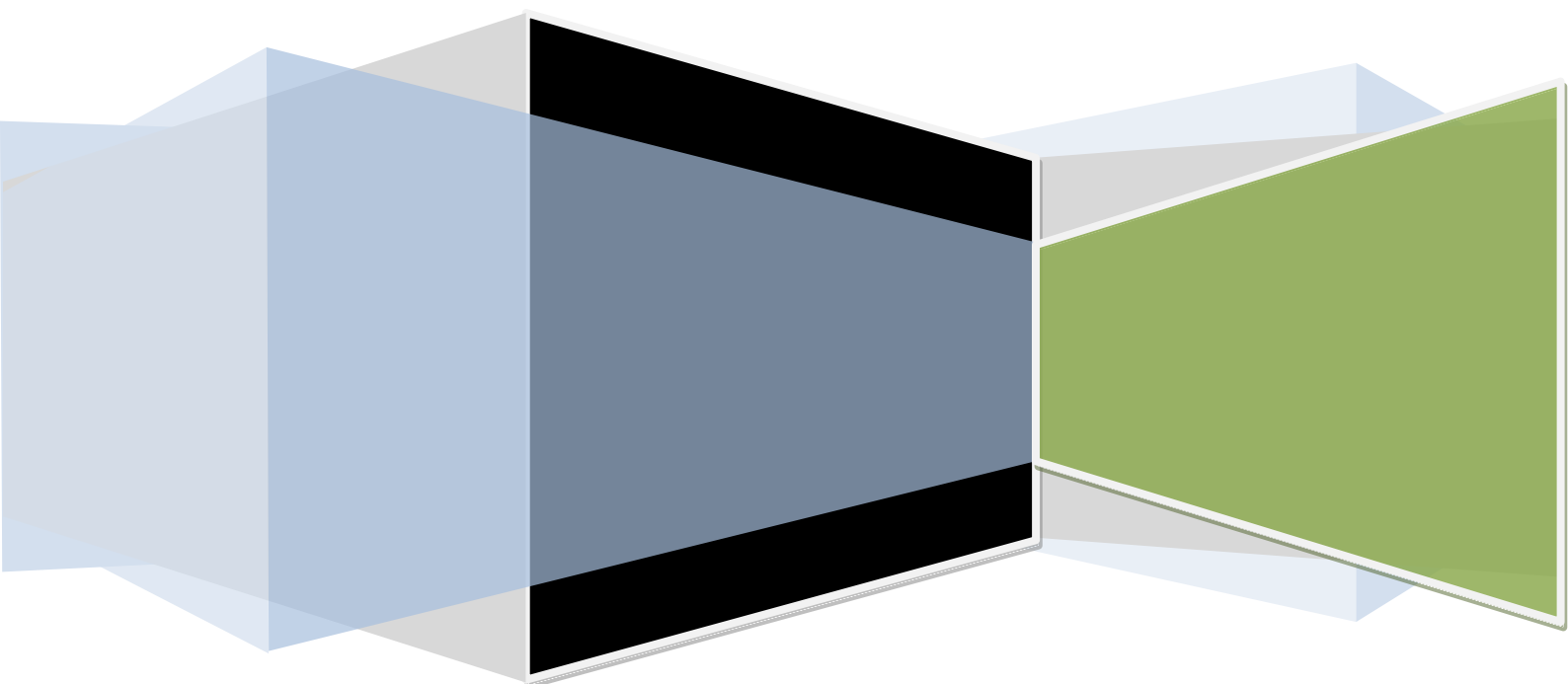


Jelige: Cersei

Bűnözés.Net

**internetes bűncselekmények Ausztriában és
Magyarországon**

OTDK dolgozat
2012.



Tartalomjegyzék

Tartalomjegyzék.....	2
„Szörfözz bátran, de vigyázz,.....	3
Bevezetés.....	3
Történeti áttekintés.....	4
Számítástechnikai Bűnözésről szóló Egyezmény	7
Jogtalan belépés.....	8
Jogtalan kifürkészés	9
Az adatok sértetlensége és a rendszer sértetlensége elleni cselekmények	10
Visszaélés eszközökkel	11
A számítástechnikai csalás	13
Internetes Bűncselekmények.....	15
Hacking	16
Spam.....	19
Phishing.....	22
Internetes bűncselekmények közösségi hálójában	29
Lehetne jobb is?	33
Forrásjegyzék	36

Bűnözés. Net

*„Szörfözz bátran, de vigyázz,
mert alattad cápák köröznek!”
(Szabó Imre)*

Bevezetés

Az utóbbi időkben egyre gyakrabban hallhatunk számítástechnikai bűncselekményekről, internetes bűnözésről. Ezek hallatán a legtöbbünknek a hackerek, az oldalak feltörése, jelszólopás jut eszünkben. A tapasztalat azonban az, hogy pontosan nem tudjuk mit is jelentenek ezek a fogalmak. Nem ismerjük pontosan a bűncselekmények jellemzőit, nem tudjuk hogyan is védekezhetnénk ellenük, és egyáltalán rendelkezésünkre állnak e hatékony védelmi eszközök.

Dolgozatomban az egyes bűncselekmények lényegi jellemzőinek feltárását követően azt vizsgáltam, hogy milyen törvényi lehetőségek állnak rendelkezésre a haza jogban az internetes bűncselekmények visszaszorítására, majd ennek fényében azt vizsgáltam, hogy az adott eszközök mennyire hatékonyak, szükségünk van e más eszközökre is, és ha igen milyen típusúakra.

A probléma átfogóbb kezelése és világosabbá tétele céljából a magyar szabályozás mellett egy szomszédos, alapvetően más mentalitású ország, Ausztria szabályozását és hatékonyságát is áttekintettem. Ezzel próbáltam rávilágítani arra, hogy a probléma forrása nálunk a törvényi szabályozásban, vagy egyéb, társadalmi tényezőkben keresendő.

Történeti áttekintés

Társadalmi létünket, életünket számos olyan tényező együttesen befolyásolja, mint például a tudomány, technika. Fejlődésük nagyban meghatározza mindennapjainkat. A technikai vívmányainak, így például a számítógépeknek, internetnek köszönhetően életünk sok szempontból kényelmesebbé, olykor gyorsabbá válik, olyannyira, hogy lassan már el sem tudjuk képzelni, mi lenne velünk internet nélkül, holott a története nem is olyan régi időkre nyúlik vissza.

Az Amerikai Védelmi minisztérium által életre hívott Fejlett Kutatási Program Ügynökség hozta létre 1969-ben az első nagyszámítógépes hálózatot, melyhez 1973-ban csatlakozott Európa, és még további 3 évet kellett várnunk az első elküldött e-mailre. 1982-ben amerikai mintára létrejött az első európai internet szolgáltatás, az EUNET. A hálózat egyre inkább az érdeklődés középpontjába került, melynek köszönhetően 1985-1986-ban két részre, az úgy nevezett MILNE T-re (katonai hálózat) és az internetre bomlott. 1991-ben a Nemzeti Kutatási Alapítvány engedélyt adott az internet kereskedelmi célú hasznosítására. Ennek következményeképpen az internet és így a számítógép is ma már számos háztartás kellékévé vált.¹

A számos jótékony hatás mellett azonban nem szabad megfeledkeznünk az internet árnyoldalairól sem, hiszen amellett, hogy számos hagyományos bűncselekmény megjelent cyber térben is, az internet teret engedett új bűncselekmények kialakulásának, elterjedésének. A számítógépes környezetben elkövetett első bűncselekmény 1959-re vezethető vissza, amikor is a Walston and Co. Alelnöke hamis lyukkártyák segítségével 250.000 USD-t sikkasztott.² A '60-as években a számítógépek tömeges elterjedése, az azokon megvalósított bűncselekmények számát is növelte, Megjelentek az úgy nevezett számítógépes vírusok, bár ekkor még egyértelműen katonai célt szolgáltak.³ A '70-es '80-as években az internet megjelenésével egy új korszak kezdődött, mind a gazdasági életben, mind a bűncselekmények körében. Az internet a bűnözés új színterévé vált. Megjelentek a számítógépes adatbázisok manipulálásával elkövetett bűncselekmények, a számítógépes hamisítások, a számítógépek biztonsági rendszerének feltörésével és a tárolt adatok jogtalan megszerzésével, illetve a szoftverek illegális másolásával megvalósított deliktumok. Mindezek mellett a büntetőjog sem mehetett el szó nélkül, hiszen már nem minden esetben megfelelő a hagyományos törvényi tényállások, például a csalás törvényi tényállásának alkalmazás ezekre a cselekményekre. Minthogy az erkölcsi szabályozás az úgynevezett Netikett már nem kellően hatékony, mind nemzetközi szinten, mind hazai szinten lépéseket tettek a törvényalkotás terén az új típusú bűncselekmények visszaszorításáért. Ulrich Sieber, a müncheni egyetem professzora az internettel kapcsolatos büntető jogalkotás kialakulásában 3 nagy reformhullámot különít el.⁴ A '70-es években a szabályozás elsősorban a személyiségi jogokhoz kapcsolódott. A második nagy szabályozási hullám a '80-as évek elején kezdődött, amikortól egyre súlyosabb problémát jelentettek a számítógépes környezetben elkövetett gazdasági bűncselekmények. A '80-as évek végén, '90-es évek elején születtek meg az első olyan szabályok, melyek célja az internetes pornográfiai visszaszorítása. Nagy előre lépést jelentett a szabályozás terén 1989-ben az Európai Tanács (89) számú ajánlása a Számítógépes

¹ NAGY Zoltán András: *Bűncselekmények számítógépes környezetben*. Budapest, AD Librum Kiadó, 2009. 11.

² SZENTKÚTI Dániel, SZÜTS Márton: *Az internet és a büntetőjogi felelősség egyes kérdései* <http://jesz.ajk.elte.hu/szentkuti15.html> (letöltve 2012-11-04).

³ *A vírusok története* <http://goo.gl/9osq2> (letöltve 2012-11-04).

⁴ Johannes BEER: *Die Convention on Cybercrime und österreichisches Strafrecht*. Trauner, 2005. 81-82.

Bűnözés. Net

környezetben elkövetett bűncselekményekről. Az ajánlás egy minimum listát és egy fakultatív listát tartalmaz a számítógépes környezetben megvalósítható bűncselekményekről.

Kiemelendő továbbá az osztrák Schmölzer-Schlich szerzőpáros munkája, akik a releváns elkövetési magatartásokat három alrendszerbe csoportosították: támadás hardver ellen, támadás szoftver ellen, támadás adat ellen.⁵

1992-ben az információs biztonság területén került kibocsátásra irányelv, majd 1995-ben az adatvédelemre vonatkozóan.⁶

1999-ben tárgyalások kezdődtek a Számítástechnikai Egyezmény megalkotásának szükségességéről. 2000-ben sor került az adatvédelmi szabályok bővítésére, majd 2001-ben létrehozták a Számítástechnikai Bűnözésről szóló Egyezményt.⁷ 2002-ben a Tanács egy ajánlást készített az információs rendszerek elleni támadásokra vonatkozólag, 2003-ban pedig létrejött a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló kerethatározat.⁸

A nemzetközi jogalkotással összhangban az egyes államok is, így Ausztria és Magyarország is létrehozták a számítástechnikai rendszerekkel, internettel kapcsolatos bűncselekményekre vonatkozó rendelkezéseiket. Az osztrák jogalkotó először 1978-ban az Adatvédelmi törvény⁹ Keretein belül rendeli büntetni a személyes adatok feldolgozását végző rendszerbe történő jogosulatlan belépést. A büntetőtörvénykönyvbe először az 1987-es Büntetőnovellával¹⁰ vezetnek be számítógépekkel kapcsolatos büntetendő cselekményeket. Új büntető tényállásként megalkotásra került a büntetőtörvénykönyv¹¹ 126/a §-a az adatok sérelmével kapcsolatosan és a számítógépes csalásra vonatkozó 148/a §. 1994-ben megalkották a kiskorúak pornográf ábrázolásának tényállását.¹² A '90-es években nemzetközi és európai mintára az internethez kötődő gazdasági tárgyú jogalkotásba kezdenek. Létrejön az új Adatvédelmi törvény,¹³ a hozzáférési jogosultságról szóló törvény,¹⁴ megalkotják az Elektronikus Kereskedelemről szóló törvényt,¹⁵ és az elektronikus aláírással kapcsolatos törvényt.¹⁶ A 2002-es büntetőnovellával¹⁷ a Számítástechnikai Bűnözésről szóló Egyezmény (továbbiakban Egyezmény) hatására számos új törvényi tényállás megalkotásra kerül sor.¹⁸ A 2003-as Szerzői jogokról szóló törvénnyel kapcsolatos novella ülteti át az Információs Irányelvet¹⁹ az osztrák jogba.

Az azóta eltelt időszakban számos további újítás következett be az osztrák büntetőjog területén. Így például a gyermekpornográfiával kapcsolatos 207. §-ban meghatározott

⁵ SZABÓ Imre: *Internetes bűncselekmények*. 2003. 5. <http://www.ajk.elte.hu/file/SzaboImre-InternetesBuncselekmenyek.pdf>(letöltve 2012-11-04).

⁶ Johannes BEER i.m. 90.

⁷ Johannes BEER i. m. 90.

⁸ Johannes BEER i. m. 93.

⁹ BGBl 1978/565.

¹⁰ BGBl 1987/605.

¹¹ Johannes BEER i. m. 80.

¹² BGBl 1994/622.

¹³ BGBl 1999/165.

¹⁴ Zugangskontrollgesetz, BGBl I 2000/60.

¹⁵ E. Commerce-Gesetz, BGBl I 2001/152.

¹⁶ BGBl 1999/190.

¹⁷ BGBl I 2002/134.

¹⁸ Johannes BEER i.m. 81.

¹⁹ Johannes BEER i. m. 81

Bűnözés. Net

tényállást kiterjesztették minden kiskorúra; bevezetésre került a készpénz-helyettesítő fizetési eszközökkel való visszaélés.

Ausztriával ellentétben nálunk csak később, 1994-ben került sor az első, számítástechnikai rendszerekkel kapcsolatos cselekmények büntetendővé nyilvánítására. A számítógépes csalásról szóló 300/C § a gazdálkodás rendjét sértő bűncselekmények között kapott helyet a magyar büntetőtörvénykönyvben.²⁰

Az első módosításra 1996-ban került sor az 1996. évi LII törvénnyel. A különböző hagyományos mobil és rádiótelefonok útján igénybe vehető szolgáltatásokkal való visszaélések miatt vált szükségessé a 300/C § (3) bekezdése.

Az 1999. évi CXX. Törvény megalkotta a 300/C (2) c. pontját.

Jelentősebb változást a magyar jogi szabályozásban a 2001. november 23-án, Budapesten elfogadott Számítástechnikai Bűnözésről szóló Egyezmény hozott, mely a 2004. évi LXXIX törvénnyel került kihirdetésre.

A magyar szabályozás kapcsán kiemelendő továbbá az Elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. Törvény (továbbiakban Ekt.), melynek különösen a kéretlen elektronikus levelek, *spamek* visszaszorítása kapcsán van jelentősége.

²⁰ SZABÓ Imre i. m. 6-7.

Számítástechnikai Bűnözésről szóló Egyezmény

Tekintettel arra, hogy mind az osztrák mind hazai számítástechnikai rendszerekkel kapcsolatos jogi szabályozás terén meghatározó szerepet tölt be a 2001. november 23-án, Budapesten aláírt Számítástechnikai Bűnözésről szóló Egyezmény, célszerűnek tartom az egyes bűncselekmények áttekintése előtt az Egyezmény vonatkozó rendelkezéseit, és annak a tagállami jogszabályokra vonatkozó hatását megvizsgálni.

