosulatlanul, nem nyilvános adatfeldolgozó rendszerből szereznek meg adatokat és ez két évig terjedő szabadságvesztést vonhat maga után. Amennyiben az adatot felhasználják azzal a céllal, hogy jogosulatlan előnyre tegyenek szert – vagyis ezáltal kárt okozzanak a sértettnek – akkor a 263a. §-ában szabályozott számítógépes csalás miatt vonhatók felelősségre és öt évig terjedő szabadságvesztéssel büntethetők.[180]

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

A CFAA 1030.§ (a)(4) bekezdése a számítógépes csalást rendeli büntetni, amely szerint, „aki tudatosan és jogosulatlanul védett számítógéphez hozzáfér, vagy jogosultságának kereteit túllépi csalási céllal és e tevékenységével elősegíti a szándékos csalást és ezáltal megszerez valamely értékkel rendelkező dolgot, azonban 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 jogosulatlan hozzáférés a védett azámítógéphez vagy a jogosultság kereteinek a túllépése több módon is elősegítheti a szándékolt csalást:

Például az elkövető egy nyilvántartásban információt módosít vagy töröl, ezt követően pedig valamilyen vagyoni előnyben részesül attól, aki ezen nyilvántartás helyességében bízott. Az egyik esetben a vádlott a hitelinformációs ügynökség nyilvántartásához fért hozzá, amelyben a hitel értékelését számára kedvezőbb értékre módosította.

A másik eset az, amikor az elkövető megszerzi az értékkel rendelkező információt, adatot és később csalásra használja fel.

[178] SZATHMÁRY (2012): i.m. 93. o.
[179] SZABÓ (2009): i.m. 615. o.
[180] NIETHAMMER, Alexander – MORAWIETS, Steffen: Germany: Cybersecurity 2019.

Utolsó esetként megemlítendő az, amikor a vádlott arra használja a számítógépet, hogy hamis, hamisított dokumentumokat állítson elő, amit később csalásra használ fel. Például a vádlott a lottó terminált használta fel arra, hogy visszadátumozott szelvényeket állítson ki a nyerő számokkal és utána átvette ezért a lottónyereményt.

A tényállásszerűséghez az elkövetőnek valamilyen mérhető értékkel rendelkező dolgot (pl. pénz, áru vagy szolgáltatást stb.) kell megszereznie. Ennek két esete különböztethető meg: az első esetében az elkövető csak információt szerez meg, azonban ennek az értéke nincs meghatározva, de számszerűsíthető értékkel kell rendelkeznie. A másik esetben a számítógép használatával követi el ezt a bűncselekményt.[181]

Példaként említhető a United States vs. Christian-ügy, amelyben a két vádlott magas beosztású katonai hivatalnok nevét és társadalombiztosítási számát szerezte meg egy nyilvános oldalról. Ezután hitelt kérvényeztek egy vezető számítástechnikai cégtől és két banktól hitelkártyát igényeltek a sértettek nevében. Hasonló eset volt a United States vs. Wahl-ügy, amikor az elkövetők a sértettek születési dátumait és társadalombiztosítási számaikat szerezték meg, majd autóvásárlásra kölcsönt igényeltek a nevükben, ezt követően pedig a befolyó összegből saját vállalkozásukat finanszírozták.[182]

[181] Amikor a törvény megalkotására sor került, akkor megszokott volt, hogy ún. szuperszámítógépek használatát a tulajdonosuk bérbe adta. Manapság ez a pont már idejét múltnak tekinthető.
[182] SZABÓ Imre: Internetes bűncselekmények, különös tekintettel az internetes csalásra. ELTE ÁJK, 2002. 18. o.

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 mint egy szolgáltatásként lehet igénybe venni vagy akár megvásárolni az ún. Darknet online feketepiacokon és fórumokon keresztül.[183] A kibertámadások végrehajtását rendkívül megkönnyíti, 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 mindegyik szerződő fél köteles legalább a számítógépes jelszavak vagy belépési adatok értékesítését, a forgalomba hozatalát vagy a más módon történő hozzáférhetővé tételét kriminalizálni.[184]

Az információs rendszerek elleni támadásokról szóló 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

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

bűncselekménynek minősüljön: az olyan 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. A bűncselekmény elkövetési tárgya az információs rendszer felhasználásával elkövetett csaláshoz vagy az információs rendszer vagy adat megsértésének 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 bocsájtják a rendelkezésére.

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.

A bűncselekmény rendbelisége ez esetben is az információs rendszerek számához igazodik. A tényállás mindkét fordulata csak szándékosan – 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 az információs rendszer vagy adat megsértését elkövesse.[185] 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. A jelszavakkal kereskedés (Trafficking in passwords) a CFAA-ban

A CFAA 1030. § (a)(6) bekezdésének értelmében „vétségként büntetendő, aki jelszavakkal vagy hasonló információkkal kereskedik, tudatosan és csalási céllal és,

(A) ha ez hatással van az államközi vagy nemzetközi kereskedelemre vagy

(B) a számítógép az Egyesült Államok kormányának használatában van."

A „kereskedés" (trafficking) tág fogalmat jelöl például megvalósul, ha az illető átadja vagy értékesíti, vagy megszerzi azzal a céllal, hogy értékesítse másnak, de önmagában a birtoklás nem meríti ki ezt az esetet a célzat hiányában, valamint a személyes használat sem. A tényállásszerűséghez nincs szükség a haszonszerzési céllal történő elkövetésre. A „jelszó" (password) szintén egy tágabb fogalom, ami nem korlátozódik például egy kifejezésre vagy kódra, ami védelmet és egyúttal hozzáférést is biztosíthat a számítógéphez, hanem ez magában foglalhat egy leírást, útmutatást vagy egyéb módszert is.[186]

A rosszindulatú programok készítése – az európai és hazai gyakorlattól eltérően – azonban nem szerepel a szankcionált magatartások között.

[185] MOLNÁR (2018): i.m. 946–954. o.
[186] U.S. DEPARTMENT OF JUSTICE: i.m. 49-51. o.

7. Az információs rendszer felhasználásával elkövetett zsarolás esetei

A számítógépes zsarolás egy hagyományos bűncselekmény modern változata, amely során károkozással fenyegetnek, amennyiben a követelésüknek nem tesz eleget a sértett.

Ez a rendelkezés alkalmazható azokra az esetekre, amikor az elkövetők 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.

Egyre gyakoribb, hogy zsarolás során használják fel a DDoS-támadásokat. 2016-ban az Europol sikeres akciót hajtott végre és letartóztatta a zsarolásokban élen járó DD4BC (Distributed Denial of Service for Bitcoin) Team hacker csoportnak a kulcsfontosságú tagjait, akik számos DDoS-támadást indítottak európai cégekkel szemben. Az elkövetők elsősorban olyan cégek oldalait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. webshopok, online szerencsejáték és fogadó cégek, energia- és pénzügyi szféra). Az általuk alkalmazott zsaroló séma a következőképpen néz ki: felmérik a célpont hálózati sérülékenységét, majd kisebb DDoS-támadásokat indítanak a céggel szemben, ezt követően a további támadások indításának elkerülése érdekében 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. DD4BC csapatnak a módszere egyre elterjedtebbé vált és már „copycat" hacker csoportok is megjelentek, akik másolják őket.[187]

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 növekvő számban bűnszervezetekhez is köthetők, akik mint egy „call center"-t működtetnek haszonszerzési céllal.[188]

[187] 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.]
[188] EUROPOL (2017): i.m. 35. o.

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, malware aktiválásával – gondoljunk csak a zsarolóvírusokra vagy trójaival megvalósuló hátsó ajtó nyitásra – és megszerzik az azon tárolt bizalmas adatokat például akár személyes adatokat, értékes gazdasági vagy üzleti titkot, kompromittáló képeket vagy a betörést követően hozzáférve a beépített webkamerához, illetve mikrofonhoz saját maguk készítenek olyan kép- 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, mely csupán 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.[189]

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.

[189] 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 számítógép károsításával való fenyegetés, avagy a számítógépes zsarolás (Threatening to damage a computer) a CFAA-ban

1030.§ (a)(7) bekezdés a számítógépes zsarolást szabályozza, amely szerint büntetendő, „aki azzal a szándékkal zsarol meg bárkit, hogy tőle pénzt vagy más értékkel rendelkező dolgot megszerezzen, és olyan üzenetet továbbít az államközi vagy nemzetközi kereskedelmen keresztül, ami olyan:

(A) fenyegetést tartalmaz, amely védett számítógépben való károkozásra vonatkozik;

(B) fenyegetést tartalmaz, amely védett számítógépben tárolt információ jogosulatlan vagy jogosultságainak kereteit túllépve történő megszerzésére vonatkozik, vagy a megszerzett információhoz fűződő titoktartást megsérti jogosulatlanul, vagy jogosultságainak kereteit túllépve; vagy

(C) pénzt vagy egyéb értékkel rendelkező 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 pénzt vagy az értékkel rendelkező dolgot megszerezze, ami a zsarolás tárgyát képezi, vagy, hogy az elkövető szándéka kiterjedt arra, hogy a fenyegetését valóban megvalósítsa.
A fenyegetést nemzetközi vagy államközi kereskedelmen keresztül kell továbbítani, azonban nem szükséges, hogy ez elektronikus úton történjen például történhet telefonhíváson, e-mailen vagy egyéb üzenetváltási rendszeren keresztül.

A kár bekövetkeztéhez elegendő – a korábban már a 1030. § (a)(5) bekezdésnél említett módon –, ha az elkövető 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.).

A 1030. § (a)(7)(B) pont két esetet foglal magában. Az első fordulatban az elkövető azzal fenyeget, hogy bizalmas információkat szerez meg a sértettől, ha a követelésnek nem tesz eleget. A második esetben az elkövető a számítógéphez való jogosulatlan hozzáférésen vagy jogosultságainak kereteinek túllépésén keresztül megszerzett információk nyilvánossá tételével fenyeget. Tehát 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) pont szerint büntetendő az, aki tartózkodik a kapcsolatfelvételtől egészen a károkozásig, majd miután hozzáfért a sértett számítógépéhez és titkosítja az adatokat rajta, akkor áll elő a követelésével, hogy pénzt kérjen a titkosítást feloldó kulcsért cserébe.

A büntetés öt évig terjedő szabadságvesztés, amennyiben a 1030. § hatálya alá tartozó másik bűncselekmény miatt is elítélik az elkövetőt, akkor a büntetés felemelkedik tíz évig terjedő szabadságvesztésre.

A 1030.§ (b) alszakasza értelmében büntetendő a 1030.§ (a) alszakaszaiban szabályozott bűncselekményeknek a kísérlete és az elkövetésben való megállapodása (előkészületi cselekménye) is.[190]

[190] U.S. DEPARTMENT OF JUSTICE: i.m. 52-55. o.

8. A tiltott adatszerzés uniós és hazai szabályozása

A Budapesti Egyezmény a jogosulatlan kifürkészést (3. cikk) határozza meg, amely szerint 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.

Az információs rendszer elleni támadásokról szóló 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 a régi 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. 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 alapeset elkövetőjének célja a személyes adat, a magántitok, a gazdasági titok vagy az üzleti titok jogosulatlan megismerése, így e bűncselekmény védett jogi tárgya az ezeknek a védelméhez fűződő társadalmi érdek.

A személyes adat tekintetében a háttérjogszabály az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.). E törvény – a hatályba lépett 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 a meghatározás, miszerint magántitok minden olyan, csak szűk körben ismert bizalmas tény, körülmény vagy adat, amelynek megőrzéséhez az érintett személynek méltányolható érdeke fűződik, illetve amelynek nyilvánosságra hozatala a sértettre nézve érdeksérelemmel jár.[191] A magántitok lehet dologi vagy eszmei jellegű. A tény, illetőleg 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. Bérces Viktor szerint a „[m]agántitok minden olyan, csak szűk körben ismert bizalmas tény, körülmény vagy adat, amelynek megőrzéséhez az érintett személynek méltányolható érdeke fűződik, illetőleg amelynek nyilvánosságra hozatala a sértettre nézve érdeksérelemmel jár.[192]

A gazdasági titok egy gyűjtőfogalmat takar, amelyhez tartozik a banktitok[193], értékpapírtitok[194], biztosítási titok[195], valamint a pénztártitok[196], amelyek lényegüket tekintve a

[191] BH 2004.170..

[192] BÉRCES Viktor: A magántitok büntetőjogi védelmének értelmezési sémái. Jogtudományi Közlöny 2017/9. 395. o.

[193] 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."

[194] 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.

[195] 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.

[196] 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

pénzügyi szektor titkainak csoportjába tartoznak. Az egyik kommentár a bűncselekmények elhatárolása során megjegyzi, hogy „a gazdasági titok a magántitok speciális változata,”[197] más titokfajtáknál csoportosításra utaló megjegyzést azonban nem tesz.[198]

Az üzleti titok fogalmát korábban a Ptk., most pedig 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.[199]

A tiltott adatszerzés deliktumának az elkövetési magatartásai a d) pont szerint az elektronikus hírközlő hálózat vagy eszköz útján[200], 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.

---

nyilvántartott összegre, illetve amely a munkáltatói tag, illetve a támogató adataira, vagyoni helyzetére, üzleti tevékenységére, tulajdonosi, üzleti kapcsolataira vonatkozik.”

[197] 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

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

[199] SZŐKE: i.m. 256. o.

[200] 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.

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 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 elkövetőnek a cselekményének magántitok, gazdasági vagy 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 is juthasson. Ez a megállapítás azonban azt jelenti, hogy a telefonbeszélgetések rögzítése során esetlegesen magántitkok, gazdasági vagy üzleti titkok is megismerhetőek és rögzíthetőek, ám ennek lehetőségéből mindössze a terhelt eshetőleges szándékára lehet következtetni, amely célzatos bűncselekmény esetében a bűnösség megállapításához nem elegendő.[201] Úgy vélem, hogy ez az információs rendszerre alkalmazva is hasonló eredményhez vezethet, itt különösen fontos vizsgálat alá vonni az illető szándékát és az eset összes körülményét, hogy bizonyítást nyerjen, hogy a tényállásban kiemelten kezelt információk valamelyikének megismerésének céljából fürkészi ki és rögzíti ezt.

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.[202]

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 [224.§ (1) bekezdés b) pont], valamint egyéb esetekben az információs adat vagy rendszer megsértéséért.

Emellett érdemes foglalkozni röviden a 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

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

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.

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[203], 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.[204]

[203] 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.
[204] CSÁK Zsolt: A drónok kapcsán felmerülő egyes büntető és eljárási jogi kérdések. In: Mezei Kitti – Nagy Zoltán András (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK. Pécs, 2019. 34. o.

9. Az informatikával összefüggő büntető eljárásjogi kérdések

9.1. Az elektronikus bizonyíték fogalma

Napjainkban az elkövetők többsége szöveges üzeneteket, e-maileket és informatikai alkalmazásokat használ a kommunikáció során, a bűncselekményeik elleplezésére és az igazságszolgáltatás elkerülésére.

