Mezei Kitti
tudományos segédmunkatárs,
MTA TK Jogtudományi Intézet
PhD hallgató, PTE ÁJK Doktori Iskola

Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására*

I. Bevezetés

A technológiai innováció lehetőséget teremtett számunkra arra, hogy új és kényelmes megoldásokat használjunk a mindennapjaink során, legyen szó tanulásról, vásárlásról, szórakozásról vagy üzletről. Az információ- és kommunikációtechnológia teljes mértékben megváltoztatta az életünket, azonnal és könnyedén tudunk kommunikálni egymással, akár nagy távolság esetén is, hatalmas mennyiségű információt, adatot vagyunk képesek összegyűjteni és tárolni. Az előnyök mellett, azonban az újításoknak megvannak az árnyoldalai is, hiszen az átlagos felhasználók mellett a bűnözők is élnek az új technológiák adta lehetőségekkel, ezáltal a fejlődés egy új típusú bűnözéshez járult hozzá, az informatikai vagy más néven számítástechnikai, számítógépes bűnözés megjelenéséhez.

Ezeknek az új típusú bűncselekményeknek a tárgya és eszköze is lehet a számítógép.[1] Eszköze amennyiben valamely hagyományos büntetőjogi tényállás megvalósításához használják fel, és tárgya, ha az információs rendszer, számítógépes adatok, programok ellen irányul. Az informatikai bűncselekményeknek azonban a mai napig nincsen egységes fogalommeghatározása. A hatékony fellépés ezzel a bűncselekmény típussal szemben megköveteli a nemzetközi bűnügyi együttműködést, illetve a büntetőjogszabályoknak a nemzetközi összehangolását, a szükséges minimumszabályoknak a megalkotását. Az információs rendszerek felhasználásával elkövetett bűncselekmények száma is fokozatosan növekszik évről évre, és emiatt különösen fontos, hogy a jogalkotók is gyors ütemben tudjanak reagálni ezekre a változásokra.

Tanulmányomban törekszem bemutatni egy történeti áttekintéssel az Európai Unió és az Egyesült Államok törekvéseit az informatikai bűnözés szabályozására vonatkozóan. Uniós szinten az Európa Tanács töltött be meghatározó szerepet az informatikai bűnözést érintő büntetőjogi rendelkezések harmonizációjának elősegítésében és már az 1970-es évektől kezdve voltak törekvések arra, hogy egy átfogó jogi dokumentum megalkotására sor kerüljön. Ennek eredménye lett *a Számítástechnikai Bűnözésről Szóló Egyezmény (a továbbiakban: Budapesti Egyezmény)*. Az 1970-es évektől az 1990-es évekig tartó időszakot három szakaszra lehet bontani a középpontba helyezett törekvések alapján:

1) az 1970-es években arra keresték a választ, hogy hogyan lehet a gazdasági bűnözésre vonatkozó szabályozást alkalmazni a számítógéppel kapcsolatos bűncselekményekre;

2) az 1980-as években új és speciális büntető anyagi jogi szabályozásról tárgyaltak és készítettek elő a számítógépes bűncselekményekkel kapcsolatban;

3) az 1990-es években a büntetőeljárásjogi rendelkezések harmonizálására törekedtek ezen a területen.[2] A tanulmány az utóbbi két időszakkal foglalkozik részletesen.

A tanulmány továbbá bemutatja az Egyesült Államoknak a szövetségi szintű törvényét, a *Computer and Fraud Abuse Act-et (a továbbiakban: CFAA)* és annak nyolc módosítását, illetve a hatályos szabályozását. Az Egyesült Államok az elsők között kísérelte meg a büntetőjogi szabályozását az egyes informatikai bűncselekményeknek és nem csak a már meglévő büntetőjogi szabályokat hívta segítségül, hanem új rendelkezéseket is alkotott. Az ilyen jellegű kísérletek egészen visszanyúlnak az 1970-es évekig és három időszak határolható el:

1) 1984 előtti időszak – kezdeti törekvések a számítógépes bűnözés szabályozására,
2) 1984-tól 1986-ig az első szabályozás;
3) 1986-tól 2008-ig a módosítások és kiterjesztések időszaka.[3]

II. Az informatikai bűnözés elleni fellépés európai dimenziói

1. OECD jelentés

Az első fontos nemzetközi jogi dokumentum a *Gazdasági Együttműködési és Fejlesztési Szervezet (OECD)* által kibocsátott 1986-os jelentés volt,

* A tanulmány az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai keretében valósult meg.

amelyben iránymutatást kívántak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez, mellyel egyúttal a kodifikáció elősegítése volt a cél. A büntetendő cselekményeket 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.

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.[4]

Henrik W. K. Kaspersen kiemelte, hogy az anyagi szabályozás mellett a büntetőeljárási jogi kérdésekkel is együttesen foglalkozni kell.[5] Ulrich Sieber is felhívta a figyelmet a határon átnyúló együttműködés fontosságára és 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).[6] A büntetőeljárás jogi vonatkozású aggodalmakra válaszul megszületett az *ET. 95. (13.) számú ajánlása*, amely az információs technológiákkal kapcsolatos eljárási problémákra törekedett megoldást nyújtani, mint például a házkutatás és lefoglalás; technikai megfigyelés; kötelezettség a nyomozó hatóságokkal való együttműködésre; elektronikus bizonyítékok; titkosítás használata; statisztika és képzés; nemzetközi együttműködés során felmerülő kérdésekre ad választ.[7]

3. Számítástechnikai Bűnözésről Szóló Egyezmény

2001 novemberében Budapesten írták alá az Európa Tanács által előkészített és már említett *Számítástechnikai Bűnözésről Szóló Egyezményt (Convention on Cybercrime)*. 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:

1) A büntető anyagi jogi részt tartalmazza (2 – 13. Cikk).
2) 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.
3) 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, illetőleg bármely bűncselekményre vonatkozó elektronikus bizonyítékok összegyűjtése érdekében" (23 – 35. Cikk).
4) A záró rendelkezésekben az egyezmény hatályára, a fenntartásokra, a módosításokra, a viták rendezésére és az egyezmény felmondására vonatkozó részekre térnek ki (36 - 48. Cikk).

Részletesen az egyezmény anyagi jogi szabályozását ismertetem, amely kimondja, hogy minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön az alábbi cselekmények jogosulatlan és szándékos elkövetése:

I. cím: A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények

2. cikk – A jogosulatlan belépés: a számítástechnikai rendszerbe vagy annak bármely részébe történő jogosulatlan és szándékos belépés.

3. cikk – A jogosulatlan kifürkészés: 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 is.

4. cikk – A számítástechnikai adat megsértése: a számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megrongálása, megváltoztatása vagy megsemmisítése.

5. cikk – A számítástechnikai rendszer megsértése: a számítástechnikai rendszer működésének, számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megrongálásával, megváltoztatásával vagy megsemmisítésével való, jogosulatlan és szándékos, jelentős mértékű akadályozása.

6. cikk – Eszközökkel való visszaélés:

a) az előállítása, az értékesítése, a felhasználása céljából való megszerzése, az ország területére való behozatala, a forgalomba hozatala vagy a más módon történő hozzáférhetővé tétele az eszközöknek, ideértve a számítástechnikai programokat, számítógépes jelszónak, belépési kódnak, illetőleg hasonló, a számítástechnikai rendszerbe vagy annak bármely részébe való belépést lehetővé tevő számítástechnikai adatokat azzal a céllal, hogy az egyezményben foglalt valamely bűncselekmény elkövetésére használják fel;
b) a birtoklása a meghatározott dolgoknak, valamely az egyezményben foglalt bűncselekmény elkövetésére való felhasználás érdekében.