Az Egyezmény anyagi jogi és eljárásjogi követelményeket is megfogalmaz a részes tagállamok számára.

Az anyagi jogra vonatkozó részben három kategóriába rendezi a releváns bűncselekményeket. Az első kategóriába a számítástechnikai rendszer és a számítástechnikai adatok hozzáférhető, sértetlensége és titkossága elleni bűncselekmények tartoznak. Ezen bűncselekmények közé tartozik a jogtalan belépés, jogtalan kifürkészés, az adatok sértetlensége elleni cselekmény, a rendszer sértetlensége elleni cselekmény, az eszközökkel való visszaélés.

A második kategóriába a számítástechnikai bűncselekmények tartoznak, melyek között említendő a számítástechnikai hamisítás és a számítástechnikai csalás.

A harmadik kategóriát pedig a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények képezik, mely alatt a gyermekpornográfiával kapcsolatos bűncselekményeket kell értenünk.

Az egyezménynek Ausztria és Magyarország is részesei, mely államok eleget téve ebből eredő kötelezettségeiknek az Egyezmény követelményeivel összhangban álló rendelkezéseket vezettek be hazai joganyagukba.

Magyarországon az Egyezmény előírásaival összhangban került módosításra a Büntetőtörvénykönyv²¹ ma is hatályos 300/C §- a Számítástechnikai rendszer és adatok elleni bűncselekményekről és a 300/E §- a Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszásáról.

Ausztriában a Büntetőtörvénykönyv²² 118/a§; 119/a§; 126/a§; 126/b§; 126/c§; 148/a tartalmazza az egyezmény követelményeinek megfelelő rendelkezéseket.

²¹ 1978. évi IV. törvény a Büntető Törvénykönyvről.

²² Bundesgesetz vom 23. Jänner 1974. über die mit gerichtlicher Strafe bedrohten Handlungen.

Jogtalan belépés

Mind az osztrák mind a magyar jogalkotó az Egyezmény meghatározásával²³ összhangban álló definíciót állapít meg a számítástechnikai rendszer vonatkozásában. Az osztrák értelmezés szerint számítástechnikai rendszernek minősülnek azon önálló vagy egymással összekötött berendezések, melyek az automatikus adatfeldolgozást szolgálják.

Ehhez hasonlóan határozza meg a magyar jogalkotó is a Büntetőtörvénykönyv 300/F §-ában a számítástechnikai rendszer fogalmát, mely alatt az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége értendő.

Míg az osztrák jogalkotó az Egyezmény rendelkezésével és rendszerével összhangban több különálló szakaszban határozza meg a számítástechnikai rendszerekkel kapcsolatos bűncselekmények alapeseteit, a magyar jogalkotó a 300/C §-ában a releváns cselekmények három alapesetét állapítja meg.

Az Egyezmény 2. cikkében²⁴ szabályozott jogtalan belépéssel kapcsolatban felmerülő jogalkotási kötelezettségének az osztrák jogalkotó a 118/a §-ban²⁵ míg a magyar jogalkotó a 300/C (1)²⁶ bekezdésében tesz eleget. A törvényhelyet a hacking törvényi tényállásának tartják.

Alapvető követelmény a számítástechnikai rendszerbe vagy annak egy részébe történő jogosulatlan belépés büntetendővé nyilvánítása. A tényállás megvalósításához további feltételként kiköthető, hogy az alapcselekményt a biztonsági intézkedések megsértésével; bűnös szándékkal; másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

Az osztrák büntetőtörvénykönyv 118/a §-a tartalmazza a jogtalan belépésre vonatkozó rendelkezéseket. A büntethetőség alapvető feltételeként a bűnös szándék meglétét és a

²³E. 1. cikk: számítástechnikai rendszer" minden olyan önálló eszköz, illetőleg egymással kapcsolatban lévő vagy összekötött eszközök összessége, melyek illetőleg melyeknek egy vagy több eleme program végrehajtásával adatok automatikus feldolgozását biztosítja.

²⁴E. 2. cikk: Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön a számítástechnikai rendszerbe vagy egy részébe történő jogosulatlan és szándékos belépés. A Fél kikötheti, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy a számítástechnikai adatok megszerzésére irányuló, illetőleg más bűnös szándékkal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

²⁵StGB 118/a: Aki abból a célból, hogy a rendszerben tárolt adatokat megismerje, illetéktelen tudomására hozza; azokat felhasználja, nyilvánosságra hozza, vagy azokhoz harmadik személy részére hozzáférést biztosítson, az adatok ilyen módon való felhasználása révén magát vagy harmadik személyt vagyoni előnyhöz juttasson, másnak vagyoni hátrányt okozzon a számítástechnikai rendszert védő speciális intézkedés kijátszásával a számítástechnikai rendszerhez jogosulatlanul biztosít hozzáférést.

²⁶Btk. 300/C (1): Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel büntetendő.

Bűnözés. Net

biztonsági intézkedések kijátszását határozzák meg, azonban a releváns cselekmények körének szűkítése véget, a cselekmény céljának meghatározásával kibővítik a tényállást.

A magyar jogalkotó a jogtalan belépést a 300/C § (1) bekezdésében szabályozza és a büntethetőség megállapításához az osztrákhhoz képest kevesebb feltételt állapít meg, és célzatot sem tartalmaz a tényállás.

Fontos, hogy mindkét részes állam hangsúlyt fektet arra, hogy a cselekményt a biztonsági intézkedés kijátszásával kövessék el. Ennek a biztonsági intézkedésnek közvetlenül kell védenie a rendszert a jogosulatlan hozzáférésektől, ilyen lehet egy tűzfal, vagy egyéb biztonsági program.

Lényegi különbség, hogy míg az osztráknál csak hozzáférést biztosít a tettes azért, hogy a célját megvalósítsa, a magyarban jogosulatlanul belép, vagy jogosultságának kereteit túllépve marad bent.

A BTK 300/C § (1) bekezdése egyenes és eshetőleges szándékkal is megvalósítható. Ehhez hasonlóan az osztrákok is elegendőnek tartják a dolus eventualist a tettesi oldalon.

Mindkét esetben megvalósítható a bűncselekmény kísérlete.

Lényegi eltérés, hogy míg nálunk közvédas bűncselekményről van szó, a jogtalan belépés az osztrák büntetőjogban magánindítványos cselekmény, viszont a felelősségre vonásnál elegendő a sértett utólagos indítványa, hozzájárulása is.

Jogtalan kifürkészés

Az Egyezmény 3. cikkében²⁷ foglalt jogtalan kifürkészés esetében eltérő szabályozási módot alkalmaz a két részes állam.

A lényegi különbség a két állam között az, hogy míg az előzőhöz hasonlóan Ausztria egy külön tényállás megalkotásával, nevezetesen a 119/a §-ában²⁸ tesz eleget jogalkotási kötelezettségének, a Btk. nem tartalmaz ide vonatkozó elkülönült tényállást. Ez azonban nem jelenti azt, hogy a jogtalan kifürkészés nem lenne büntetendő cselekmény. Ennek bizonyításához abból kell kiindulnunk, hogy a számítástechnikai rendszer tágabb értelmezésében megállapítható, hogy számítástechnikai rendszernek minősülnek az egyes berendezések összekapcsolása révén létrejött hálózatok, valamint adattovábbítást, kapcsolatfelvételt biztosító műszaki berendezések is. Egyes berendezések összekapcsolásán nem feltétlenül fizikai kapcsolatot kell érteni. „Összekapcsolásnak számít az elektronikus vagy optikai jeleket továbbító kábelek, vagy vezetékek útján történő összekapcsolódás, a rádióhullám, infravörös illetve rövidhullám segítségével vagy műholdas sugárzás igénybevételével létrejött kapcsolódás is.”²⁹ Ennek alapján megállapítható, hogy az internet is

²⁷ E. 3. cikk: Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön a számítástechnikai rendszeren belüli, a számítástechnikai rendszerből származó vagy a számítástechnikai rendszerbe irányuló számítástechnikai adatoknak nem nyilvános továbbítása során technikai eszközök felhasználásával történő jogosulatlan és szándékos kifürkészése, ideértve az ilyen számítástechnikai adatokat továbbító, a számítástechnikai rendszerből származó elektromágneses sugárzást. A Fél kikötheti, hogy a bűncselekményt bűnös szándékkal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

²⁸ StgB 119/a: Aki abból a célból, hogy egy számítástechnikai rendszerbe továbbított adatokat megismerje, illetéktelen tudomására hozza; azokat felhasználja, nyilvánosságra hozza, vagy azokhoz harmadik személy részére hozzáférést biztosítson, az adatok ilyen módon való felhasználása révén magát vagy harmadik személyt vagyoni előnyhöz juttasson, másnak vagyoni hátrányt okozzon a számítástechnikai rendszert a hozzá kapcsolt berendezésen segítségével, a rendszer elektromágneses sugarainak felfogásával vagy más egyéb módon kifürkészi bűncselekményt követ el.

²⁹ SZABÓ Imre i. m. 8.

Bűnözés. Net

számítástechnikai rendszernek minősül, vagyis alkalmazhatjuk rá a Btk. számítástechnikai rendszert érintő rendelkezéseit.

További lényeges körülmény, hogy a Btk. 178. §-ának³⁰ kommentárja alapján megállapítható, hogy az internet távközlési berendezésnek minősül. Így az Egyezmény 3. cikkében foglalt jogtalan kifürkészés a levéltitok megsértése kapcsán válik büntetendővé.³¹

Az adatok sértetlensége és a rendszer sértetlensége elleni cselekmények

A magyar jogalkotó az Egyezmény 4.³² és 5.³³ cikkével összhangban alkotta meg a Btk. 300/C § (2)³⁴ bekezdését, mely az első bekezdést mintegy kiegészítve már nem csak a jogosulatlan belépést illetve a jogosultság kereteinek túllépését, hanem az ott tárolt, feldolgozott, kezelt vagy továbbított adat jogosulatlan megváltoztatását, törlését vagy hozzáférhetetlenné tételét, valamint a számítástechnikai rendszer működésének jogosulatlan akadályozását is büntetni rendeli.

Az osztrák büntetőtörvénykönyv a magyartól eltérően két külön szakaszban a 126/a §-ban³⁵ és a 126/b §-ban³⁶ tesz eleget az adatok és rendszer sértetlensége elleni cselekmények büntetendővé nyilvánítására vonatkozó kötelezettségének.

A két részes állam egymáshoz hasonlóan az adatok megváltoztatását, törlését, hozzáférhetetlenné tételét bünteti, viszont eltérés jelentkezik abban, hogy az osztráknál mindezek megvalósítása csupán egy közvetett eredményt valósít meg. Az osztrákoknál a

³⁰ Btk. 178. §: (1) Aki másnak közlést tartalmazó zárt küldeményét, a tartalmának megismerése végett felbontja, megszerzi, vagy ilyen célból illetéktelen személynek átadja, úgyszintén aki távközlési berendezés útján továbbított közleményt kifürkész, ha súlyosabb bűncselekmény nem valósul meg, vétséget követ el, és pénzbüntetéssel büntetendő.

(2) A büntetés egy évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekményt foglalkozás vagy közmegegyezés felhasználásával követik el.

(3) A büntetés

a) két évig terjedő szabadságvesztés, ha az (1) bekezdésben meghatározott bűncselekmény,

b) büntett miatt három évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős érdeksérelmet okoz.

³¹ Szabó Imre i. m. 8.

³² E. 4. cikk: Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön a számítástechnikai adatok jogosulatlan és szándékos megkárosítása, törlése, megromlása, megváltoztatása vagy megsemmisítése. A Fél fenntarthatja magának azt a jogot, hogy kiköti, hogy az 1. bekezdésben meghatározott cselekmény eredményeként jelentős kár következzen be.

³³ E. 5. cikk: Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön a számítástechnikai rendszer működésének számítástechnikai adatok bevitelével, továbbításával, megkárosításával, törlésével, megromlásával, megváltoztatásával vagy megsemmisítésével való, jogosulatlan és szándékos, jelentős akadályozása.

³⁴ Btk. 300/C § (2): Aki

a) számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl, vagy hozzáférhetetlenné tesz,

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.

³⁵ StGB 126/a §: Aki másnak azáltal okoz kárt, hogy automatikusan feldolgozott, továbbított, átadott adatokat, mellekkel nem vagy nem kizárólag rendelkezik, megváltoztat, töröl, vagy egyébként használhatatlanná tesz vagy megsemmisít hat hónapig terjedő szabadságvesztéssel vagy pénzbírsággal sújtandó.

³⁶ StGB 126/b §: Aki a számítástechnikai rendszer működőképességét jogosulatlanul súlyosan megzavarja azáltal, hogy adatokat bevisz, továbbít és a cselekménye nem a 126a szakasz alapján minősül bűncselekmény miatt 6 hónapig terjedő szabadságvesztéssel vagy pénzbírsággal sújtandó.

Bűnözés. Net

bűncselekmény eredménye, hogy másik személynél kár, mégpedig vagyoni kár következzen be. Az osztrák jogalkotó a vagyoni kár, mint eredmény miatt egy minősített esetet is megfogalmaz a 126/b § -ban.

A fogalmakat azonos módon értelmezik, és az adatok sértetlensége elleni cselekményeknél mindkettő hangsúlyt fektet a jogosulatlanságra.

A rendszer sértetlensége elleni cselekményeknél a fentiekhez képest plusz elkövetési magatartásként jelenik meg mindkettőben az adat bevitele illetve továbbítása is.

A Btk. 300/C § (2) b) pontjában meghatározott tényállás az engedély kereteit megvalósítva is elkövethető, vagyis nem kell, hogy jogosulatlanul történjen a belépés, de a megváltoztatásnak jogosulatlannak kell lennie. Az osztrák jogalkotó azonban ilyenre nem ad lehetőséget.

Mindkét állam meghatározza a cselekmény eredményét is, vagyis a rendszer működésének akadályozását.

Fontos, hogy mindkét állam célja a tényállás megvalósításával, hogy a rendszer egészének védelmét biztosítsa, és ne csak az egyes adatokat.

A cselekmények egyenes és eshetőleges szándékkal is megvalósíthatók.

Fontos kiemelni, hogy az osztrák büntető törvénykönyv 126/c §-ban meghatározott bűncselekmény szubszidiárius jellegű. Csak abban az esetben minősül a 126/c § alapján a cselekmény, ha az nem valósítja meg az adatok sértetlenségének védelméről szóló 126/a §-t.

A szóhasználat kapcsán kiemelendő, a magyar jogalkotó által használt akadályozás és az osztrák jogalkotó által használt súlyos zavarás kifejezés. A Btk. értelmében az akadályozás azt jelenti, hogy a rendszer egyáltalán nem, vagy nem rendeltetésszerűen működik. Az osztrákok által használt zavarás szóból azonban még csak a nem rendeltetésszerű működés következne, amely azonban a *spamming*-tilalom tényállását is megvalósítja, mely szabálysértésnek minősül, és a közigazgatás területére tartozik. A két esetkör elhatárolása végezt vezet be a jogalkotó a súlyos jelzőt. Az osztrák büntető törvénykönyv kommentárja szerint a zavarásnak olyan mértékben súlyosnak kell lenni a tényállás megvalósításához, hogy az majdnem egyenértékű legyen a rendszer teljes megbénulásával.³⁷ További követelmény, hogy fennálljon az ok-okozati összefüggés a súlyos zavarás és a rendszer működésének zavarása között.

Fontos megjegyezni, hogy mind a magyar mind az osztrák jogalkotó e tényállásokban tesz eleget az Egyezmény 7. cikkében³⁸ foglalt számítástechnikai hamisítás büntetendővé nyilvánítására vonatkozó kötelezettségének.

