Sorbán Kinga
Büntető Eljárásjogi és Büntetés-végrehajtási Jogi Tanszék
Témavezető: Finszter Géza egyetemi tanár

Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói

Bevezetés

Az infokommunikációs technológiák ma már a mindennapjaink szerves részét képezik, azok az eszközök, amelyeket 10-15 éve még science-fiction filmekben láthattunk, ma már a kezünkben vannak. A számítógép, az Internet és az ezekkel kapcsolatban álló eszközök rendkívül praktikusak és megkönnyítik az élet minden területét. Megvannak azonban a technológia veszélyei is, a számítógépen dolgozva ugyanis majdnem akkora esélyünk van bűncselekmény áldozatává válni, mint éjszaka az utcán sétálva. Az infokommunikációs technológiák ugyanúgy hatással vannak a bűnözésre, mint a mindennapi életre. A bűnelkövetők is megtanulták hasznosítani a modern technika vívmányait, befészkelték magukat a virtuális térbe, ennek következében ma már a legtöbb „hagyományos" bűncselekmény elkövethető valamilyen informatikai eszköz segítségével is. Emellett megjelentek olyan új deliktumok, amelyeknél az információs rendszer, illetve az információs rendszerben tárolt adat nem csupán a bűncselekmény elkövetésének eszköze, hanem egyenesen az elkövetés tárgya. Ezek a bűncselekmények azért alakulhattak ki, mert az infokommunikációs eszközök annyira beépültek a társadalmi, gazdasági viszonyokba, hogy a rendszerek biztonsága, megbízható működése, valamint a rajtuk tárolt adatok integritásának védelme az egész modern társadalom számára jelentős, és ekként védelemre szoruló érdekké lépett elő. Ki kell emelni az informatikai bűncselekményeknek egy másik fontos aspektusát is: a kibertéren keresztül végrehajtott támadások nem csak a gazdasági szereplőket, illetve a magánszemélyeket célozhatják meg, hanem magát az államot is. Az állam sérelmére elkövetett informatikai bűncselekmények alááshatják az állami működés hatékonyságát, az állam- és közbiztonság szempontjából érzékeny adatok nyilvánosságra kerülhetnek, valamint ezek a deliktumok egyes kritikus infrastruktúrákra is veszélyt jelentenek.

A közelmúltban még azon folyt a vita, hogy ki kell-e terjeszteni a jog uralmát a virtuális térre, vagy hagyni kell ezt a területet, úgynevezett „jog nélküli zónaként működni”. Ma már kétség sem fér hozzá, hogy a digitális világban ugyanúgy szükség van szabályokra, mint a fizikai világban, ám ez az állítás sokszor még megválaszolásra váró kérdésekhez vezet. Elsőként például ahhoz, hogy amennyiben hatékonyan szeretnénk szabályozni a digitális világot, pontosan milyen szabályokra van szükségünk? Ugyanazokat a szabályokat kell-e alkalmazni, mint a materiális világban, vagy olyan rendszert kell kialakítani, amely a virtuális tér sajátosságaira van szabva? Gyakori kérdés továbbá az is, hogy egy-egy ügyben melyik ország szabályai alkalmazandóak. Mivel az Internet globális hálózat, amely a világ összes számítógépét összeköti, a nemzeti határoknak itt csekély a jelentősége. Vannak ugyan olyan országok (pl. Kína), ahol a kormány korlátozza az állampolgárok hozzáférését a világhálóhoz, illetve bizonyos tartalmakhoz, azonban a demokratikus országokban az Internet nyíltságához kétség sem férhet. Könnyen előfordulhat tehát, hogy a bűncselekmény elkövetője nem azonos országban, de még csak nem is azonos kontinensen tartózkodik, mint a bűncselekmény sértettje. Sőt az sem szükségszerű, hogy a bűncselekménynek csak egy sértettje legyen, az elkövető egyszerre akár több ezer különböző országokban tartózkodó sértett sérelmére is elkövetheti a bűncselekményt. Több elkövető esetén sem biztos, hogy mindegyikük azonos országban tartózkodik. Problémát jelenthet az is, ha a sértett országában az adott cselekményt a büntetőjog szankcionálni rendeli, az elkövető országában azonban nem. Az elektronikusan tárolt adatok törékeny természetéből adódóan számos kérdést vet fel az is, hogy a nyomozó hatóságok hogyan szerezhetik meg az úgynevezett digitális bizonyítékokat, illetve milyen intézkedéseket tehetnek az ilyen típusú bizonyítékok megszerzése érdekében.

Az államok viszonylag hamar felismerték, hogy nem elég ezen deliktumok pusztán nemzeti szintű szabályozása és a hatékony fellépés érdekében nemzetközi összefogásra van szükség, amelynek keretében tisztázni kell az informatikai bűncselekményekhez kapcsolódó fogalmakat, a joghatósági kérdéseket, illetve a tényállásokat. Szükségessé vált ezen felül olyan szupranacionális szervezetrendszer kialakítása, amely hatékonyan képes koordinálni a tagállamok hatóságainak együttműködését és biztosítja az információáramlást az egyes országok között.

A kiberbiztonság kapcsolata az informatikai bűncselekményekkel

Az informatikai bűncselekmények elleni harc összetett folyamat, amelyben az elkövetett bűncselekményre adott reakció csak a jéghegy csúcsa. A büntetőjog eszközei csak kis részét képezik azoknak az intézkedéseknek, amelyek segítenek a digitális világ védelmében és biztonságának megőrzésében, és amelyeket összefoglaló néven a kiberbiztonság eszközeinek nevezünk. Mielőtt tehát belemélyednénk az informatikai bűncselekmények elleni nemzetközi fellépés rejtelmeibe, érdemes egy pillantást vetnünk a rendszerre, amelyben ezek a deliktumok megjelennek. Mivel a kiberbiztonság kapcsán felmerülő jogi, technikai és szervezeti kihívások alapvetően globális jellegűek, elengedhetetlen a koherens, nemzetközi együttműködés keretein belül kialakított stratégia, amely számba veszi az érintett országok szerepét, illetve a már létező stratégiákat. A nemzetközi együttműködés szükségességét felismervén több internacionális szervezet foglalkozott a kiberbiztonság kérdésével. Kiemelkedő ezek közül az International Telecommunications Union (ITU) nevével fémjelzett Global Cybercrime Agenda, valamint az Európai Unió Kiberberbiztonsági Stratégiája. A nemzetközi ajánlások iránymutatásait követve az utóbbi időben Magyarország is tevékenyen foglalkozik a kérdéssel, hazánkban a kiberbiztonság fő irányait a 2013-ban megalkotott Nemzeti Kiberbiztonsági Stratégia tartalmazza.

Ahhoz, hogy megérthessük a fenti stratégiák mibenlétét, elsőként azt kell tisztázni, mit is takar pontos a kiberbiztonság fogalma. Szerencsére számos olyan nemzetközi dokumentumot találhatunk, amelyben megjelenik a kiberbiztonság definíciója, nemzeti szinten pedig Magyarország kiberbiztonsági stratégiája is definiálja.

A nemzetközi meghatározások közül érdemes kiemelni az International Telecommunications Union (ITU) X.1205 számú ajánlását, valamint az Európai Unió Kiberbiztonsági Stratégiáját.

ITU-T X.1205 számú ajánlása a kiberbiztonság áttekintéséről így definiálja a fogalmat: *„A kiberbiztonság azoknak az eszközöknek, politikáknak, biztonsági koncepcióknak, biztonsági intézkedéseknek, iránymutatásoknak, kockázatkezelési megközelítéseknek, cselekményeknek, képzéseknek, jó gyakorlatoknak, biztosítékoknak és technológiáknak a gyűjteménye, amelyeket fel lehet használni a kiberkörnyezet, valamint a szervezetek és a felhasználók eszközeinek védelmére*”.[1]

[1] Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk

Az Európai Unió Kiberbiztonsági Stratégiája[2] pedig következőképpen határozza meg a fogalmat: *„A kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket."*

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

A három fogalommeghatározásban közös, hogy a kiberbiztonság meghatározott eszközök és intézkedések alkalmazását jelenti, amelyek közös célt szolgálnak: a kibertér, a virtuális környezet védelmét az azt fenyegető támadásoktól. Ezek az eszközök nem feltétlenül jogi jellegűek, nagy szerepe van az ipari szereplőkkel való együttműködésnek, a technikai fejlesztéseknek és az oktatásnak is. A büntetőjogi szankció előírása egyértelműen a jogi eszközök közé tartozik, azonban megjegyzendő, hogy a büntetőjog itt is csupán ultima ratio megoldásként jelenik meg.

Az International Telecommunications Union (ITU) 2007. május 17-én elindította a Kibervédelem Globális Menetrendjét (Global Cybersecurity Agenda – GCA). Ez gyakorlatilag egy hálózat, amely lehetővé teszi a nemzetközi párbeszéd és kooperáció kialakítását. A menetrend célja választ találni a kiberbiztonság növekvő kihívásaira. A GCA öt olyan intézkedéscsoportok határozott meg, amelyek révén érvényesíteni szeretné a stratégiai célkitűzéseit, ezek:

1. Jogi intézkedések: ennek a területnek a célja, hogy tanácsokat adjon arra, hogyan lehet a nemzetközi joggal összhangban, jogi szabályozás útján leküzdeni az infokommunikációs eszközökkel elkövetett bűncselekményeket.
2. Technikai és eljárási intézkedések: a második terület azokra az intézkedésekre fókuszál, amelyek a szoftver termékek sebezhetőségével kapcsolatosak, beleértve az akkreditációs rendszereket, jegyzőkönyveket és előírásokat.

---

management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user's assets.