A szakirodalomban ezekre vonatkozóan a digitális vagy elektronikus bizonyíték elnevezés jelenik meg, amelyek már a második generációs bizonyítékok körébe tartoznak.[205]

Az elektronikus bizonyíték (electronic evidence) fogalma alatt legáltalánosabb értelemben ideértendő minden olyan bizonyító erejű információ és adat, amelyeket bináris formában tároltak vagy továbbítottak (pl. IP címek, e-mailek, kép- és videófelvételek stb.).[206]

Casey szerint a digitális bizonyíték minden olyan adat, amely alátámaszthatja, hogy bűncselekmény, vagy amely összekapcsolja a bűncselekményt annak elkövetőjével.[207]

Marie-Helen Keles szerint az elektronikus bizonyíték magában foglal bármely olyan információt, amely kinyerhető számítástechnikai rendszerekből vagy más digitális eszközökből, és amennyiben a bűncselekménnyel összefüggésbe hozható, akkor bizonyítékként felhasználható az eljárás során.[208]

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."[209]

Valamennyi fogalomnál közös, hogy büntetőjogilag releváns információkra vonatkoznak és amelyeket információs rendszeren tárolnak, vagy továbbítanak.[210]

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).[211]

---

[205] FENYVESI Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 438-440. o.
[206] SCIENTIFIC WORKING GROUPS ON DIGITAL EVIDENCE AND IMAGING TECHNOLOGY: Digital & Multimedia Evidence Glossary. 2016. 7. o.
[207] CASEY: i.m. 7. o.
[208] KELES, Marie-Helen: Computer Forensics: Cybercriminals, Laws and Evidence. Second Edition, Jones & Bartlett Learning, 2015. 76-77. o.
[209] PESZLEG Tibor: Interneten, számítógépen történő nyomrögzítés. Ügyészek Lapja 2005/1. 25. o.
[210] SORBÁN Kinga: A digitális bizonyítékok a büntetőeljárásban. Belügyi Szemle 2016/11. 84. o.
[211] Budapesti Egyezmény Preambuluma és 14. cikk 2. bekezdés a)-c) pont

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.[212]

9.2. A hatályos büntető eljárásjogi szabályozás hazánkban

Az új büntetőeljárásról szóló 2017. évi XC. számú törvény (a továbbiakban: 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: a forgalomi adatot (traffic data)[213], a tartalomra vonatkozó adatot (content data)[214] és az előfizetőre vonatkozó adatot (subscriber data)[215]. Ezeknek a megkülönböztetésére azért van

[212] SORBÁN (2016): i.m. 82-83. o.

[213] 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.

[214] 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.

[215] 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.

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.[216]

Ahol az új 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.[217]

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.[218]

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.[219]

9.3. Az elektronikus adattal összefüggő kényszerintézkedések

9.3.1. A kutatás

Az eddigi házkutatás elnevezést az új Be. kutatásra változtatta meg, amely terminológia így igazodik a kényszerintézkedés tartalmához, amely alapján a tárgya nem csupán a helyiségek, illetve körülhatárolt 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,

[216] SZABÓ (2011): i.m. 16. o.
[217] Be. 204. § (1) bekezdés a) – d) pont
[218] PESZLEG: i.m. 24. o.
[219] WANG, Shiuh-Jeng: Measures of retaining digital evidence to prosecute computer-based cyber-crimes. Computer Standars & Interfaces 29. 2007. 218. o.

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.[220]

Emellett ilyenkor bevett gyakorlat, hogy az információs rendszerben olyan vizsgálatokat végeznek, amelyekre később nem biztos, hogy lehetőségük lesz például egy adatot felhőszolgáltatásban tárolnak.[221]

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[222] nem csak egészségügyi intézmények kezelhetnek. Adatkéréssel az egészségügyi adatok továbbra is csak az ügyészség engedélyével szerezhetők be.

9.3.2. 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, ügyész és a nyomozó hatóság is elrendelhet.

E jogintézmény kulcsfontosságú szerepet játszik a kibertérben elkövetett bűncselekmények felderítésében az elektronikus bizonyítékok megszerzésének és megőrzésének eszközeként.

---

[220] VADÁSZ: i.m. 30. o.

[221] DORNFELD László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2. 119-120. o.

[222] 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 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)".

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 régi Be.-be az adat lefoglalását a 2013. évi CLXXXVI. törvény 21. §-a illesztette be a törvény szövegébe. Ezt megelőzően bevett gyakorlatként volt érvénybe 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.[223]

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.[224] 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,
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. 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

[223] VADÁSZ: i.m. 20. o.
[224] 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

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 feltünteti. 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, azonban ha a lefoglalást végző nem rendelkezik kellő szakértelemmel, fontos bizonyítékok veszhetnek el (pl. a metaadat[225], a cache tartalma[226] 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, azonban ez igazán csak kisebb mennyiségű adatállomány esetén alkalmazható hatékonyan.[227]

A teljes rendszer lefoglalásának a hátránya, hogy annak egyes hardver részei (pl. videókártya, alaplap, tápegység stb.) gyorsan amortizálódnak és az elhúzódó büntetőeljárásnak köszönhetően a lefoglalás elszenvedőjét akár komoly anyagi kár is érheti ezáltal, vagy akár a vállalkozás működését is veszélyeztetheti. Emellett problémát jelenthet adatvédelmi szempontból is, mert a lefoglalt számítógép olyan személyes adatokat is tartalmazhat, amelyek nincsenek összefüggésben a büntetőeljárással vagy több személy adatait is tartalmazhatja (pl. egy céges hálózat számítógépeinek vagy szervereinek lefoglalásakor).[228] Amennyiben lehetőség van a szelektálásra, az ilyen jellegű adatokat már eleve ki kell vonni a lefoglalás köréből, ha pedig azok a rögzítést követően, utólag jutnak a hatóság tudomására, úgy a szükséges biztonsági intézkedések megtétele mellett, törlésükről 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.[229]

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.

[225] A metaadatok az elektronikusan elérhető adatoknak a leíró adatai, vagyis strukturált információ az adatokról.
[226] Cache (gyorsítótár): a számítástechnikában az átmeneti információtároló-elemeket jelenti, melyek célja az információ-hozzáférés gyorsítása.
[227] SORBÁN (2016): i.m. 89. o.
[228] SORBÁN (2016): i.m. 89. o.
[229] LACZI Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. Magyar Jog 2001/12. 726-738. o.

Az adatvédelmi biztos állásfoglalásában felhívta a figyelmet arra, hogy az eljáráshoz nem szükséges személyes adatokhoz való hozzáférés csak ésszerű időtartamra korlátozható, és egy félévig elhúzódó lefoglalás már ezen túl mutat.[230]

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.[231] Peszleg is az emberi méltóság, személyiségi és kegyeleti jogok tiszteletben tartását hangsúlyozza.[232]

Az adatvédelmi biztos beszámolója alapján ismertté vált rendőrségi gyakorlat szerint a személyes adatokhoz csak az igazságügyi informatikai szakértő, 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.[233] A Nemzeti Nyomozó Iroda gyakorlata alapján a lefoglalt rendszerről teljes másolatot készítenek, és ezt vizsgálják át az eljárás során, ami korlátozza az adatokhoz való hozzáférők körét.[234]

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 lehetséges az eredeti adattartalom visszaállítása (pl. RAID tömbök[235] esetén)”.[236] 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.[237]

Az új Be.-ben a szükségesség-arányosság követelménye a 315. § (4) bekezdésében kiemelten jelenik meg, mert a jogalkotó rögzíti, hogy a büntetőeljárás szempontjából

[230] Az adatvédelmi biztos beszámolója, 2009. Forrás: hwww.naih.hu/files/Adatvedelmi-biztos-beszamoloja-2009.PDF
[231] MOHÁCSI Barbara: Bűnüldözési érdek contra emberi jogok - az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. Magyar Jog 2008/12. 827-832. o.
[232] PESZLEG: Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük. Ügyészek lapja, 2010/2. 23. o.
[233] TRÓCSÁNYI Sára: Első oldal. Infokommunikáció és jog 2009/6. 1. o.
[234] DORNFELD (2018): i.m. 123. o.
[235] RAID: tárolási technológia, mely segítségével az adatok elosztása vagy replikálása több fizikailag független merevlemezen, egy logikai lemez létrehozásával lehetséges.
[236] PESZLEG: i.m. 27. o.
[237] VADÁSZ: i.m. 19. o.

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 elmondható, hogy 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 vonatkozó kísérletek.[238]

9.3.4. 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 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

[238] 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.

bélyegzővel láthatja el. Ha az adatok egy belső hálózaton (intranet) érhetőek el, akkor a rendszergazdát kell kötelezni az adatok megőrzésére.[239]

9.3.5. Az elektronikus adat ideiglenes és végleges hozzáférhetetlenné tétele

Az új 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 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.[240]

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 tárhelyszolgáltató, valamint tárhelyszolgáltatást is végző közvetítő szolgáltató kötelezhető, 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;

[239] 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

[240] GAIDERNÉ HARTMANN Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele - egy új intézmény első évei. Magyar Jog 2015/2. 106-107. o.

- 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.[241]

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[242] szerint és alhálózati maszk,

b) domain név,

c) URL cím,

d) portszám.[243]

---

[241] 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.

[242] 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 nyomozóhatóságnak 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.

[243] A rendelet 141. § (3) bekezdése meghatározza a fogalmukat is, azonban ezek az átlagos felhasználónak e jelentések kevés támpontot adnak az egzakt, kellően pontos, így 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;

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.[244]

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.

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”[245] 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.[246] 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.

„portszám”: a TCP/IP és az UDP, illetve SCTP protokollokban az adott célszerveren a logikai csatlakozást meghatározó jelzőszám.

[244] GAIDERNÉ HARTMANN: i.m. 115. o.

[245] 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.

[246] GAIDERNÉ HARTMANN: i.m. 111-112. o.

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.[247]

Emellett lehetőség van a kényszerintézkedés előtt időnyerés végett, hogy az ügyészség vagy a nyomozó hatóság a szolgáltatókat felhívja az önkéntes eltávolításra, azonban ez nem kötelező rájuk nézve (Be. 338. §).

9.4. 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 igazságügyi együttműködésre és kölcsönös jogsegélyre van szükség, azonban az eljárás jelenleg túl 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 sok időbe kerül az ilyen bizonyítékok begyűjtése, illetve hogy széttagolt a jogi szabályozás kerete. Jelentős bírósági döntések is születtek már e kérdéskörben, amelyek szintén rámutattak arra, hogy mennyi probléma rejlik a jelenlegi helyzetben.[248] 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 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 hatékony együttműködésnek a megteremtése velük.

---

[247] DETREKŐI Zsuzsa: Blokkolás Magyarországon - hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig. Infokommunikáció és jog 2014/4. 184-186. o.

[248] 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.

Az elektronikus bizonyítékok beszerzésének a gyorsítása és hatékonyabbá tételének érdekében az Európai Tanács elfogadta álláspontját a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szóló rendeletről, amelynek következő lépése ennek az Európai Parlament előtt való megtárgyalása.

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 (például e-mailek, szöveges üzenetek vagy alkalmazásokban futó szövegek) bármely, az Unióban szolgáltatásokat kínáló és más tagállamban letelepedett vagy képviselettel rendelkező szolgáltatótól, amely köteles 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 képes a meglévő európai nyomozási határozat esetében 120 nap, míg a kölcsönös jogsegély eljárás esetén pedig 10 hónap a válaszadási határidő.

A rendelet meghatározza az elektronikus bizonyíték fogalmát, amelynek 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.[249] A szabályozás négy adatkategóriát határoz meg amelyre, a határozatok vonatkozhatnak:

Előfizetői adat (subscriber data), amely az előfizető vagy vásárló azonosítását szolgálja mint például ilyen a név, születési idő, postacím, számlázási és fizetési adat, telefonszám vagy e-mail cím.

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[250].

[249] TOSZA, Stanislaw: The European Commision's Proposal on Cross-Border Access to E-evidence. eucrim 4/2018 214. o.

[250] Az IP címek 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 eltérő megítélés alá esik országonként. Lásd 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.

Mindkét esetben 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.

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.[251] 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 másik országban található szolgáltatót vagy annak jogi képviselőjét, hogy biztosítsa a kért elektronikus bizonyítékot a részére.[252] A tranzakciós vagy tartalmi adatok – az utóbbi két kategória esetében egyedi küszöbérték alkalmazása mellett – kizárólag olyan bűncselekményekkel összefüggésben kérhetők, amelyek büntetési tételének felső határa a kibocsátó államban legfeljebb három év szabadságvesztés, illetve bizonyos, kibertérben elkövethető vagy terrorizmussal kapcsolatos bűncselekmények esetében.

Mindezekre tekintettel az elektronikus bizonyíték és 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, kivéve, ha kollízió van harmadik ország jogával, amelyet vélhetően egy felülvizsgálati eljárás keretében fognak vizsgálni.

[251] TOSZA: i.m. 214. o.
[252] http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm [2019.02.21.]

Az elektronikus bizonyítékok egy egérkattintással könnyedén megváltoztathatók vagy törölhetők, ezért sor kerül egy másik fontos jogintézmény bevezetésére, hogy megakadályozzák ezt, az ún. adatok törlését a megőrzésre kötelező európai határozat (European Preservation Order) segítségével. Ez 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 kellett alapítani őket vagy másik 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, internet domain névvel és IP címmel összefüggő szolgáltatás. 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 a gyanúsítottak azonosításához.[253]

A rendelet javaslata 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

[253] 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 12 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.]

kikérik, így az a lehetőség, hogy a szolgáltató felülvizsgálatot kérhet, ha például a határozat nyilvánvalóan sérti az Európai Unió Alapjogi Chartáját.[254]

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 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.[255]

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. Ez továbbá javítja jogbiztonságot is a vállalkozások és szolgáltatók számára, mert a jövőben az elektronikus bizonyítékok közlésének elrendelésére vonatkozó azonos szabályokat kell majd alkalmazni valamennyi szolgáltatóra nézve.[256]

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 „a szolgáltatónak meg kell őriznie, el kell tárolnia és rendelkezésre kell bocsátania minden vezetékes és elektronikus tartalmat, amely egy vásárlóval vagy feliratkozóval kapcsolatos, és a szolgáltató birtokában, őrizetében, ellenőrzése alatt van, függetlenül attól, hogy a felvételt, az információt a szolgáltató az Egyesült Államokon belül vagy kívül tárolja."[257]

[254] http://europa.eu/rapid/press-release_IP-18-3343_hu.htm [2019.02.21.]
[255] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52018PC0226 [2019.02.21.]
[256] 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.
[257] DASKAL, Jennifer: Unpacking the CLOUD Act. eucrim 4/2018. 220-224. o.

10. A titkosítás és az önvádra kötelezés tilalma

A titkosításnak (encryption) – például jelszavas, kriptográfiai vagy egyéb titkosítást nyújtó szoftveres védelem – mindennapi használata elterjedt, ezért ezt már a bűnelkövetők is kihasználják a nyomaik leplezésére. A titkosított eszközökkel és adatokkal a probléma az, hogy nem ismerhetők 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, ami azt jelenti, hogy senki sem kötelezhető arra, hogy önmagát terhelő vallomást tegyen vagy önmaga ellen bizonyítékot szolgáltasson.[258]

Azonban 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[259], míg az Egyesült Királyságban két évig[260], Belgiumban egy évig terjedő szabadságvesztéssel rendelik büntetni ezt.[261] 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 vallomásra, valamint az adat már tárolva van valahol, ami a gyanúsított akaratától függetlenül létezik. Belgiumban a bíróságok ítéletei között nincs 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 és mind a gyakorlatban is, vélhetően idő kérdése, hogy valamelyik ügy közül az egyik eljut a strasbourgi 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[262] jellemző így például ujjlenyomat vagy írisz, ez is különösen megnehezítheti a nyomozó hatóságok helyzetét és az eljárás lefolytatását, mert egyre több eszköznél jelenik meg ezeknek

[258] Be. 7. § (3) bekezdés

[259] Amennyiben kétséget kizáróan kiderül, hogy a kód átadása megakadályozta volna a bűncselekményt vagy ezáltal a bűncselekménnyel okozott hátrány vagy kár csökkenthető lett volna.

[260] 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.

[261] DORNFELD (2017): i.m. 248. o.