Visszaélés eszközökkel

Az osztrák jogalkotó a 126/c §-ban³⁹ az Egyezmény 6. cikkével⁴⁰ összhangban a büntethetőség alapfeltételeként határozza meg a bűnös szándék fenn álltát a program, az ehhez hasonló berendezés, hozzáférési adat létrehozásakor.

³⁷ Johannes BEER i. m. 187-188.

³⁸ E. 7. cikk: Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön a számítástechnikai adatoknak olyan, jogosulatlan és szándékos bevitele, megváltoztatása, törlése vagy megsemmisítése, melynek eredményeként nem valódi adatok jönnek létre, és melynek az a célja, hogy úgy lehessen azokat figyelembe venni vagy jogszerű célra felhasználni, mintha valódi adatok lennének, függetlenül attól a tényről, hogy az adatok közvetlenül olvashatók vagy érthetők. A Fél a belső jogában kikötheti, hogy csalárd szándék vagy hasonló tartalmú bűnös szándék fennállása alapozza, meg a büntetőjogi felelősséget.

³⁹ StGB 126/c § (1): Aki

Bűnözés. Net

Kiemelendő, hogy nem minden számítástechnikai program valósítja meg a tényállást, csak azok, melyeket bűnös szándékkal hoztak létre, és melyről valószínűsíthető, hogy azt a fent meghatározott bűncselekmények valamelyikének elkövetéséhez fogják felhasználni. Ilyenek elsősorban a crackprogramok és Sniffer-szoftver⁴¹. A valószínűsíthető kifejezéshez hozzá kell tenni, hogy annál egy átlagos technikai, informatikai tudással rendelkező ember tudása, valószínűsítése mértékadó.

A tényállás a program létrehozását említi, ez alatt azonban nem csak a program újonnan történő létrehozását kell érteni, hanem egy már meglévő program megfelelő átvételét is.

A magyar Btk. 300/E §-hoz⁴² hasonlóan az osztrák büntető törvénykönyv is lényegében egy előkészületi cselekményt sui generis bűncselekményként rendel büntetni.

1) olyan számítástechnikai programot, melynek jellege alapján valószínűsíthető, hogy azt számítástechnikain rendszerbe történő jogellenes hozzáférés, telekommunikációs titok megsértése, adatok jogellenes kifürkészése, adatok sértése, egy számítástechnikai rendszer működőképességének zavarása vagy csalárd adatfeldolgozás céljából került létrehozásra vagy adaptálásra, illetve ezzel hasonló berendezést vagy

2) számítástechnikai jelszót, hozzáférési kódot vagy ezekhez hasonló adatot, melyek a számítástechnikai rendszerhez vagy annak egy részéhez való hozzáférést teszik lehetővé;

Azzal a szándékkal létrehoz, bevezet, forgalomba hoz, elidegenít, hozzáférhetővé tesz, megszerez, birtokol, hogy az első pontban meghatározott bűncselekmények elkövetéséhez felhasználja, 6 hónapig terjedő szabadságvesztéssel vagy pénzbírsággal büntetendő.

(2). Az első bekezdés alapján nem büntethető, aki önként megakadályozza, hogy az első bekezdésben meghatározott számítógépes program vagy az ahhoz hasonló berendezés, jelszó, hozzáférési kód, vagy ahhoz hasonló adat a 118/a §, 119 §, 119/a §, 126/a §, 126/b §, vagy 148/a §-ban meghatározott cselekmények elkövetéséhez felhasználják.

Nem büntethető a tettes akkor sem, ha nem áll fenn az ilyen felhasználás veszélye, vagy a közreműködése nélkül is megszűnik a veszély, vagy az erre vonatkozó ismeretek hiányában a tettes önkéntesen és komolyan törekszik a vélt veszély elhárítására.

40 E. 6. cikk: 1. Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön az alábbi cselekmények jogosulatlan és szándékos elkövetése:

a) az előállítása, az értékesítése, a felhasználás céljából való megszerzése, az ország területére való behozatala, a forgalomba hozatala vagy a más módon történő hozzáférhetővé tétele:

i elsődlegesen a 2-5. Cikkben meghatározott valamely bűncselekmény elkövetése érdekében létrehozott vagy átalakított eszköznek, ideértve a számítástechnikai programot;

ii egy jelszónak, egy belépési kódnak, illetőleg a számítástechnikai rendszerbe vagy egy részébe való belépést hasonlóan lehetővé tevő számítástechnikai adatnak,

Azzal a szándékkal, hogy azt a 2-5. Cikkben foglalt valamely bűncselekmény elkövetésére használják fel; valamint

a fenti a) pont i és ii alpontjában meghatározott dolgoknak a 2-5. Cikkben foglalt valamelyik bűncselekmény elkövetésére való felhasználása érdekében történő birtoklása. A Fél a belső jogában kikötheti, hogy a büntetőjogi felelősséget meghatározott számú dolog birtoklása alapozza meg.

2. Jelen Cikkben foglaltak nem alapozzák, meg a büntetőjogi felelősséget abban az esetben, ha a jelen Cikk 1. bekezdésében foglalt előállításnak, értékesítésnek, felhasználás céljából való megszerzésnek, az ország területére való behozatalnak, forgalomba hozatalnak vagy más módon történő hozzáférhetővé tételnek nem célja a jelen Egyezmény 2-5. Cikkében meghatározott bűncselekmény elkövetése, mint például az engedélyezett kísérlet vagy valamely számítástechnikai rendszer védelme.

3. A Fél fenntarthatja magának azt a jogot, hogy részben vagy egészben nem alkalmazza a jelen Cikk 1. bekezdését, feltéve, hogy a fenntartás nem a jelen Cikk 1. bekezdése a) pontjának ii alpontjában meghatározott értékesítésre, forgalomba hozatalra vagy más módon történő hozzáférhetővé tételre vonatkozik.

⁴¹ Snifferek- tolvajok a hálózaton. <http://goo.gl/dA6cZ>.

⁴² Btk. 300/E §: Aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot

a) készít,

b) megszerez,

c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.

Bűnözés. Net

Fontos azonban, hogy a büntethetőséget nem befolyásolja annak ténye, hogy ezeket a programokat, adatokat ténylegesen fel is használják a cselekmény elkövetéséhez, hiszen a létrehozással már befejezetté válik a cselekmény.

Lényeges, hogy az osztrák jogalkotó a magyar jogalkotótól eltérően az adatok bevitelét és birtoklását is az elkövetési magatartások között említi, az elkövetési tárgyakat viszont egyformán határozza meg a két részes állam.

Míg az osztrák jogalkotó elegendőnek tartja az eshetőleges szándék fennállását a tettesi oldalon, a magyar jogalkotó egyenes szándékot követel meg

Lényegi eltérés, hogy az eszközökkel való visszaélés kapcsán az osztrák jogalkotó egy, míg a magyar 2 alapesetet határoz meg. A Btk. 300/E § (2) bekezdése értelmében az is megvalósítja a törvényi tényállást, aki az elkövetéshez szükséges tudását, ismereteit bocsátja más rendelkezésére.

Ebből következik az is, hogy szűkül a tettesek köre, hiszen a korábbiakkal ellentétben csak a speciális ismeretek birtokában lévő valósíthatja meg a 2. bekezdésben meghatározott bűncselekményt.

Kiemelendő, hogy mindkét állam jogalkotója rendelkezik büntethetőség megszüntető esetekről, melynek feltételei eltérőek. Ezzel kapcsolatban az osztrák büntetőtörvénykönyv két esetet is említ, nevezetesen, nem lesz büntethető a bűncselekmény tettese, ha önként megakadályozza azt, hogy a létrehozott eszközöket az említett bűncselekmények elkövetéséhez felhasználják. Ezen túl azonban, akkor sem lesz büntethető a tettes, ha ugyan a bűncselekmény elkövetésének veszélye nem állt fenn, vagy az az ő közreműködése nélkül elhárult, azonban az erről való tudásának hiányában aktívan törekszik arra, hogy az eszközöket ne használhassák fel a cselekmények megvalósításához.

A magyar jogalkotó ettől eltérő feltételeket határoz meg. Nem lesz büntethető, aki a 300/E § (3) bekezdésében meghatározott feltételeknek eleget tesz. Vagyis, aki - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adat készítése a hatóság tudomására jutott volna, tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

A számítástechnikai csalás

A tagállami jogalkotóknak az Egyezmény számítástechnikai csalásra vonatkozó 8. cikke⁴³ szolgált alapként.

(2) Az (1) bekezdés szerint büntetendő, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő, számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja.

(3) Nem büntethető az (1) bekezdés a) pontja esetén, aki - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adat készítése a hatóság tudomására jutott volna tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását

⁴³ E. 8. cikk: Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön a másnak jogosulatlanul és szándékosan történő vagyoni károkozás, amelyet

Bűnözés. Net

A tényállás létrehozásával a magyar jogalkotó elsősorban a gazdasági érdek védelmét tartotta szem előtt. A törvényhely gazdasági jelentőségét alátámasztja, hogy a cselekmény abban az esetben válik büntethetővé, ha annak következtében vagyoni kár áll be.

A Btk. 300/C § (3)⁴⁴ bekezdésében meghatározott bűncselekmény célja a jogtalan haszonszerzés. Ehhez kötődően azt is ki kell emelni, hogy a bűncselekményt az is megvalósíthatja, aki ugyan jogosult a cselekmények végrehajtására, de azokat adott esetben a jogtalan haszonszerzés miatt valósítja meg. Ebből következik az is, hogy a cselekmény csak egyenes szándékkal valósítható meg, de a kárral kapcsolatosan elegendő az eshetőleges szándék is.

Az osztrák jogalkotó a tényállás megalkotásakor abból indult ki, hogy valójában a vonatkozó szabály már 2002-ben létezett, ami összhangban is volt a konvencióval, de annak elkövetési magatartásokra vonatkozó rendelkezései miatt a már meglévő osztrák tényállást bővíteni kellett, nevezetesen a hozzáférhetetlenné tétel szófordulat törvénybe foglalásával.⁴⁵

A magyarhoz képest az osztrák büntetőtörvénykönyvben egy pluszként jelenik meg a program megváltoztatásával történő befolyásolás.

Az elkövetési magatartásra vonatkozó szóhasználatban eltérés mutatkozik, hiszen a 148/a §⁴⁶a rendszer befolyásolását írja el, míg a Btk. 300/C § (3) bekezdése a rendszer működésének akadályozását. A befolyásolás, mint köztes eredmény jelenik meg; egy feltétel, mellyel ok-okozati összefüggésben kell állnia a bekövetkezett vagyoni kárnak.

Minkét részes állam a vagyoni kár mértékéhez igazodó minősített esetet határoz meg, és követelmény, hogy a szándék kiterjedjen a minősített esetben meghatározott értékekre is, mely tovább erősíti a cselekménynek a gazdasági élet védelme érdekében szükséges büntetendővé nyilvánítását.

a) számítástechnikai adatok bevitelével, megváltoztatásával, törlésével vagy megsemmisítésével;

b) számítástechnikai rendszer működése elleni bármilyen más cselekménnyel, anyagi haszon saját vagy más részére történő jogosulatlan megszerzése szándékával követnek el.

⁴⁴ Btk. 300/C § (3): Aki jogtalan haszonszerzés végett

a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl, vagy hozzáférhetetlenné tesz, vagy

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza,

és ezzel kárt okoz, büntetett követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(4) A (3) bekezdésben meghatározott bűncselekmény büntetése

a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,

b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,

c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz.

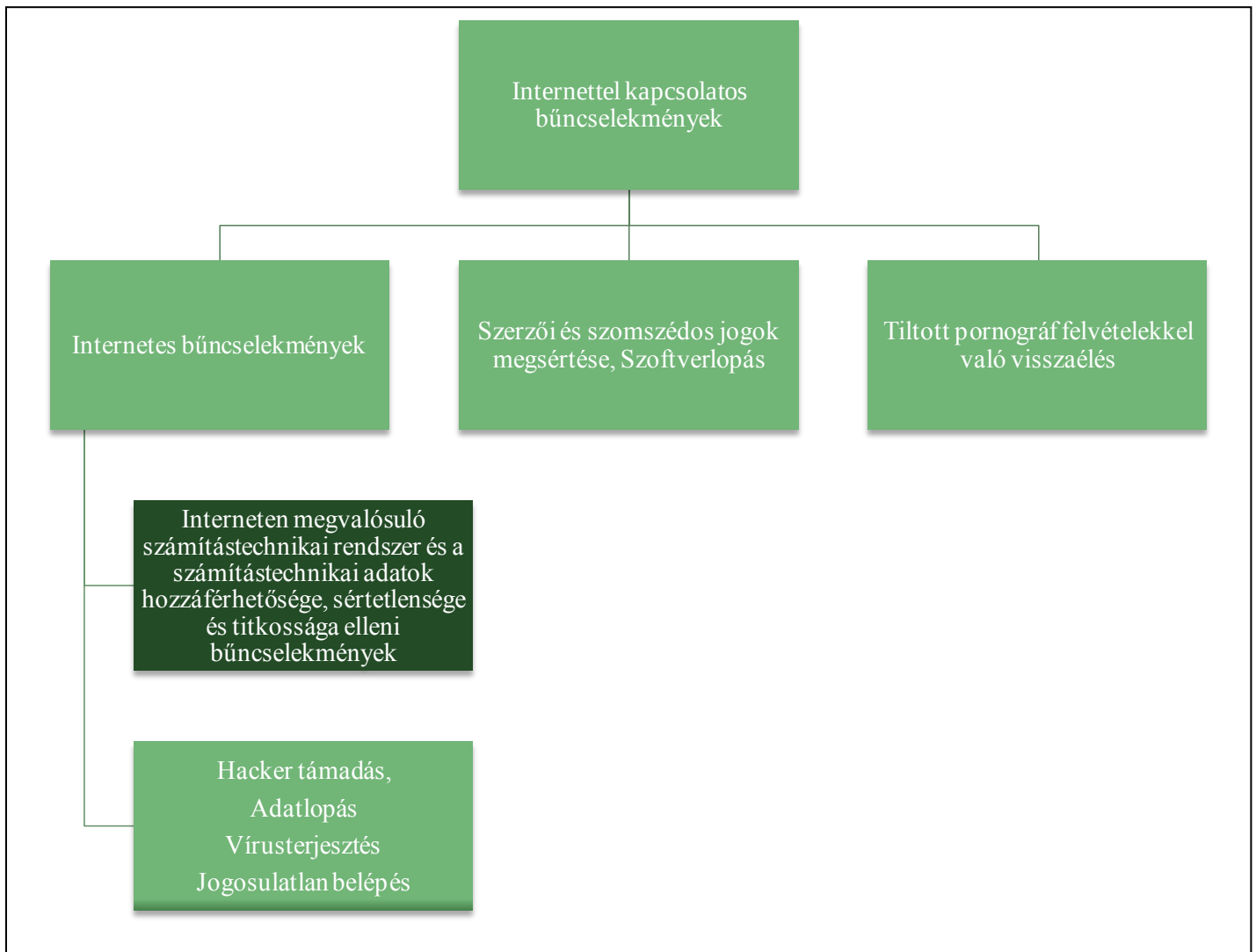
⁴⁵ Johannes BEER i. m. 193.

⁴⁶ StGB 148/a: Aki azzal a szándékkal, hogy egy harmadik személyt jogellenesen vagyoni előnyhöz juttasson, másnak vagyoni kárt okoz azáltal, hogy egy automatikus adatfeldolgozás eredményét a program módosításával, adatok hozzáadásával, módosításával, törlésével, megsemmisítésével vagy egyébként a feldolgozási folyamatba való beavatkozással befolyásolja 6 hónapig terjedő szabadságvesztéssel vagy pénzbírsággal sújtandó. Aki a cselekményt üzletszerűen követi el, vagy a cselekménye 3000 eurót meghaladó kárt okoz 3 évig terjedő szabadságvesztéssel sújtandó, ha a cselekmény folytán az okozott kár az 50000 eurót meghaladja 1-10 évig terjedő szabadságvesztéssel büntetendő.