[2] Az Európai Unió kiberbiztonsági stratégiája

3. Szervezeti struktúrák: általános keretrendszerek és válaszadási stratégiák a kibertámadások megelőzésére, felismerésére, valamint a kríziskezelésre, beleértve az egyes országok kritikus információs infrastruktúra rendszereinek védelmét.
4. Kapacitásépítés: e terület célja a kapacitás-építő mechanizmusok kidolgozása, amelyek felhívják a társadalom figyelmét, know-how-t közvetítenek és erősítik a kiberbiztonság jelenlétét a nemzeti politikában.
5. Nemzetközi együttműködés: célja kifejleszteni nemzetközi együttműködési stratégiát, párbeszédet és a kiberveszélyek leküzdésének koordinációját.[3]

Az EU kiberbiztonsági stratégiája szintén öt pontban határozza meg azokat a kiemelt területeket, amelyekkel foglalkozni kell a kiberbiztonság megteremtése érdekében:

1. A kibertámadásokkal szembeni ellenálló képesség elérése;
2. A számítástechnikai bűnözés drasztikus csökkentése;
3. A kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében;
4. A kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
5. A kibertérre vonatkozó összefüggő nemzetközi szakpolitika létrehozása az Európai Unió számára, és az Unió alapértékeinek támogatása.

Az GCA-val, illetve az EU kiberbiztonsági stratégiájával ellentétben a magyar stratégia nem nevesíti külön az informatikai bűncselekmények elleni fellépést, sem a céljai közt, sem a célok eléréséhez szükséges feladatok közt. Kimondja viszont, hogy igazodik az EU által tett ajánlásokhoz, valamint megvalósítandó célként rögzíti, hogy Magyarország *„rendelkezzen hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességekkel a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen.”* A célok eléréséhez szükséges feladatok körében pedig rendelkezik szakosított intézmények létrehozásáról, illetve többlépcsős jogalkotási tevékenységéről. A stratégia nem fejti ki bővebben a többlépcsős jogalkotási tevékenységet, a szakosított intézmények kapcsán azonban megjegyzi, hogy *„a kiberbiztonsággal összefüggő feladatok ellátását a specifikus szakértelemmel és hatáskörrel rendelkező szervezetekhez szükséges telepíteni, amely szervezetek nem csak egymással, hanem az adat- és titokvédelem területén hatósági feladatokat ellátó más szervezetekkel is együttműködnek. A feladatellátás érinti a nemzetbiztonsági, honvédelmi, bűnüldözési, katasztrófavédelmi és létfontosságú intézmények és létesítmények védelmével kapcsolatos*

[3] http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

feladatokat ellátó szervezeteket, valamint az elektronikus információbiztonság területén hatósági jogosítványokkal rendelkező intézményeket." Mivel a kibervédelemmel kapcsolatos feladatok ellátásban szerepet kapnak rendvédelmi szervek is, alappal feltételezhető, hogy a többlépcsős jogalkotási folyamat hatással lesz a büntető anyagi és eljárásjogi szabályokra is.

Az alábbi tanulmányban azokat a nemzetközi valamint európai szintű dokumentumokat foglalom össze, melyek hatással vannak a magyar büntető anyagi és eljárási jogra, valamint a nyomozó hatóságok munkájára.

Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói

Egyesült Nemzetek Szervezete (ENSZ)

Az ENSZ több előremutató lépést tett az informatikai bűncselekmények leküzdése érdekében. Ezek közül az alábbiak a legfontosabbak:

- Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről (1994);
- Az ENSZ Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról;
- Az ENSZ Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról;

Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről[4]

A ENSZ 8. kongresszusa után, az ENSZ Közgyűlése elfogadta a 45/121. számú határozatot a számítógépes bűncselekmények szabályozásáról. E határozat alapján az ENSZ 1994-ben kézikönyvet adott ki a számítógépes bűncselekmények megelőzéséről és kezeléséről. Megjegyzendő, hogy a dokumentum végig a számítógépes bűncselekmény (*computer crime*) megjelölést használja, amely nem fedi le teljesen azoknak az eszközöknek

[4] Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről http://www.uncjin.org/Documents/EighthCongress.html

a körét, amelyekre, vagy amelyeken keresztül ilyenfajta bűncselekményeket lehet elkövetni. A kézikönyv nem határozza meg pontosan a számítógépes bűncselekmény fogalmát, azonban nevesíti azokat a tulajdonságokat, melyekkel ezek a deliktumok rendelkeznek. A kézikönyv a számítógépes bűncselekmény (*computer crime*), valamint a számítógéppel kapcsolatos bűncselekmény (*computer-related crime*) fogalmakat – helytelenül – szinonimaként használja, meg kell azonban jegyzeni, hogy a két fogalom elhatárolására csak később került sor. A kézikönyv felsorolja a számítógépes bűncselekmény leggyakoribb típusait, amelyek a következők:

1. A számítógép manipulációjával elkövetett csalás (*fraud by computer manipulation*);
2. Számítógépes hamisítás (*computer forgery*);
3. Károkozás számítógépes adatokban vagy programokban, illetve a számítógépes adatok vagy programok megváltoztatása (*Damage to or modifications of computer data or programs*)
4. Jogosulatlan hozzáférés számítógépes rendszerekhez és szolgáltatásokhoz (*Unauthorized access to computer systems and service*)
5. Jogi védelem alá eső számítógépes programok jogosulatlan reprodukálása (*Unauthorized reproduction of legally protected computer programs*)

Az ENSZ Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról[5]

2000-ben a Közgyűlés elfogadott egy határozatot, hogy felvegye a harcot az információs technológiák bűncselekményekhez való felhasználásával szemben. Ebben a határozatban a Közgyűlés számos olyan intézkedést azonosított, amelyek segítenek az információs technológiákkal való visszaélés megelőzésében. Az intézkedések a következők:

1. Az államoknak biztosítaniuk kell, hogy a jogszabályaik és joggyakorlatuk felszámolja a védett zónákat az információs technológiákkal való visszaélések esetében.
2. Az információs technológiákkal való nemzetközi jellegű visszaélések esetében koordinálni kell a nyomozó hatóságok együttműködését a nyomozásban és a vádemelésben az érintett államok között.
3. Az államoknak meg kell osztaniuk egymással az információikat azokról a problémákról, amelyekkel az információs technológiák bűncselekményekhez való felhasználása elleni harc során találkoznak.

[5] Az ENSZ Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/63

4. A nyomozó hatóságok személyzetét ki kell képezni és felszereléssel kell ellátni az információs technológiákkal való visszaélések elleni fellépés érdekében.
5. A jogrendszereknek védeniük kell az adatok számítógépes bizalmasságát, integritását és elérhetőségét a jogosulatlan megkárosítástól, és biztosítaniuk kell, hogy a visszaéléseket büntetni rendelik.
6. A jogrendszereknek lehetővé kell tenniük a bűnügyi nyomozásokkal kapcsolatos elektronikus adatok megőrzését, és az ezekhez való gyors hozzáférést.
7. Közös támogatási rezsimekkel kell biztosítaniuk az információs technológiákkal való visszaélések időszerű kivizsgálását, és az ilyen ügyekben keletkezett bizonyítékok összegyűjtését és cseréjét.
8. A nyilvánosság figyelmét fel kell hívni az információs technológiákkal való visszaélések megelőzésének és üldözésének szükségességére.
9. Az információs technológiákat a megvalósítható mértékig úgy kell tervezni, hogy segítsenek megelőzni és felderíteni a visszaéléseket, azonosítani az elkövetőket és összegyűjteni a bizonyítékokat.
10. Az információs technológiákkal való visszaélések elleni küzdelem olyan megoldások kifejlesztését igényli, amelyek számba veszik mind a személyes szabadságjogok és a magánélet védelmét, mind a kormányzat cselekvési lehetőségeinek megőrzését az ilyen jellegű visszaélések elleni küzdelemben.

Az ENSZ Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról[6]

2002-ben az ENSZ Közgyűlése újabb határozatot fogadott el az információs technológiával való visszaélések elleni küzdelem témakörében. A határozatban az ENSZ sürgeti a tagállamok közötti együttműködés erősítését, ugyanakkor felismeri, hogy problémákat okozhatnak az államok közötti különbségek az információs technológiákhoz való hozzáférésben és azok felhasználásában. Felhívja a tagállamokat arra, hogy az információs technológiákkal való visszaélések visszaszorítására koncentráló nemzeti jogszabályok, politikák és gyakorlat kialakításakor vegyék figyelembe a nemzetközi és regionális szervezetek munkáját és eredményeit.

[6] Az ENSZ Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/56/121

Interpol

Az Interpol célja, hogy globálisan koordinálja a digitális bűncselekmények felderítését és megelőzését. Ennek érdekében felállította a Digital Crime Centre-t, amely kutatás-fejlesztési tevékenységet lát el. Az Interpol jelenleg három területen működik, ezek:

1. Harmonizáció: a hatékony kiberbűncselekmények elleni fellépés alapvető eleme a hatékony bűnüldözés, az Interpol azonban felismerte, hogy az összes érintett szektort – privát, akadémiai, közintézmények – be kell vonni a kibertér biztonságossá tételébe. Ennek érdekében arra törekszik, hogy összehangolja a különböző szektorok munkáját, illetve elősegíti, hogy megosszák egymással a tapasztalataikat.
2. A kapacitás bővítése: az Interpol szerint biztosítani kell, hogy a rendőrség tartsa a tempót a technológiai fejlődéssel és rendelkezzen a szükséges szakértelemmel, hogy megfelelően tudják kezelni a folyamatosan változó digitális bűncselekményeket mind nemzeti, mind nemzetközi szinten.
3. Operatív és forenzikus tevékenység: az Interpol támogatja a tagországokban az informatikai elemet tartalmazó nyomozásokat, valamint segíti a közös műveletek koordinációját. Ennek érdekében működteti a Cyber Fusion Centre-t, amely segítséget nyújt az Interpol tagországainak a nyomozás minden szakaszában, valamint a kártékony internetes tevékenységet valós időben vizsgálja és elemzi. Emellett igazságügyi szakértői labort (Digital Forensics Laboratory) működtet.