II. cím: A számítógéppel kapcsolatos bűncselekmények

7. cikk – A számítógéppel kapcsolatos hamisítás: a számítástechnikai adatoknak olyan, jogosulatlan és szándékos bevitele, megváltoztatása, törlése vagy megsemmisítése, melyek eredményeként nem valódi adatok jönnek létre abból a célból, hogy úgy lehessen azokat figyelembe venni vagy jogszerű célra felhasználni, mintha valódi adatok lennének, függetlenül attól a ténytől, hogy közvetlenül olvashatók vagy érthetők-e.

8. cikk – A számítógéppel kapcsolatos csalás: a másnak jogosulatlanul és szándékosan történő vagyoni károkozás, amelyet

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

III. cím: A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények:

9. cikk – A gyermekpornográfiával kapcsolatos bűncselekmények: gyermekpornográfia készítése számítástechnikai rendszer útján történő forgalomba hozatal céljából; felajánlása vagy hozzáférhetővé tétele számítástechnikai rendszer útján; továbbítása vagy forgalomba hozatala számítástechnikai rendszer útján; saját vagy más részére számítástechnikai rendszer útján történő megszerzése; egy számítástechnikai rendszerben vagy egy számítástechnikai adattárolóegységen való birtoklása.

10. cikk – Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.

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 nem tartalmazza mint például a személyazonosság lopást, a gyermekekkel történő szexuális célú kapcsolattartást, illetve a kiberterrorizmusra és a kéretlen levélre (spam) sem tér ki. Magyarországon a 2004. évi LXXIX. törvénnyel hirdették ki az egyezményt, ezzel összhangban a régi 1978. évi Büntető Törvénykönyvbe a 300/C. § szakaszba a számítástechnikai rendszer és adatok elleni bűncselekményt vezették be, valamint egyéb más törvényi tényállásokat kiegészítették a meghatározottak szerint.[8]

Ugyanebben az évben *az Európai Tanács 2001/413/IB kerethatározata* került elfogadásra a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről.[9]

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" (cookie) irányelvvel*, amely alapján a viselkedésalapú reklám célba juttatásához használt cookie-k kizárólag az érintettek hozzájárulását követően helyezhetők el a felhasználók számítógépein.[10]

Az Europol szervezetén belül 2002-ben hozták létre *a Csúcstechnológiai Bűnözési Központot (High Tech Crime Centre)*.[11]

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.[12]

4. 2005/222/IB tanácsi kerethatározat

2005-ben pedig *az információs rendszerek elleni támadásokról szóló 2005/222/IB tanácsi kerethatározat* elfogadására került sor,[13] 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 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.

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. 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, amelyek a kritikus infrastruktúrákat támadják. A Cyborg az Europol malware elemző rendszerét alkalmazza annak érdekében, hogy segítse az igazságügyi informatikai vizsgálatokat és az ún. *Joint Investigation Teams* munkáját, hogy hatékonyan feltudják deríteni a nagyobb hordereju, nemzetközi műveleteket mint például a botneteket. A *Focal Point Twins* pedig olyan esetekkel foglalkozik, amikor a gyermekek szexuális kizsákmányolásáról van szó. 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, magas fokú fenyegetésekre. A J-CAT 2014-ben indult köszönhetően az EC3, EUCTF, FBI és az Egyesült Királyság Nemzeti Bűnüldözési Ügynökség (NCA) közös együttműködésének (pl. 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.

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.[14]

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

2013 augusztusában az Európai Parlament és Tanács *2013/40/EU számmal irányelvet*[15] 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 - számítógéphálózatok 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:

- *információs rendszerekhez való jogellenes hozzáférés:* 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;

- *információ rendszerekbe való jogellenes beavatkozás:* valamely információs rendszer működésének számítógépes adatok szándékos és jogosulatlan bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása vagy elrejtése, vagy ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele révén történő súlyos akadályozása vagy megszakítása, legalább a súlyosabb esetekben bűncselekménynek minősüljön;
- *adatokba való jogellenes beavatkozás:* 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;
- *jogellenes adatszerzés:* 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.