[262] GDRP 4. cikk 14. pontja meghatározza a „biometrikus adat" fogalmát: „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."

az alkalmazása például okostelefonoknál, laptopoknál stb. Az itt felvázolt problémát megoldva, példaként megemlítendő Norvégia mint első állam, amely a büntető eljárásjogában engedi a biometrikus titkosítás feloldását, vagyis a nyomozó hatóság jogosult elrendelni azt, hogy a gyanúsított a biometrikus hitelesítéssel hozzáférést biztosítson az eszközökhöz vagy adatokhoz. Abban az esetben, ha ezt megtagadja, akkor – arányos mértékben – kényszert (erőszakot) alkalmazhatnak vele szemben a védelem feloldásához (pl. az ujjnak a lenyomatolvasóhoz való helyezésével).[263] Az erőszak alkalmazásához azonban az ügyészség engedélyére van szükség, amennyiben a késedelem a nyomozást veszélyezteti, akkor a rendőrség mérlegelve a helyszínen hozhat döntést 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 gyanúsítottól - a kényszerítő erő elfogadható használatával - olyan tárgyakat és anyagokat, amelyek a gyanúsított 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 gyanúsítottal szemben valamely testi jellemzőjét használják fel, ami a gyanúsított akaratától független, és nem kell magára nézve terhelő vallomást tennie. Ez azt a célt szolgálja, hogy a nyomozó hatóság olyan információkhoz férjen hozzá – a fizikai akadályt leküzdve –, amelyre már törvényes alapjuk van a lefoglalás körében. Ezzel szemben a gyanúsítottat 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.[264]

A titkosításnak 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 a szoftver szolgáltató a végpontok közötti titkosítást alkalmaz a kommunikációhoz (pl. Skype), végül az utolsó eset, amikor a felhasználók által használt végpontok közötti titkosítást. Az első két esetben a szolgáltató a titkosítás feloldását tudja biztosítani, ezért általában ezekre vonatkozóan létezik szabályozás és nyomozó hatóság

[263] KOOPS – KOSTA: i.m. 894-895. o.
[264] BRUCE, Ingvild: Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure. Digital Evidence and Electronic Signanute Law Review 2017/14. 26-30. o.

kérheti a dekódolást. Ezzel szemben az utolsó két eset problematikus, mert a szolgáltatók nem rendelkeznek a végpontok közötti titkosítás feloldásához szükséges kulcsokkal.[265]

A titkosítással kapcsolatban érdemes az új Be. rendelkezését is vizsgálni, amely a büntetőeljárás során a bíróság, az ügyészség és az ügyészség engedélyével a nyomozó hatóság adatszolgáltatást kérhet az elektronikus hírközlési szolgáltatótól, 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.[266]

[265] KOOPS – KOSTA: i.m. 891. o.
[266] PARTI Katalin: Az elektronikus hírközlési szolgáltatók együttműködési kötelezettsége a büntetőeljárás során a gyakorlat tükrében. Belügyi Szemle 2018/10. 30-31. o.

11. A joghatóság és a kiadatás kérdései

Az egyik legnagyobb probléma a kiberbűncselekményekkel kapcsolatban az joghatóság kérdése. Az államok joghatóságukat általában a 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 ott 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, mert előfordulhat, hogy az elkövető és a sértett különböző országokban van, továbbá a bűncselekmény által érintett információs eszköz vagy adat harmadik országban található, valamint tovább bonyolíthatja a helyzetet, amennyiben az elkövető valamelyik harmadik ország közbeiktatásával követi el a bűncselekményt. Mindez joghatósági összeütközésekhez[267] és párhuzamos eljárások megindításához vezethet a gyakorlatban.[268]

Michal N. Schmitt szerint bármelyik ország, amelyből az elkövető működteti a bűnözői infrastruktúrát joghatóságot élvez, mert az elkövető és az elkövetéshez használt eszközök is az adott állam saját területén találhatók. 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 joghatóság alkalmatlansága alapvetően az informatikai bűncselekmények jellegével magyarázható, pontosan azzal, hogy technikai nehézségeket okoz az ilyen típusú bűncselekmények elkövetőinek a nyomon követése, vagyis annak a pontos meghatározása, hogy hol követték el a bűncselekményt. Az elkövetők számára rendelkezésre állnak különböző módszerek és programok, hogy elrejtsék helyzetüket és személyazonosságukat, így földrajzilag azonosíthatatlannak mutatkoznak például az az IP cím hamisítás („spoofing") révén, valamint a proxy szerverek vagy VPN (Virtual Private Networks) használatával. Mindkettő lehetővé teszi, hogy úgy tüntesse fel mintha az illető egy másik helyről kapcsolódna az internetre, az IP

[267] A szakirodalomban kettő típusa van: a negatív és pozitív joghatósági összeütközés, azonban utóbbi jellemző a kiberbűncselekményeknél. A negatív esetén egy állam se képes vagy hajlandó a joghatóság érvényesítésére, míg a pozitív esetén több állam is megteszi ezt ugyanarra a bűncselekményre nézve. Például 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. Másik gyakori eset például a vírus fertőzések, amely bűncselekményeknek az eredménye általában több országot is érint. Lásd BRENNER, Susan W. – KOOPS, Bert-Jaap: Approaches to Cybercrime Jurisdiction. J. High Tech. L. 1. 2004. 40-41. o.

[268] DORNFELD (2017): i.m. 243. o.

címet elrejtve, azonban előbbi esetén nincs titkosítva a forgalom, míg utóbbi nagyobb biztonságot nyújtva titkosítja is azt. További problémát jelenthet, amennyiben botnet infrastruktúrát, azaz zombigépeket használnak fel a bűncselekmény elkövetéséhez, amelyek gyakran különböző országokban találhatóak. A zombi hálózatok irányító központjait tudatosak különböző államok területein szórják szét és szükség esetén percek alatt, más esetekben néhány perces rendszerességgel változtatják „digitális székhelyüket", ezáltal megnehezítve a lokalizálásukat és a fizikai rajtaütést. A digitális helyszín sokszor semmilyen közelségben sincs az elkövetők tényleges hollétével, sőt még ha lenne is, akkor sem feltétlenül bizonyítható. Összeségében megállapítható, hogy a legnagyobb problémát az anonimitás jelenti, amelyet számos program használata nyújthat így említve párat például a Tor, Anonymouse, The Cloak és a különböző e-mail titkosítást biztosító szoftverek.[269]

Susan W. Brenner felhívja a figyelmet területi elvnek a kiterjesztésére az informatikai bűncselekmények vonatkozásában amely szerint: ha az elkövető részben vagy egészben az adott ország területén követte el a bűncselekményt akkor például a joghatóságot érvényesítheti azaz 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.[270]

Emellett érdemes említést tenni a jogirodalomban elfogadott cselekményegység elméletre, melynek lényege szerint, a materiális bűncselekmény belföldön elkövetettnek tekintendő, ha a hazai büntetőtörvény szempontjából jelentős bármelyik mozzanata, így akár az elkövetési magatartás, vagy akár az eredmény belföldön valósul meg.[271]

A Budapesti Egyezmény is ezt követve rögzíti, mert elsősorban a területi elv jelenik meg, másodsorban az állampolgársági (22. Cikk). Tehát az Egyezményben foglalt bűncselekmények esetén az az állam állapíthatja meg a joghatóságát, amelynek a területén, a lobogóját viselő hajónak fedélzetén; a lajstromozott repülőgépének fedélzetén követték el a bűncselekményt, vagy amelyet állampolgára követett el, ha a bűncselekmény az elkövetés helyének joga szerint büntetendő, vagy ha a bűncselekmény nem tartozik egyetlen állam joghatósága alá sem. Utóbbi

[269] MAILLART, Jean-Baptiste: The limits of subjective territorial jurisdiction in the context of cybercrime. ERA Forum 2018 September. 4-5 o.
[270] BRENNER, Susan W.: Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law. 2001. 18. o.
[271] SZABÓ Imre: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6. 48. o.

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, 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 az, aki megfelelőbben tudja lefolytatni az eljárást.

Ugyanezt követi az információs rendszerek elleni 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.

Azonban fontos kitérni arra is, hogy problémát jelenthet az is, hogy egyes országok nem adják ki az állampolgárukat semmilyen körülmények között sem, vagy más ország állampolgára esetén, a területükön elkövetett bűncselekményének gyanúsítottját. Ezt általában az államok közötti két- vagy többoldalú kiadatási egyezmények biztosítják.[272]

A Budapesti Egyezmény is érinti a kiadatásra vonatkozó alapelveket, mely szerint akkor kerülhet sor az egyezményben szabályozott bűncselekményekre vonatkozóan kiadatásra, ha mindkét érdekelt fél szabályozása szerint legalább egy év vagy ennél súlyosabb szabadságvesztéssel büntetendőek. 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

[272] GRABOSKY: i.m. 104. o.

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.[273]

[273] Budapesti Egyezmény 24. cikk 1-7. bekezdés

III. A GAZDASÁGI BŰNCSELEKMÉNYEK AZ INTERNETEN

1. A bankkártyákkal és az átutalásokkal összefüggő visszaélések

Az elmúlt időszakban a digitalizáció, a technológia fejlődése 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 függnek 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 a vásárlásait és egyéb tranzakcióit az interneten intézi, valamint bankkártyával fizet.

Egyetértve azzal a kriminológiai állásponttal, amely szerint abban az esetben, ha egy új technikai eszköz bevezetésére kerül sor, akkor ez után szükségképpen számolni kell azon bűnelkövetők megjelenésével is, akik vissza kívánnak élni az ilyen eszközzel, és e cselekményük a társadalom védelme érdekében büntetőjogi reagálást igényel a jogalkotó részéről.[274] Ezt igazolja a bankkártyák használatának az elterjedése is, mert rövid időn belül megjelent a bankkártyákkal kapcsolatos bűnözés is, amelyre különösen jellemző, hogy egy szervezett, specializált és folyamatosan alkalmazkodó bűnelkövetésről van szó, és célja a bankszektor biztonsági intézkedéseinek kijátszása, valamint az új fizetési technológiák kihasználása.

Jelen résznek a célja a bankkártyával kapcsolatos kérdéseknek a vizsgálata és nem térek ki más nem készpénzes fizetési eszközökre.

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[275] eleget téve a tényállások módosítására és

[274] AMBRUS István – DEÁK Zoltán: Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből. Belügyi Szemle 2011/2. 85. o.
[275] 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.

egységesítésére került sor. A 2003. évi II. törvény 25-28.§- ai a tényállások elnevezését 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. §). A korábbi Btk. gazdasági bűncselekmények elnevezésű fejezetében, ezen belül is a pénzügyi bűncselekmények cím alatt szabályozta a jogalkotó, míg később az új Btk.-ba átkerültek a pénz- és bélyegforgalom biztonsága elleni bűncselekményekről szóló fejezetbe.

A bankkártyákkal kapcsolatos visszaéléseknek két típusa különböztethető meg az ún. „card-present csalás" és a „card-not-present csalás" és ezen csoportosítás mentén fogom ismertetni a szabályozást.[276]

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, amikor a bankautomatákra ún. skimmer (miniatűr adatrögzítő) eszközöket telepítenek. Egyre többféle eszközzel találkozhatunk például 3D-nyomtatóval készített billentyűzet, hamis ATM-nyílások, billentyűzetre néző kamerák. Ezen kívül arra is van példa, hogy közvetlenül az automatát fertőzik meg erre a célra kifejlesztett, rosszindulatú szoftverrel és így gyűjtik a gyanútlan felhasználók bankkártya adatait (pl. az interneten kézikönyvek érhetőek el a különféle ATM automatákhoz, ami a telepítést megkönnyíti).[277]

Amennyiben sikeresen megszerezték az adatokat, akkor ezek segítségével klónkártyákat készíthetnek és visszaélhetnek velük. A másik esetkör, amikor a rádiófrekvenciás jeleket rögzítik. Ebben az esetben az új és kényelmes fizetési megoldást nyújtó, PayPass-kártyával történő fizetést használják ki, ahol 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.[278]

[276] EUROPOL (2018): i.m. 40-45. o.
[277] CLOUGH: i.m. 226. o.
[278] 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.

Érdemes megemlíteni, hogy az ún. EMV (Europay Mastercard Visa) chipekkel ellátott kártyák megnehezítik a visszaélések lebonyolítását, 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 ennek köszönhetően a skimming technikát addig fogják hatékonyan kihasználni, amíg a mágnescsíkos kártyák használatát be nem tiltják teljesen.[279]

A bankkártyákkal kapcsolatos bűncselekményeknek jogi tárgya elsősorban a pénzforgalom zavartalan működéséhez fűződő társadalmi érdeknek a védelme.

Ezek az 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.[280] 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 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.[281]

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 az, 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

[279] EUROPOL (2018): i.m. 40. o.
[280] MOLNÁR (2018): i.m. 763. o.
[281] MOLNÁR (2018): i.m. 764. o.

elemeket átadja, megszerzi, az ország területére behozza, onnan kiviszi, vagy azon átszállítja. Ennek azért van különösen jelentősége, mert sokszor a bankkártyáknak, valamint az adatoknak a megszerzése mögött az a végső cél áll, hogy a különböző internetes Darknet fórumokon értékesítsék azokat, amelyekre nem mellesleg igen nagy kereslet is 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.[282] Az elvétel esetén pedig a bűncselekmény befejezetté válásához nincs szükség további elkövetési magatartásra, így a tartós birtokba helyezkedésre vagy annak szándékára, valamint pénzfelvétel megkísérlésére.[283] 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[284].

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 csalása miatt vonható felelősségre az illető.

Ezzel át is térnék a card-not-present csalás esetére, amikor a bankkártya fizikailag nincs jelen az elkövetéskor, így az offline fizetésnél használt védelmek sem mint az aláírás, PIN-kód és chip technológia. Ide tartoznak 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. Ezek a módszerek egyben érintik az internetes vásárlási tranzakciókat is.

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 céges rendszerekre. A botnetek képesek nagy mennyiségű személyes vagy egyéb titkos adat megszerzésére. Általában jól ismert bankok, pénzintézetek – vagy jól ismert cégek, szolgáltatók, sőt akár állami szervek – nevében küldenek e-mail üzeneteket, melyekben azt

[282] MOLNÁR (2018): i.m. 766. o.
[283] BH 2017.177.
[284] BH 2009.349.

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 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 az adathalászoknak az adatbázisába kerül. Ezt követően a bankszámlán található összegeket rövid időn belül más számlákra utalják át. Amennyiben a bankkártya adatokat adja meg, akkor az elkövetők már rendelkezhetnek is vele.

Másik módszer az ún. VoIP (Voice over IP), avagy vishing csalás, amikor IP-alapú telefont, hangüzenetküldő eszközt használnak arra az elkövetők, hogy az ügyfél telefonszámát hívják és megkérik adategyeztetési céllal, hogy közölje a bankkártya adatait, mert például letiltották azt és újra aktiválni kell.

Előbbi esetben, amikor 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 – amelynek a bankkártya is minősül – való visszaélése, amely esetén az elkövető a jogosulatlanul megszerzett ilyen eszköz felhasználásával okoz kárt. 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.[285] Ezzel szemben a készpénz-helyettesítő fizetési eszköz hamisítása nem szükségszerű eszközcselekménye a 375. § (5) bekezdésébe ütköző csalási cselekménynek, ezért egymással valóságos anyagi halmazatban állnak.[286]

[285] BH 2015.244.
[286] MOLNÁR (2018): i.m. 765. o.

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[287] és az ügyfeleik kárát megtérítik, ha azoknak nem volt felróható a bűncselekmény elkövetése, és ezáltal valóban ők lesznek a károsultak az esetek többségében. Ezt a Legfelsőbb Bíróság is kimondta a döntésében, hogy a bankkártya visszaélések tényleges károsultjai – és így a sértettjei – a bankkártyákat kibocsátó pénzintézetek.[288]

Emellett 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, hogy a szolgáltatónál vagy adóhatóságnál esedékes díjat, illetve tartozást 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 és formailag is úgy hozzák létre, hogy annak egyedi vonásai ne keltsenek gyanút. A támadást mindig megelőzi a kiszemelt célpontoknak a tanulmányozása (pl. munkahelyüket, viselkedésüket, szervezeti struktúrát 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) küldenek e-mailt, amelyben kérik, hogy egy sürgős banki tranzakciót hajtson végre, ezt pedig követhetik további levelek vagy akár telefonhívások, amelyben 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 megerősítést kérni. A másik eset, amikor nyilvánosan bejelentett eseménykor kerül sor a támadásra (pl. vállalati fúziók esetén), amikor bizonytalanság állhat fenn. Az ún. „whaling" esetében pedig a célpontok a szervezet vezetői.[289]

Ezek az említett esetek a hagyományos értelemben vett, Btk. 373. §-a szerinti csalásnak minősülnek.