Az informatikai bűncselekmények elleni fellépés európai dimenziói

Az informatikai bűncselekmények elleni európai fellépés fő irányvonalait az Európai Unió, valamint az Európa Tanács határozzák meg. A szabályozás területén két dokumentum játszik kulcsszerepet: az egyik az Európa Tanács által 2001-ben elfogadott Cybercrime Convention, a másik az Európai Parlament és a Tanács 2013. augusztus 12-i 2013/40/EU számú irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

Európa Tanács

Az Európa Tanács közismerten regionális nemzetközi szervezet, kormányközi együttműködés keretében jött létre. A szervezet jelenleg 47 tagot számlál.

A Miniszteri Bizottság R (89) 9 számú ajánlása a számítógéppel kapcsolatos bűnözésről[7]

Az Európa Tanács Miniszteri Bizottsága 1985-ben szakértői bizottság felállításáról döntött, amelynek a feladata a számítógépes bűncselekmények (*computer crimes*) jogi vonatkozásainak vizsgálata volt. A kutatás eredményei nyomán a Miniszteri Bizottság ajánlást adott ki a számítógéppel kapcsolatos bűncselekményekről (*computer related crimes*),[8] amelyben elemezte azokat a büntető anyagi jogi rendelkezéseket, amelyek az elektronikus bűncselekmények elleni harchoz – beleértve a számítógépes csalást és hamisítást – szükségesek. Az ajánlás a számítógéppel kapcsolatos bűncselekmény fogalmát nem határozza meg, illetve szinonimaként használja a számítógépes és a számítógéppel kapcsolatos bűncselekmény fogalmait. A dokumentum összesen tizenkét tényállást különböztet meg, amelyeket két csoportra oszt: az első egy úgynevezett „minimumlista" mely 8 tényállást, a második egy opcionális lista mely 4 tényállást tartalmaz.

A minimumlista elemei a következőek:

1. Számítógéppel kapcsolatos csalás (*computer-related fraud*): Aki azzal a szándékkal, hogy a maga vagy más személy számára jogtalan gazdasági előnyhöz jusson, számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl, illetőleg hozzáférhetetlenné tesz, vagy az adatfeldolgozást bármilyen egyéb módon befolyásolja, úgy, hogy azok hatással vannak az adatfeldolgozás eredményére, ezáltal más személynek gazdasági vagy birtokbeli kárt okoz, számítógéppel kapcsolatos csalást követ el.

2. Számítógépes hamisítás (*computer forgery*): Aki a nemzeti jog által meghatározott módon, vagy körülmények között számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl, illetőleg hozzáférhetetlenné tesz, vagy az adatfeldolgozást bármilyen egyéb módon befolyásolja, úgy hogy az megfelel a hamisítás bűntettének, amennyiben az ilyen típusú bűncselekmények hagyományos tárgyára tekintettel követte el, számítógépes hamisítást követ el.

3. Károkozás számítógépes adatokban és programokban (*damage to computer data or programs*): Aki számítógépes adatot, vagy programokat jogtalanul töröl, károsít, eltérít, vagy hozzáférhetetlenné tesz, kárt okoz.

[7] Recommendation No. R (89) 9, adopted by the Committee of Ministers - http://www.oas.org/juridico/english/89-9&final%20Report.pdf

[8] Council of Europe. European Committee on Crime Problems: Computer-related Crime. Recommendation No. R (89) 9 on computer-related crime - http://www.oas.org/juridico/english/89-9&final%20Report.pdf

4. Számítógépes szabotázs (*computer sabotage*): Aki azzal a szándékkal, hogy egy számítógép vagy telekommunikációs rendszer működését gátolja számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl, vagy hozzáférhetetlenné tesz, a számítógépes rendszer működését befolyásolja, számítógépes szabotázst követ el.
5. Jogosulatlan hozzáférés (*unauthorized access*): Aki egy számítógépes rendszerbe, vagy számítógépes hálózatba jogtalanul, a biztonsági intézkedéseket kijátszva belép, jogosulatlan hozzáférést követ el.
6. Jogosulatlan lehallgatás (*unauthorized interception*): Jogosulatlan lehallgatás olyan kommunikációtechnikai módszerrel, amely számítógépes rendszer vagy hálózat útján valósul meg.
7. Védett számítógépes programok jogellenes reprodukálása (*unauthorised reproduction of a protected computer program*): Aki jog által védett számítógépes programot jogtalanul reprodukál, terjeszt, vagy a nyilvánosság számára hozzáférhetővé tesz, bűncselekményt követ el.
8. Topográfiák jogosulatlan reprodukálása (*unauthorised reproduction of a topography*): Aki jog által védett félvezető termék topográfiáját jogtalanul reprodukálja, vagy a félvezető terméket reprodukálás céljából jogtalanul hasznosítja, importálja, vagy jogtalanul félvezető terméket gyárt topográfia használatával, bűncselekményt követ el.

Az opcionális lista elemei pedig az alábbiak:

1. Számítógépes adatok vagy programok megváltoztatása (*alteration of computer data or computer programs*): Aki a számítógépes adatokat vagy programokat jogtalanul megváltoztatja bűncselekményt követ el.
2. Számítógépes kémkedés (*computer espionage*): Aki kereskedelmi vagy üzleti titkot jogtalanul, illetve jogi felhatalmazás nélkül, helytelen eszközökkel megszerez, közzétesz, átruház vagy felhasznál, azzal szándékkal, hogy a titok jogosultjának gazdasági veszteséget okozzon, illetőleg magának vagy másnak jogtalan gazdasági előnyt szerezzen, bűncselekményt követ el.
3. Számítógép jogosulatlan használata (*unauthorised use of a computer*): Aki a számítógépes rendszert vagy hálózatot jogosulatlanul oly módon használja, hogy
    - elfogadja a jelentős kockázatát annak, hogy a rendszer használatára jogosult személynek kára keletkezik, vagy a rendszerben, illetve annak működésében kár keletkezik,
    - szándéka arra irányul, hogy a rendszer használatára jogosult személynek kára keletkezzen, vagy a rendszerben illetve annak működésében kár keletkezzen,
    - a rendszer használatára jogosult személynek kára keletkezik, vagy a rendszerben illetve annak működésében kár keletkezik,

    bűncselekményt követ el.

4. Védett program jogosulatlan használata (*unauthorised use of a computer program*): Aki jog által védett és jogtalanul reprodukált számítógépes programot jogtalanul használ azzal a szándékkal, hogy magának vagy másnak jogtalan gazdasági előnyt szerezzen, vagy a jog tulajdonosának kárt okozzon, bűncselekményt követ el.

Ez a szabályozás azonban hamar meghaladottá vált, sok kritika érte. Siegler Eszter szerint[9] a minimum és fakultatív lista nem jó, mert a felvázolt tényállások között sok átfedés van, illetve hiányzik a számítógéppel kapcsolatos bűncselekmények fő típusainak éles elhatárolása, és ez a szabályozást kiszámíthatatlanná áttekinthetetlenné teszi. A szerző egyetért a fentiekkel, továbbá rávilágít arra, hogy sok esetben magukat a tényállásokat sem fogalmazzák meg pontosan. A számítógépes adatok vagy programok megváltoztatása címszó alatt például csak annyit ír az ajánlás, hogy aki számítógépes adatokat vagy programokat megváltoztat, bűncselekményt követ el, azonban nem rendelkezik arról, hogy a megváltoztatás csak szándékosan történhet, vagy akár gondatlanságból is.

A Miniszteri Bizottság R (95) 13 számú ajánlása a büntetőeljárás információs technológiával kapcsolatos problémáiról[10]

1995-ben a Miniszteri Bizottság újabb ajánlást fogadott el, amelyben a következő hét pontban foglalja össze azokat a problémákat, amelyek a büntetőeljárás során felmerülhetnek, amennyiben informatikai bűncselekményekről van szó:

1. Átvizsgálás és lefoglalás (*search and seizure*): A számítógépes rendszerek átvizsgálásának, valamint a bennük tárolt adatok lefoglalásának, és az átvitel közben keletkező adatok lehallgatásának jogi elhatárolását egyértelműen kell felvázolni és alkalmazni. A büntetőeljárási jogoknak meg kell engedniük a nyomozó hatóságok számára, hogy átvizsgálják a számítógépes rendszereket és lefoglalják az adatokat hasonló feltételekkel, mint a tradicionális házkutatás és lefoglalás esetében. A rendszerért felelős személyt tájékoztatni kell a rendszer átvizsgálásáról és a lefoglalt adatok típusáról. Azoknak a jogorvoslatoknak, amelyek alkalmazhatóak az általános házkutatás és lefoglalás esetében, ugyanúgy alkalmazhatónak kell lenni a számítógépes rendszerek átvizsgálására és a bennük tárolt adatok lefoglalására. Az átvizsgálás végrehajtása alatt a nyomozó hatóságoknak megfelelő biztosítékok

[9] Dr. SIEGLER Eszter: A számítógéppel kapcsolatos es a számítógépes bűncselekmények, Magyar Jog 1997/12.

[10] A Miniszteri Bizottság R (95) 13 számú ajánlása a büntetőeljárás információs technológiával kapcsolatos problémáiról http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp

mellett rendelkezniük kell azzal a jogosítvánnyal, hogy kiterjesszék a keresést egyéb, a joghatóságuk alá tartozó számítógépes rendszerekre, amelyek hálózaton keresztül össze vannak kapcsolva, illetve lefoglalja a bennük található adatokat, amennyiben azonnali intézkedésre van szükség. Ahol az automatikusan feldogozott adat megfelel egy tradicionális dokumentumnak, a büntető eljárásjog dokumentumok átvizsgálásával és lefoglalásával foglalkozó szabályainak ezekre is ki kell terjednie.