Internetes Bűncselekmények

A törvényi szabályozás nemzetközi háttere, mint fentebb láttuk adott. Ahhoz azonban, hogy ezeket a szabályokat és magát a számítástechnikai, különösen internetese bűncselekmények problematikáját megértsük szükséges áttekintenünk az egyes bűncselekmények jellegzetességeit.

Ehhez szükséges az internetes bűncselekmények más bűncselekményekhez viszonyított „helyét” meghatároznunk.



Dolgozatom témája kifejezetten az internetes bűncselekményekre korlátozódik, ezen belül is három, véleményem szerint meghatározó jelentőségű bűncselekménnyel, a *hackinggel*, *spammel* és a *phishinggel* foglalkozok. Mindhárom bűncselekmény jellemzője, hogy az Egyezmény 1. kategóriájába, a számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetetlensége, sértetlensége és titkossága elleni bűncselekmények kategóriájába tartozik

Hacking

Az első büntetőjogilag értékelhető cselekmények számítógépes környezetben jóval a számítógépek és az internet tömeges elterjedése előtt, a '40-es években jelentek meg. Ezeket a cselekményeket *phreaking*nek nevezzük, mely lényegében az elektronikus *hacking* első megnyilvánulási formája.⁴⁷

Kezdetben minden számítógép használat hackernek tekintettek, aki átlagon felüli ismeretekkel rendelkezett az informatika világában, és képes volt akár órákon keresztül a gép előtt ülni, hogy valamilyen súlyos hardver, vagy szoftver hibára megoldást találjon.

Azóta a fogalom köszönhetően a nyilvánosságnak és a médiának jelentősen beszűkült és elsősorban azokat jelöli, akik rebellis, gyakran illegális módon tevékenykednek a számítógépes környezetben. Sőt manapság már nem is nagyon használható úgy a *hacker* megjelölés, hogy abból ne következtenénk valamiféle illegális tevékenységre, holott az ilyen tevékenységet folytatókat valójában nem is *hacker*nek, hanem *cracker*nek hívják.

Alapvetően a *hacking* csak a számítástechnikai rendszerekbe, hálózatokba történő jogosulatlan bejutást jelenti. A sikeres bejutást követően megvalósított cselekmények nem tartoznak a *hacking* fogalmi körébe. A *hacking* pusztán eszköz cselekményként értékelhető.

A hacker nem kívánja megváltoztatni, megsemmisíteni a rendelkezésére álló adatokat, célja pusztán egy bonyolult védelmi rendszer kijátszása. Számos ismert *hacker* elmondása szerint, az ő céljuk nem egy bűncselekmény elkövetése, pusztán dicsőség szerzés, és az, hogy felhívják a többi *hacker* figyelmét a tudásukra. Koránt sem minden *hacker* „rossz” *hacker*. Éppen ezért célszerű két kategória kialakítása. Az egyik kategóriába tartoznak a *black-hat* *hackerek*, akik tudásukat bűncselekmény elkövetéséhez használják fel, és nagyon gyakran „megbízás” alapján járnak el. Erre jó példa a *spammerek* tevékenysége, akik nagyon gyakran *hackereket* bíznak meg a címzettek e-mail címének megszerzésével. A másik kategóriába a *white-hat* *hackerek* tartoznak. Az ő cselekményeik során hiányzik a bűnös szándék. Céljuk elsősorban az, hogy a rendszer feltörésével rávilágítsanak a biztonsági rendszer hibáira és később megoldást találjanak rá.⁴⁸ Pontosan ezért a *white-hat* *hackerek* nagy része informatikai cégek alkalmazásában áll, és a programok, biztonsági eszközök fejlesztésénél játszanak közre. A fogalom torzulását jelzi az is, hogy az összes számítástechnikai körben bűncselekményt elkövetőt hajlamosak vagyunk *hacker*nek titulálni, míg azokat, akik tevékenységükkel egy-egy hibára kívánják felhívni a figyelmet már biztonságtechnikai szakértőként kezeljük, holott ők is *hackerek*.

A *hacker* célja tehát a rendszerhez való hozzáférés biztosítása, ennek ellenére nagyon gyakran használják a *Crasher*,⁴⁹ *Cracker*⁵⁰ és *Phreaker*⁵¹ fogalmakat a *hacker* szinonimájaként. A *chrasher* a rendszerbe történő bejutást követően a rendszert károsító változtatásokat hajt végre. A *Cracker* célja a bejutáson túl a teljes védelmi rendszer kiiktatása, míg a *Phreaker* tevékenysége a telefonos hálózatokhoz kapcsolódik, és célja a jogosulatlan lehallgatás vagy akár más költségére történő telefonhasználat.⁵²

⁴⁷ Johannes BEER i. m. 39.

⁴⁸ *Hackerek*. <http://goo.gl/jFuH4>(letöltve 2012-11-04).

⁴⁹ Johannes BEER i. m. 39.

⁵⁰ *Hacker, Cracker, Script Kiddies*. <http://goo.gl/0115U>(letöltve 2012-11-04).

⁵¹ *Phreaker Sticker*. <http://goo.gl/y08d6>(letöltve 2012-11-04).

⁵² Nagy Zoltán András i. m. 68.

Bűnözés. Net

Tekintettel arra, hogy a *hacking* tulajdonképpen a legtöbb interneten elkövethető bűncselekmény eszköz cselekménye, kiemelten fontos az azzal szembeni nemzetközi és nemzeti fellépés.

A Számítástechnikai Egyezmény 2. cikke⁵³ a *hacking* elleni fellépéssel kapcsolatos alapvetők követelményeket fogalmaz meg a tagállamok jogalkotásai számára.

Az osztrák jogirodalom a büntetőtörvénykönyv 118/a §-t⁵⁴ tekinti a *hacking* törvényi tényállásának, míg nálunk ezt lényegében a Btk. 300/C § -a⁵⁵ és a 300/E §-a⁵⁶ testesíti meg.

⁵³ E. 2. cikk: Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménynek minősüljön a számítástechnikai rendszerbe vagy egy részébe történő jogosulatlan és szándékos belépés. A Fél kikötheti, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy a számítástechnikai adatok megszerzésére irányuló, illetőleg más bűnös szándékkal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el.

⁵⁴ StgB. 118/a §: Aki abból a célból, hogy a rendszerben tárolt adatokat megismerje, illetéktelen tudomására hozza; azokat felhasználja, nyilvánosságra hozza, vagy azokhoz harmadik személy részére hozzáférést biztosítson, az adatok ilyen módon való felhasználása révén magát vagy harmadik személyt vagyoni előnyhöz juttasson, másnak vagyoni hátrányt okozzon a számítástechnikai rendszert védő speciális intézkedés kijátszásával a számítástechnikai rendszerhez jogosulatlanul biztosít hozzáférést.

⁵⁵ Btk. 300/C §: (1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl, vagy hozzáférhetetlenné tesz,

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő

(3) Aki jogtalan hasznoszerzés végett

a) a számítástechnikai rendszerbe adatot bevisz, az abban tárolt, feldolgozott, kezelt vagy továbbított adatot megváltoztat, töröl, vagy hozzáférhetetlenné tesz, vagy

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését akadályozza,

és ezzel kárt okoz, büntetést követ el, és három évig terjedő szabadságvesztéssel büntetendő.

(4) A (3) bekezdésben meghatározott bűncselekmény büntetése

a) egy évtől öt évig terjedő szabadságvesztés, ha a bűncselekmény jelentős kárt okoz,

b) két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekmény különösen nagy kárt okoz,

c) öt évtől tíz évig terjedő szabadságvesztés, ha a bűncselekmény különösen jelentős kárt okoz.

⁵⁶ Btk. 300/E §: Aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot

a) készít,

b) megszerez,

c) forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz, vétséget követ el, és két évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a 300/C. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő, számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja.

(3) Nem büntethető az (1) bekezdés a) pontja esetén, aki - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adat készítése a hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

Bűnözés. Net

A korábban már leírtaknak megfelelően mindkét állam vonatkozó rendelkezései a számítástechnikai rendszerbe vagy annak egy részébe történő jogosulatlan belépés, vagyis a *hacking* ellen kívánnak fellépni. Ennek megfelelően fontos a *hackerkedés* mint tevékenység jellemzőinek számba vétel és törvényi tényállásba foglalása. A *hacker* tevékenysége mindig olyan rendszer ellen irányul, amelyhez nincs belépési jogosultsága, ezért fontos a törvényi tényállásokban a jogosulatlanság kihangsúlyozása. A fent kifejtetteknek megfelelően a *hacker* tevékenysége mindig valamilyen biztonsági intézkedés kijátszására irányul. Ehhez a cselekményhez kötődő szándék az, mely meghatározza, hogy a cselekmény bűncselekménynek minősül-e és ezért fel kell ellene lépni, vagy nem bűncselekmény, hanem kifejezetten elfogadott tevékenység és ezért támogatni kell. Ennek megfelelően az osztrák jogalkotó kihangsúlyozza, hogy az elkövető a számítástechnikai rendszer védelmét bűnös szándékkal sérti meg, míg a magyar törvény szövegéből erre következtetni lehet.

Kiemelendő, hogy a *hacker* célja mindig egy biztonsági intézkedés kijátszása, ezért mindkét államban a bűncselekménynek csak szándékos alakzata van. Abból kifolyólag, hogy mint azt már fent említettem, a *hacker* az esetek többségében nem egy konkrét gépet akar feltörni, hanem feltör egy gépet és csak utána nézi meg, hogy hová is sikerült bejutnia, a bűncselekmény eshetőleges szándékkal is megvalósítható. Abból adódóan, hogy nem biztos, hogy a *hackernek* ténylegesen sikerül bejutni a rendszerbe, mindkét államban megvalósítható a bűncselekmény kísérlete is.

Fontos kiemelni azonban azt a lényegi eltérést, hogy míg az osztrák jogalkotó csak a rendszerhez való hozzáférés biztosítását említi, a magyar jogalkotó a rendszerhez való hozzáféréshez szükséges ismeretek átadását, valamint a rendszerben való jogosulatlan bennmaradást is e körben rendeli büntetni.

Kiemelendő, hogy a magyar jogalkotó a *hackerkedés* kapcsán több elkövetési magatartást határoz meg. Így például büntetni rendeli az adatok megváltoztatását, törlését. A különbség elsősorban felfogásbeli különbségeken alapszik. Itt kell megemlítenünk a *hackereket* érintő fogalmi elmosódásokat, bizonytalanságokat. Az egyik álláspont szerint hacker az, aki pusztán a rendszerhez való hozzáférést biztosítja, de magát a számítástechnikai rendszert nem kívánja megváltoztatni. Ettől élesen el kell határolni a *crackert*, akinek célja a rendszer adatainak megváltoztatása, viszont a *cracker* csak programokat ír/ átír, de a rendszerbe való bejutás alapvetően nem az ő feladata, hanem a *hackeré*. Sokan a bűnös szándékú, úgynevezett *black-hat hackereket* *crackernek* tekintik, míg a *white-hat hackereket* *hackernek*. Egy másik felfogás azonban nem tesz különbséget *hacker* és *cracker* között, azokat mintegy szinonimaként használja.⁵⁷ Ezek alapján azt mondható, hogy a magyar szabályozás annak a felfogásnak felel meg, mely nem tesz különbséget a két fogalom között, így lényegében egy törvényi tényálláson belül rendeli őket büntetni. Ezzel szemben az osztrák felfogás a *hackereket* és *crackereket* külön választó elgondolást látszik támogatni.

Összességében elmondható, hogy a szigorú törvényi szabályok pusztán a károsító cselekmények ellen irányulnak, de soha nem fogják megszüntetni a *hackerkedés* jelenségét. Adataink továbbra sincsenek biztonságban az illetéktelen behatolásokkal szemben, de azt is be kell látni, hogy nem is szabadna teljes egészében kiiktatni a *hackerkedés* jelenségét, hiszen biztonsági rendszereink hatékonyságát pontosan nekik köszönhetjük és csak így, hatékony eszközökkel van lehetőségünk védekezni a többi internetes bűnelkövetővel szemben.

⁵⁷ *Hackerkedés, crackerkedés*. <http://goo.gl/ItcjC> (letöltve 2012-11-04).

Spam

Az interneten elkövethető bűncselekmények között kiemelkedő szerepet játszik a *spam*, hiszen a statisztikák szerint az elküldött e-mailek 95 % át a levélszemetek, az úgy nevezett *spamek* teszik ki.⁵⁸ A *spam* jelensége igen korán kialakult, az elsőt 1978-ban továbbították Amerikában. Bár eredetileg pusztán időtakarékosági igények álltak a háttérben, mégis óriási felkavarodást keltett azok között, akik az internet nyíltságának korlátai mellett érveltek.⁵⁹

Tekintettel arra, hogy a '70-es, '80-as években elsősorban tudományos célból, főleg egyetemek és akadémikusok használták az internetet, a '80-as években eltűnni látszott a jelenség. A számítógépek és vele együtt az internet tömeges elterjedése a háztartásokban, azonban teret nyitott a mai értelemben vett spam elterjedésének és 2003-ban már naponta legalább 2 milliárd kéretlen levelet küldtek szét a világban.

Az eredetileg ártalmatlannak gondolt levéllánc időközben globális problémává nőtte ki magát. A nagy mennyiségű levélszemét nem csak elárasztja a postaládáinkat, de lassítja az internetet is, nem beszélve arról, hogy ilyenkor lényegében olyan személy használja az e-mail címünket, akinek azt nem bocsátottuk rendelkezésére. Problémát jelentenek a napi szinten milliójával továbbított szexuális tartalmú üzenetek és a spamellenes programok beszerzése és telepítése idő- és költségigényes. Túl azon, hogy számos gondot okoznak a kéretlen levelek az egyes felhasználóknak, a *spameknek* komoly gazdasági kihatásuk is.⁶⁰ A Yellowcube tanulmánya szerint egy 100 fős vállalatnál, ahol minden dolgozó postafiókjába napi 40 spam érkezik, csak a spam miatti munkaidő-kiesés havonta 600 000 forint kárt okoz, éves szinten pedig 8-10 millió forint veszteséggel lehet számolni.

Az okozott károkra tekintettel egyre fontosabbá válik a hatékony szabályozás bevezetése mind nemzetközi, mind nemzeti szinten. 2000-től kezdődően megjelentek az első Európai Közösségi irányelvek melyek közvetve, vagy közvetlenül a *spamek* visszaszorítását célozták. Az európai szintű szabályozás kapcsán kiemelendő az Elektronikus Kereskedelemről szóló Irányelv, valamint a 2002-es Adatvédelmi Irányelv, és a Számítástechnikai Egyezmény 5 cikke is tartalmaz ide vonatkozó rendelkezéseket.

A probléma felismerésének hatására és az európai szintű szabályok, irányelvek megjelenésének köszönhetően az egyes államok is elkezdtek kiépíteni saját szabályozás rendszerüket. 2000 óta Dániában, 2001. óta Magyarországon, 2003. óta pedig az Egyesült Királyságban és Ausztriában is tilos a *spam*.⁶¹

A nemzetközi fellépések hatására mind Magyarországon, mind Ausztriában megszülettek az első olyan szabályok, melyek kifejezetten a kéretlen levelek ellen irányulnak.

Magyarországon 2001-ben hozták a kéretlen elektronikus levelek visszaszorítását is lehetővé tevő 2001. évi CVIII. törvényt (Ektv.).⁶² A törvény 2005-ös módosítása során jött létre a ma is hatályos szöveg, mely alapjaiban megtartotta az eredeti szöveget, és elsősorban szóhasználati valamint a *spam*-re vonatkozó különös szabályokat kiegészítő változásokat vezetett be.