A Készenléti Rendőrség Nemzeti Nyomozó Iroda rendelt el nyomozást hasonló ügyben, a Robert Bosch Elektronikai Kft. feljelentése alapján, mert ismeretlen személy vagy személyek

[287] 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.
[288] BH 2004.11.452.
[289] EUROPOL (2016): i.m. 32. o.

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 az elkövetők és onnan megszerezték a szükséges adatokat, valamint több postafiókot is lemásoltak, levelezésekhez hozzáfértek. A megadott bankszámlaszámot egy Lengyelországban működő bank vezette és egy fiktív lengyel cég nevén volt, amelyet a jogsegélykérelemnek köszönhetően a hatóságok 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.[290]

[290] Ez az átatuláshoz kapcsolódó csalás az angolszász rendvédelmi terminológiában „E-mail Business Compromise" elnevezéssel jelenik meg. A felvázolt esetről részletesen írt lásd NAGY Tamás: Business E-mail Compromise, avagy az átutalásokhoz kapcsolódó csalások. Belügyi Szemle 2018/7-8. 66-82. o.

2. A szervezett bűnözés az interneten

2.1. Bevezetés

A digitális gazdaság fejlődésének köszönhetően mind a bűnözés és mind az elkövetők motivációja jelentős mértékben megváltozott. Az informatikai hálózatok vonzó környezetté váltak a különböző profit-orientált bűnözők számára, mert a kockázat minimalizálása mellett jelentős profitra tudnak szert tenni.

A kibertér tökéletes környezetet jelent a bűnelkövetők számára, mert a határokon átível, magasfokú anonimitást biztosít és nincs szükség arra, hogy jelen legyenek az adott bűncselekmény elkövetésének a helyszínén.[291] Ez különösen kedvező, 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 technológiai fejlődést kihasználó elkövetők bűnelkövetése két csoportba osztható: 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-kereskedés) és másrészről vannak azok, amelyek a már említett módon a technológiai vívmányok nélkül nem léteznének, azaz a kiberbűncselekmények köre.[292]

Kétségtelen tény, hogy a hagyományos szervezett bűnözői csoportok számára is kedvezővé vált a modern technológiák használata, azonban az kérdéses, hogy milyen mértékben terjed ki a tevékenységi körül például a kiberbűnözésre. Emellett jellemző rájuk, hogy az ún. bűnözői feketegazdaságban[293] fejtik ki a különféle illegális tevékenységüket - melyet 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 kérdés merül fel:

---

[291] GYARAKI: i.m. 235. o.

[292] 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.

[293] 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."

- az internet egy új színteret jelent-e a tradicionális szervezett bűnözői csoportok számára a különböző illegális tevékenységük folytatásához és/vagy
- lehetőséget teremt az új típusú, „szervezett" kiberbűnözői csoportok működéséhez, amik kifejezetten a kiberbűncselekmények elkövetésére specializálódnak.

2.2. A szervezett bűnözés fogalma és a hazai szabályozás

A szervezett bűnözői csoportok működését és értékrendjét meghatározzák azok az országok, társadalmak, illetve kultúrák, amelyekben működésüket 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.[294] 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, azonban emellett jellemzően foglalkoznak még fegyverkereskedelemmel, embercsempészéssel, termékhamisításokkal és a kiberbűnözéssel is, melyeket járulékosan a pénzmosás követ.[295]

A nagyobb „tradicionális", hierachikus szervezett csoportoktól kezdve a kisebb és lazább szerkezetű csoportok vannak jelen, akiket sok esetben „felbérelt" önálló speciális szaktudással rendelkező bűnözők 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, akikkel szemben folyamatban lévő nyomozás is van, 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 kiberbűncselekményekkel kapcsolatban figyelhető meg, és ezeket növekvő számban önálló bűnelkövetők is mint egy vállalkozásként folytatnak akár többen együtt alkalmi

[294] TÓTH Mihály – KŐHALMI László: A szervezett bűnözés. In: Borbíró Andrea - Gönczöl Katalin - Kerezsi Klára - Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016. 608. o.
[295] ABADINSKY, Howard: Organized crime. Ninth Edition, Wadsworth Cengage Learning, 2010. 203. o.

jelleggel, hogy vállalkozásukat működtessék, ami általában illegális árucikkekkel való kereskedést vagy különféle szolgáltatások nyújtását jelenti.[296]

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.[297]

2000 óta az Egyesült Nemzetek keretében létrejött nemzetközi szervezett bűnözés elleni Egyezmény határozza meg a nemzetközi fogalmát a szervezett bűnözői csoportnak, amely értelmében bizonyos ideig fennálló, három vagy több főből álló strukturált csoportról[298] van szó, amely összehangoltan működik egy vagy több, az Egyezményben meghatározott súlyos bűncselekmény[299] elkövetése céljából, közvetlen vagy közvetett módon pénzügyi vagy más anyagi haszon megszerzésére törekedve.

Ezt a definíciót vette át az országok többsége, így Magyarország is. Ennek fényében a hatályos Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 459.§ (1) bekezdés 1. pontja határozza 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.

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,

[296] 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.]

[297] KORINEK László: A szervezett bűnözés lényegi elemei. In: Harmadik Magyar Jogászgyűlés – Magyar Jogász Egylet. Budapest, 1996. 65-72. o.

[298] 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.

[299] Az Egyezmény definiálja továbbá a súlyos bűncselekményt is, melynek értelmében legalább négy év szabadságvesztéssel vagy súlyosabb büntetéssel büntethető bűncselekményt megvalósító magatartást jelenti.

de nem jön létre bűnszervezet. E fogalomnak a negatív eleme, hogy nem jöhet létre bűnszervezet.[300]

Áttérve azonban a bűnszervezet fogalmi ismérveinek részletes vizsgálatára: az "összehangolt működés" tartalmát tekintve nem más, mint a benne cselekvő személyek egymást erősítő hatása. Ugyanakkor az összehangoltság meglétének – természetéből adódóan – nem feltétele a bűnszervezetben cselekvők közvetlen kapcsolata, a más cselekvések, illetve a más cselekvők kilétének konkrét ismerete. A bűnszervezetben elkövetés azzal szemben is megállapítható, aki – eseti jelleggel – akár egyetlen cselekményt tettesként vagy részesként valósít meg, tehát 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. 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. hatályos rendelkezései nem tesznek különbséget a bűnszervezeten belüli cselekvés hiearchiája ("posztjai"), aktivitása, intenzitása szempontjából, ezek a büntetéskiszabás körében értékelendő körülmények.[301] A bűnszervezet megállapításához nem többletkövetelmény a bűnös profitszerzési célzat.[302]

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.[303] 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

[300] Lásd bővebben GELLÉR Balázs - AMBRUS István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017. 410-425. o.
[301] 4/2005. számú BJE határozat; TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009. 148-151. o.
[302] BH 2008.139.
[303] BH 2018.4.106.

kihasználják az internet nyújtotta előnyöket és például az illegális tevékenységüket az online piacterekre kiterjesztve folytatják (pl. kábítószer-kereskedelem, gyermekpornográf tartalmak terjesztése stb.).

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.[304] Ezt erősíti a Kúria friss 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. A bűnszervezeten belüli személyes ismeretség valamennyi elkövetővel nem feltétele a megállapításának, és a bűnszervezetnek nem törvényi kritériuma a hierarchikus kapcsolat sem.[305] 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.[306] Amennyiben mégis hierarchikus szervezetről van szó, akkor a bűnszervezet vezetője felbujtóként tartozik felelősséggel a bűnszervezet tagjai által elkövetett bűncselekményekért.[307]

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.[308]

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

[304] BH 2010.11.472.
[305] BH 2016.9.234.
[306] CSÁK Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018. 328-329. o.
[307] EBH 2008.1849.
[308] BH 2014.131.

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, mely 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.[309] Ez alapján legalább két bűncselekmény szükséges a 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 delictumával foglalkozni, mert az új Btk. hatályba lépését követően már nem a sértettek számához igazodik, hanem törvényi egység jön létre[310], 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.[311]

Összességében elmondható, hogy a bűnszervezet fogalmába a bűnöző célzatú tartós struktúrák számos formája beilleszthető, amely alkalmas lehet arra, hogy egyrészről kifejezze az alkalmi kisebb súlyú bűnszövetséghez viszonyított többletkriminalitást, másrészről magában foglalja a szervezettség súlyosabb formájában rejlő veszélyességet is. A bűnszervezet keretében történő elkövetéshez bármely szándékos bűncselekmény esetén súlyos általános részi jogkövetkezmények[312] társulnak - mivel a hatályos szabályok szerint általános jellegű minősítő

[309] AMBRUS István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014. 20. o.
[310] OTT István: Dogmatikai kérdések a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye kapcsán. Magyar Jog 2016/12., 717-721. o.
[311] Balassagyarmati Törvényszék B.210/2014/127.
[312] 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];

körülmény -, míg a bűnszövetség esetében a bűncselekmény súlya közömbös, de csak akkor állapítható meg, ha a Különös Részben minősítő körülményként szerepel.[313]

A Btk. 321.§ (1) bekezdése szerint bűnszervezetben részvétel bűntette miatt büntetendő, aki bűncselekmény bűnszervezetben történő elkövetésére felhív, ajánlkozik, vállalkozik, a közös 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 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.[314] 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

---

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].

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

[314] 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.

bocsátásában testet öltő magatartás és az anyagi eszközök rendelkezésre bocsátása, esetleg a tekintélyen, befolyáson alapuló pszichikai támogatás között.[315]

Ezzel szoros összefügésben érdemes arra kitérni, hogyha egy adott, kívül álló 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 kapcsolódnak és ezek a súlyos bűncselekmények megvalósulását biztosítják, akkor a bűnszervezetben részvétel bűntettét valósítják meg.

A kiberbűncselekmények vonatkozásában fontos kiemelni a 2013/40/EU irányelvet az információs rendszerek elleni támadásokról, mert kimondja, hogy helyénvaló súlyosabb szankciókat megállapítani, ha az információs rendszer elleni támadást bűnszervezetben követik el, valamint, ha jelentős számú információs rendszert érint.[316]

2.3. A kiberbűnözői csoportok tipológiája

A kiberbűnözői csoportok tipológiáját átfogóan Michael McGuire vizsgálta, 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 a kibertérben, emellett újabb és kevésbé szoros kapcsolatú bűnözői csoportok jelennek meg. A bűnözői csoportok különböző szintű szervezettséget mutatnak, attól függően, hogy a tevékenységüket csak online fejtik ki, vagy online eszközöket használnak, hogy lehetővé tegyék a bűncselekmények elkövetését a „való” világban, vagy ezek kombinációja jelenik meg online és offline is.

MCGUIRE egy 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.

[315] TÓTH (2015): i.m. 7. o.
[316] 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.]

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 ilyen az Anonymous hacktivista csoport is.

A „hub" csoportok szintén online működnek, de a „swarm"-hoz képest szervezettebbek és hiearchikusabbaknak tekinthetők, mert meghatározott „irányító, létrehozó" kulcstagok köré csoportosulnak „az egyszerű" tagok. A tevékenységük széleskörű magában foglalhatja a crimeware[317] terjesztést, az adathalász támadásokat (phishing) 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 a kibertér nyújtotta előnyöket is kihasználják már.

A „hierarchies" azok a tradicionális bűnözői csoportok, akik illegális tevékenységüket a kibertérben 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

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

zsarolást kibertámadások felhasználásával követik el.[318] A nemzetközi szindikátusok is érintettek a kiberbűnözésben mint például a Triádok vagy Yakuzák, akik szoftver kalózkodással, bankkártya hamisításokkal és csalásokkal is foglalkoznak.[319]

Az „aggregate" csoportok pedig lazán szervezettek, ad hoc jelleggel működnek. Például mobiltelefonokat használnak a csoport tevékenységének a koordinálásához vagy a nyilvános zavargás szervezéséhez.[320]

A téma szempontjából két csoportot érdemes kiemelni és részletesen ezek összehasonlításával foglalkozik a szerző: a „hierarchies", a tradicionális szervezett bűnözői csoportok és a „hub" mint az új típusú kiberbűnözői csoport.

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

A tradicionális szervezett bűnözői csoportok általában etnikailag homogének, formailag és hierarchikusan strukturáltak, egy 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, az internet felhasználásával.[321]

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 szakmeretüknek, 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 annak érdekében, hogy ellenőrzésük alatt tarthassák az általuk dominált piacot, addig a területi

[318] MCGUIRE, Michael: Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security. 2012.
[319] KIM-WANG, Raymond - Choo-GRABOSKY, Peter: Cybercrime. In: Paoli, Letizia: The Oxford Handbook of Organized Crime. Oxford University Press, 2014. 485. o.
[320] BROADHURST – GRABOSKY - ALAZAB-CHON: i.m. 7. o.
[321] MALAS, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017. 365 o.

kontroll a kibertérben nyilván nem kivitelezhető a virtuális környezet sajátosságaiból adódóan, éppen ezért kedvező feltételeket biztosít azok számára is, akik amúgy az adott piacról kiszorulnának. Továbbá a kontroll mechanizmus még nehezebbé vált, 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). Az új típusú szervezett bűnözés működése a digitális környezetben hasonlóságot mutat a modern vállalati világhoz különösen, ami az alkalmazott árazási stratégiát, szolgáltatás-alapú versenyt, innovációt és az „ügyfélszolgálatot" illeti. 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 meghatározó tényezővé váltak, mert az emberek 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 és kifinomultság határozza meg a különféle kibertámadások terén, illetve a specializáció vagyis munkamegosztás az elkövetők között, a kommercializáció és az integráció, ami azt jelenti, hogy az egyes jogsértéseket további jogsértés követi mint például az adatlopást követően 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 arra vonatkozóan, hogy az illegális tevékenységüket elfedjék. 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 innovációnak köszönhető, hogy a bűnözői ökoszisztémában új minták jelentek meg - amit mindkettő csoport ki is használ - mint például az áruk elhelyezésével, alvállalkozásokkal és kapcsolatépítéssel kapcsolatban. A bűnözők olyan rendszert alkalmaznak, amelyek

hasonlóságot mutatnak a jogszerűen működő vállalkozásokéhoz a B2B (Business-to-Business) modellhez, mint például a C2C (Criminal-to-Criminal) modellek, amelyek elérhetővé teszik az illegálisan megszerzett adatokat és eszközöket a digitális hálózatokon keresztül. Az információs rendszerek és programok sebezhetőségeit használják ki ahhoz, hogy crimeware-t hozzanak létre.[322]

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, amelyek a felhasználók tudta nélkül megfertőzött számítógépekből állnak és ezek az elkövetők által távolról irányíthatók mint egy „zombigépként". 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 adathalászati technikák alkalmazásával.[323]

2.5. Specializáció és munkamegosztás

A kiberbűnözői iparág egy tág spektrumú tevékenységi kört ölelhet fel, amelyben a különféle elkövetők funkcionálisan specializálódnak az egyes tevékenységekre, tehát a munkamegosztás jelen van és a feladatok megosztása a következőképpen alakulhat:

A programozók azok, akik a különböző rosszindulatú programokat (malware) írják meg és egyéb eszközöket rendelkezésre bocsájtják, 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 ún. „root level access", illetve „god level access" szintű hozzáférést szerezzenek.

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

A csalás specialisták pedig különböző ún. social engineering 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, ún. „money mule"-ok 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.[324]

2.6. Az online feketepiacok 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[325] vagy a Darkneten, melyekkel bármilyen kiberbűncselekmény elkövethető. 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 „The Onion Router" (TOR), I2P vagy Freenet, amelyek magasfokú titkosítással vannak ellátva. A bűnelkövetők kihasználják ezeket, mert a használatuk révén könnyedén eltudják rejteni a személyazonosságukat, az internetes forgalmukat és a szerverük helyét.