2. Megfigyelés (*Technical surveillance*): Az információtechnológia és a telekommunikáció konvergenciájának szempontjából felül kell vizsgálni a bűnügyi nyomozások célját szolgáló technikai intézkedéseket pl. telekommunikáció lehallgatása, és ahol szükséges módosítani kell ezeket az alkalmazhatóságuk biztosítása végett. Ez a rész tárgyalja azokat a problémákat, amelyek a megfigyeléssel, a lehallgatással és a forgalmi adatok összegyűjtésével kapcsolatosak, különös figyelmet fordítva a jelenlegi szabályok felülvizsgálatának kérdésére.
3. A nyomozó hatóságokkal való együttműködés kötelezettsége (*Obligations to co-operate with the investigating authorities*): A legtöbb jogrendszer megengedi, hogy a nyomozó hatóságok utasítsanak bizonyos személyeket arra, hogy adják át a birtokukban lévő tárgyakat, amelyekre a bizonyítás során szükség van. Ezzel párhuzamosan rendelkezéseket kell hozni arról is, hogy utasíthassák ezeket a személyeket arra, hogy a birtokukban lévő információs rendszerben tárolt adatokat a szükséges formában adják át a nyomozó hatóságnak. A nyomozó hatóságoknak rendelkezniük kell azzal a képességgel, hogy utasítsák azokat a személyeket, akiknek adataik vannak az információs rendszerben, hogy átadják az információs rendszerhez, valamint a benne tárolt adatokhoz való hozzáféréshez szükséges összes információt. A büntetőeljárási jognak azt is biztosítania kell, hogy hasonló utasítást lehessen adni olyan személyeknek is, akik ismeretekkel rendelkeznek az információs rendszer működéséről vagy azokról az intézkedésekről, amelyeket a benne tárolt adatok védelmében alkalmaztak. A telekommunikációs szolgáltatásokat nyilvános vagy magán hálózatokon kínáló szolgáltatókra speciális kötelezettségeket kell telepíteni, hogy olyan információkat adjanak át, amelyekkel azonosítható a felhasználó, amennyiben a nyomozó hatóság erre utasítja őket.
4. Elektronikus bizonyítékok (*Electronic evidence*): El kell ismerni a közös igényt az elektronikus bizonyítékok oly módon történő összegyűjtésére, megőrzésére és bemutatására, ami a legjobban biztosítja és tükrözi integritásukat és hitelességüket mind a nemzeti büntetőeljárásban, mint a nemzetközi együttműködésben. Ezért azokat az eljárásokat és technikai módszereket, amelyek az elektronikus bizonyítékok kezelésére vonatkoznak, tovább kell fejleszteni oly módon, amely biztosítja az államok közötti kompatibilitást.
5. Titkosítás használata (*Use of encryption*): Olyan intézkedéseket kell tenni, amelyek minimalizálják a bűncselekmények nyomozásakor a kriptográfia használatának negatív hatásait, anélkül, hogy a feltétlenül szükségesnél jobban érintenék legitim használatát.

6. Kutatás, statisztika, képzés (*Research, statistics and training*): Tovább kell vinni az informatikai bűncselekményekről rendelkezésre álló adatok elemzését, beleértve a modus operandi és a műszaki szempontok vizsgálatát. Meg kell fontolni speciális szakosított egység létrehozását az ilyen speciális szakértelmet igénylő bűncselekmények vizsgálatára.
7. Nemzetközi együttműködés (*International co-operation*): Az átvizsgálás jogának kiterjesztését más számítógépes rendszerekre azokban az esetekben is alkalmazni kell, amikor a rendszer más ország joghatósága alá tartozik, amennyiben azonnali intézkedésre van szükség. Annak érdekében, hogy elkerülhető legyen az állami szuverenitás, illetve a nemzetközi jog megsértése, az ilyen kiterjesztett átvizsgálásra és lefoglalásra egyértelmű jogi szabályokat kell alkotni. Elérhetőnek kell lennie olyan gyorsított és megfelelő eljárásoknak, valamint összekötő rendszernek, amelyek alapján a nyomozó hatóságok igényelhetik, hogy a külföldi hatóságok gyűjtsék össze a bizonyítékokat. A megkeresett hatóságoknak felhatalmazással kell rendelkezniük a telekommunikációval kapcsolatos forgalmi adatok megosztására, a telekommunikáció lehallgatására, illetve a forrásának azonosítására. E célból a jelenlegi kölcsönös jogsegély eszközeit ki kell egészíteni.

A Számítástechnikai bűnözésről szóló egyezmény és a kiegészítő jegyzőkönyvek[11]

Az Európa Tanács számítástechnikai bűnözésről szóló (Cybercrime) egyezményét 2001-ben fogadták el Budapesten, 2011 júliusáig 47 állam írta alá és 31 ratifikálta. A számítástechnikai bűnözésről szóló egyezményt a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv[12] követte.

Az egyezmény azon felül, hogy dogmatikailag letisztultan csoportosítja a bűncselekményeket, definiálja a számítógépes környezetben megjelenő technikai fogalmakat.

Az értelmező rendelkezések körében az egyezmény több alapfogalmat definiál, mint számítástechnikai rendszer (*computer system*), számítástechnikai adat (*computer data*), szolgáltató (*service provider*), illetve forgalmi adat (*traffic data*), viszont a számítástechnikai bűncselekmény *(cybercrime*) fogalmának meghatározásával adós marad.

[11] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

[12] A számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv - http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

Az egyezmény értelmezésekor probléma adódhat abból, hogy az új Btk. hatályba lépésével a magyar büntetőjog már nem használja sem a számítástechnikai rendszer, sem a számítógépes/számítástechnikai bűncselekmény fogalmát, hiszen azokat a valamivel tágabb, információs rendszer, illetve informatikai/információs bűncselekmények fogalmakra cserélte. Az egyezmény és a magyar büntető törvénykönyv a számítástechnikai rendszer, valamint az információs rendszer fogalmakat ugyanazzal a tartalommal töltötte meg, azonban ez a megegyezés csak látszólagos. Ha vetünk egy pillantást a Btk. kommentárjára, kiderül, hogy a magyar jog az információs rendszer fogalma alatt nem csak számítástechnikai, hanem telekommunikációs eszközöket is ért. Manapság azonban a számítástechnikai eszközök és a telekommunikációs eszközök nem határolhatóak el élesen egymástól, példaként említve egy okostelefont, amely egyszerre telefon és miniatűr számítógép.

Az egyezmény második része a büntető anyagi jogi szabályokkal foglalkozik, és négy csoportra osztja a bűncselekményeket. Az első csoportot képezik a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények, amelyek mindegyikét a tartalmazza a magyar Btk. is. Ebbe a csoportba az alábbi bűncselekmények tartoznak:

1. Jogosulatlan belépés
2. Jogosulatlan kifürkészés
3. Számítástechnikai adat megsértése
4. Számítástechnikai rendszer megsértése
5. Eszközökkel való visszaélés

A második csoportba a számítógéppel kapcsolatos bűncselekmények taroznak, amelyek az alábbiak:

1. Számítógéppel kapcsolatos hamisítás
2. Számítógéppel kapcsolatos csalás

Ezen a ponton az egyezmény némiképp eltér attól a csoportosítástól, ami a magyar jogirodalomban többnyire megszokott. Hazánkban ugyanis általában az informatikai bűncselekményeket két csoportra szokás osztani: tisztán informatikai jellegű bűncselekményekre, illetve a hagyományos számítógéppel elkövetett bűncselekményre. Előbbi csoportba azok a deliktumok tartoznak, amelyeknek az elkövetési tárgya az információs rendszer, a hálózat illetve a bennük tárolt adat, utóbbi csoportba pedig azok a bűncselekmények tartoznak, amelyeknél a számítógép az elkövetés eszköze, így ez a csoport nagyon színes képet mutat. A nálunk meghonosodott csoportosításból némiképp kilóg az

információs rendszer felhasználásával elkövetett csalás bűntette, hiszen ezt a tisztán informatikai bűncselekmény közé sorolják, azonban nem jellemző rá az informatikai bűncselekmények összes tulajdonsága. Az információs rendszer felhasználásával elkövetett csalások tekintetében az elkövetés tárgya nem a számítógép, az elkövető cselekménye sem a rendszer működésében, sem az abban tárolt adatokban nem okoz kárt és nem akadályozza azok megfelelő működését sem. Ebben az esetben pusztán annyiról van szó, hogy a tettes az információs rendszerbe valótlan adatokat visz be, vagy a rendszerben tárolt adatokat megváltoztatja, megsemmisíti vagy törli, és ezzel kárt okoz.

A harmadik cím számítástechnikai adatok tartalmával kapcsolatos bűncselekményekről a negyedik pedig a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekményekről szól. Előbbi kategóriába a gyermekpornográfiával kapcsolatos bűncselekmények tartoznak.

Az egyezmény kiegészítő jegyzőkönyve kriminalizálja továbbá a rasszista és faji megkülönböztetést, a bántalmazást, valamint a népirtás és az emberiesség elleni bűncselekmények tagadását, következményeinek minimalizálását, elfogadását illetve támogatását. Büntetni rendeli ezen felül ezek támogatását is.