⁵⁸ 95% of email is spam. <http://goo.gl/MALfQ> (letöltve 2012-11-04).

⁵⁹ Michael SPECTER: *Damn spam- The losing war on junk e-mail*. <http://goo.gl/qL9gW> (letöltve 2012-11-04).

⁶⁰ Spam károk és megoldások: http://yellowcube.hu/wp-content/uploads/2007/01/bodis_akos.ppt.

⁶¹ SÜTŐ János: *Spamtelenül*. Budapest, SZAK Kiadó, 2008. 15-23.

⁶² 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

Bűnözés. Net

Ausztriában a reklám célú, illetve tömegesen továbbított elektronikus levelekkel kapcsolatos szabályokat 1997-ben megalkotott Távközlési törvény, az úgy nevezett *Telekommunikationsgesetz*⁶³ tartalmazta. A törvény 2002-es módosításával jött létre a ma is hatályos szabályozás, mely a korábbival ellentétben kifejezetten *spam*-tilalmi törvények tekinthető.⁶⁴

Annak kapcsán, hogy a törvények pontosan mikre terjednek ki, a hatályosság címszó alatt felsoroltakon túlmenően segítséget nyújtanak a fogalom meghatározások is. Az osztrák jogalkotó a *spam* alatt olyan kereskedelmi küldeményt ért, mely nem csak kereskedelmi célú lehet, de megjeleníthet politikai, társadalmi célú reklámokat is.⁶⁵ Ezzel szemben a magyar jogszabály a reklámokról általánosságban beszél, így vitatott, hogy a külön törvényben szabályozott társadalmi célú és politikai reklámokra kiterjed-e az Ektv. hatálya.

A két állam szabálynak alapvető adatvédelmi célja azonos, vagyis a védelem nem csak a személyes adatokra, hanem minden további adatra is kiterjed.

Fontos azonban, hogy míg az osztrák jogalkotó egy kifejezett *spam*-tilalmi törvényt hozott létre, addig a magyar törvény az Ektv. általános szabályai mellett különös szabályokat állapít meg a kéretlen elektronikus hirdetésekre.⁶⁶

Mindkét törvény az európai szabályozással összhangban úgy nevezett *opt-in*⁶⁷ rendszert vezetett be a hazai szabályozásba. A rendszer lényege, hogy főszabályként csak akkor küldhető elektronikus levél a felhasználónak, ha az előzetesen egyértelműen hozzájárult ahhoz. Azok a küldemények azonban, melyeket a címzett előzetes hozzájárulás nélkül továbbítottak, *spam*nek minősülnek és a cselekmény büntethetővé válik. Az osztrák jogalkotó viszont egy egyértelmű kivételt is meghatároz az előzetes engedély meglétének kötelezettsége alól. Nem kell előzetes engedély, ha a címzett adataihoz a küldő a korábban általa értékesített termék vagy szolgáltatás kapcsán jutott hozzá, és a küldeményében a már értékesítetthez hasonló saját terméket kíván népszerűsíteni.

Eltérések mutatkoznak a két törvény szóhasználatában, hiszen az osztrák TkG. 107. § (2), (3) bekezdése az elektronikus küldemény –mely lehet szöveges, képi vagy hang üzenet-kifejezést használja, míg a 107. § (5) bekezdése a magyarhoz hasonlóan a jóval szűkebb körű elektronikus hirdetéseket említi.

Mindkét törvény megköveteli, hogy a küldő elérhetősége valami módon megismerhető legyen a címzett számára azért, hogy felvehesse vele a kapcsolatot, ha a továbbiakban nem szeretne elektronikus hirdetést kapni. Ezzel összefüggésben az osztrák jogalkotó elegendőnek tartja, ha a küldő egy valós elérhetőségi címet ad meg, a magyar törvény viszont jóval részletesebben állapítja meg a feladó által közlendő valós adatokat.

Az osztrák törvény megsértése esetére nem tartalmaz különös eljárási szabályokat, az Ektv. azonban előírja, hogy az elektronikus hirdetésre vonatkozó különös szabályok megsértése esetén főszabály szerint kérelemre a Nemzeti Média- és Hírközlési Hatóságnál indul eljárás.

Abban az esetben, ha a feladó megsérti a törvényi rendelkezéseket az osztrák jogszabályok értelmében szabálysértést követ, ellene közigazgatási per indítható és akár 37 000 eurónyi pénzbírsággal is sújtható.

⁶³ Telekommunikationsgesetz 2003.

⁶⁴ TkG. 107 §: tilos elektronikus levelet vagy sms-t küldeni a fogyasztóknak előzetes hozzájárulásuk nélkül, ha az elektronikus levél célja direkt marketing, vagy ha több mint 50 címre küldték el. Nem szükséges az előzetes hozzájárulás, ha a küldő fél a címzett adataihoz egy termék vagy szolgáltatás kapcsán jutott hozzá, és azt egy hasonló termék vagy szolgáltatás marketingjének céljára használják, és a fogyasztó könnyen és ingyenesen lemondhatja a reklámot. Továbbá senkinek sem szabad olyan levelet küldeni, mely elrejtí a feladó valódi azonosságát, vagy amelyik nem tartalmaz egy érvényes címet, amelyre a címzett el tudja küldeni leiratkozási kérelmét. A 109§ értelmében a törvényt sértőkre akár 37 ezer euró összegű bírság is kiszabható.

⁶⁵ Johannes BEER i. m. 157.

⁶⁶ Ektv. 14. §

⁶⁷ Dietmar JAHNEL: *Informatikrecht*. Springer, 2002. 13-131.

Bűnözés. Net

A magyar jogban azonban az Ektv. megsértőjének cselekménye gyakran a büntető törvénykönyv rendelkezéseibe ütközik és ilyenkor ellene büntető eljárás indul, más esetekben az okozott károk megtérítése iránt polgári per is indítható.

Mindkét állam *spam* elleni fellépése kapcsán a törvényi szabályozás mintegy kiegészítéséként meg kell említenünk, az úgy nevezett *Robinson listát*.⁶⁸

Az említett opt-in rendszerek mellett – csak a címzett előzetes engedélye alapján küldhető elektronikus hirdetés- létezik egy úgy nevezett opt-out rendszer is.⁶⁹ A rendszer lényege, hogy a címzettnek lehetősége van arra, hogy kifejezetten kérje, hogy számára ne továbbítsanak elektronikus hirdetést. A rendszer gyengesége, hogy ilyenkor bár a feladó értesül arról, hogy a továbbiakban adott címre ne küldjön hirdetést, viszont ezzel párhuzamosan tudomására jut az is, hogy az adott e-mail cím aktív, azt biztosan látogatják, és a később haszonszerzés céljából ezt a címet eladhatja más *spammereknek*.

A probléma kiküszöbölésére tesz kísérletet az Elektronikus Kereskedelmi Irányelv⁷⁰, mely opt-out lista, úgy nevezett Robinson lista létrehozást irányozza elő. A lista lényegében egy nemzeti, de központi alapon működő lista, melyre minden olyan személy bejegyeztetheti magát, aki a jövőben nem kíván elektronikus küldeményt kapni.

Ahhoz, hogy a lista „céljai” megvalósuljanak, fontos, hogy a *spamek* kiszűrhetők legyenek, melyek csak az egyedi azonosításuk mellett lehetséges. Az azonosíthatóságot vagy magának a tartalomnak (tárgymegjelölés által) vagy a küldemény technikai adatainak kell biztosítani.

Ausztriában az E-commerce Gesetz⁷¹ alapján a Rundfunk- und Telekom-Regulierungs GmbH-nak kötelessége egy olyan lista vezetése, melyre az olyan személyek és vállaltok díjmentesen bejegyeztethetik magukat, akik az elektronikus küldemény útján megvalósuló kereskedelmi kommunikáció lehetőségével nem kívánnak élni.

A Magyarországon hatályos törvények (1995. évi CXIX törvény) szerint minden direkt marketinggel foglalkozó vállalkozás kell, hogy ilyen listát vezessen a *spam* elleni fellépés hatékonyabbá tétele érdekében.

Összességében elmondható, hogy mind nemzetközi mind nemzeti szinten megtették az első lépéseket a *spamek* és az ezek okozta károk visszaszorítása, elkerülése érdekében. Mindaddig azonban, amíg az egyes felhasználókban nem tudatosul a *spam* visszaszorításának igénye, amíg a kéretlen levelek jó része eléri a célját, hiába a törvényi szabályozás. Amíg a *spam* a leghatékonyabb és egyben legolcsóbb eszköz a direkt marketing terén, a számuk csak növekedni fog.

⁶⁸ Robinson lista. <http://goo.gl/wKP6C> (letöltve: 2012-11-04).

⁶⁹ Interjú Dr Mayer Erikával az elektronikus kereskedelemről szóló törvényjavaslattal kapcsolatban. <http://goo.gl/aBEm3> (letöltve: 2012-11-04).

⁷⁰ Elektronikus Kereskedelmi Irányelv <http://goo.gl/Ty7Cu> (letöltve: 2012-11-04).

⁷¹ E-commerce Gesetz. BGBl I 2001/152.

Phishing

Hasonlóan az eddig tárgyalt internetes bűncselekményekhez, a *phishing*, vagy más néven adathalászat az egyike azon bűncselekményeknek, melyek leginkább veszélyeztetik az internetezők adatainak biztonságát.

A *phishing* elnevezés többek szerint a *password harvesting fishing*⁷² kifejezésből alakult ki, és elsősorban jelszavaink megszerzésére irányuló tevékenység volt. A probléma azonban mára már jóval kiterjedtebbé vált, hiszen az elkövetők célja már nem csak belépési azonosítók, jelszavak megszerzése, hanem lényegében minden személyes adat az érdeklődési körük tárgyát képezi.

Egyre gyakrabban hallunk arról, hogy nagy tekintélyű cégek, bankok küldenek értesítést, hogy adjuk meg személyes adatainkat, belépési azonosítónkat, vagy a személyes adatok biztonságának megerősítése végett változtassuk meg őket. Az esetek túlnyomó többségében aztán kiderül, hogy a feladó alapján hitelesnek vélt értesítés, valójában mégsem annyira a mi adatink biztonságát kívánja elősegíteni. Az ilyen, többségében e-mail formájában érkező értesítés célja ugyanis pontosan az adataink csalárd módon történő megszerzése, vagyis a *phishing*, még pedig oly módon, hogy lényegében önként adjuk át féltve őrzött jelszavainkat. A módszer pedig nem is olyan bonyolult, elegendő például egy megbízható bank honlapjával látszólag majdnem teljesen azonos oldalt létrehozni, majd innen értesítést küldeni a felhasználónak, hogy az új banki szolgáltatás igénybevételhez az adott oldalon regisztrálnia kell. Az óvatlan felhasználó bízva az oldal hitelességében nyomban eleget is tesz a kérésének, és tálcán kínálja személyes adatait az adathalász csalárd módon felépített weboldalán.

Az adathalászat lényege tehát a felhasználók adatainak megszerzése, ahol a problémát elsősorban az jelenti, hogyan szerzik meg az adatokat, milyen eszközökkel veszik rá a felhasználókat személyes adataik kiszolgáltatására.

A *phishing* azonban nem szabad összekevernünk a *pharminggal*, mely szintén egy csalárd módon felépített weboldalt használ az adatnak megszerzésre, de a cselekményt annyival egészül ki, hogy egy rosszindulatú szoftver vagy kémsoftver segítségével az eredeti lapról mintegy eltérítik a felhasználót a hamis weboldalra.⁷³

A jelenség nem új, már az 1990-es évek közepéről ismert adathalász támadás. Egy adathalász az Amerika Online⁷⁴ belső emberének adta ki magát, és üzenetben a potenciális áldozatokat arra kérte, hogy adják meg a jelszavukat az azonosításukhoz vagy a számlájuk ellenőrzéséhez. Míg az első ilyen támadások alapvetően a banki-pénzügyi szektort vették célba és viszonylag kis számban fordultak elő, ma már jóval szélesebb kört érint a *phishing* és ez a technikai fejlődéssel együtt nagyban hozzájárult a sikeres támadások számának nagyarányú növekedéséhez.

Az Anti Phishing Working Group által évente készített felmérések jól mutatják a bűncselekmény számának növekedését, valamint a veszélyeztetett területek bővülését.⁷⁵

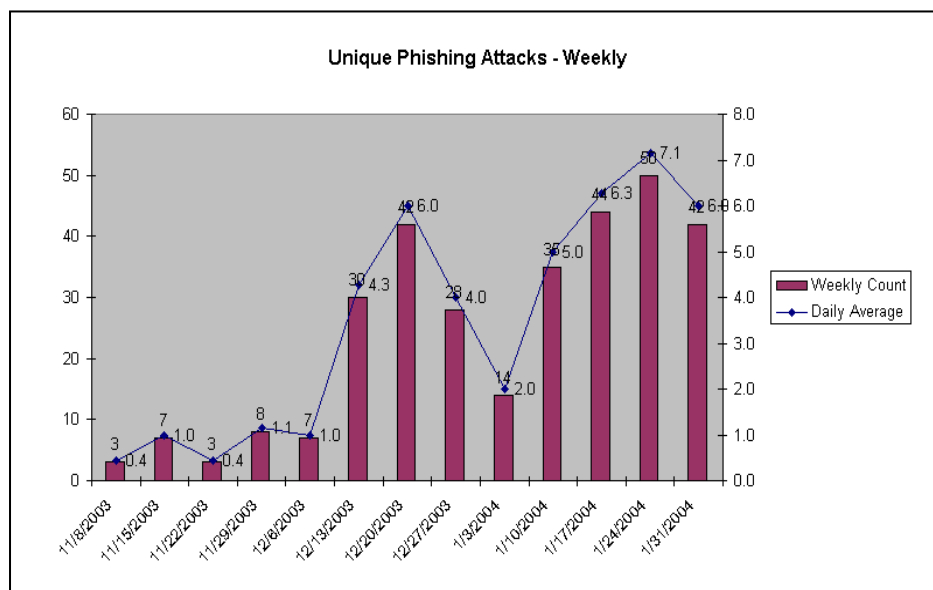
⁷² Az adathalászatról (*phishing*, *pharming*). <http://goo.gl/VEBJk>(letöltve: 2012-11-04).

⁷³ Az adathalászatról (*phishing*, *pharming*). <http://goo.gl/VEBJk>(letöltve: 2012-11-04).

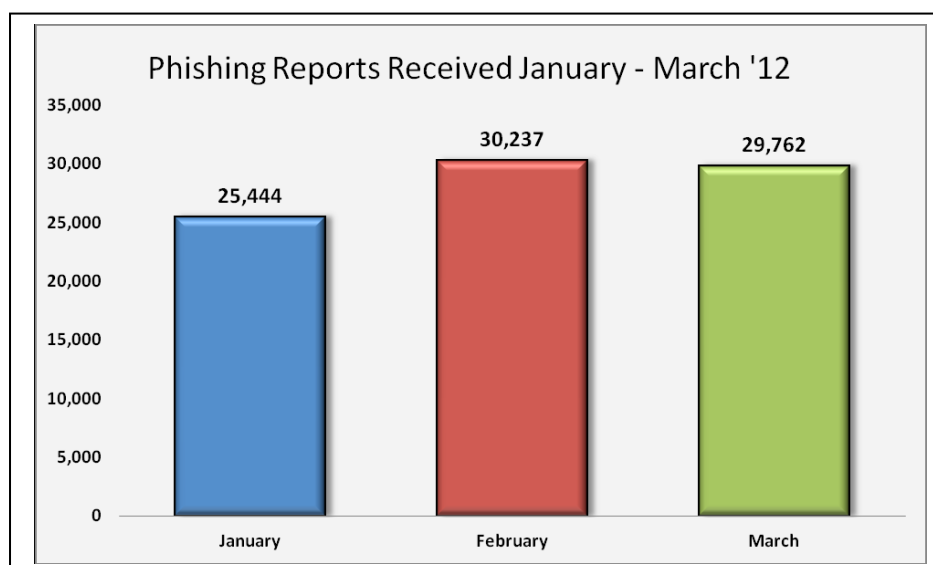
⁷⁴ Adathalászat, adatvédelem és spam. <http://goo.gl/lXKrI> (letöltve: 2012-11-04).