Ahogy már korábban említésre került ezt az üzleti modellt az önálló kiberbűnözőktől kezdve – akik számára a kibertér 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, akár a kiberbűnözőktől.

A különböző illegális online tevékenységek egy egyre fejlettebb és önálló digitális feketegazdaságot hoztak létre, amelyen belül speciális weboldalakat üzemelnek, ún. online feketepiactereket és fórumokat, amelyeket arra használnak, hogy a tilalmazott árukkal

[324] CHABINSKY, Steven R. (2010): https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom [2018.03.05.]
[325] A hagyományos böngészők használatával szabadon elérhető része az internetnek.

kereskedjenek és szolgáltatásokat hirdessenek, amiket együttesen „hidden services”-nek, azaz rejtett szolgáltatásoknak hívnak.

A leghíresebb online feketepiacok a Silk Road, Alphabay[326] és Hansa volt. A Silk Road-ot Ross William Ulbricht alapította és üzemeltette - mint adminisztátor - 2011 és 2013 között, Dread Pirate Roberts néven, és így többek között kábítószer-kereskedelem bűnszervezetben történő elkövetésért, informatikai bűncselekmények bűnsegédjeként, valamint pénzmosásért és hamisított személyazonosító okmányokkal való kereskedésért életfogytiglan szabadságvesztésre ítélték. Az oldal leállítását követően rövid időn belül útjára indult a Silk Road 2.0 és azóta is számos hasonló céllal létrehozott weboldal található.[327]

A nemzetközi bűnügyi együttműködésnek köszönhető, hogy az Alphabay és a Hansa - mint két legnagyobb fórum - működését sikerült leállítani. Mindez az amerikai Szövetségi Nyomozó Iroda (Federal Burea of Investigation, FBI), a Kábítószer-Ellenes Hivatal (Drug Enforcement Agency, DEA), valamint a holland nemzeti rendőrség és az Europol közreműködésével valósult meg.[328]

A piactereken és fórumokon belül gyakran jelen van egy merev és egyedülálló struktúra, 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 megbízható személyek, gyakran az alfórum témájában jártas szakemberek és ezért annak a tartalmát kezelik. A fórumokon találhatók nagyszámú 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, hogy különféle kiberbűncselekmény elkövetésében részt vehessenek a megszerzett ismeretek és eszközök révén.[329]

[326] Érdekesség, hogy az Alphabay több mint 200 000 felhasználóval és 40 000 eladóval rendelkezett. 250 000 listázott kábítószer és mérgező vegyszerek, valamint több mint 100 000 listázott egyéb illegális termék volt elérhető. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down [2018.08.21.]
[327] United States v. Ulbricht, 31 F. Supp. 3d 540, 569-70 (S.D.N.Y. 2014)
[328] U.S. DEPARTMENT OF JUSTICE: Report of the Attorney General’s Cyber Digital Task Force. Washington, 2018. 137-138. o.
[329] EUROPOL: The Internet Organised Crime Assessment (IOCTA). 2014. 19-21. o.

Az illegális árukkal való kereskedésnek a Darkneten keresztül számos előnye van mind az eladók és 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 és közvetítő nélkül tranzakciókat folytathatnak le. Ezeket magasfokú anonimitás jellemez, amely során egyik félnek sem kell személyes adatot megadnia, bár a vásárló számára a fizikai áruk vásárlásakor nyilván meg kell adni egy szállítási címet, azonban manapság a kézbesítés különböző anonim helyekre is történhet (pl. csomag automatákba), így az áruk átvételekor is biztosítható az áruért érkező személy anonimitása. A tranzakciók lebonyolításához általában a nehezen lenyomozható virtuális fizetőeszközöket használnak.

Az online feketepiacokon, illetve fórumokon jellemzően az alábbi áruk adásvétele zajlik: kábítószer, gyermekpornográf tartalmak, hamis és hamisított áruk, fegyverek 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 kábítószer előállításban, forgalmazásban és terjesztésben, amely során a kibertér 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 a havi bevétele az első nyolc Darknet piactérnek 10,6 millió és 18,7 millió euró között mozog, ami kizárólag a kábítószer-kereskedelemből származik, és nem számítjuk bele az egyéb, a csak receptre kapható gyógyszereket és a dohányárut.[330] A kábítószer-kereskedelemet a Btk. 176.§-ban szabályozza, mely szerint, 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.§), teljesítményfokozó szerrel visszaélés (Btk. 185.§). Végül a gyógyszerhamisítás (Btk. 185/A.§) is.

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014 [2018.03.25.]

[330] EUROPOL (2017): i.m. 49-50.

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, az aki tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf műsorban szerepeltet, és egy évtől öt évig terjedő szabadságvesztéssel büntetendő.[331]

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 vonhatóak legyenek, akik a gyermekpornográf anyagokhoz online hozzáférnek, például külön erre a célra létrehozott oldalakon keresztül nézik, anélkül, hogy letöltenék azt (így 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 abból, hogy az elkövető ismétlődő jelleggel látogatja a weblapot vagy szolgáltatásként fizet érte. Az egyes joghatóságokban ez a jogsértés a birtokláson belül kerül szabályozásra (pl. Németországban), a magyar szabályozásnak pedig még nem része. A cache-ben tárolt képek

[331] 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.

nem elegendőek a felelősségre vonáshoz a birtoklásért, anélkül, hogy bizonyítást nyerne az, hogy az adott személynek tudomása lenne az elkövetett magatartásról.[332]

2.6.3. Hamis és hamisított termékekkel kereskedés

Az Europol szerint a hamis és hamisított termékek is népszerűek, amelyek széles skálája elérhető mind a Suface Weben és a Darkneten is: ruházati termékek, ékszerek, „kalóz" szoftverek, gyógyszerkészítmények, előfizetések különböző TV és zenei platformokhoz, online játék fiókokhoz, valamint a legkeresettebb termékek közé tartoznak a hamis, meghamisított pénzek és személyazonosító okmányok.

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.[333] Az adat befolyásolja az illegális piacok 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).[334] A bankkártya és az online bankfiók adatok a legkeresettebbek. Így a következő bűncselekmények

[332] DORNFELD – MEZEI: i.m. 34. o.
[333] EUROPOL (2014): i.m. 19-21. o.
[334] TROPINA (2012): i.m. 162. o.

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.§)[335].

A pénzügyi adatokon kívül még elérhetőek lakcímek, telefonszámok, e-mail címek, e-pénztárcák, társadalmibiztosítási számok 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. További népszerű szolgáltatás, hogy a DDoS támadások indítására szolgáló botneteket, illetve a létrehozásukra szolgáló eszközöket, programokat lehet igénybe venni (DDoS-for-hire vagy DDoS-as-a-Service) – napi vagy havi díjjal átlagosan 5$ és 1000$ közötti áron.[336] Hasonlóképpen a különböző rosszindulatú programokhoz (pl. vírusokhoz) is hozzá lehet jutni szolgáltatásként mint például a legkönnyebb pénzszerzési módhoz: a zsarolóvírushoz (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 elemei kikerültek a „szabadpiacra" és tovább fejlesztve már hasonló mechanizmusokat tartalmazó malware-ek is elérhetővé váltak mint a DuQu).[337]

Azért különösen veszélyes a Criminal-as-a-Service üzleti modell, mert könnyen hozzá lehet jutni a kiberbűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár kész bűnözői infrastruktúrához, és ezért is 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. Ennek

[335] 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. http://ugyeszseg.hu/a-darknet-hasznalatanak-veszelye-birosag-ele-allitas/ [2019.03.15.]

[336] EUROPOL: (2014): i.m. 19-21. o.

[337] 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.

megfelelően a Btk. 424.§-ban szabályozza az információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét, melynek értelmében büntetendő, aki jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz; valamint aki, a jelszó vagy számítástechnikai program készítésére vonatkozó szervezési ismeret másnak a rendelkezésére bocsájtja. A megszerzett ismeretekkel kiberbűncselekményeket tudnak elkövetni, amit a Btk. a 423.§-ban az információs rendszer vagy adat megsértése bűncselekmény körében szabályozza mind a jogosulatlan és a jogosultság keretének túllépésével elkövetett módozatokat így az (1) bekezdés a jogosulatlan belépést (ún. hacking), (2) bekezdés a) pontjában az információs rendszer akadályozását, (2) bekezdés b) pontjában az adat megváltoztatását, törlését vagy hozzáférhetetlenné tételét, végül a (3) és (4) bekezdés szerinti minősített esetek valósulnak meg, ha jelentős számú információs rendszert, illetve közérdekű üzemet érint a bűncselekmény.

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 a gazdasági kémkedés vagy személyes adatok gyűjtését a meghatározott célponttól.

Fordításokhoz kapcsolódó szolgáltatások: A támadások sokszor országspecifikusak és előfordulhat, hogy az elkövető nem feltétlenül beszéli a cél ország nyelvét, ezért igénybe vehet szolgáltatást fordítóktól, akik helyesen megfogalmazott szövegeket nyújtanak nekik, ezzel maximalizálva 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 általuk az meghatározott díj ellenében.[338] 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.[339] Ezek a szolgáltatások magukban foglalják az online és offline megoldások kombinációit, amelyeknek a középpontjában általában a pénzfutárok, az ún. „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

[338] EUROPOL (2014): i.m. 19-21. o.
[339] TÓTH (2002): i.m. 375. o.

elkövetésében.[340] A pénzmosásnak (Btk. 399.§) a három fázisa, így az elhelyezés, rétegzés és az integráció ezekben az esetekben is megvalósul. Ezzel szoros összefügésben új trendként jelent meg, hogy a nagyobb összegek tisztára mosása úgy történik, hogy azt kisebb összegű tranzakciókra bontják (micro money laundering), melynek előnye, hogy kevésbé feltűnő.[341]

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

3. A pénzmosás az interneten

3.1. Általános bevezető

A pénzmosás is azon bűncselekmények köréhez tartozik, amelyet szervesen érint az informatikai fejlődés és az elkövetését jelentősen megkönnyítette. Gondoljunk csak a bankoknak és az egyre bővülő online szolgáltatásaikra, amelyeken keresztül könnyedén tudunk rövid időn belül akár több utalást is végezni, mindezt anélkül, hogy be kellene fáradnunk egy bankfiókba.

Daniel Adeoyé Leslie kísérletet tett arra is, hogy az ún. „cyberlaundering" fogalmát meghatározza, amely elnevezés a pénzmosás és a technológia kettősét foglalja magában, így ennek tekinti azt az esetet, ha számítógépet használnak a pénzmosás során így például egy tranzakció lebonyolításához. A számítógép az eszköz, azonban a színteret ehhez az internet biztosítja.[342]

Jelen fejezetben elsősorban a pénzintézetekkel és a pénzügyi műveletekkel összefüggésben felmerülő kérdéseket vizsgálom a hazai szabályozás fényében.[343]

3.2. 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

[342] LESLIE, Daniel Adeoyé: Legal Principles for Combatting Cyberlaundering. Law, Governance and Technology Seriec Volume 19. Springer 2014. 55. o.

[343] Érdekességként említhetők még más pénzmosási sémaként a következők: A hagyományos szervezett bűnözői csoportok számára népszerű bevételi forrást jelentenek az általuk üzemeltetett különböző online szerencsejáték oldalak is, amelyek alkalmasak az illegális bevételek tisztára mosására. A virtuális hálózatokon is, akár a valós térben elterjedtek a különféle szerencsejátékok és fogadási oldalak. Általában az ismeretlen felhasználókkal korrektnek nevezhető módon játszanak, de a „bennfentes" felhasználók csak vesztenek, vagyis csak befizetnek oda. Emellett még a különböző online játékok is példaként szolgálhatnak. A „Second Life" játékban 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. Sőt, ahhoz, hogy előbbre jusson, pénzbefizetéssel ez is elérhetővé lesz. 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 – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70. 29. o.

más által elkövetett alapbűncselekményhez kapcsolódó pénzmosás minősült bűncselekménynek.

A virtuális térben végrehajtott pénzmosásnak is ugyanaz a célja, mint a valós térben, azaz jellemzően gazdasági tevékenységek alatt folytatott illegális pénzügyi művelet, amelynek célja az, 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 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.

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.[344] 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, ami már köszönhető részben az internet használatának is.

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 a korábbi Btk.-tól (315.§ 2. bekezdés) – 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[345] 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

[344] TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. Budapest: KJK Kerszöv 2002. 357. o.

[345] 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.

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.[346] 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 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.[347]

E kérdésben egyetértek Tóth Mihály 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.[348] 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.[349]

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."[350] 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

[346] FÖLDVÁRI József: Büntetőjog – Általános rész. Budapest, Osiris Kiadó, 2001. 128. o.
[347] 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.
[348] 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.
[349] A teleologikus értelmezés büntetőjogi alapkérdéseiről bővebben lásd SZOMORA Zsolt: A jogi tárgy funkciói és a jogtárgyharmonikus értelmezés. Bűnügyi Szemle 2009/2. 11–17. o.
[350] MOLNÁR (2009): 519. o.

bűncselekmény egyértelmű megállapíthatósága érdekében szükséges a célzatot megalapozó körülmények tényállásba foglalása is.[351] Ezzel szoros összefüggésben megemlítendő, hogy Megemlítendő, hogy a Varsói Egyezmény[352] 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".

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.[353]

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.[354]

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.[355]

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.[356] 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.

[351] Debreceni Ítélőtábla Bf.II.390/2013/12.
[352] Az Európa Tanács pénzmosásról, a bűncselekményből származó jövedelmek felkutatásáról, lefoglalásáról és elkobzásáról, valamint a terrorizmus finanszírozásáról szóló, Varsóban, 2005. május 16-án kelt Egyezménye
[353] Miskolci Törvényszék 11.B.986/2010/75.
[354] Fővárosi Törvényszék 2.B.282/2012/21.
[355] BH2006.143; Heves Megyei Bíróság B.582/2010/199.
[356] KÁRMÁN Gabriella – MÉSZÁROS Ádám – TILKI Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3. 92. o.

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".[357]

A saját pénzmosással kapcsolatban fontos kihangsúlyozni, hogy csak azok a magatartások nyerhetnek önálló büntetőjogi értékelést, amelyek nem szükségszerű velejárói az 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.[358]

Ezzel szoros összefüggésben a saját pénzmosás felveti a látszólagos anyagi halmazatot érintő büntetlen utócselekmény kérdéskörét is.[359] 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.

[357] GÁL István László: A pénzmosás. Complex Kiadó, Budapest, 2004. 76. o.
[358] 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.
[359] 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.

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 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.[360]

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 az I. rendű 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. Az I. rendű vádlott a Kft. nevében történt valuta-átváltásokat igazoló bizonylatokat a könyvelőjének átadta, azokat nem kívánta elrejteni, vagy eltitkolni.[361]

Szabó Imre álláspontja is ezt erősíti, mely 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

[360] AMBRUS István: Egység és halmazat – régi dogmatikai kérdés, új megközelítésben. Generál Nyomda Kft. Szeged, 2014. 281. o.
[361] BH 2006.143.

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.[362]

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.[363]

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.[364]

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. Az új Btk. szabályozásában lényegi változás az alapbűncselekményeket érintette, mert a régi Btk. értelmében a szabadságvesztéssel büntetendő cselekményhez kapcsolódhatott pénzmosás, míg az új Btk. ezek körét bővítette és elegendő, ha büntetendő cselekményhez kapcsolódik járulékos jelleggel.[365] Tehát a pénzmosás az alapbűncselekményből származó dologra elkövetett járulékos magatartásokat rendeli önállóan büntetni, ezért az elkövetése fogalmilag kizárt mindaddig, amíg az alapcselekmény – vagy az

[362] SZABÓ Imre: A pénzmosás a bírói gyakorlat tükrében. Ügyészek Lapja 2017/1. 56. o.
[363] Fővárosi Törvényszék 12.B.1229/2011.
[364] Fővárosi Ítélőtábla 5.Bf.38/2010/38.
[365] 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.