Véleményem szerint a fent felvázolt két csoportosítás keveréke lenne a legideálisabb. A tisztán informatikai bűncselekmények csoportját nem szükséges átalakítani, azonban a további csoportokban másféle megközelítést javasolnék. Az információs rendszerrel kapcsolatos bűncselekmény elnevezés jó összefoglaló elnevezés lehet azokra a deliktumokra, amelyeknél a számítógép csak az elkövetés eszköze azonban úgy vélem, ezen a kategórián belül további alegységekre van szükség, hogy ezt a nagyon sokszínű bűncselekményhalmazt némiképp rendszerezni lehessen. Az egyezmény egyik nagy hibájának tartom, hogy nem fogja át teljes körűen azokat a magatartásokat, amelyeket manapság jellemzően információs rendszer felhasználásával követnek el. Az egyezmény nem vesz figyelembe olyan új trendeket mint a cyberbullying (internetes zaklatás), sextortion valamint a személyazonosság-lopás (identity-theft), a botnetek elterjedése, az Internetet terrorista célú használata, pedig ezek tipikusan olyan cselekmények ahol a számítógépes hálózat, illetve az Internet kulcsszerepet játszik. Ennek feltehetően az az oka, hogy egy nemzetközi egyezmény kiegészítése és módosítása körülményes és hosszadalmas feladat, ezért nem várható el tőle, hogy alkalmazkodjon az ilyen folyamatosan változó és bővülő magatartásokhoz.

Az egyezmény harmadik része az eljárási szabályokat, negyedik része pedig a nemzetközi együttműködés szabályait tartalmazza. Az eljárási

szabályok nagy része a magyar jogrendszerben is megtalálható, ilyen a tárolt számítástechnikai adat gyors megőrzése, amely a Be.-ben a kényszerintézkedések között információs rendszerben tárolt adat megőrzésére kötelezés címen szerepel, vagy a közlésre kötelezés, amely a lefoglalás szabályai között kapott helyet, és a tárolt számítástechnikai adat átvizsgálása, amely a házkutatás című részben található. Nem ismeri viszont a magyar jogrendszer a házkutatás kiterjesztését más rendszerre. Az Egyezmény alapján ugyanis ha a nyomozó hatóság alappal feltételezheti, hogy a keresett adatok egy része más információs rendszerben található és ezek az adatok a kiinduló rendszer számára hozzáférhetőek, akkor a hatóság haladéktalanul kiterjesztheti az átvizsgálást vagy a más hasonló módon történő hozzáférést a másik rendszerre is. Ilyen lehet például egy felhő, vagy egy FTP szerver. Érdekes kérdés viszont, hogy mi a teendő abban az esetben, ha a felhasználó a számítógépén keresztül hozzáfér egy olyan FTP szerverhez, amelyben jogsértő tartalmakat (pl. gyermekpornográfiát) találnak. Ebben az esetben ugyanis az adathordozó, vagyis a szerver egy teljesen más helyen található, és a felhasználó számítógépétől függetlenül működik és elérhető. Az adathordozó lefoglalása csak abban az esetben lehetséges, amennyiben a nyomozó hatóság a házkutatást erre a helyszínre fizikailag is kiterjeszti.

Problémát okozhatnak továbbá az olyan új technológiák, amelyekre az egyezmény elfogadásakor még nem gondoltak, így a VOIP (Voice Over Internet Protocoll), amely a távközlés olyan formája, ahol a beszélgetés nem hagyományos telefonhálózaton, hanem az Interneten vagy más adathálózaton folyik. VOIP használata esetében pusztán az előfizető azonosításával nem határozható meg a hívó fél tartózkodási helye, valamint a telefonszámokra sincs külön szabvány, a felhasználó nem kötelező a hagyományos számgazdálkodás szerinti azonosítókat használni (pl. Skype felhasználónév akár betűből is állhat).

Európai Unió

Az Európai Unió számos jogi eszközt dolgozott ki az informatikai bűncselekmények tekintetében, ám ezeknek az intézkedéseknek az a hátrányuk, hogy csak az Unió 27 tagállamára kötelezőek. Az Európai Unió működéséről szóló szerződés (EUMSZ) 83. cikkének (1) bekezdése szerint az Európai Parlament és a Tanács szabályozási minimumokat állapíthat meg bűncselekményi tényállások és büntetési tételek meghatározásához egyes különösen súlyos bűncselekmények esetében. „*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."[13] Az alábbi uniós jogi aktusok tartalmaznak az informatikai bűncselekményekkel kapcsolatos rendelkezéseket:

- Az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól ("Elektronikus kereskedelemről szóló irányelv" – 2000);
- A Tanács 2001/413/IB számú kerethatározata a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről (2001);
- A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról (2005);
- Az Európai Parlament és a Tanács 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (2006);
- Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

Az Európai Parlament és a Tanács 2000/31/EK irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól ("Elektronikus kereskedelemről szóló irányelv")[14]

Az e-kereskedelmi irányelv alapvetően nem büntetőjogi jellegű dokumentum, mégis érdemes megemlíteni, mivel az irányelv által szabályozott tárgykörök *„a számítógépes hálózatokon keresztül végzett gazdasági tevékenységek széles skáláját ölelik fel"*[15], ebből kifolyólag az irányelv néhány olyan rendelkezést is tartalmaz – például a közvetítő szolgáltatók felelőssége –, amelyek az informatikai bűncselekmények esetében is relevanciával bírnak.

A közvetítő szolgáltatók büntetőjogi felelőssége a magyar jogirodalomban is gyakran tárgyalt téma[16], mivel azonban a büntetőjogi

[13] Az Európai Unió Működéséről szóló szerződés - http://europa.eu/pol/pdf/consolidated-treaties_hu.pdf
[14] http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32000L0031&qid=1427107923613&from=EN
[15] (18)
[16] Ld. pl.: SZABÓ Imre: Az internet közvetítő szolgáltatóinak büntetőjogi felelősségéről

felelősség megállapítása nem képezi ezen értekezés tárgyát, csak néhány jelentősebb gondolatról ejtek szót.

Az Internet világában a felhasználón és a tartalomszolgáltatón kívül számos olyan szereplő van, akik valamilyen módon részt vesznek az információáramlás biztosításában, valamint annak elősegítésében, hogy a tartalomszolgáltató által kínált tartalom eljusson a fogyasztóhoz, ezek a közvetítő szolgáltatók. A közvetítő szolgáltatóknak több fajtája ismeretes, ezek:

- Internetszolgáltatók (*Internet service provider*): ezek az információt távközlő hálózaton továbbítják, vagy a távközlő hálózathoz hozzáférést biztosítanak, vagyis ők biztosítják a felhasználó számára az adatátvitelt és az ehhez szükséges infrastruktúrát, hálózati erőforrásokat.
- Tárhelyszolgáltatók (hosting provider): ezek a szolgáltatás igénybe vevője által biztosított információt tárolják (pl. szervereken)
- Gyorsítótárolás (*cache*): A gyorsítótár olyan átmeneti információtároló elemet jelent, amelynek a célja az információ-hozzáférés gyorsítása. A gyorsítás egyszerűen azon alapul, hogy a gyorsítótár gyorsabb tárolóelem, mint a hozzá kapcsolt elemek, így ha ezen területek tartalma korábban már bekerült a gyorsítótárba (mert már valaki/valami hivatkozott rá korábban), az ilyen adatokat a cache tárolóból elő lehet hívni.
- Keresőszolgáltatás (*search engine*): információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (*google, bing*).

Az irányelv bizonyos feltételek teljesülése esetén mentesíti a közvetítő szolgáltatókat, hiszen a tevékenységük többnyire csak egyszerű továbbításra, illetve adattárolásra korlátozódik, a tárolt információ tartalmáról, így jogsértő voltáról nem feltétlenül van tudomásuk, és a tartalomszolgáltatókkal ellentétben nem rendelkeznek szerkesztői felelősséggel sem. A mentesülés egyik feltétele azonban, hogy amint a közvetítő szolgáltató észleli, a jogsértő adatokat, köteles azokat haladéktalanul eltávolítani.

A Tanács 2001/413/IB kerethatározata a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről[17]

A kerethatározat kötelezettséget ír elő a tagállamok számára, hogy harmonizálják a nevezett deliktumokkal kapcsolatos büntetőjogi

[17] http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32001F0413&qid=1427790882359&from=EN

szabályokat, amikor kimondja, hogy *„ezeket a magatartásokat valamennyi tagállamban bűncselekménynek kell minősíteni, és az ilyen bűncselekményeket elkövető vagy azokért felelősséggel tartozó természetes és jogi személyekkel szemben hatásos, arányos és visszatartó erejű szankciókat kell előírni.”*[18]

A kerethatározat fogalommeghatározásai meglehetősen hiányosak, hiszen a dokumentum mindössze két fogalmat definiál, a „fizetőeszköz” valamint a „jogi személy” fogalmát. A határozat szóhasználata meglehetősen esetlen, hiszen a „fizetőeszköz” fogalmát úgy határozza meg, hogy kivonja alóla az ún. törvényes fizetőeszközöket (bankjegyeket, érméket), vagyis a készpénzt, ezen felül példálózó felsorolással határozza meg a készpénz-helyettesítő fizetési eszközöket[19].

A dokumentum négy formáját határozza meg a fizetési eszközökkel kapcsolatos bűncselekményeknek, ezek:

a) a fizetőeszköz ellopása vagy más módon történő jogellenes eltulajdonítása;
b) fizetőeszköz jogosulatlan felhasználás céljából történő hamisítása vagy meghamisítása;
c) lopott vagy más módon jogellenesen eltulajdonított, illetve hamis vagy hamisított fizetőeszköz elfogadása, megszerzése, szállítása, más személy részére történő értékesítése vagy átruházása, illetve birtoklása jogosulatlan felhasználás céljából;
d) lopott vagy más módon jogellenesen eltulajdonított, illetve hamis vagy meghamisított fizetőeszköz jogosulatlan felhasználása.