⁷⁵ Anti Phishing Working Group statisztikai adatai. <http://goo.gl/5gP14>.

1. ábra⁷⁶



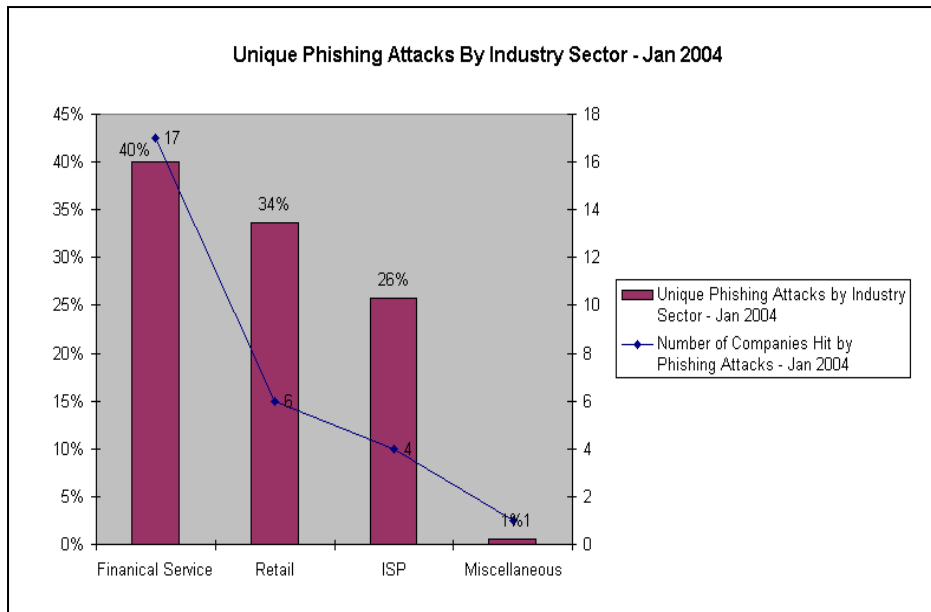
2. ábra⁷⁷



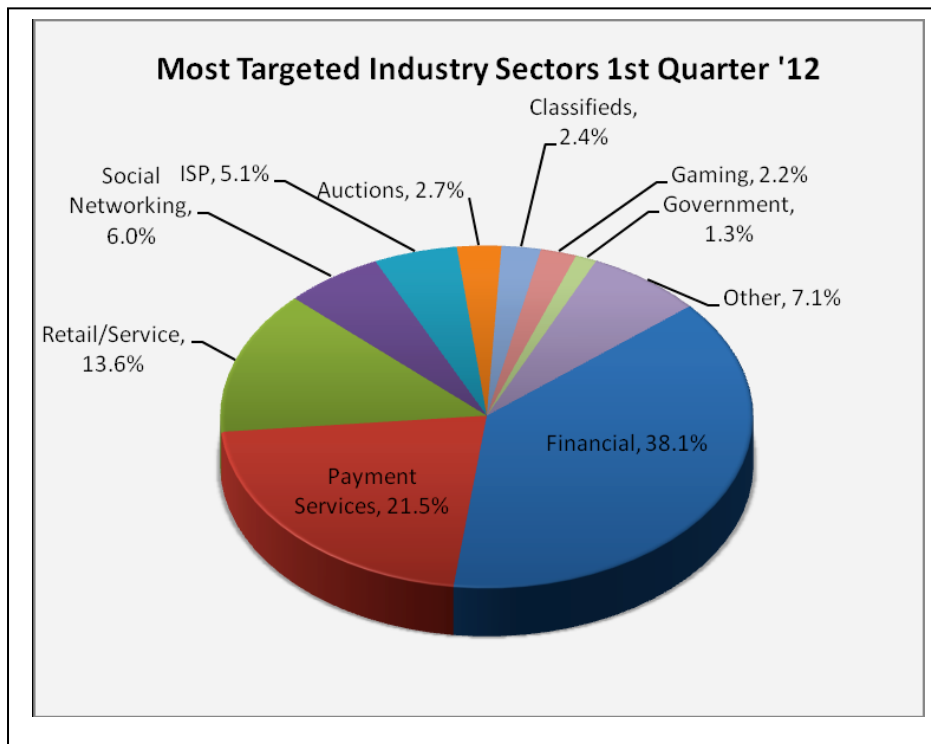
⁷⁶ 1. ábra: sikeres adathalász támadások 2003-2004 fordulóján heti lebontásban, <http://www.antiphishing.org/>.

⁷⁷ 2. ábra: sikeres adathalász támadások a 2012 január-március közötti időszakban, <http://www.antiphishing.org/>.

3. ábra⁷⁸



4. ábra⁷⁹



⁷⁸ 3. ábra: A sikeres adathalász támadások ipari szektoron belüli megoszlása 2004 januárjában, <http://www.antiphishing.org/>.

⁷⁹ 4. ábra: Az adathalász támadások által leginkább veszélyeztetett területek az ipari szektoron belül 2012. első negyedévében, <http://www.antiphishing.org/>.

Bűnözés. Net

A phishing internetes bűnözők körében képviselt népszerűségének oka az, hogy viszonylag egyszerűen és sokféle módon kivitelezhető. Egy linkre való kattintás, jelszóváltás, de akár hívás, sms, e-mail vagy akár egy bogbejegyzés is eszközül szolgálhat az elkövetőknek.⁸⁰

Egyre gyakoribbak a kifejezetten adathalászat céljára kifejlesztett programok.

Az adathalász támadások közös jellemzője, hogy minden esetben egy figyelemfelkeltő értesítés érkezik a felhasználóhoz, ami gyors cselekvésre szólítja fel, így biztosítva a támadás sikerét, aminek ha eleget tesz, valamilyen előnyhöz jut, például részt vesz egy nyereménysorsoláson ellenkező esetben hátrány érheti, így például törlődik a regisztrációja. Így biztosítva a támadás sikerét.

A *phishing* népszerűségének hátterében sokáig az állt, hogy a kezdeti időkben közvetlen pénzszerzési lehetőséget biztosított az adathalász számára, ellentétben a *hackinggel* vagy a *spammel*, ahol sok esetben csak közvetetten, a megszerzett adatok értékesítése után jutnak az elkövetők anyagi előnyhöz. A *phishing* célja a felhasználók bankszámla információinak megszerzésével a közvetlen pénzszerzés volt. A '90-es évek közepétől egészen 2006-2007-ig a bank szektor volt a leginkább veszélyeztetett. Idővel a korábbi tendencia annyiban módosult, hogy a pénzszerzés mellett a személyazonosság lopás is jövedelmező üzletté nőtte ki magát, így a bank-és pénzügyi szektor mellett más területek is veszélyeztetetté váltak.

Mindezek mellett kiemelendő, hogy a többi internetes bűncselekménytől eltérően a *phishing* esetében fontos szerepet kap az emberi tényező. Az adathalászat alapvetően az emberi hiszékenységre épít. Míg más internet specifikus bűncselekmény esetében az elkövetők elsősorban a technikai akadályok kijátszására koncentrálnak, a *phishing* esetében jóval nagyobb szerepe van a felhasználók hiszékenységének. Amint ugyanis a felhasználó elhiszi, hogy az adott e-mail az általa jól ismert banktól érkezik, hiába léteznek adatvédelmi beállítások, hiszen a felhasználó önként hozzájárul adatai felhasználáshoz. Be kell látnunk, hogy a hagyományos adatvédelmi eszközök már nem elegendők.

Éppen ezért az adathalászat visszaszorításánál nem elegendő a végrehajtó szervek és a biztonsági szakemberek hatékony fellépése, szükséges a felhasználók felvilágosítása is, hogy mi az, amitől tartaniuk kell, és hogyan védekezhetnek az ilyen típusú csalásokkal szemben.⁸¹

A CERT-Hungary Nemzeti Hálózatzbiztonsági Központ az adathalászat kapcsán megpróbálja felhívni a felhasználók figyelmét a veszélyekre, illetve segítséget kíván nyújtani, hogy minél nagyobb arányban megelőzhetőek legyenek a sikeres támadások. Rámutat arra, hogy az adathalászat területén egységes, minden helyzetre illő megoldás nem létezik és csak a felhasználón, és az odafigyelésén múlik, hogy sikeres-e a támadás, avagy sem. Javaslatokat tesz a Központ arra vonatkozóan, hogy ismerhetjük fel a csalárd weboldalakt. Így például egy bank esetében a címsáv egésze vagy egy része zöld színben jelenik meg, ami a biztonságos HTTPS kapcsolatot jelenti. Ez pedig azt jelenti, hogy az adatok titkosításra kerülnek a weboldal és a felhasználó között.⁸²

5. ábra⁸³



⁸⁰ Adathalászat, veszélyek az Interneten. <http://goo.gl/27XHa> (letöltve: 2012-11-04).

⁸¹ Adathalászat, adatvédelem és spam. <http://goo.gl/W4FB9> (letöltve: 2012-11-04).

⁸² Adathalászat, <http://goo.gl/rovLU> (letöltve 2012-11-04).

⁸³ 5. ábra: valós banki oldal címsávja, <http://goo.gl/4zBvq> (letöltve 2012-11-04).

Bűnözés. Net

Fontos továbbá, hogy a bankok és a pénzügyi intézetek sosem kérik a felhasználónevet és a jelszót ügyfeleiktől.

Lényeges körülmény tehát a *phishing* visszaszorításánál a felhasználók aktív részvétele, amihez elengedhetetlen a megfelelő tájékoztatás.

A tudatos felhasználó mellett azonban itt is szükség van a megfelelő jogi eszközökre a bűncselekmény hatékonyabb visszaszorítása érdekében.

Ennek megfelelően az Egyezmény 6. cikke⁸⁴ az adathalászat visszaszorítását célozza. Az Egyezmény a *phishing* elkövetése során két elemet emel ki, és teszi kívánatossá azok bűncselekménnyé nyilvánítását. Ennek megfelelően az 1. bekezdés a) pontjának i. alpontja magát a *phishing* megvalósítását elősegítő program előállítását, értékesítését, felhasználás céljából történő megszerzését, az ország területére történő behozatalát, forgalomba hozatalát vagy más módon történő hozzáférhetővé tételét rendeli büntetni. Az ii. alpontban pedig maga a *phishing* válik büntethetővé, de csak abban az esetben, ha azt eszközcselekményként használják a jogtalan belépés, jogtalan kifürkészés, adatok sértetlensége elleni cselekmények, a rendszer sértetlensége elleni cselekmények elkövetéséhez. Fontos kitétel, hogy ebben az esetben is csak akkor lesz bűncselekmény az adott cselekmény, ha azt jogosulatlanul és szándékosan követik el. A 6. cikk 2. bekezdése a mentesítő ok lehetőségét irányozza elő arra az esetre, ha a *phishing* nem szolgál eszközi a fenti bűncselekmények elkövetéséhez, így például engedélyezett kísérlet, vagy valamely számítástechnikai rendszer védelme az alapvető célja.

Az Egyezmény rendelkezéseivel összhangban az osztrák büntetőtörvénykönyv 126/c §-a⁸⁵ és a Btk. 300/E §-a tartalmazza a szükséges rendelkezéseket a *phishing* visszaszorítása

⁸⁴ E. 6. cikk: (1) Mindegyik Szerződő Fél megteszi azokat a jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy - belső jogával összhangban - bűncselekménnyé minősüljön az alábbi cselekmények jogosulatlan és szándékos elkövetése:

a) az előállítása, az értékesítése, a felhasználás céljából való megszerzése, az ország területére való behozatala, a forgalomba hozatala vagy a más módon történő hozzáférhetővé tétele:

i. elsődlegesen a 2-5. Cikkben meghatározott valamely bűncselekmény elkövetése érdekében létrehozott vagy átalakított eszköznek, ideértve a számítástechnikai programot;

ii. egy jelszónak, egy belépési kódnak, illetőleg a számítástechnikai rendszerbe vagy egy részébe való belépést hasonlóan lehetővé tevő számítástechnikai adatnak,

azzal a szándékkal, hogy azt a 2-5. Cikkben foglalt valamely bűncselekmény elkövetésére használják fel; valamint

b) a fenti a) pont i és ii alpontjában meghatározott dolgoknak a 2-5. Cikkben foglalt valamelyik bűncselekmény elkövetésére való felhasználása érdekében történő birtoklása. A Fél a belső jogában kikötheti, hogy a büntetőjogi felelősséget meghatározott számú dolog birtoklása alapozza meg.

(2) Jelen Cikkben foglaltak nem alapozzák meg a büntetőjogi felelősséget abban az esetben, ha a jelen Cikk 1. bekezdésében foglalt előállításnak, értékesítésnek, felhasználás céljából való megszerzésnek, az ország területére való behozatalnak, forgalomba hozatalnak vagy más módon történő hozzáférhetővé tételnek nem célja a jelen Egyezmény 2-5. Cikkében meghatározott bűncselekmény elkövetése, mint például az engedélyezett kísérlet vagy valamely számítástechnikai rendszer védelme.

3. A Fél fenntarthatja magának azt a jogot, hogy részben vagy egészben nem alkalmazza a jelen Cikk 1. bekezdését, feltéve, hogy a fenntartás nem a jelen Cikk 1. bekezdése a) pontjának ii alpontjában meghatározott értékesítésre, forgalomba hozatalra vagy más módon történő hozzáférhetővé tételre vonatkozik.

⁸⁵ StGB 126/c §: Aki olyan számítástechnikai programot, melynek jellege alapján valószínűsíthető, hogy azt számítástechnikai rendszerbe történő jogellenes hozzáférés, telekommunikációs titok megsértése, adatok jogellenes kifürkészése, adatok sértése, egy számítástechnikai rendszer működőképességének zavarása vagy csalárd adatfeldolgozás céljából került létrehozásra vagy adaptálásra, illetve ezzel hasonló berendezést vagy Számítástechnikai jelszót, hozzáférési kódot vagy ezekhez hasonló adatot, melyek a számítástechnikai rendszerhez vagy annak egy részéhez való hozzáférést teszi lehetővé

azzal a szándékkal létrehoz, bevezet, forgalomba hoz, elidegenít, hozzáférhetővé tesz, megszerez, birtokol, hogy az első pontban meghatározott bűncselekmények elkövetéséhez felhasználja, 6 hónapig terjedő szabadságvesztéssel vagy pénzbírsággal büntetendő. Az első bekezdés alapján nem büntethető, aki önként megakadályozza, hogy az első bekezdésben meghatározott számítógépes program vagy az ahhoz hasonló

Bűnözés. Net

érdekében. Hasonlóan az Egyezményhez mindkét állam törvényi tényállása a *phishinget* más, a törvényi tényállásokban pontosan meghatározott bűncselekmények eszközcselekményeként rendeli büntetni. A vonatkozó törvényi tényállások mind a *phishing* megvalósításához szükséges program vagy más hasonló berendezés létrehozásával, forgalomba hozatalával, elidegeníthetővé tételével, vagy más hasonló módon való hozzáférhetővé tételével kapcsolatos cselekményeket, mind magát az adathalászatot büntetni rendelik. Ezáltal látszólag egy széleskörű védelmet biztosítanak az adathalászat ellen. A probléma azonban az, hogy a *phising* csak akkor válik büntethetővé, ha azzal más, a törvényszövegben pontosan meghatározott bűncselekményeket követnek el. Minden más esetben azonban az adathalászat nem bűncselekmény.