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.[366]

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.[367]

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.”[368]

A büntetőjogi szakirodalomban uralkodó álláspont, hogy a két cselekmény között csak valódi anyagi halmazat állapítható meg.[369] A pénzmosás az alapbűncselekményhez képest más társadalomra veszélyességgel, valamint önálló jogi tárggyal rendelkező bűncselekmény,[370] 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

[366] MOLNÁR (2018): i.m. 800. o.
[367] GELLÉR – AMBRUS: i.m. 432. o.
[368] Bfv.I.830/2017/16.
[369] 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.
[370] A pénzügyi szektor és a gazdaság egyéb szereplőinek a törvényes működéséhez fűződő érdek, valamint a szervezett bűnözés elleni fellépés eredményességéhez fűződő érdek.

elkövetett bűncselekmény is alapcselekménye lehet a pénzmosásnak, feltéve, ha az alapcselekmény mindkét országban tényállásszerű és büntetendő.[371]

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 körülmény sem értékelhető kétszeresen, de semmi sem maradhat értékelés nélkül.[372] Ammenyiben egy adott tevékenység - vagy mulasztás - két vagy több bűncselekmény törvényi tényállásának eleme, az csak az egyik bűncselekmény megállapításánál lehet figyelembe venni.[373] A bűncselekmény minősítése során a bírói gyakorlatban is szerepet kaphat az azonos körülmény kétszeres büntetőjogi értékelésének a tilalma.[374]

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.

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[375], 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

---

[371] 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.

[372] BELOVICS Ervin – GELLÉR Balázs – NAGY Ferenc – TÓTH Mihály: Büntetőjog – Általános rész. HVG-Orac Lap- és Könyvkiadó Kft. Budapest, 2015. 76-77.

[373] 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.

[374] BH 2000.279.

[375] „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.

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.

3.3. Az ún. „money mule" jelenség

A saját pénzmosáson kívül külön foglalkozom a Btk. 400. § (1) bekezdésében szabályozott gondatlan alakzattal is, amely az ún. „money mule" jelenséghez, azaz a pénzfutár személyek felhasználásával elkövetett cselekményekhez kapcsolódik. Ez Európa szerte ismert pénzmosási technika és gyakran alapbűncselekményként a kiberbűncselekmények jelennek meg.[376]

Például a már jól ismert adathalász technikát alkalmazva az ismeretlen személyek különböző bankok áloldalait készítik el, majd ezt követően megtévesztő elektronikus leveleket küldték szét a banki ügyfeleknek, hogy az oldalt meglátogatva lépjenek be a banki azonosítójukkal, számlaszámukkal és jelszavukkal. A megtévesztést követően az elkövetők a megszerzett adatok birtokában belépnek a sértettek számlájára és banki tranzakciókat kezdeményeznek, és ezzel kárt okozva nekik.

A pénzfutárokat általában megtévesztő módon, jogszerű tevékenység látszatát keltve toborozzák, szervezik be (pl. legálisnak tűnő és rendkívül kedvező állásajánlattal) az interneten keresztül (pl. e-mailen keresztül vagy közösségi oldalak használatával). Ezt követően vállalják, hogy különböző pénzösszegek fogadására pénzintézeteknél bankszámlát nyitnak vagy a meglévő számlájukat rendelkezésre bocsájtják, és az onnan felvett összegeket ismeretlen megbízójójuk számára készpénzben átadják vagy továbbutalják 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.[377]

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.[378] A „money mule" a tudattartalmának vizsgálata kiemelten fontos, mert ez lesz a minősítésnek az alapja. A dolog eredetét átfogó tudattartalomra az elkövetés körülményeiből,

[376] EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2018.
[377] TROPINA, Tatiana: Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum 2014. 5-6. o.
[378] KÁRMÁN – MÉSZÁROS – TILKI: i.m. 90. o.

azaz az elkövetési magatartás megvalósításával kapcsolatos ténymegállapításokból (pl. a bankszámlára érkező pénzösszegek nagyságrendjéből, a terhelt és megbízója között kapcsolatból[379]) 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.

Az ilyen, általában pénzmosásként értékelt cselekmények közös jellemzője továbbá, hogy az alapbűncselekmény elkövetésének és az eredetleplezés színhelyének országa különböző.[380]

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.[381]

[379] Fővárosi Törvényszék B.555/2015/15.
[380] SISÁK Attila: A pénzmosás elleni küzdelem tapasztalatai egy nyomozó hatóság gyakorlatában. Kriminológiai Közlemények 72. 91. o.
[381] 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 kihívásai

4.3. A kriptovalutákról általában

A blockchain technológia[382] és az erre alapuló kriptovaluták használatának elterjedése kihívások elé állítják a jogalkotókat és jogalkalmazókat egyaránt. A Bitcoin 2009-es megjelenése óta, a kriptovaluták témakörét különböző szakpolitikai döntéshozók vizsgálták eltérő megközelítést alkalmazva, azonban közös vonás, hogy valamennyien a virtuális fizetőeszközök egyik alcsoportjának sorolták be.[383] Az Európai Központi Bank a virtuális fizetőeszközöket három csoportra osztotta: a zárt rendszerrel rendelkezőkre, amelyek nem válthatóak 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.[384]

Fontos megemlíteni, hogy a sajátos jellegűknél fogva a kriptovaluták nem tekinthetők pénznek, mert a pénzkibocsátás egy intézmény által, szigorúan szabályozott keretek között történik, az alábbiak szerint: jegybankok, valamint hitelintézetek által hitelezés keretében vagy elektronikus pénz kibocsátásával ún. e-money licenc birtokában. Ezzel szemben a kriptovaluták nem rendelkeznek központi kibocsátóval, hanem komplex matematikai feladatokat megoldó számítógépek hálózatának segítségével jönnek létre. Fizikai formában nem, csak digitálisan

---

[382] 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

[383] Lásd részletesen: 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., http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

[384] 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

érhetők el, de törvényes fizetőeszközre át- és visszaválthatók, valamint 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 értékét kizárólag annak kereslete és kínálata határozza meg.

A kriptovaluták – mint ahogy az elnevezésük is utal rá – alapját 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.[385]

A Bitcoin elnevezés egyben egy digitális fizetési rendszert is magában foglal, amelynek a kifejlesztése Satoshi Nakamoto nevéhez fűződik.[386] Kliensszoftverre ingyenes, nyílt forráskódú[387], 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.[388] Digitális javaknál felmerül egy probléma, ami a fizikai formában létező eszközöknél nem. Egy adott pénzérme vagy bankjegy fizikailag csak egyvalakinek a birtokában lehet, míg a virtuális javakat korlátlan mennyiségben másolhatunk, így több, az eredetivel

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

[386] 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.

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

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

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 érme elköltésére, amelyik időben előbb következett be, ezáltal kiküszöbölhető a „kétszeres elköltés problémája".[389]

Az utaláshoz egy kulcspár szükséges, ami áll egy nyilvános kulcsból (public key), ez másnéven a Bitcoin-cím[390], ami hasonló a bankszámlacímhez és mindenki számára nyilvános, valamint egy privát kulcsból (private key)[391], ami mint egy 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.[392] 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.[393] 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 a legbiztonságosabb 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).

---

[389] TÜZES Marcell: Bitcoin - A pénz új formája. Infokommunikáció és jog 2012/4. 156. o.
[390] 1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55
[391] 5JBvhsfA5JesmcVTGNrb3gkHGgv67hwY5hUws1Pmdj65jRM9nPF
[392] ESZTERI Dániel: Bitcoin - Az anarchisták pénze vagy a jövő fizetőeszköze? Infokommunikáció és Jog 2012/2. 71. o.
[393] SZATHMÁRY (2015): i.m. 642-643. o.

- Agypénztárca (brain wallet): amikor a felhasználó megjegyzi a privát kulcsot.[394]

Érdemes ismertetni a kriptovaluták piacán jelenlévő kulcsszereplőket is:

- 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[395] (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.[396]

A Bitcoinon kívül érdemes az egyéb kriptovalutákról, ún. altcoinokról[397] 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[398] futtat, éppen ezért az alkalmazásában sokkal nagyobb potenciál 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

[394] SIMON Béla: A kriptovaluták rendészeti kihívásai. In: Mezei Kitti - Nagy Zoltán András (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK. Pécs, 2019. 171. o.
[395] TÜZES Marcell: Bitcoin - A pénz új formája. Infokommunikáció és jog 2012/4. 157. o.
[396] HOUBEN - SNYERS: i.m. 25-27. o.
[397] 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).
[398] 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.

tranzakciókat biztosít: a Bitcoin esetén 10 perc egy utalás, míg az Etherum használatakor 14 másodperc.[399]

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.[400]

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 tranzakciók is nyilvános szerepelnek 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.[401]

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.[402]

A legnagyobb kihívást a kriptovaluták használatában az jelenti, hogy pszeudoanonimitást biztosítanak, vagyis a tranzakciók nem köthetők konkrét személyekhez, mert ezen utalásokhoz nincs szükség személyazonosításra vagy hitelesítésre.

Nehezíti a helyzetet, hogy a decentralizáltágnak köszönhetően a virtuális fizetési rendszerek nem rendelkeznek központi felügyeleti szervvel, vagyis a büntetőeljárás során az eljáró

[399] GIRASA, Rosario: Regulation of Cryptocurrencies and Blockchain Technology: National and International Perspectives. Palgrave Macmillan, 2018. 39-40. o.
[400] HOUBEN - SNYERS: i.m. 48-49. o.
[401] HOUBEN - SNYERS: i.m. 45-46. o.
[402] EUROPOL (2018): i.m. 58. o.

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.

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, emellett a kriptovaluta átváltó szolgáltatók tevékenysége is részletesen szabályozott, működésük regisztrációhoz kötött és szigorú kiberbiztonsági, valamint pénzmosás és terrorizmusfinanszírozás elleni küzdelem érdekében támasztott követelményeknek kell megfelelniük.[403] 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.[404]

A központi bankok általában egységes állásfoglalásokat fogalmaztak meg e kérdésben, így például az Európai Központi Bank és a Magyar Nemzeti Bank is már több 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. Ezen eszközök esetében hiányoznak a megfelelő felelősségi, garanciális és kárviselési szabályok is, amelyek például visszaélés, ellopás esetén védenék a fogyasztók érdekeit.[405]

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.[406] 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.[407]

---

[403] A módosított Payment Services Act No. 59. of 2009.
[404] BLEMUS, Stéphane: Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide. Corporate Finance and Capital Markets Law Review 2017/4.
[405] https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2016-evi-sajtokozlemenyek/fokozott-kockazatot-hordoznak-a-vilaghalon-elerheto-virtualis-fizetoeszkozok
[406] Lásd: ESZTERI (2012): 71-78. o.; valamint SZATHMÁRY (2015): i.m. 643-644. o.
[407] ESZTERI Dániel: Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és jog 2017/1.

4.4. A kriptovaluták bűnelkövetési célú felhasználása

Az Europol az évente közzétett Internetes Szervezett Bűnözésre Vonatkozó Fenyegetettségi Elemzéseiben (IOCTA) 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 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, 1 esetben a Terrorelhárítási Központ volt.[408]

A következők részben részletesen elemzem a kriptovalutákkal összefüggő bűncselekményeket, középpontba helyezve az uniós és a hazai szabályozást.

4.4.1. Csalás

A kriptovaluták megvásárlására általában vagy egy másik ilyen eszközzel rendelkező felhasználótól, vagy egy erre szakosodott tőzsdén keresztül van lehetőség.
Ennek köszönhetően megjelent egy olyan csalás módszer is, amely alapján az elkövetők Bitcoin értékesítését ígérik a sértetteknek, azonban a megbízásokat 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. [409]

A tőzsdékre általában semmilyen szabályozás nem vonatkozik, a felhasználók számára semmi nem garantálja, hogy befizetett törvényes fizetőeszközükért cserében valóban meg is fogják kapni a megfelelő mennyiségű kriptovalutát.

Érdemes említést tenni egy hazai esetről, amelyről részletesen Eszteri írt. A konkrét eset történeti tényállása a következő: a sértett és az I. rendű vádlott az e-mail üzenetváltás útján

[408] NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: Éves jelentés – 2017. év, 11. o.
[409] NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: i.m. 11. o.

megállapodtak abban, hogy a sértett tulajdonában lévő 15 egységnyi Bitcoin-t 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 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.[410]

Emellett érdemes felhívni a figyelmet az egyre népszerűbb „Initial Coin Offering”-re (a továbbiakban: ICO), amely egy nyilvános forrásgyűjtési módot jelent valamely ötlet vagy vállalkozás finanszírozásához, egy blokklánc hálózat támogatásán keresztül. Ennek során az ötletgazda ún. tokeneket bocsát ki és kínál eladásra a támogatók részére hivatalos fizetőeszközért, vagy gyakrabban kriptovalutáért cserébe (pl. Bitcoin vagy Ether) -, így az ötletgazda, vagyis az ICO kibocsátója az eladott tokenekből szerez pénzt az

[410] ESZTERI (2017): 25-26. o.

ötletmegvalósításához. Ezek a kriptoeszközök például megtestesíthetnek egy jövőbeni áru vagy szolgáltatás igénybevételére jogosultságot, az esetek többségében azonban nem mutatható ki a tokennel megtestesített érték. Gyakoriak a visszaélések, amikor az ICO-val összegyűjtött pénzből nem kezdik el megvalósítani a kitűzött célt és ez nem is állt szándékukban, ezáltal a csalás tényállását valósítják meg.[411] Ezért a jegybankok többsége is figyelmeztet, hogy rendkívül kockázatos és spekulatív befektetési formának számítanak ezek. A kriptovalutákhoz hasonló módon országonként eltérő a szabályozásuk, eddig az ICO-kal szemben a leghatározotabb fellépés Kína részéről történt, mert a központi bank illegálisnak minősítette az ICO-n keresztüli tőkebevonást és ezek azonnali beszüntetését rendelte el.[412] Érdemes megemlíteni Máltát, mert egy hiánypótló törvénycsomagot adott ki, amelyben részletesen szabályozza a virtuális eszközöket, szem előtt tartva a befektetők védelmét.[413]

Amint láthatjuk a kriptovalutával összefüggésben elkövetett vagyon elleni bűncselekmény minősítése egyes esetekben a Btk. 373. §-ban szabályozott, hagyományos értelemben vett csalásnak felel meg. A kriptovalutákkal kapcsolatban elkövetett csalásnál érdemes a kárnak – mint tényállási elemnek – a fogalmával is részletesen foglalkozni. A büntetőjog a kár fogalmának tartalmi elemeit a polgári jogtól eltérően határozza meg.[414] 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 vagyonelemre tekinthetünk, és 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

[411] Az Egyesült Államokban az FBI letartóztatta az AriseBank igazgatóját azért, mert a befektetőket tévedésbe ejtve 4 millió dollár értékben kárt okozott nekik. A vád szerint egy ICO során a vállalkozásához, amit „az első decentralizált banki platformként" hirdetett különböző szolgáltatásokkal, és ezekre vonatkozóan nem rendelkezett engedélyekkel. 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.]

[412] https://fintechzone.hu/kriptovalutak-legfrissebb-fejlemenyek/ [2019.01.31.]

[413] A csomag három törvényt tartalmaz a következőkről: 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.

[414] DEÁK Zoltán: A kár büntetőjogi fogalmáról - megjegyzések egy eseti döntés margójára. Magyar Jog 2012/6.

meghatározható anyagi értéknagyság.[415] 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.[416]

4.4.2. A pénzmosás és a terrorizmusfinanszírozás

A pénzmosás nagy 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 köszönhető a decentralizált infrastruktúrának és a pszeudoanonim tranzakcióknak, mivel a személyazonosság elrejtését nagy hatékonysággal teszik lehetővé. A tranzakciók szolgálhatják a legális üzleti műveletek elszámolását, de az illegális tevékenységekét is.

A bűncselekményből származó pénzek kriptovalutákra történő átváltása, majd különböző címekre való továbbutalása 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, amiről még szó lesz.