Megjegyezendő továbbá, hogy a kerethatározat nem csak a materiális eszközöket (csekkek, váltók, hitelkártyák és más kártyák) részesíti védelemben, hanem magát az elektronikus pénzt, amely *„készpénz átvétele illetőleg számlapénz átutalása ellenében kibocsátott elektronikus pénzeszközön tárolt pénzérték*” is. Ezért a 3. cikk azokról a számítógépes bűncselekményekről szól,[20] amelyek pénz vagy pénzbeli érték

[18] (9)

[19] 1. cikk: „fizetőeszköz” a törvényes fizetőeszközök (bankjegyek és érmék) kivételével minden olyan materiális eszköz, amely különleges természeténél fogva önállóan vagy más (fizető)eszközzel együtt birtokosát vagy használóját képessé teszi pénz vagy pénzbeli érték átruházására; ilyen például a hitelkártya, az eurocsekk kártya, a pénzügyi intézmények által kibocsátott más kártyák, az utazási csekkek, az eurocsekkek és más csekkek és váltók, amelyek a hamisítás vagy a jogosulatlan felhasználás ellen például kivitelezésük, kódolásuk vagy a rajtuk lévő aláírás folytán védettek.

[20] 3. cikk: Minden tagállam megteszi a szükséges intézkedéseket annak biztosítása érdekében, hogy bűncselekménynek minősüljön az alábbi magatartások szándékos elkövetése:

- számítógépes adatok, különösen azonosító adatok jogosulatlan bevitele, módosítása, törlése vagy hozzáférhetetlenné tétele, vagy
- számítógépes program vagy rendszer működésébe való jogosulatlan beavatkozás

útján pénz vagy pénzbeli érték átruházása vagy átruháztatása, amely más személy számára jogellenes vagyoni hátrányt okoz abból a célból, hogy a bűncselekmény elkövetőjének vagy harmadik személynek abból jogellenes vagyoni előnye származzon.

átruházására vagy átruháztatására irányulnak. Ez a cikk kétféle magatartástípust foglal magában, egyrészt számítógépes adatok, különösen azonosító adatok jogosulatlan bevitelét, módosítását, törlését vagy hozzáférhetetlenné tételét, másrészt a számítógépes program vagy rendszer működésébe való jogosulatlan beavatkozást. A cselekmény célzatos (a cél a jogellenes vagyoni előny szerzése) és eredményt is tartalmaz (más személy számára jogellenes vagyoni hátrányt okoz). Fontos kiemelni, hogy ennek a deliktumnak minden esetben eleme a pénznek vagy pénzbeli értéknek az átruházása, hiszen amennyiben ez nem valósul meg, helyette a meglévő tényállási elemek függvényében más deliktumok, például információs rendszer vagy adat, megsértése, illetve az információs rendszer felhasználásával elkövetett alapesete csalás valósulhatnak meg.

Mivel az ilyen típusú bűncselekmények erősen technológiai jellegűek a kerethatározat rendelkezéseket tartalmaz arra is, a megvalósításukat lehetővé tévő eszközök jogosulatlan előállítását, megszerzését, értékesítését, átruházását is szankcióval sújtsák a tagállami büntető-törvénykönyvek.

A jelenlegi magyar szabályozás szinte teljesen összhangban van a kerethatározat rendelkezéseivel. Az alábbi összefoglaló táblázat azt mutatja, hogy a határozatban nevesített deliktumok, hogy helyezkednek el a magyar büntető-törvénykönyv rendszerében:

2. cikk a) fizetőeszköz ellopása vagy más módon történő jogellenes eltulajdonítása	**393.§ - Készpénz-helyettesítő fizetési eszközzel visszaélés** Aki a) egy vagy több 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,
2. cikk b) fizetőeszköz jogosulatlan felhasználás céljából történő hamisítása vagy meghamisítása	**392.§ - Készpénz-helyettesítő fizetési eszköz hamisítása** Aki felhasználás céljából a) készpénz-helyettesítő fizetési eszközt meghamisít, b) hamis készpénz-helyettesítő fizetési eszközt készít,
2. cikk c) lopott vagy más módon jogellenesen eltulajdonított, illetve hamis	**393.§ - Készpénz-helyettesítő fizetési eszközzel visszaélés** b) hamis vagy meghamisított, az a)

vagy hamisított fizetőeszköz elfogadása, megszerzése, szállítása, más személy részére történő értékesítése vagy átruházása, illetve birtoklása jogosulatlan felhasználás céljából	pontban meghatározott módon elvett vagy megszerzett készpénz-helyettesítő fizetési eszközt, vagy az elektronikus készpénz-helyettesítő fizetési eszközön tárolt adatokat vagy az ahhoz kapcsolódó biztonsági elemeket átad, megszerez, az ország területére behoz, onnan kivisz, vagy azon átszállít,
2. cikk d) lopott vagy más módon jogellenesen eltulajdonított, illetve hamis vagy meghamisított fizetőeszköz jogosulatlan felhasználása.	**375.§ Információs rendszer felhasználásával elkövetett csalás** (5) Az (1)-(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.
3. cikk • számítógépes adatok, különösen azonosító adatok jogosulatlan bevitele, módosítása, törlése vagy hozzáférhetetlenné tétele, vagy • számítógépes program vagy rendszer működésébe való jogosulatlan beavatkozás útján pénz vagy pénzbeli érték átruházása vagy átruháztatása, amely más személy számára jogellenes vagyoni hátrányt okoz abból a célból, hogy a bűncselekmény elkövetőjének vagy harmadik személynek abból jogellenes vagyoni előnye származzon.	**375. § Információs rendszer felhasználásával elkövetett csalás** (1) 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.
4. cikk a fizetőeszköz jogosulatlan felhasználása céljából történő hamisításának vagy meghamisításának elkövetésére különösen alkalmas berendezés, tárgy, számítógépes program vagy más eszköz, illetve a számítógépes cselekmények elkövetésének célját szolgáló számítógépes program jogosulatlan előállítása, elfogadása, megszerzése, más személy részére történő értékesítése vagy átruházása, illetve birtoklása	**394§ - Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése** Aki készpénz-helyettesítő fizetési eszköz hamisításához vagy a készpénz-helyettesítő fizetési eszközön lévő adat technikai eszközzel való rögzítéséhez szükséges anyagot, eszközt, berendezést vagy számítástechnikai programot készít, megszerez, tart, átad, forgalomba hoz, az ország területére behoz, onnan kivisz, vagy azon átszállít, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

Lényegi különbség valójában csak egy ponton figyelhető meg, mégpedig az informatikai bűncselekményeket szabályozó cikk és a magyar büntető törvénykönyv szövege között. A magyar szabályozás nem tekinti külön tényállásnak azt az esetet, amikor az információs rendszer

felhasználásával elkövetett károkozás pénz vagy pénzbeli érték átruházása útján valósul meg, hiszen az ily módon elkövetett bűncselekmény tökéletesen illeszkedik az információs rendszer felhasználásával elkövetett csalás tényállásába is.

A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról[21]

2005 februárjában az Európai Unió Tanácsa elfogadta az információs rendszerek elleni támadásról szóló kerethatározatot. Ebben a kerethatározatban a korábban használatos számítógépes rendszer fogalom helyett már az információs rendszer (*information system*) fogalom jelenik meg. Az egyes fogalmak összevetésekor megfigyelhető, hogy annak ellenére, hogy a megjelölés különbözik (információs rendszer – számítógépes rendszer) a fogalmak tartalma gyakorlatilag megegyezik. Ez nem csak nemzetközi viszonylatban igaz, hiszen az új Btk. hatályba lépésekor a korábbi számítógépes rendszer kifejezés gyakorlatilag csak új nevet kapott, a tartalma látszólag változatlan marad. Ezek alapján joggal tehető fel a kérdés, valójában meg kell-e különböztetnünk a számítógépes rendszert az információs rendszertől, illetve a számítástechnikai bűncselekményt az informatikai bűncselekménytől.

A kerethatározat leszűkíti az üldözendő magatartások körét 3 magatartásra, ezek:

1. Információs rendszerekhez való jogsértő hozzáférés
2. Rendszerbe való jogsértő beavatkozás
3. Adatokba való jogsértő beavatkozás

A kerethatározat hibája, hogy a jogi felelősség formájának megválasztását gyakorlatilag a tagállamokra bízza, amikor kimondja, hogy a nevezett cselekmények legalább a jelentősebb esetekben minősüljenek bűncselekménynek. Nem definiálja azonban a jelentősebb esetek kritériumait, ezért a tagállamoknak viszonylag nagy a mozgásterük, így nem feltétlen szükséges büntetőjogi szankcióval fenyegetniük ezeket a cselekményeket. Ez a megközelítés gyakorlatilag azt sugallja a bűnelkövetők számára, hogy ha egy bűncselekményt (pl. csalást) nem a fizikai világban, hanem az Interneten keresztül követnek el, a cselekmény súlyától függetlenül enyhébb elbánásban részesülhetnek, amennyiben a

[21] http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32005F0222&qid=1427799018036&from=EN

bűncselekmény elbírálására joghatósággal rendelkező tagállam úgy dönt, hogy az információs rendszeren keresztül elkövetett csalást nem, vagy enyhébben bünteti, mint a hagyományos csalást.

A kerethatározatot 2013-ban felváltotta az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv.

> *Az Európai Parlament és a Tanács 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról*[22]

Az adatmegőrzési irányelvről annak ellenére is érdemes pár szót ejteni, hogy az Európai Unió Bírósága 2014. április 8. napján az Európai Unió Alapjogi Chartájával való ütközése miatt érvénytelennek nyilvánította.

Az irányelv megalkotásának célja az volt, hogy „*a bűncselekmények megelőzése, kivizsgálása, felderítése és üldözése érdekében az adatok megőrzését előíró nemzeti rendelkezések közötti jogi és technikai különbségek akadályokat jelentenek az elektronikus hírközlés belső piaca számára, mivel a szolgáltatások nyújtóira eltérő követelmények vonatkoznak a megőrizendő forgalmi és helymeghatározó adatok típusait, valamint a megőrzés feltételeit és idejét illetően*”.