A tagállamoknak közös megközelítést kell kialakítaniuk a fent említett bűncselekmények tényállás elemeire vonatkozóan. Továbbá a tagállamoknak a legalább a súlyosabb esetekben bűncselekménynek kell minősíteniük azokat az eseteket, amikor az irányelvben foglalt bűncselekmények elkövetéséhez felhasználnak eszközöket (pl.: számítógépes programok készítése, belépési kódok, jelszavak felhasználása az információs rendszerhez való hozzáféréshez).

Az irányelv a közös fogalommeghatározások használatának fontosságát hangsúlyozza ki, hasonlóan, mint a korábbi kerethatározat (információs rendszer, számítógépes adatok, jogi személy és jogosulatlanul). A bűncselekmény elkövetésének minden esetben szándékosnak kell lennie. Valamennyi az irányelvben foglalt bűncselekményre való felbujtás illetve az elkövetéshez nyújtott bűnsegélynek bűncselekménynek kell minősülnie. Az adatot érintő jogellenes beavatkozás és jogellenes adatszerzés esetében pedig a kísérlet is büntetendő. Azonban az irányelv nem állapít meg büntetőjogi felelősséget abban az esetben, ha az ezen irányelvben felsorolt bűncselekmények objektív kritériumai teljesülnek, azonban a cselekményeket nem jogsértő szándékkal követték el (pl.: az adott személynek nincs tudomása arról, hogy az adott hozzáférés jogosulatlan).

A tagállamoknak hatékony, arányos és visszatartó erejű szankciókat kell alkalmazniuk, és szabadságvesztést és/vagy pénzbüntetést is magukban kell foglalniuk.

Súlyosabb szankció megállapításának van helye, ha az információs rendszer elleni támadást bűnszervezetben követik el, vagy ha a támadás átfogó, azaz jelentős számú információs rendszert érint, vagy súlyos kárt okoz, abban az esetben is, ha a támadás valamely tagállam vagy az Unió kritikus infrastruktúrája ellen irányul. A tagállamoknak a jogrendszerük által a súlyosbító körülményekre vonatkozóan megállapított szabályokkal összhangban súlyosbító körülményeket kell meghatározniuk a nemzeti jogukban. De lege ferenda szükségesnek mutatkozik például a magyar szabályozásra nézve, hogy a minősített eseteket bővítse a szervezett bűnözés keretében.[16]

Az informatikai támadásokat számos körülmény megkönnyítheti, például ha az elkövetőnek alkalmazotti minőségében hozzáférése van az érintett információs rendszerek részét képező biztonsági rendszerekhez. A nemzeti jog keretében a büntetőeljárás során megfelelően figyelembe kell venni az említett körülményeket.

Továbbá az irányelv felhívja a figyelmet a személyazonosság-lopás illetve a személyazonossághoz kapcsolódó egyéb bűncselekmények elleni hatékony fellépés relevanciájára, amikor egy másik személy személyes adataival visszaélve követték el a bűncselekményt 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.

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 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.

Az új 2012. évi C. Büntető Törvénykönyvünkről szóló törvény a következő bűncselekményeket rendeli büntetni: nóvumként jelenik meg a vagyon elleni bűncselekmények között az információs rendszer felhasználásával elkövetett csalás (375.§), illetve a külön fejezetben szabályozott tiltott adatszerzést, információs rendszer vagy adat megsértését, illetve az információs rendszer védelmét biztosító technikai intézkedés kijátszását (422-424.§).