Hasonlóan a fentiekhez a magyar Btk. is büntetni rendeli a *phising* előkészületét, és magát az adathalászatot is, ha azt más a Btk. 300/C §-ában meghatározott bűncselekmények elkövetéséhez használják fel. Lényegi különbség azonban, hogy míg a 126/c § esetében elegendő az eshetőleges szándék a tettesi oldalon, a magyar jogalkotó egyenes szándékot követel meg.

Korábban említettek szerint, mindkét tényállás kiemeli az adathalászat elkövetését lehetővé tevő programot, mellyel a tettes maga követi el a felsorolt bűncselekmények valamelyikét, vagy azt más rendelkezésére bocsátja, a bűncselekmény elkövetése céljából. Illetve a számítástechnikai rendszerbe vagy annak egy részébe való bejutást lehetővé tevő adat, egyéb belépési azonosító, melyet feltehetőleg adathalászat útján szereztek meg, és melyek segítségével a rendszerbe jutva követik el a megjelölt bűncselekményeket.

A vonatkozó törvényi tényállásokban jelzett elkövetési magatartások lényegében megegyeznek, viszont az osztrák büntetőjog a program, jelszó, azonosító birtoklását is, és nem csak a készítését, forgalomba hozatalát, megszerzését, vagy más módon való hozzáférhetővé tételét rendeli büntetni.

Bár a tényállás a program létrehozását említi, ez alatt azonban nem csak a program újonnan történő létrehozását kell érteni, hanem egy már meglévő program megfelelő átvételét is.

Fontos azonban, hogy a büntethetőséget nem befolyásolja annak ténye, hogy ezeket a programokat, adatokat ténylegesen fel is használják a cselekmény elkövetéséhez, hiszen a létrehozással már befejezetté válik a cselekmény.

A *Strafgesetzbuch* (StgB.) rendelkezéseivel ellentétben a magyar jogalkotó, már a *phishing* megvalósításához szükséges ismeretek mások rendelkezésre bocsátását is büntetni rendeli, ha ez abból a célból történik, hogy azokat felhasználva a meghatározott bűncselekményeket elkövessék.

Megjegyzendő továbbá, hogy az Egyezmény rendelkezésinek megfelelően mindkét jogalkotó megteremtette a mentesülés lehetőségét. Eltérés mutatkozik azonban abban, hogy míg a magyar jogalkotó a cselekmény eredményének olyan módon való elhárításához köti a mentesülést, hogy az elkövető tevékenységét bejelenti a hatóságnak, mielőtt az arról tudomást szerzett volna, és az elkészített dolgot a hatóságnak átadja valamint lehetővé teszi az elkészítésben részt vevő más személy kilétének megállapítását. Az *StgB.* rendelkezései szerint azonban elegendő a mentesüléshez, ha az elkövető önkéntesen megakadályozza az eredmény

berendezés, jelszó, hozzáférési kód, vagy az ahhoz hasonló adat a 118/a §, 119. §, 119/a §, 126/a §, 126/b §, vagy a 148/a §-ban meghatározott cselekmények elkövetéséhez használják.

Nem büntethető a tettes akkor sem, nem áll fenn az olyan felhasználás veszélye, vagy a közreműködése nélkül is megszűnik a veszély, ha az erre vonatkozó ismerek hiányában a tettes önként és komolyan törekszik a vélt veszély elhárítására.

Bűnözés. Net

bekövetkezését, vagy törekszik annak elhárítására, bár a tényleges veszély nem állt fenn. Az osztrák jogalkotó tehát nem követeli meg a hatóságnak való bejelentést.

Összességében tehát elmondható, hogy az adathalászat visszaszorítása érdekében mindkét tagállam megtette a kezdeti lépéseket azzal, hogy az Egyezmény rendelkezéseivel összhangban létrehozta saját büntető tényállást. A probléma azonban koránt sem megoldott, ugyanis a törvényi tényállások alapvetően eszköz cselekményként értékelik az adathalászatot, és így csak viszonylag szűk körben kerül sor felelősségre vonásra. Látnunk kell azonban, hogy az adathalászat mára olyan jelentőséggel rendelkezik, hogy nem elegendő pusztán más bűncselekmények elkövetésének eszközeként értékelnünk.

Egy másik lényegi hiányosság a szabályozás kapcsán, hogy a korábbi trendeknek megfelelően a törvényi tényállások elsősorban a jelszavak és belépési azonosítók jogtalan megszerzésére koncentrálnak, és nem veszik figyelembe, hogy az adathalászat az adatok jóval szélesebb körét érinti, és a számítástechnikai rendszerekbe történő bejutást lehetővé tevő adatokon túl, legszemélyesebb adataink sincsenek biztonságban. Feltehetőleg ez a szabályozásbeli hiányosság is oka annak, hogy a személyiséglopás jövedelmező üzletté tudta kinőni magát.

Internetes bűncselekmények közösségi hálójában

A fenti bűncselekmények közös jellemzője, hogy azok tipikus elkövetési helye az internet. Tekintettel arra, hogy az internet, az utóbbi években uralkodó médiummá nőtte ki magát, a bűnelkövetők körében is fókuszváltás következett be. Az internet nyújtotta anonimitás, a gyorsan változó, fejlődő virtuális tér, a szinte teljes nyomon követhetetlenség, ideális közeget biztosít az illegális cselekményeknek. Éppen ezért, nem csak a hagyományosnak mondható bűncselekmények tevődnek át egyre nagyobb számban az internetre, hanem mellettük újabb, kifejezetten erre az elkövetési helyre specializált bűncselekmények jönnek létre. Sőt ezen cselekmények, melyeket internetes bűncselekményeknek nevezünk, párhuzamosan az internet fejlődésével maguk is állandó változásban vannak, ezzel is megnehezítve a bűnüldöző szervek munkáját.

Míg korábban elmondható volt, hogy a bűnelkövetők az internet egészére koncentráltak, ma már itt is változás figyelhető meg.

A gyakorlat ugyanis azt mutatja, hogy az interneten töltött idő túlnyomó többsége ma már a közösségi portálokra tevődik, megelőzve a korábban vezető e-mailt is.⁸⁶

A változó fogyasztói szokásokhoz, igazodva a bűnelkövetők figyelme is áttevődik, és ma már az internetes bűncselekmények közösségi portálokra történő specializációja is megjelent.

2006-ban megjelent a *spamek*, legújabb típusa az úgynevezett közösségi hálózati spam.⁸⁷

Ennek hátterében az áll, hogy a *spamek* 40% a közösségi portálon terjed, sőt a *Facebookon* továbbított üzenetek mintegy 8 %-a *spam*.

Eltérően a hagyományosnak tekinthető *spamdexinghez*,⁸⁸ mely a keresőkre koncentrál, ez a típus a látogatókat állítja középpontjába. A célszemélyek ugyanis az adott portálon belül megadják legszemélyesebb adataikat, érdeklődési körüket, így lehetővé válik akár kisebb csoportokat célba venni. Ez jóval kedvezőbb a *spammerek* számára, hiszen korábban külön szolgáltatókat kellett alkalmazni, hogy a felhasználók keresési tevékenységére koncentrálnak megpróbálják meghatározni azok érdeklődési körét. Most viszont bizonyos keresési feltételek, szűrők segítségével, könnyen és gyorsan megtalálhatják a célszemélyeket. A *spammerek* elsődleges célja ugyanis a reklámok, hirdetések továbbítása felhasználók felé, ezzel is növelve fogyasztói körüket. Nem mindegy az, hogy például egy új kifejezetten diákoknak szóló bankszámlanyitási lehetőséget tömegesen küldik szét a megszerzett e-mail címekre, vagy a célszemélyek körét egyszerű beállítással leszűkítik a diákokra. A lehetőségek adottak, ennek köszönhetően azonban korábban nem látott számban terjednek a *spamek*.

A módszer egyszerű. A közösségi portálok legkedveltebb funkciói közé tartoznak a *like* és *share* funkciók. Míg előbbivel tetszésünket fejezhetjük ki, utóbbi lehetővé teszi, hogy ezt megosszuk ismerőseinkkel is. A *spemmernek* pedig nincs más dolga, mint *hackerek* bevonásával olyan alkalmazásokat, figyelemfelkeltő linkeket létrehozni, melyre rákattintva a várttól teljesen eltérő hirdetési felületre kerülünk. Sokszor „lájkolnunk” kell egy linket ahhoz, hogy a kívánt tartalmat megtekinthessünk, viszont gyakran ilyenkor is egy nem kívánt oldalra kerülünk. Ezt a jelenséget *likejackingnek*, vagyis lájkeltérítésnek nevezzük.⁸⁹

⁸⁶ David KIRCKPATRICK: *A Facebook jelenség*. GABO, 2011. 284.

⁸⁷ *Social Networking Spam- 5 rules for Marketers*. <http://goo.gl/23E4F>(letöltve 2012-11-04).

⁸⁸ *Spamdexing*. <http://goo.gl/gjD4S>(letöltve 2012-11-04).

⁸⁹ *Likejacking- a spammerek elérték a közösségi oldalakat* <http://goo.gl/v9kXa>(letöltve 2012-11-04).

6. ábra⁹⁰



Gyakori az úgynevezett *meghívó spam*, egy közösségi portálra való meghívónak álcázott spam.

Itt emelném ki, hogy szigorú értelemben véve, a valódi meghívók küldése is *spamnek* számít.⁹¹

Kisebb százalékban a *spamek* vírusok, vagy egyéb kártékony programok terjesztését tűzik ki célul, ezért is kell körültekintőek lennünk, mielőtt megosztanánk, vagy „lájkolnánk” egy oldalt.

A közösségi oldal azonban nem csak a *spammer* „játsszótere”.

A *spammerek* tevékenységét ugyanis nagyban megkönnyítik az adathalászok, hiszen a rengeteg személyes adatot tartalmazó közösségi oldalak tálcán kínálják magukat a *phishing*, azaz adathalászat számára. A *phishing* lényege az, hogy eltérően a szigorúan vett *hackingtől*, nem az oldal feltörésével jutnak be az érintett személy profiljára, hanem látszólag legális eszközökkel, hiszen maga a felhasználó adja meg a szükséges belépési azonosítókat, jelszavakat. A probléma gyökere tehát nem a bejutásban keresendő, hanem abban hogyan bírják rá a felhasználót, hogy megadja a szükséges adatokat.

A megoldási módok itt is változatosak. Leggyakoribb megoldás, az oldalak levelező rendszerén keresztül történő e-mail küldés. Ennek a lényeg, hogy az adathalász, egy elsősorban a felhasználóhoz köthető, megbízható cég, vállalat nevében küld e-mailt, arra biztatva őt, hogy az esetleges biztonsági beállítások megerősítése érdekében, vagy egy új

⁹⁰ 6. ábra: *Likejacking*, Symantec-17. *Internetbiztonsági tanulmány* http://www.cert-hungary.hu/sites/default/files/news/symantec_internetbiztonsagi_tanulmany_eloadas_hun.pdf.

⁹¹ SÜTŐ János i. m. 5-8.

Bűnözés. Net

szolgáltatáshoz való hozzáférés céljából adják meg belépési azonosítóikat, bankszámlaszámukat. A felhasználó bízva a vállalat hitelességében, hírnevében eleget is tesz a kérésnek. Az adathalásznak ezután nincs más dolga, mint haszon reményében továbbítani a megszerzett adatokat a *spammerek* felé, vagy biztosabb nyereség reményében maguk használják azokat.

A *phishing spam*hez köthető változata az, amikor hamis alkalmazásokat, *meghívó spameket* hoznak létre, és rábírják a felhasználót, hogy adja meg az adott közösségi oldalhoz, vagy más portálhoz tartozó belépési adatait. Az így megszerzett információval aztán belépnek az illető személy profiljára, és egy automatizált program segítségével *spameket* küldenek az ismerősöknek, újabb adatok beszerzése érdekében, vagy értékesítik a megszerzett adatokat reklámtevékenységet végző szolgáltatók felé.⁹²

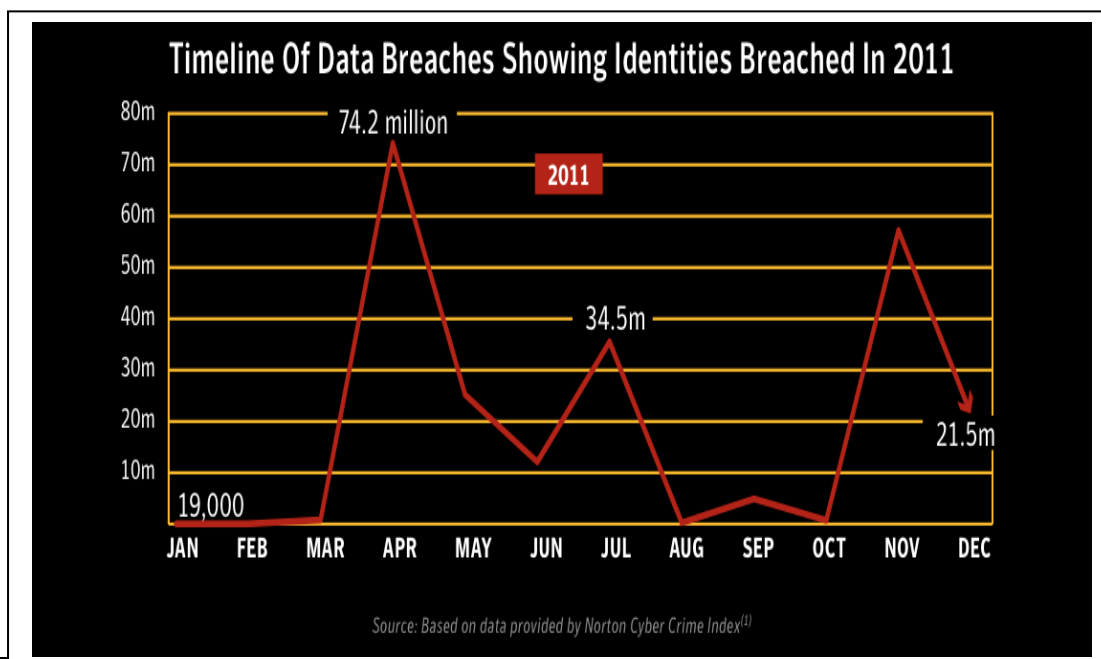
A veszély komolyságát példázza, hogy 2012 júniusában a *LinkedIn*⁹³ nevű, vállalkozóknak, cégeknek szánt közösségi oldalt adathalászok támadták meg, melynek eredményeképpen körülbelül 6,5 millió személyes adatot, jelszót sikerült megszerezniük.⁹⁴

A jelenség már nálunk is felütötte a fejét. 2009-ben a *Network.hu* magyar közösségépítő oldal nyereményjátékot hirdetett azon felhasználók körében, akik megadják más közösségi portálhoz tartozó belépési azonosítójukat. Az így megszerzett adatokkal, aztán beléptek az érintettek profiljára, és tömeges küldtek *spamet* az ismerősöknek.⁹⁵

A nagyobb problémát azonban egy másik típusú *phishing* jelenti. Mégpedig az, amikor közvetlen haszonszerzésre vágyik az adathalász. Ilyenkor a cél már nem feltétlenül a közösségi oldalakra történő bejutás, és kéretlen elektronikus levelek továbbítása, hanem személyes adatok gyűjtése, ami valljuk be, nem túl bonyolult egy olyan közegben, ahol mindenkinek az a célja, hogy minél többet mutasson meg magából, akár ismeretleneknek is.