Az irányelv szerint a tagállamoknak az alábbi adatkategóriák megőrzését kell biztosítania:

1. a közlés forrásának megtalálásához és azonosításához szükséges adato;
2. a közlés címzettjének azonosításához szükséges adatok;
3. a közlés napjának, időpontjának és időtartamának megállapításához szükséges adatok;
4. a közlés típusának megállapításához szükséges adatok;
5. a felhasználók (feltételezett) kommunikációs berendezésének azonosításához szükséges adatok;
6. mobil kommunikációs eszköz helyének megállapításához szükséges adatok.

Az irányelv alapján a közlés tartalmát felfedő adat azonban nem őrizhető meg.

[22] http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32006L0024&qid=1427876516458&from=EN

A magyar szabályokat az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban Eht.) 159/A. §-a rögzíti, bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettség cím alatt, ami teljes mértékben megfelel az irányelv előírásainak.

Az Európai Unió Bírósága a C-293/12. és C-549/12. számú Digital Rights Ireland valamint Seitlinger és társai egyesített ügyekben hozott ítéletben[23] azért nyilvánította érvénytelennek az irányelvet, mert az irányelv széles körű és súlyos beavatkozást jelent a magánélet tiszteletben tartásához és a személyes adatok védelméhez való alapvető jogba. A bíróság álláspontja szerint *„ezen adatok együttesen véve igen pontos következtetések levonását tehetik lehetővé azon személyek magánélete vonatkozásában, akiknek az adatait megőrizték, így például a napi szokások, az állandó vagy ideiglenes tartózkodási helyek, a napi vagy egyéb helyváltoztatások, a gyakorolt tevékenységek, az e személyek társadalmi kapcsolatai és az általuk látogatott társadalmi közegek tekintetében."* A bíróság azt is aggályosnak találta, hogy az irányelv általános jelleggel állapít meg szabályokat, és nem alkalmaz semmilyen megkülönböztetést, korlátozást vagy kivételt, így tehát olyan személyek adatait is megőrzik, akik nem állnak büntetőeljárással kapcsolatban. Az irányelv nem rendelkezik arról sem, hogy az adatok későbbi felhasználásának egyes, pontosan körülhatárolt súlyos bűncselekmények megelőzése és felderítése vagy ezekkel kapcsolatos büntetőeljárások céljára kell korlátozódnia, ezért fennáll a lehetősége a személyes adatok visszaélésszerű felhasználásának.

Megjegyzendő, hogy az irányelv érvénytelenné nyilvánítása nem érinti a nemzeti intézkedések érvényességét, így az Eht. szabályai továbbra is hatályban vannak, az EUB ítéletének tükrében azonban érdemes lenne felülvizsgálni a rendelkezéseket, hiszen azok a fenti okokból kifolyólag a magyar alkotmányossági követelményeknek sem felelnek meg. A TASZ jogvédő szervezet álláspontja szerint: *„a kérdés különös súlyát az adja, hogy a jelenlegi 9 millió 358 ezer mobiltelefon-előfizető, és a 3,3 millió vezetékes telefon-előfizető nagyjából lefedi a teljes magyar társadalmat. …Nem képzelhető el egy jogállamban olyan nemzetbiztonsági, bűnüldözési, bűnmegelőzési, honvédelmi vagy közrenddel kapcsolatos cél, amelynek megvalósításához gyakorlatilag a teljes lakosság kommunikációs és mozgási adatait évekre visszamenő tárolni szükséges."*[24] Az ítélettel összefüggésben az Eht. szabályain felül kritika érheti a Be. egyes rendelkezéseit is. A törvény ugyanis a 178/A. §-ában

[23] http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=HU&mode=req&dir=&occ=first&part=1&cid=526042

[24] http://tasz.hu/files/tasz/imce/TASZ_Eht_velemeny.pdf

úgy rendelkezik, hogy a nyomozó hatóság – többek között – a hírközlési szolgáltatást nyújtó szervezettől az ügyész jóváhagyása nélkül is igényelheti adatok szolgáltatását, amely nem tagadható meg. Ezzel a jogalkotó fontos alkotmányossági garanciát iktatott ki, hiszen éppen az ügyészi jóváhagyás lenne hivatott biztosítani, hogy a nyomozó hatóság csak indokolt esetben és meghatározott céllal élhessen az adatszerzés lehetőségével. A jelenlegi szabályok alapján azonban a nyomozó hatóságoknak lehetőségük van arra, hogy általános jelleggel, gyakorlatilag bármely ügy kapcsán beszerezzék a terhelt távközlési adatait, azokban az esetekben is, amikor az ügy jellege egyébként nem tenné indokolttá. Megjegyzendő, hogy a Be. ugyan rendelkezik arról, hogy az adatszolgáltatás iránti megkeresésre csak akkor kerülhet sor, ha az az ügy jellege miatt szükséges, azonban az ügyészi jóváhagyás „kiiktatása" miatt gyakorlatilag nincs, aki ellenőrizné, hogy a konkrét esetben valóban szükség van-e az adatokra, ennek eldöntése teljes mértékben az adott ügyben eljáró nyomozóhatóságtól függ. Aggodalomra adhat okot továbbá az is, hogy a Be. rendelkezései szerint *„a nyomozó hatóság a gyanúsítottról, a feljelentettről, illetőleg az elkövetéssel gyanúsítható személyről kérhet adatot, azaz utóbbi esetben olyan személyről is, akit még ugyan megalapozott gyanú nem terhel, de valamilyen oknál fogva, mint elkövető a hatóság látókörébe került."*[25]

Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról[26]

Fontos változás a 2005/222/IB kerethatározathoz képest, hogy az új irányelv különös figyelmet fordít az úgynevezett botnetekre és a személyazonossághoz kapcsolódó bűncselekményekre, valamint súlyosabb szankciókat helyez kilátásba abban az esetben, ha az informatikai bűncselekményt bűnszervezetben követik el. Ezen felül előírja, hogy a büntetőeljárás során figyelembe kell venni azt a körülményt, ha a bűncselekményt az elkövető alkalmazotti minőségben követi el.

Az irányelv által felvetett megoldások egy része egyelőre még nem tükröződik a magyar Büntető törvénykönyvben. A Btk. 423. és 424. §-aiban szabályozott információs rendszer vagy adat megsértése, illetve az információs rendszer védelmét biztosító technikai intézkedés kijátszása

[25] Be. Kommentár
[26] http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=HU

esetei, illetve a gyermekpornográfia nem minősülnek súlyosabban bűnszervezetben való elkövetés esetén. Az információs rendszer felhasználásával elkövetett csalás, készpénz-helyettesítő fizetési eszközzel visszaélés, készpénz-helyettesítő fizetési eszköz hamisításának elősegítése tényállások azonban igen. Nem szól a magyar Btk. azokról az esetekről sem, amikor az elkövető a cselekményt alkalmazotti minőségben követi el, egyedül a levéltitok megsértését minősíti súlyosabban a törvény azokban az esetekben, amelyekben az elkövető a bűncselekményt foglalkozás vagy közmegbízatás felhasználásával követi el.

Végig kell gondolnunk azt is, hogy a személyazonossághoz kapcsolódó bűncselekmények, például a személyazonosság-lopás hol helyezhetőek el a magyar büntető kódexben. A személyazonosság-lopás (*identity theft*) kétlépcsős folyamat. Első lépésként az elkövető eltulajdonítja a személyes adatokat (pl. személyi igazolvány számot, TAJ számot), majd következő lépésként ezek birtokában önmagát a sértettnek kiadva visszaélést követ el. A visszaélés több formában megjelenhet, például bűncselekmény elkövetése, egészségügyi, illetve egyéb szolgáltatások igénybe vétele stb. Véleményem szerint nem szükséges külön tényállást létrehozni az ilyen típusú bűncselekményekre, hiszen azok beilleszthetőek a már létező tényállások közé. Az első lépcső, azaz a személyes adatok megszerzése, többféle tényállás megvalósításával is megtörténhet. A tiltott adatszerzés egyik esete, amikor valaki *„személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti*". A Btk. Kommentárja szerint a kifürkészés *„olyan magatartás, amely a közlemény tartalmának az elektronikus hírközlő hálózat útján történő továbbítása során való megismerésére irányul. Ez gyakorlatilag bármilyen technológiával történő lehallgatást jelent."* Információs rendszerek tekintetében megvalósítható pl. billentyűzetleütés rögzítő programokkal (*keylogger*), vagy adathalász tevékenységgel (*phising*).

Az adat megszerzése után következik a második lépcsőfok, azaz annak visszaélésszerű felhasználása. A felhasználásra a személyes adattal visszaélés vétségének szabályai vonatkoznak. A Btk. 219.§-a így szól: *„Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel …*". Az adatkezelés fogalmát az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény a következőképpen határozza meg: *„az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így*

különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése." A fentiek alapján a személyazonosság-lopás minden esete tényállásszerű, hiszen vagy haszonszerzési célzattal követik el (pl. egészségügyi ellátások, egyéb szolgáltatások igénybe vétele), vagy oly módon, hogy az sértettnek jelentős érdeksérelmet okoz (pl. bűncselekmény elkövetése esetén a következmények viselése, jó hírnév, méltóság sérelme).

A személyazonosság-lopást el kell határolnunk az információs rendszer felhasználásával elkövetett csalástól, hiszen mindkét esetben haszonszerzési célzattal történik a cselekmény és mindkét esetben adatot kezelnek. Az elhatárolás egyik szempontja, hogy az információs rendszer felhasználásával elkövetett csalás esetében az elkövetés tárgya az információs rendszer, míg a személyes adattal való visszaélésnek nincs elkövetési tárgya. Személyazonosság-lopás esetében a felhasználás pillanatában az adat már kikerült az információs rendszerből, az elkövető tudomására jutott, az adattal való visszaélés pedig nem szükségszerűen valósul meg információs rendszer útján. További szempont, hogy az információs rendszer felhasználásával elkövetett bűncselekmény eredménybűncselekmény, ezért minden esetben kár keletkezik. Az információs rendszer felhasználásával elkövetett csalás bármely információs rendszerben tárolt adatra elkövethető, míg a személyes adattal visszaélés kizárólag személyes adatokra.