III. Az Egyesült Államok büntetőjogi szabályozása az informatikai bűncselekményekre vonatkozóan

1. A kezdeti szabályozási törekvések 1984-ig

Az első számítógépes törvényt 1984-ben fogadták el *Counterfeit Access Device and Computer Fraud and Abuse Act* címmel, amelyet később 1986-ban az első módosítással egybekötve változtattak meg Computer Fraud and Abuse Act-re. A CFAA-t megelőzően néhány jogtudós azon a véleményen volt, hogy a számítógépes bűncselekmények lényegében hagyományos bűncselekményeknek tekinthetők, amelyeket különböző technológiai eszközök használatával követnek el, ezért velük szemben a tradicionális büntetőjogi rendelkezések alkalmazását megfelelőnek gondolták. 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.

Azonban 1984-ben végül elfogadásra került a már említett CFAA, az első szövetségi törvény, amely kifejezetten a számítógépes bűncselekmények szabályozását célozta. A CFAA kezdetben három bűncselekményt vezetett be.[17] Az első 1030.§ (a)(1) bekezdésben szabályozott bűncselekménynél a védett jogi tárgy a nemzetbiztonsági titok. 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.[18]

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 tulaj-

donai 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.[19]

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*[20] 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.

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

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.

5. A hatodik módosítás: 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.[21]

6. A hetedik módosítás: 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)[22] 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.

7. A nyolcadik módosítás: 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.

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.[23]

8. A CFAA hatályos szabályozása

1. táblázat: A hatályos CFAA-ban szabályozott bűncselekmények

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

8.1 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 nemzetet előnyhöz juttasson és ezért szándékosan közli, átadja, továbbítja (vagy kísérletet tesz rá) vagy visszatartja az információt.

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

Számítógéphez való hozzáférés és információszerzés vétsége miatt büntetendő a 1030.§ (a)(2) bekezdése értelmében, aki szándékosan, jogosulatlanul hozzáfér a számítógéphez vagy jogosultságainak kereteit túllépve információt megszerez: (A) pénzintézet pénzügyi nyilvántartásából vagy fogyasztóvédelmi szervtől; (B) az Egyesült Államok kormányzati szervétől vagy (C) védett számítógépről. Bűntett miatt büntetendő az, aki gazdasági előnyért, anyagi haszonszerzésért, vagy más bűncselekmény, tiltott cselekmény elősegítése érdekében követi el bűncselekményt vagy 5.000$ értéket meghaladó információt szerez meg.

8.3 Behatolás kormányzati számítógépbe (Tresspassing in a government computer)

Ez azt az esetkört hivatott szabályozni bűncselekményként, amikor kívülállók behatolnak szövetségi kormányzati számítógépekbe, még akkor is, ha közben nem szereznek információt. 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 az Egyesület Államok kormánya használja, vagy érdekében használják, és e tevékenység befolyásolja a számítógép működését.

8.4 Hozzáférés csalási és haszonszerzési céllal, avagy számítógépes csalás (Accessing to defraud and obtain value)

A 1030.§ (a)(4) bekezdés a számítógépes csalást rendeli büntetni: aki tudatosan, jogosulatlanul hozzáfér védett számítógéphez 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.

8.5 Számítógép vagy információ károsítása (Damaging a computer or information)

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 az, 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 sérelmeket 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 biztonságra nézve; (5) az igazságszolgáltatásban, a honvédelemben, a nemzetbiztonságban használt számítógép sérelmére kövessék el; (6) károkozás 10 vagy több védett számítógép sérelmére egy év alatt.

8.6 Jelszavakkal kereskedés (Trafficking in passwords)

1030.§ (a)(6) bekezdés értelmében vétségként büntetendő, aki jelszavakkal vagy hasonló információkkal kereskedik (pl. átadja vagy értékesíti, vagy megszerzi azzal a céllal, hogy átadja vagy értékesítse másnak, de csupán a birtoklás nem meríti ki ezt az esetet a célzat hiányában), tudatosan és csalási céllal és, ha ez hatással van az államközi vagy nemzetközi kereskedelemre vagy a számítógép az Egyesült Államok kormányának használatában van.

8.7 Számítógép károsításával való fenyegetés, avagy a számítógépes zsarolás (Threatening to damage a computer)

A 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.