Az integráció megtörténhet a virtuális fizetőeszközöknek az árukra és szolgáltatásokra való váltásával vagy közvetlenül, vagy pedig 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.

[415] MOLNÁR (2009): i.m. 702. o.
[416] ESZTERI (2017): i.m. 30. o.

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.[417]

A kriptovaluták átváltásával kapcsolatban különböző szolgáltatások érhetők el, amik 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).

„Mixing" vagy „tumbling" szolgáltatások, amelyek vagy egy közös, nagyobb összeget tartalmazó címet bontanak fel kisebbekre vagy fordítva több, kisebb összeget egyesítenek egy közös címen.[418] 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.[419]

Atomic swap használatával harmadik fél közbeiktatása nélküli más kriptovalutára történő átváltásra van lehetőség okosszerződés révén.

Ezeknek a szolgáltatóknak ezidáig nem volt uniós kötelezettségük arra vonatkozólag, hogy a gyanús tevékenységeket azonosítsák, így a bűnelkövetők – és akár a terrorista csoportok is[420] – képesek lehetnek pénzt utalni az uniós pénzügyi rendszerbe vagy a virtuális fizetőeszköz rendszereken belül azáltal, hogy elrejtik az átutalások, valamint magasfokú anonimitást élveznek ezeken a platformokon.

Az Európai Bizottság javaslatára 2018. május 30-án az Európai Parlament és Tanács (EU) 2018/843 irányelvet fogadta el a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv (a továbbiakban: ötödik pénzmosási irányelv), valamint a 2009/138/EK és a

[417] 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

[418] ESZTERI (2017): i.m. 27. o.

[419] https://shapeshift.io/

[420] Az Europol jelentése szerint megfigyelhető a terrorizmusfinanszírozás terén a kriptovaluták használata, azonban az ismert esetek száma alapján ez még nem számottevő. Lásd: EUROPOL: European Union Terrorism Situation and Trend Report 2018. 12. o.

2013/36/EU irányelv módosításáról. Ezek közül kiemelten az ötödik pénzmosás elleni irányelvvel foglalkozom, mert ez érinti a virtuális fizetőeszközöket. Újdonság, hogy először kerül meghatározásra a 3. cikk 19. pontjában a „virtuális fizetőeszköz" fogalma, amelynek 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[421], a pénz átfogóbb fogalmával[422], 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 irányelv célja a virtuális fizetőeszközök valamennyi lehetséges felhasználásának szabályozása.

Jelentős lépés, hogy az irányelvnek 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 az irányelv 3. cikkének 19. pontja meghatározza, amelynek értelmében: „olyan szervezet, amely ügyfelei nevében virtuális fizetőeszközök tartására, tárolására és átutalására szolgáló kriptográfiai magánkulcsok megőrzésével kapcsolatos szolgáltatást nyújt".

Az új szabályozás lényegét tekintve abból indul ki, hogy a virtuális fizetőeszközök rendszerének decentralizáltságából adódik, hogy hiányzik a központi felügyeleti szervük, akihez lehetne fordulni információkért. Azonban az 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.

[421] 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.

[422] 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.

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 irányelv a 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.).[423]

Az ötödik pénzmosási 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 az irányelvnek a hatálya.

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

[423] 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 azokra a fiókokra vonatkozó dokumentumokat, amelyeken egy bármely típusú tranzakció keretében (legyen szó adásvételről, átváltásról vagy utalásnak a fogadásáról) 20,000 $-ral megegyező értékű műveletre került sor 2013 és 2015 közötti egyik évben. Ezek az információk azért rendkívül fontosak, mert elősegíthetik a felhasználók azonosítását és a további eredményes nyomozati munkát. 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.).

annak lehetőségét, hogy a felhasználók önkéntes önbevallás formájában nyilatkozatot tehessenek a kijelölt hatóságoknak.

Az irányelvet a tagállamok kötelesek 2020. január 10-ig kell átültetni a nemzeti jogukba. A Bizottság 2022. január 11-ig, majd azt követően háromévente jelentést készít ezen irányelv 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 minősül-e. 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.[424]

A következőkben a pénzmosás hazai szabályozását vizsgálom a kriptovaluták vonatkozásában. 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,

[424] C-264/14. sz. Skatteverket kontra David Hedquist ügy

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 büntetőjogi és a büntetőeljárásjogi szabályok szempontjából. 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 a következőképpen történhetne: vagyoni értéket önmagában vagy feldolgozása révén biztosító, fizetésre használt elektronikus adat vagy adatok összessége, ideértve a fizetés elektronikus nyilvántartási egységét is.[425]

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 igénybe vételekor, 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 minősül-e a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény értelmében. Jelenleg azonban még nem. Ez rámutat arra, hogy nemcsak magát a kriptovalutát kell a jognak kezelnie, hanem annak különböző hasznosítási formáját 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.

[425] SZATHMÁRY (2015): i.m. 646. o.

Virtuális fizetőeszközök bevonásával olyan hagyományos és jól ismert pénzmosási módszerek is új színezetet kaphatnak, mint az ún. „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.[426]

4.4.3. Darknet piacterek és fórumok

A kriptovalutákkal kapcsolatos első visszaélések a Darknethez köthetők, ahol a különböző feketepiactereken és fórumokon – a magas fokú anonimitást biztosító és éppen ezért nehezen lenyomozható – virtuális fizetőeszközöket (pl. Bitcoin, Ether, Monero, Zcash) mint egy fizetőeszközként használnak 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 egy hagyományos bűncselekmény, de a technológiai fejlődésnek köszönhetően már az infokommunikációs technológia és a virtuális fizetési rendszerek felhasználásával is elkövethető. Általában a számítógépes környezetben e bűncselekmény az elkövetők részéről fenyegetéssel valósul meg például a DDoS-támadások indítását, vagy a zsarolóvírus által titkosított adatok törlését, vagy a jogosulatlanul megszerzett személyes adatok nyilvánosságra hozatalát helyezik kilátásba, majd a „váltságdíjat" kriptovaluták formájában kérik.[427]

A zsarolás eredmény-bűncselekmény, amelynek az eredménye a vagyoni hátrány, amely a Btk. 459. §-a (1) bekezdésének 17. pontja értelmében a kárból, azaz a vagyonban okozott értékcsökkenésből és az elmaradt vagyoni előnyből tevődik össze.

[426] NEMZETI ADÓ- ÉS VÁMHIVATAL KÖZPONTI IRÁNYÍTÁSA PÉNZMOSÁS ÉS TERRORIZMUSFINANSZÍROZÁS ELLENI IRODA: Éves jelentés - 2016. év, 15. o.

[427] Lásd MEZEI Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jogászegyleti Értekezések 9-10. Budapest, 2018. 169. o.

4.4.5. Az információs rendszer elleni bűncselekmények

A kriptovaluták népszerűsége a bűnelkövetők számára új célpontokat szolgáltatott: a kriptovaluta felhasználókat, a már említett átváltó és letétkezelő pénztárca-kezelő szolgáltatókat, valamint kriptotőzsdéket és 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.[428] 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, azonban a pénzforgalmi szolgáltatók által üzemeltett rendszerekkel szemben ilyen esetben semmilyen szabályozás sem védi az ügyfeleket.

Ezekben az esetekben a számítógépes környezet elengedhetetlenül szükséges a kriptovalutákkal kapcsolatos visszaélések elkövetéséhez, így indokolt ezeket a virtuális „lopásokat" informatikai bűncselekményként értékelni.[429]

Az elkövető a Btk. 375. §-ába ütköző információs rendszer felhasználásával elkövetett csalást valósítja meg, amennyiben megszerzi a virtuális pénztárcát, azaz a wallet.dat fájlt vagy az online pénztárca-szolgáltatónál tárolthoz hozzáfér egy kibertármadás következtében, akkor az adott tárcához tartozó kriptovalutával is rendelkezni tud, így amennyiben pénzügyi műveletet hajt végre, akkor ezzel kárt okoz. A letétkezelő pénztárca-szolgáltatókkal és átváltókkal szemben elkövetett támadások gyakoriak (pl. Mt. Gox és Coincheck esete).[430] A károkozás hiányában a 423. § szerinti információs rendszer vagy adat megsértésének deliktumáért vonható felelősségre (pl. előfordul, hogy a szolgáltatóktól jogosulatlanul megszerzik a felhasználói adatokat, majd azokat felhasználják). A másik egyre gyakoribb eset az ún. „cryptojacking", amely bármely olyan folyamatot takar, amelynek során a jogosult felhasználó engedélye nélkül a számítógépnek a feldolgozási sebességét vagy sávszélességét használják célzottan

[428] EUROPOL (2018): i.m. 8. o.
[429] 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.
[430] 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 elkülönjenek a tőzsdéétől. A Mt. Gox esetén a kettő még azonos volt. A jelenlegi szabályozásnak köszönhetően naponta kell ellenőrizniük, hogy rendelkeznek-e megfelelő fedezettel.

kriptovaluta bányászatra (pl. ez történhet malware fertőzés révén vagy a felhasználó által meglátogatott honlapba beépítve).[431]

A rosszindulatú programnak a készítője, valamint azaz elkövető, aki a privát kulcsot átadja, hozzáférhetővé teszi, megszerezi, vagy forgalomba hozza, az a 424. § szerinti információs rendszer védelmét biztosító technikai intézkedés kijátszásáért felel.

Az információs rendszer elleni bűncselekmények elkövetési tárgyaként mint számítástechnikai adat jelenik meg a virtuális pénztárca.

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.[432]

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.

Összeségében elmondható, hogy a Bitcoinnal történő visszaélések tekintetében általában nem is a bűncselekmény helyes minősítése okozhat problémát a gyakorlatban, hanem, hogy az

[431] EUROPOL (2018): i.m. 19. o.
[432] 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.]

elkövetés tárgyát hogyan sorolhatjuk be jogi szempontból és annak értékét hogyan értékelhetjük. Örvendetes lenne ezért egy konkrét virtuális vagyontárgyakkal kapcsolatos szabályozás kialakítása a jövőben, amire a kriptovaluták jelensége jó indokot ad.

4.5. A kriptovalutákkal összefüggő büntető eljárásjogi kérdések

A kriptovaluták egységes szabályozásának és jogi besorolásuknak a hiánya büntetőeljárásjogi szempontból is kihívást jelent, mert felmerül a kérdés, hogy lefoglalás tárgyát képezhetik-e vagy sem. Az Egyesült Államokban és az Egyesült Királyságban is sor került a kriptovaluták lefoglalására[433], valamint Dél-Koreában a Legfelsőbb Bíróság először hozott a kriptovalutákkal kapcsolatban döntést, amelyben mérhető értékkel rendelkező eszközöknek tekinti őket, és mivel értékkel rendelkeznek, ezért lefoglalhatók.[434]

Az új Be. szabályozása szerint lefoglalni az ingó dolgot, a számlapénzt, az elektronikus pénzt vagy az elektronikus adatot lehet. A jövőben a decentralizált virtuális fizetőeszközök lefoglalás tárgyát képezhetik mint elektronikus adat. Az új 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.[435]

A kriptovaluták esetében problémát jelent az, hogy a jogosult soha nincs fizikai birtokában a kriptovaluta-egységeinek. Mindenképpen a privát kulcsra van szükség, 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, azonban fenn állhat annak a veszélye, hogy a jogosult előzőleg biztonsági másolatot készített róla, és akkor továbbra is rendelkezhet a kriptovaluta egyenlege felett. A másik probléma, hogy a privát kulcs – valamint esetenként a jelszavak – nélkül a hatóság nem tud hozzáférni a kriptovaluta-egységekhez, a gyanúsított pedig nem köteles ezeket átadni a nyomozó hatóság számára, ezért

[433] 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.]
[434] http://www.koreatimes.co.kr/www/biz/2018/05/488_249868.html [2019.01.21.]
[435] 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

különösen nagy körültekintést igényel a nyomoknak a felkutatása (pl. az információs rendszeren belül kutatva a pénztárca fájl, valamint a többi pénztárca típus vagy privát kulcs után)[436]. 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, amikor 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. Ezáltal tud teljes mértékben megvalósulni a vagyoni érték feletti rendelkezési lehetőségnek az akadályozása.[437] 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 új 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. Ha 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 elkerülve a hatósági visszaéléseket mint a Silk Road esetében, amikor a nyomozók ellopták a hatósági pénztárcából.[438] Éppen ezért a hatósági tárcának a legalkalmasabb az ún. „multisig" vagy

[436] Lásd a kriptovaluák lefoglalásának a lépéseit részletesen HALÁSZ Viktor: A Bitcoin működése és lefoglalása a büntetőeljárásban. Belügyi Szemle, 2017/7-8. 128-146. o.
[437] SZATHMÁRY (2015): i.m. 646. o.
[438] https://www.ethnews.com/two-more-years-in-prison-for-ex-secret-service-agent-who-stole-government-seized-bitcoin [2019.01.12.]

„multisignature” tárca típus, amely csak akkor engedélyezi a kriptovaluták küldését, ha az elegendő számú privát kulccsal igazolást kap, az előre meghatározott kulcsok közül. Ezt a rendszert bármilyen kombinációban ki lehet alakítani a felek megegyezése szerint.[439]

[439] FURNEAUX, Nick: Investigating cryptocurrencies – Understanding, extracting and analyzing blockchain evidence. Wiley, 2018. 71. o.

IV. ÖSSZEFOGLALÁS

Összeségében elmondható, hogy mind az Európai Unióban és mind az Egyesült Államokban a kezdeti törekvések az informatika bűnözéssel kapcsolatban egészen az 1970-es évekig nyúlnak vissza. További közös vonásként említhető, hogy a meglévő, hagyományos bűncselekményekre vonatkozó szabályozás helyett megkezdődött a speciális és önálló anyagi büntetőjogi rendelkezések megalkotása ezen új típusú bűncselekményekre vonatkozóan. Az Európa Tanács több évtizedes munkájának eredményére 2001-ig kellett várni, amikor is elfogadásra került az első kötelező erejű, multilateriális jogi dokumentum, a Budapesti Egyezmény. Az egyezmény célja a számítástechnikai bűnözés elleni küzdelem alapjainak a megteremtése. Az egyezmény az aláíró felek számára keretet biztosít a nemzetközi együttműködéshez és olyan államok számára is nyitott a ratifikációja, amelyek nem tagjai az Európa Tanácsnak, így többek között az Egyesült Államok is ratifikálta. Valamennyi, az informatikai bűnözést szabályozni célzó új, nemzetközi dokumentumnak, kezdeményezésnek az alapjait a Budapesti Egyezmény adja és a mai napig a legjelentősebb egyezménynek számít ezen a területen, azonban vannak szabályozási hiányosságai, mert a technológiai fejlődés már meghaladta. Ezért a másik nagy előrelépést uniós szinten a 2013-as új irányelv jelentette, amely az információs rendszerek elleni támadásokkal szemben lép fel a minimumszabályok megalkotásával és az eddig hiányos szabályozást az új típusú támadásokra vonatkozóan részben orvosolta (pl. botnetek, kritikus infrastruktúrák elleni támadások, személyazonosság-lopás), és ezeket a tagállamoknak kötelezően át kellett ültetniük a saját jogrendszerükbe, és a tagállamok közötti bűnügyi együttműködés erősítése révén.

Az Egyesült Államok szövetségi szinten, először 1984-ben, az uniós törekvésekhez képest előbb szabályozta már a számítógépes bűncselekményeket a CFAA-ban. Ahhoz, hogy a törvény lépést tudjon tartani a technológiai fejlődéssel már nyolcszor módosították 1986-tól 2008-ig. A módosítások elsődleges célja az volt, hogy a törvény hatályát minél szélesebb körben kiterjesszék, például a szövetségi érdekű számítógép szűk fogalmától egészen eljutottak egy sokkal tágabb értelemben vett számítógép meghatározáshoz, amely alá vonható lényegében majdnem valamennyi háztartási eszköz, amelyet a világ bármely részén használnak. A CFAA hatályos szabályozása hét bűncselekményt tartalmaz, azonban egy kiforrót esetjog még hiányzik e területen.