Europol – Európai Kiberbűnözési Központ (European Cybercrime Centre – EC3)

Az Európai Bizottság 2012. március 28-án „*Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása*" címmel közleményt fogadott el, amellyel életre hívta az Európai Kiberbűnözési Központot (European Cybercrime Centre – EC3). A központ 2013. január 11-én kezdte meg a működését. Ez a fókuszpontja az Európai Unió kiberbűnözés elleni küzdelmének, tevékenységével hozzájárul az online, határon átnyúló bűncselekményekre történő gyors reagáláshoz. A Központnak összesen 5 feladatköre van:

1. Adatfúzió: adatokat gyűjt a kiberbűnözésről és ezeket feldolgozza, kiberbűnözési helpdesket üzemeltet a tagállami nyomozó hatóságok számára.
2. Műveletek: támogatja a nyomozást minden EU tagállamban, támogatja a közös nyomozócsoportok létrehozását egy vagy több tagállam együttműködésével, megteremi az együttműködést az EU-n kívüli partnerekkel, valamint koordinálja a komplex nemzetközi ügyek nyomozását szoros együttműködésben az Eurojusttal és az Interpollal.
3. Stratégia: értékeli a kibertérből érkező fenyegetéseket, elemzi a trendeket és előrejelzi az új fejleményeket a kiberbűnözés alakulásában.
4. Kutatás-fejlesztés és képzés: szoros együttműködésben dolgozik a CEPOL-al, szervezi a nyomozó hatóságok tagjainak, a bíróknak, az ügyészeknek a képzését, forenzikus eszközök fejlesztésén dolgozik.
5. Kitekintés: együttműködik a privát szférával, a civil szférával, az egyetemekkel valamint a CERT-ekkel, annak érdekében, hogy képesek legyenek átfogóan észlelni a kiberbűncselekményeket és fellépni ezek ellen. Együttműködik olyan nemzetközi szervezetekkel, mint az EUCTF, CIRCAMP, ENISA és ECTEG.

A Központ szervezetén belül három fókuszpont működik, amelyek mindegyike a kiberbűnözés egy-egy nagy részterületére koncentrál:

1. *FP Cyborg* (Kiberbűncselekményekkel foglalkozó Fókuszpont): a Számítástechnikai bűnözésről szóló egyezményben nevesített, tisztán informatikai jellegű bűncselekmények nyomozásával foglalkozik, támogatja a tagállamokat a kiberbűncselekmények megelőzésében és annak különböző formái elleni küzdelemben.
2. *FP Twins* (Gyermekek szexuális kizsákmányolásával foglalkozó Fókuszpont): a gyermekek szexuális kizsákmányolása elleni fellépésre koncentrál. Célja az elkövetők azonosítása, valamint a résztvevő tagállamok közötti kapcsolatok kialakítása. További feladata a határokon átnyúló esetekben a modus operandi feltárása, valamint a bűnelkövetői hálózatok kommunikációs módszereinek elemzése azzal a céllal, hogy felbontsák őket. Ezen túlmenően az áldozatok azonosítására is koncentrál annak érdekében, hogy megállítsa a további kizsákmányolásukat és lehetővé tegye, hogy az érintett tagállami hatóságok megkezdjék az ellátását.
3. *FP Terminal*: támogatást nyújt az EU tagállamainak számos bankkártyás csalással kapcsolatos nyomozásban.

Európai Kiberbűnözés Elleni Akciócsoport (European Cyber Crime Task Force)

Az Európai Kiberbűnözés elleni akciócsoportot 2010-ben alakították. A szakértői csoport az Europol, az Eurojust és az Európai Bizottság

képviselőiből, valamint a tagállami kiberbűnözéssel foglalkozó egységek vezetőiből áll. A szakértői csoport hozzájárul az informatikai bűncselekmények elleni küzdelem harmonizált európai megközelítésének fejlesztéséhez és támogatásához, valamint célba veszi azokat a problémákat, amelyeket az információs technológia bűncselekményekhez való felhasználása okoz.

Európai Multidiszciplinárius Platform a bűnügyi fenyegetés ellen (European Multidisciplinary Platform against Criminal Threats)

Az EMPACT Program lényegében az Európai Unió égisze alatt, a nemzetközi szervezett bűnözés elleni hatékony fellépés érdekében kialakított feladatrendszer, amelynek keretében több különböző prioritást (például: informatikai bűncselekmények, emberkereskedelem, szintetikus drogok, illegális migráció, stb.) érintően végeznek közös munkát a kijelölt EMPACT nemzeti szakértők az EUROPOL segítségével. A kiberbűnözés prioritás keretében a cél a számítógépes bűnözés, valamint az internet bűnözési célú használata elleni harc. A prioritáson belül a bankkártyabűnözést, a kibertámadások és gyermekek online szexuális kizsákmányolása elleni küzdelmet fogják össze.

Európai Hálózat és Információbiztonsági Ügynökség (ENISA)

Az Európai Parlament és a Tanács 2004. március 10-i, az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendelete 2004-ben felállította az Európai Hálózat- és Információbiztonsági Ügynökséget azzal a céllal, hogy biztosítsa a magas szintű és hatékony hálózat- és információbiztonság megteremtését a Közösségen belül, valamint, hogy kifejlessze a hálózat- és információbiztonság kultúráját az európai unióbeli polgárok, fogyasztók, vállalkozások és a közszektor szervezetei érdekében, elősegítve ezáltal a belső piac zavartalan működését. Az ENISA az informatikai bűnözés témakörében több útmutatót tett közzé, például a kiberbűncselekmények hálózat és információbiztonsági aspektusairól[27], illetve az elektronikus bizonyítékok összegyűjtéséről[28].

[27] http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

[28] http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-

Konklúzió

Ha megszámoljuk, hány nemzetközi dokumentum foglalkozik az informatikai bűncselekményekkel, világosan látszik, hogy viszonylag új, ám felemelkedőben lévő területről beszélhetünk. Az Internet és az infokommunikáció világa a nemzetközi és az európai jogban is az érdeklődés fókuszába került. Megfigyelhető azonban az is, hogy egyelőre még egyfajta útkeresés folyik. Még nem alakultak ki igazán egységes fogalmak, és a bűncselekményi kategóriák is folyamatos változásban vannak. Nincs könnyű dolguk a jogalkotóknak ezen a területen, hiszen az a technikai környezet, amelynek a szabályrendszerét ki kellene alakítaniuk maga is folyamatos, állandó fejlődésben van, így könnyen az az érzésünk lehet, hogy a bűnelkövetők mindig egy lépéssel a jog előtt járnak. Példaként felhozható, hogy pár éve még hatalmas divatnak számított az illegális tartalmak *warezon* keresztül történő beszerzése, mára viszont a *torrent* technológia hódít. Pár éve pedig még azt sem gondoltuk volna, hogy a digitális pénz (*Bitcoin*), amely nem függ sem központi kibocsátóktól, sem a hatóságoktól a világ jó néhány országában teljesen legitim és elfogadott fizetőeszköz lesz. Mindezen nehézségek ellenére a nemzetközi szervezetek felvették a kesztyűt és a tagállamokkal közösen azon munkálkodnak, hogy megfelelő szabályrendszert teremtsenek, illetve összehangolják és segítsék a nyomozó hatóságok munkáját.

Felhasznált dokumentumok

Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról – http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=HU

Az Európai Unió kiberbiztonsági stratégiája

Az ENSZ Kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről http://www.uncjin.org/Documents/EighthCongress.html

---

guide-for-first-responders

Az ENSZ Közgyűlésének 55/63 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/63

Az ENSZ Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/56/121

Az Európai Unió Működéséről szóló szerződés - http://europa.eu/pol/pdf/consolidated-treaties_hu.pdf

Council of Europe. European Committee on Crime Problems: Computer-related Crime. Recommendation No. R (89) 9 on computer-related crime - http://www.oas.org/juridico/english/89-9&final%20Report.pdf

A Miniszteri Bizottság R (95) 13 számú ajánlása a büntetőeljárás információs technológiával kapcsolatos problémáiról http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről http://www.complex.hu/kzldat/t0400079.htm/t0400079_0.htm

A számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv - http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

A Tanács 2001/413/IB kerethatározata a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről - http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32001F0413&qid=1427790882359&from=EN

A Tanács 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról – http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32005F0222&qid=1427799018036&from=EN

Az Európai Parlament és a Tanács 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról – http://eur-lex.europa.eu/legal-

content/HU/TXT/PDF/?uri=CELEX:32006L0024&qid=1427876516458&from=EN

Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról – http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=HU

Felhasznált irodalom

A Büntetőeljárásról szóló törvény Kommentárja

BACSKÓ László: Bűnözés az Interneten; http://iroga.hu/internet&politika/bacsko.htm

SIEGLER Eszter: A számítógéppel kapcsolatos es a számítógépes bűncselekmények, Magyar Jog 1997/12

SZABÓ Imre: Az internet közvetítő szolgáltatóinak büntetőjogi felelősségéről, Doktori disszertáció http://www.cybercrime.hu/sites/default/files/Publikaltverzio_vegleges_0.pdf

***

Fight against cybercrime at international level

Summary

The aim of this study is to provide a comprehensive summary of all the international and regional cybercrime laws that have an impact on Hungarian legislation in some way. These cybercrime related laws usually contain both substantive and procedural elements. The paper identifies the most prominent international and regional organisations which deal with cybercrime: on international level the United Nations is engaged in cybercrime and cybersecurity issues, while on the regional level the most significant organisations are the Council of Europe and the bodies and agencies of the European Union. The study also intends to collect and describe those law enforcement agencies (mostly related to Interpol and Europol) that deal with the issues of investigating cybercrime and cooperating on an international field.