A 1030.§ (b) alszakasza értelmében büntetendő a 1030.§ (a) alszakaszaiban szabályozott bűncselekményeknek a kísérlete és az elkövetésben való megállapodása (előkészületi cselekménye) is.[24]

IV. Összefoglalás

Összefoglalva, 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. Az másik nagy előrelépést uniós szinten a 2013-as új irányelv jelentette, amely az információs rendszerek elleni támadásokkal szemben lép fel a minimumszabályok megalkotásával, amelyeket a tagállamoknak kötelezően át kellett ültetni saját jogrendszerükbe, és a tagállamok közötti bűnügyi együttműködés erősítése révén. A Budapesti Egyezményhez képest előrelépés, hogy az eddig hiányosnak mondható, új típusú támadások szabályozását hivatott orvosolni, mint például a botneteket, illetve kritikus infrastruktúrák ellen irányuló támadásokat.

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 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 hiányzik e területen.

Fontos belátni, hogy az informatikai bűnözés egy komplex problémakört foglal magában, melylyel szemben többlépcsős stratégiának az alkalmazása vált indokolttá. Ebben kiemelt jelentősége van elsődlegesen a prevenciónak, különösen a felhasználókhoz igazított oktatásnak, ismeretterjesztésnek. Fontos a harmonizált, egységes nemzetközi szabályozás megteremtése mind anyagi, mind eljárásjogi tekintetben nemzetközi szinten. A fokozott együttműködés elősegítése is lényeges elem a magánszektor és a bűnüldöző hatóságok között, illetve az egyes bűnüldöző hatóságok között. Szükséges továbbá, hogy az új kihívásokra a jogalkotók adekvát módon és gyorsan reagáljanak, mint például az online fekete piacokra és a virtuális fizetőeszközökre mint a bitcoin, a célzott támadásokra, az új platformok védelmére, különösen az Internet of Things és mobilinformatikai eszközök sebezhetőségének kihasználásának megakadályozására és a kritikus infrastruktúrák biztonságának a biztosítására.

Jegyzetek

[1] Polt Péter: A számítógépes bűnözés. Belügyi Szemle 1983. 6. sz. 60-64. o.

A számítógép kifejezést a mindennapi szóhasználatban hajlamosak vagyunk kizárólag az asztali számítógépekre vagy laptopokra gondolni, elfeledkezünk azonban arról, hogy az információtechnológia fejlődése rendkívüli mértékben megnö-

velte a komplex számítási feladatok elvégzésére képes eszközök körét. Ennek megfelelően a számítógép alatt értjük a desktopok és a laptopok mellett a táblagépeket, okostelefonokat, a játékkonzolokat, a szervergépeket, PDA-kat és akár egyes nyomtatókat is és még sorolhatnánk.

[2] Wang, Qianyun: A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. PhD Thesis. Erasmus University Rotterdam, 2016. 72-73. o.

[3] Wang: i.m. 99-100. o.

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

[5]Kaspersen, W.K. Kaspersen: 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.

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

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

[8] Nagy Zoltán András: A számítógépes környezetben elkövetett bűncselekmények. Ad librum, 2009. 40-56. o.

[9] 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.]

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

[11] Szalárdi Gábor: A csúcstechnológiai bűnözés elleni küzdelem támogatása. Belügyi Szemle 2012. 6. sz. 98-99. o.

[12] https://europa.eu/european-union/about-eu/agencies/enisa_hu [2017.11.21.]

[13] http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32005F0222 [2017.11.21.]

[14] 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.

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

[16] 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.]

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

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

[19] Wang: i.m. 102-106. o.

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

[21] Wang: i.m. 108-111. o.

[22] 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.

[23] Kerr: i.m. 1568-1571. o.

[24] Computer Crime and Intellectual Property Section Criminal Division: Prosecuting Computer Crimes. 2014. 12-55. o.