Fontos belátni, hogy az informatikai bűnözés egy komplex problémakört foglal magában, mellyel szemben többlépcsős stratégiának az alkalmazása válik indokolttá. Ebben kiemelt

jelentősége van elsődlegesen a prevenciónak, különösen a felhasználókhoz igazított oktatásnak, ismeretterjesztésnek, mert sokszor ezek a bűncselekmények elkerülhetők lennének, ha körültekintőbben járnának el és ezáltal kiküszöbölhető lenne a sértetti közrehatás, amely jelentősen megkönnyíti az elkövetők számára az elkövetést. Elsődlegesen nem a felelősség keresése cél, hanem a károk, negatív következményeknek a lehetőség szerinti elkerülése vagy legalább azok mérséklése. Ez pedig általában nem a büntetőjog feladata.[440]

Emellett fontos, hogy a jogalkalmazók (pl. bíróság, ügyészség, rendvédelmi szervek) számára is biztosítva legyen a modern technológiákkal összefüggő jogi kihívásokat érintő, speciális oktatás. Örvendetes, hogy erre vonatkozóan már megfigyelhetők európai és hazai törekvések is.[441]

A fokozott együttműködés elősegítése is lényeges elem a magánszektor és a bűnüldöző hatóságok, illetve az egyes bűnüldöző hatóságok között, mert az eddigi tapasztalat is azt mutatja, hogy a sikeres felderítésekhez, a hatékony nyomozás lefolytatásához mindez nélkülözhetetlen.

Fontos a harmonizált, egységes nemzetközi szabályozás megteremtése mind anyagi, mind eljárásjogi tekintetben nemzetközi szinten, ami azért is kihangsúlyozandó, mert egy határokon átívelő bűnözésről van szó és az elkövetők kihasználhatják a különböző országok jogrendszerének a szabályozási hiányosságait, azok differenciáltságát. Például az Európai Unióban a szabályozást sikerült egységesíteni az új irányelv révén.

Az országok általában különböző megoldást alkalmaznak a kiberbűncselekményekre vonatkozóan vagy egy külön törvényben történő szabályozást választanak, vagy a többségük a nemzeti büntető törvénykönyvébe iktatott rendelkezéseket alkalmaz egy önálló fejezetben vagy a különös részben szétszórtan elhelyezett tényállásokkal megvalósítva.

Magyarországon az új. Btk.-ban az informatikai bűncselekmények önálló fejezetbe lettek illesztve, ami mindenképpen egy jó megoldásnak és haladásnak tekinthető az új védett jogi tárgyakra tekintettel. A hazai szabályozás mind a Budapesti Egyezmény és a 2013-as irányelv rendelkezéseivel is összhangban áll, és az informatikai támadásokat széleskörűen szabályozza. Azonban kritikai megjegyzéseim és javaslataim a következők:

[440] KORINEK (2010): i.m. 51. o.

[441] Például az Európai Jogi Akadémia (Academy of European Law) rendszeresen szervez képzéseket, szemináriumokat az technológiákkal összefüggésben. 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.; Magyarországon az Országos Bírósági Hivatal a kiberbűnözéssel kapcsolatos bírósági hálózat felállításáról döntött. Mind a bíróság és mind az ügyészség rendszerén belül erre vonatkozó képzések jelentek már meg. https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja

- Az információs rendszerben végzett művelettel jogtalan haszonszerzés nélkül is kárt tudnak okozni, ezért indokolt lenne ennek egy külön fordulatba történő szabályozása az információs rendszer vagy adat elleni bűncselekménynél.
- Ezzel szoros összefüggésben véleményem szerint szükség van a kár büntetőjogi fogalmának a kiterjesztése egy értelmező rendelkezéssel.
- A közérdekű üzem és az uniós 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 fogalmak közelítése indokolt.
- Megfontolandó az is, hogy 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 a jogalkotó ezt az egyes bűncselekményeknél (pl. csalás, zsarolás) minősített eseteként szabályozza.

Az új büntetőeljárásról szóló törvényünk is már a kor kívánalmainak megfelelő rendelkezéseket tartalmaz, így már külön nevesíti a bizonyítási eszközök között az elektronikus adatot, valamint részletesen szabályozza a rá épülő kényszerintézkedéseket. A Be. azonban a lefoglalás módszertani kérdéseivel nem foglalkozik, annak ellenére, hogy ennek komoly jelentősége van, ezért a lefoglalás menetére vonatkozóan hiányzik még egy világos útmutatás, ami az ezzel kapcsolatos kérdéseket orvosolná. A szabályozás előremutató, mert már olyan kérdésekkel is foglalkozik mint a virtuális vagyontárgyak lefoglalása (pl. a fizetésre használt kriptovaluták). Azonban ez még nem nyújt megoldást a teljes problémára, mert a hatóságokat több tényező is hátráltathatja a nyomozás során például a titkosított (pl. jelszóval vagy biometrikus azonosítóval védett) informatikai eszközök, a privát kulcs ismeretének a hiánya, valamint az a tény, hogy a jogosult soha nincs fizikai birtokában a kriptovalutáknak, ezért önmagában a lefoglalás nem elégséges, hanem ezeket kikényszerített tranzakcióval lehetne kizárólag biztosítani.

Az Európai Unión belül egy régóta fennálló problémát kívánnak orvosolni az új elektronikus adatok határon átnyúló megszerzésére vonatkozó rendelettel, amely megteremtené annak a lehetőségét, hogy a hatóságok közvetlenül az internetszolgáltatókat keressék meg az elektronikus bizonyítékokkal kapcsolatban. Ez nagy előre lépést jelent a hatékonyabb és gyorsabb büntetőeljárások lefolytatása érdekében.

A kiberbűncselekményekkel kapcsolatban a másik jelentős eljárásjogi problémaként a joghatóság kérdése emelhető ki, ami a kiberbűnözés sajátosságában keresendő, hogy

transznacionális jellegű. Emellett az elkövetők számára rendelkezésre állnak különböző módszerek és programok, hogy elrejtsék helyzetüket és személyazonosságukat, így földrajzilag azonosíthatatlannak mutatkozhatnak. A legnagyobb problémát az anonimitás jelenti, amelyet számos program használata nyújthat számukra. Amennyiben a joghatóság megállapítása és az eljárás lefolytatása megtörténik, akkor pedig sokszor a kiadatás jelent további problémát.

A bankkártyákkal és különböző átutalásokkal kapcsolatos visszaélések az informatikai bűnözés egyik kiemelt területeként kezelhető. Az elkövetők az ún. skimming technikákat alkalmazzák a card-present csalás terén, hogy a fizikailag hozzáférhető bankkártya adatokat megszerezzék, míg ennél nagyobb számban vannak jelen az interneten megvalósuló card-not-present csalások, amelyek során különböző adathalász technikák alkalmazásával szerzik meg a gyanútlan sértettek adatait, amelyek továbbra is rendkívül nagy kihívást jelentenek különösen a pénzintézetek körében. Az elkövetők gyakran értékesítik a megszerzett adatokat a Darknet fórumokon keresztül.

A bűnelkövetők gyorsan átveszik és integrálják az új technológiákat a különböző bűncselekmények elkövetésekor és olyan üzleti modellt alkalmaznak, amelyeknek az alapját egyre inkább az internet használata jelenti. A hagyományos szervezett bűnözői csoportok esetében is megfigyelhető az informatikai újítások kihasználása, amely magában foglalja az interneten történő terjeszkedést mint például az illegális online kereskedelmet és a széles körben hozzáférhető, titkosított kommunikációs csatornák használatát és egyéb informatikai újításokat. Megállapítható, hogy az új technológiai vívmányok lényeges és maradandó hatással vannak a bűnözés természetére. Az is kétségtelen tény, hogy az informatikai bűnözés egy hatalmas profit-orientált és szolgáltatás-alapú üzletté nőtte ki magát, azonban az még mindig nem világos, hogy ez a piac milyen mértékben van az egyes tradicionális szervezett bűnözői csoportok kezében, illetve mennyiben tekinthető az új típusú kiberbűnözöi csoportok tevékenysége szervezett bűnözésnek egyáltalán. Ugyanis a szervezett bűnözés és az informatikai bűnözés kapcsolatára vonatkozóan még mindig nincs egy világos koncepció, különösen azért, mert nehéz a szervezett bűnözés hierarchikus, homogén struktúrájába az informatikai bűnözést beilleszteni. A „kiberbűnözői ipar" rendkívül erőssé és fejletté vált, azonban még mindig a fejlődésének korai szakaszában van, éppen ezért kevés a rendelkezésre álló adat, különösképpen a szervezettségi szintjére vonatkozóan. Összeségében elmondható, hogy az internet mint egy új színtérként szolgál mind a régi és mind az új típusú „szervezett" bűnözésnek, illetve mindkettő egymás mellett tud működni anélkül, hogy egymást kizárnák és ez köszönhető az online tér speciális jellegének.

A pénzmosással összefüggésben megállapításra került, hogy az online banki műveletek felvethetik ugyan a pénzmosás gyanúját, azonban a saját pénzmosás deliktumának megállapításához szükséges eredetleplezési célzatot nem lehet kiterjesztően értelmezni. Ennek következtében kiemelten fontos az utócselekmények célzatának a körültekintő vizsgálata, vagyis az, hogy az elkövető által kifejtett leplezési cselekményeknek mi a céljuk. Azok az alapbűncselekményből származó haszon realizálását szolgálják-e, vagy magát az alapbűncselekmény leplezését, annak érdekében, hogy az illető a büntetőjogi felelősségre vonást elkerülje, vagy valóban a pénz bűnös eredetét és annak további útját kívánják leplezni továbbá, hogy ezek a műveletek mennyiben alkalmasak a leplezési cél eléréséhez. A friss kúriai döntés felhívta a figyelmet arra is, hogy fokozottan vizsgálni kell, hogy az adott cselekmény az alapbűncselekmény tényállási elemének részeként vagy önállóan, – pénzmosásként – értékelendő, elkerülve ezáltal a kétszeres értékelést. A pénzmosás gondatlan alakzata esetében - így a pénzfutárok alkalmazásakor - pedig fokozottan kell vizsgálni az elkövető tudattartalmát.

Fontos, hogy az informatikai kihívásokra a jogalkotás adekvát módon és gyorsan tudjon reagálni, azonban ez az esetek többségében nem vagy csak késedelmesen valósul meg. A kriptovaluták jó például szolgálhatnak erre, mert a mai napig egy szürke zónát képeznek és jogi státuszuk bizonytalan. Azonban az kétségtelen, hogy a decentralizált rendszernek és a pszeudoanonim tranzakcióknak köszönhetően a bűnelkövetési célú felhasználásuk egyre inkább jelen van. A kriptovalutákkal kapcsolatban felmerülő visszaélések tekintetében általában 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 értékelhetjük. Örvendetes lenne ezért egy konkrét virtuális vagyontárgyakkal kapcsolatos szabályozás kialakítása a jövőben, amire a kriptovaluták jelensége jó indokot ad erre. A jövőben továbbra is a legnagyobb kihívást a titkosítást és anonimitást biztosító eszközök bűnelkövetési célú felhasználása fogja jelenteni, amely további szabályozási kérdéseket fog felvetni.

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 – Nagy Zoltán András (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK. Pécs, 2019. 10-11.o.

AMBRUS István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014.

APPAZOV, Artur: Legal aspects of cybersecurity. University of Copenhagen, Faculty of Law, 2014.

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.

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.

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. I. évfolyam 1. szám

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, 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.

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.

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION: The National Information Infrastructure Protection Act of 1996.

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.

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 – Nagy Zoltán András (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK. Pécs, 2019.

CSÁK Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018. 328-329. o.

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.

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.

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.

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.

EUROPOL: European Union Serious and Organised Crime Threat Assessment (SOCTA) – Crime in the age of technology. 2017.

EUROPOL: European Union Terrorism Situation and Trend Report 2018.

EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2018.

EUROPOL: The Internet Organised Crime Assessment (IOCTA) 2016.

EUROPOL: The Internet Organised Crime Assessment (IOCTA). 2014.

FATF: Virtual Currencies - Key definitions and Potential AML/CFT Risks. 2014.

FENYVESI Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8.

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 12 October 2018.

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. o.

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.

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.

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.

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

HOUBEN, Robby - SNYERS, Alexander: Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Union, 2018.

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.

KÁRMÁN Gabriella - MÉSZÁROS Ádám - TILKI Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3.

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.

KERR, Orin S.: Computer Crime Law. Fourth Edition. West Academic Punlishing 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: Vagueness Challenges to the Computer Fraud and Abuse Act. Minnesota Law Review 2010. 1

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

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: The Internet and its Opportunities for Cybercrime. Tilburg School Legal Studies Paper Series No. 09/2011.

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: A kibertér védelme. Dialog Campus Kiadó. Budapest, 2018.

KŐLVART, Merit - POOLA, Margus - RULL, Addi: Smart Contracts. In: Kerikmäe, Tanel - Rull, Addi (eds.): The Future of Law and eTechnologies. Springer, 2016.

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.

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.

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: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. Jura 2018/1.

MIK, Eliza: Smart contracts: terminology, technical limitations and real world complexity. Law, Innovation and Technology 2017/2.

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: Gazdasági bűncselekmények. HVG-ORAC. Budapest, 2010.

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.

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.

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 – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70.

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.

NAGY Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról.

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 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. Ad librum Kft. Budapest, 2009.

NAGY Zoltán András: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda. Belügyi Szemle 1999/11.

NAGY Zoltán András: A számítógépes környezetben elkövetett bűncselekmények kriminológiai aspektusairól. In: Gál István – Nagy Zoltán András: Az informatika és a büntetőjog. Pécs, 2006.

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.

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.

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. SZABÓ Imre: Informatikai bűncselekmények. In: Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve. Budapest, CompLex, 2008.

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: "10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és jog 2010/38.

Payment Services Act No. 59. of 2009.

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.

POSKRIAKOV, Fedor - CHIRIAEVA, Maria - CAVIN, Christophe: Cryptocurrency compliane and risks: An European KYC/AMLP perspective. In: Dewey, Josias (ed.): Blockchain & Cryptocurrency Regulation 2019. Global Legal Group, 2019.

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.

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 rendészeti kihívásai. In: Mezei Kitti - Nagy Zoltán András (szerk.): A bűnügyi tudományok és az informatika. PTE ÁJK. 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.

SISÁK Attila: A pénzmosás elleni küzdelem tapasztalatai egy nyomozó hatóság gyakorlatában. Kriminológiai Közlemények 72.

SMITH, Russel G. – GRABOSKY, Peter – URBAS, Gregor: Cyber Criminals on Trial. Cambridge University Press, 2004.

SORBÁN Kinga: A digitális bizonyítékok a büntetőeljárásban. Belügyi Szemle 2016/11.

SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Királyságban. Belügyi Szemle 2015/9.

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 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: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6.

SZABÓ Imre: Internetes bűncselekmények, különös tekintettel az internetes csalásra. ELTE ÁJK, 2002.

SZALÁRDI Gábor: A csúcstechnológiai bűnözés elleni küzdelem támogatása. Belügyi Szemle 2012/6. SZONGOTH Richárd – VETTER Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. Belügyi Szemle, 2018/7-8.

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.

SZOMORA Zsolt: A jogi tárgy funkciói és a jogtárgyharmonikus értelmezés" Bűnügyi Szemle 2009/2.

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

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 214. o.

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. 5.

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: 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.

TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.

TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 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: 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. 2014.

U.S. DEPARTMENT OF JUSTICE: Report of the Attorney General's Cyber Digital Task Force. Washington, 2018.

U.S. DEPARTMENT OF JUSTICE: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Law. 2009.

URCUYO, Michael S.: From Internet trolls to seasoned hackers: protecting our financial interests from Distributed-Denial-Of-Service attacks. Rutgers Computer & Technology Law Journal Vol. 42., 2016.

VADÁSZ Viktor: A számítógép demisztikálása. Ügyészek Lapja 2010/2.

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.

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.

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 [2017.10.21.]

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