Gyakori problémát jelent ennek eredményeképpen a személyes adatokkal való visszaélés, az azokkal való kereskedelem.

7. ábra⁹⁶



⁹² David KIRCKPATRICK i. m. 284-286.

⁹³ Már itthon is tanítják a *LinkedIn*. <http://goo.gl/9OfWW> (letöltve: 2012-11-04).

⁹⁴ Támadás érte a *LinkedIn*, több millió jelszó szivároghatott ki. <http://goo.gl/zpCBu> (letöltve 2012-11-04).

⁹⁵ WikiSpam: *Phishing*. <http://goo.gl/tG5zD> (letöltve 2012-11-04).

⁹⁶ 7. ábra: A személyiség lopásra irányuló adathalász tevékenység alakulása 2011-ben. Symantec-17. Internetbiztonsági tanulmány http://www.cert-hungary.hu/sites/default/files/news/symantec_internetbiztonsagi_tanulmany_eloadas_hun.pdf (letöltve 2012-11-04).

Bűnözés. Net

A *phishing* legjövedelmezőbb formája azonban a bankszámla adatokkal való visszaélés. Az álnéven, különösen a felhasználó bankja nevében küldött e-mailek rendkívüli meggyőző erővel rendelkeznek. A felhasználó ilyenkor gyakran komolyabb mérlegelés nélkül megadja bankszámla információt, ahonnan már csak egy lépés az adathalász számra a jövedelemszerzés.

Ugyan az utóbbi adathalász tevékenység még viszonylag nehezen valósítható meg a közösségi portálok segítségével, a jövő viszont egyre inkább abba az irányba tart, hogy növelve a felhasználói élményt, egyszerűsítve a mindennapokat, mindent egy helyen, egy oldalon tegyen lehetővé. A *Facebook* hosszú távú elképzelései között szerepel banki szolgáltatások, így az átutalás lehetővé tétele az oldalon.⁹⁷ Ennek működéséhez azonban, elkerülhetetlenné válik a bankszámla információ közzététele, ami nagyban meg fogja könnyíteni az adathalászok munkáját.

⁹⁷ David KIRCKPATRICK i. m. 357-358.

Lehetne jobb is?

Az egyes cselekmények jellemzőinek, és a cselekményekre vonatkozó törvényi szabályozás áttekintése után, fontos a szabályozás hatékonyságának vizsgálta.

A Symantec által évente készített jelentések jól mutatják hazánk helyzetét más országokhoz viszonyítva az internetes bűncselekmények kapcsán.

8. ábra⁹⁸

LEGFERTŐZÖTTEBB ORSZÁGOK AZ EMEA RÉGIÓBAN

	Overall 2011 Region Rank	Overall 2011 World Rank	Overall REGION 2011 Malicious Code Rank	Overall REGION 2011 Spam Rank	Overall REGION 2011 Phishing Hosts Rank	Overall REGION 2011 Bots Rank	Overall REGION 2011 Network Attacking Countries Rank	Overall REGION 2011 Web Attacking Countries Rank
Germany	1	5	5	12	1	2	2	2
Russia	2	6	3	1	5	10	3	4
United Kingdom	3	7	1	14	2	5	1	3
Italy	4	9	9	8	8	1	4	7
Algeria	5	13	21	16	27	52	36	1
Poland	6	15	14	9	7	3	7	9
France	7	17	7	24	4	7	5	6
Spain	8	18	13	11	6	6	6	10
Pakistan	9	19	10	2	40	19	21	24
Netherlands	10	20	18	15	3	14	10	5
Turkey	11	21	4	22	11	8	8	12
Ukraine	12	23	15	3	10	23	9	11
Hungary	13	25	51	35	14	4	16	18
Romania	14	26	19	6	9	28	12	8
Egypt	15	27	2	25	42	31	23	36
Israel	16	31	16	17	24	9	17	16
Saudi Arabia	17	32	6	10	44	39	14	23
Iran	18	33	12	7	30	34	28	33
Belarus	19	35	34	4	37	38	31	102
Kazakhstan	20	36	35	5	39	44	33	40

Symantec Corporation INTERNETBIZTONSÁGI TANULMÁNY

9. ábra⁹⁹

LEGFERTÖZÖTTEBB VÁROSOK

RANK	CITY	COUNTRY	WORLDWIDE %	EMEA %
1	TAIPEI	TAIWAN	9,361030375	28,98959655
2	ROME	ITALY	3,528029502	9,325461181
3	BUENOS AIRES	ARGENTINA	3,382853593	11,80415357
4	TOKYO	JAPAN	2,922250564	9,049737206
5	BUDAPEST	HUNGARY	2,470895164	6,531191682
6	PETAH TIQWA	ISRAEL	1,271430341	3,36070724
7	LONDON	UNITED KINGDOM	1,222168936	3,230497071
8	SZEGED	HUNGARY	1,136806213	3,00486212
9	SHANGHAI	CHINA	1,096021801	3,394202191
10	SAN PAULO	BAZIL	1,061876711	3,705320205

Symantec Corporation INTERNETBIZTONSÁGI TANULMÁNY

⁹⁸ 8. ábra Symantec-17. Internetbiztonsági tanulmány http://www.cert-hungary.hu/sites/default/files/news/symantec_internetbiztonsagi_tanulmany_eloadas_hun.pdf.

⁹⁹ 9. ábra Symantec-17. Internetbiztonsági tanulmány http://www.cert-hungary.hu/sites/default/files/news/symantec_internetbiztonsagi_tanulmany_eloadas_hun.pdf.

Bűnözés. Net

A vizsgált statisztikai adatok alapján megállapítható, hogy Magyarország világviszonylatban is kiemelkedő helyen áll az internetes bűncselekmények számát tekintve. Azt mondhatjuk tehát, hogy bár megvannak a szükséges törvényi szabályok a visszaszorítás érdekében, azonban ezek nem kellően hatékonyak.

Felmerül a kérdés, hogy a hatékonyság hiánya a törvényhelyek hiányosságaira, hibájára vezethető vissza, vagy más egyéb okok állnak a probléma hátterében.

A Symantec éves jelentései alapján a velünk szomszédos Ausztria, Magyarországhoz képest jóval hátrébb, világviszonylatban a 43. helyen szerepel az internetes bűncselekmények számát tekintve.¹⁰⁰

Tekintettel azonban arra, hogy mind Ausztria, mind Magyarország szerződő államai a Számítástechnikai Egyezménynek, szabályozásuk csak kis mértékben tér el. Tényállásaik lényegi vonásaikban azonosak, néhány kisebb eltérés mutatkozik közöttük, így például a magyar Btk. általában súlyosabb büntetési tételeket állapít meg a *Strafgesetzbuch*nál.

Első ránézésre tehát azt a következtetést kellene levonnunk, hogy Ausztriában a hasonló törvényi szabályozás hatékonyabban érvényesül. A valóságban azonban ez nem így van.

A statisztikák ugyanis azt a téves látszatot keltik, mintha Ausztriában nem okozna olyan mértékű károkat az internetes bűnözés, mint sok más államban, viszont tudnunk kell azt is, hogy ezek a statisztikai adatok az adott ország lakosságának nagyságához viszonyítják a bűnözői aktivitást.¹⁰¹ Nem mondhatjuk tehát, hogy Ausztriában kellően nagy visszatartó erővel rendelkeznek a törvényhelyek, és ezért náluk kevésbé nagy hangsúlyt kellene fektetni más, visszaszorítást segítő eszközök kialakítására.

Azt láthatjuk, hogy mind nemzetközi, mind nemzeti szinten rendelkezésünkre állnak az internetes bűncselekmények elleni fellépést biztosító törvényhelyek, ezek azonban nem rendelkeznek kellő visszatartó erővel, és a bűncselekmények jellegzetességei kihívások elé állítják a jogalkotókat. A *hacking* esetében ugyanis megvalósítható a tökéletes bűncselekmény, hiszen egy oldal feltörése és a nyomok eltüntetése átlagosan 10 percet vesz igénybe.¹⁰² Azt is látnunk kell, hogy irreális lenne, valamennyi *hacker*-tevékenységet megtiltani, gondoljunk csak a *white-hat* *hackerek* biztonságtechnikai fejlesztő tevékenységére. A *spam* esetében problémát okoz, hogy a felhasználók körében nem kellően tudatosított a jelenség veszélye, így a rendelkezésre álló védelmi eszközök, mint az opt-in rendszer és a Robinson-listák sincsenek kellő mértékben kihasználva.

A *phishing* esetében komoly gondot jelent a meglévő törvényi szabályozás hiányossága, hiszen mint azt láttuk a cselekmény, csak akkor válik büntethetővé, amennyiben más, pontosan meghatározott bűncselekmények elkövetése érdekében valósítják meg. Itt is hiányzik a felhasználók megfelelő szintű tájékoztatása a cselekmény jellegzetességeit, veszélyeit illetően. Gyakran felelőtlenül adják meg adataikat vagy regisztrálnak ismeretlen oldalakon. Komoly problémákat jelenthet az adatvédelmi beállításokba vetett túlzott bizalom.

Összességében elmondhatjuk, hogy a jelenlegi szabályozottsági szint nem elegendő, szükség van a meglévő szabályok pontosítására, kiegészítésére, továbbá új szabályok megalkotására. Mindezek mellett azonban a hatékony visszaszorítás érdekében a társadalom aktívabb részvételére van szükség. Ehhez elengedhetetlen a felhasználók tájékoztatását, felhívását célzó programok létrehozása, és arra való ösztönzése, hogy a meglévő eszközöket, mint a Robinson listát, alkalmazzák. Fontos, hogy tudatosuljon a felhasználókban annak a

¹⁰⁰ Internet-Sicherheitsbericht Österreich 2012 <http://goo.gl/wlIsU> (letöltve 2012-11-04).

¹⁰¹ Internet-Sicherheitsbericht Österreich 2012 <http://goo.gl/wlIsU> (letöltve 2012-11-04).

¹⁰² Vázlat a magyar hacker szubkultúráról <http://adminhost.0fees.net/subkul.htm> (letöltve 2012-11-04).

Bűnözés. Net

jelentősége, hogy az észlelt jogsértéseket jelentsék a hatóságok felé, hogy azok megfelelően felléphessenek ellene.

Továbbra is fontos a hatóságok, szakértők továbbképzése, melyben nagy szerepe lehet a manapság egyre gyakoribb nemzetközi számítástechnikai konferenciáknak.

További megoldási lehetőségként említendő, hogy Ausztriában a kormányzat feladatának tartja az internetes bűncselekmények elleni hatékony fellépést. Ezért a 2012-es évre vonatkozóan országos program került kidolgozásra ezen bűncselekmények visszaszorítása érdekében, mely program megvalósítását egy kifejezetten erre a célra létrehozott szervezetnek kell véghezvinnie.¹⁰³ A program hatékonysága a jövő kérdése, de a jelenlegi viszonyok között reális lehetőségnek mutatkozik az internetes bűncselekmények ellen vívott harcban.

¹⁰³ Internet-Sicherheitsbericht Österreich 2012 <http://goo.gl/wlIsU> (letöltve 2012-11-04).

Forrásjegyzék

1978. évi IV. törvény a Büntető Törvénykönyvről

2001. évi CVIII. Törvény az Elektronikus Kereskedelmi Szolgáltatások, valamint az Információs Társadalommal Összefüggő Szolgáltatások Egyes Kérdéseiről

1995. évi CXIX törvény a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről

2003. évi C. törvény az elektronikus hírközlésről

Számítástechnikai Bűnözésről szóló Egyezmény Budapest, 2001. november 23.

Bundesgesetz vom 23. Jänner 1974. über die mit gerichtlicher Strafe bedrohten Handlungen

Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce –Gesetz ECG)

Telekommunikationsgesetz 2003.

Anthony F.Iasi-Lynn M. Brenner-Al Servati: Az intranet Bibliája I.-II., Kossuth Kiadó, 1997.

ASS. Prof. Christian Bergauer, Die Kriminalität im Cyberspace, in: Salzburger Nachrichten 28.06.2011

Bacsó László, Bűnözés az interneten, <http://www.doksi.hu/get.php?lid=3242>

Balogh Zsolt György: Jogi Informatika, Nordex Kft. Dialog Campis Kiadó, 1998.

Christian Bertel, Klaus Schwaighofer: Österreichisches Strafrecht- Besonderer Teil I-II. Springer, 2010.

David Krickpatrick: A Facebook jelenség, GABO, 2011

Debra Yang Wong, Brian m Hoffstadt: Counterig the cyber-Crime Threat, American Criminal Law Review, Vol. 43. Issue 2 (2006)

Detlef Kröger, Claas Hanken: Casebokk Internetrecht – Rechtsprechung zum Internetrecht, Springer DE.2002

Detrekői Zsuzsa: Szabályozható -e az internet?, Infokommunikáció és Jog, 39. szám

Dietmar Jahnel, Informatikrecht, Springer, 2002.

Dr. Békés Imre, Dr. Belovics Ervin, Dr. Busch Béla, Dr. Gellér Balázs, Dr. Margitán Éva, Dr. Molnár Gábor, Dr. Sinku Pál: Büntetőjog- Általános rész, HVG-ORAC Kiadó Kft. 2009

Bűnözés. Net

Dr. Belovics Ervin, Dr. Molnár Gábor, Dr. Sinku Pál: Büntetőjog- Különös rész, HVG-ORAC Kiadó, 2009.

Dr. Ibolya Tibor: A „torrentrazziák” büntetőjogi megítélése, <http://ibolyatibor.atw.hu/>

Dr. Madai Sándor, A csalás büntetőjogi értékelése, HVG-ORAC Kiadó, 2011.

Farkas Szabó András: A szerzői jog és az internet, <http://www.dura.hu/html/jogvedelem/szerzoijognet.htm>

Frederic Barbier, Catherine Bertho Lavenir: A Média Története – Didero-tól az internetig, OSIRIS Kiadó Kft., 2004.

Frank A. Koch: Internet-Recht, Oldenbourg Verlag München Wien

Gelányi Anikó: Amit a gyermekpornográfiáról tudni illik, lehet, vagy éppen kell, Infokommunikáció és Jog, 35. szám

Gerlinde Füßel, Die österreichische Strafgewalt für Internet-Straftaten, Diplomarbeit aus Strafrecht. 2006.

Gregor Walter: Internetkriminalität: Eine Schattenseite der Globalisierung SWP, 2008.

Johannes Beer: Die Convention on Cybercrime und österreichisches Strafrecht, Trauner, 2005.

John R. Mills: Counterinsurgency in Cyberspace, Georgetown Journal of International Affairs, Vol. 11, Special Issue 2011.

Jóri András: Adatvédelmi Kézikönyv, OSIRIS Kiadó Kft., 2005

Kazári Csaba: Hacker, Cracker, Warez, Vogel Burda Communications Kft., 2003.

Lengyel Veronika: Az internet világa, ComputerBooks, 1995.

Michael Gervais: Cyber Attacks and the Laws of War, Berkeley Journal of International Law, Vol. 30 Issue 2 (2012)

Mrinalini Singh, Shivam Singh: Cyber Crime Convention and Trans Border Criminality, Masaryk University Journal of Law and Technology, Vol. 1. issue 1 (2007)

Parti Katalin: Gyermekpornográfia az interneten, Bíbor Kiadó 2009

Peter Warren, Michael Streeter: Az internet sötét oldala, HVG. Kiadó, 2005.

Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szempontból, Infokommunikáció és Jog, 38. szám/40. szám/41. szám/ 42. szám/ 44. szám

Nagy Zoltán András, Bűncselekmények a számítógépes környezetben, AD Librum Kiadó, 2009.

Bűnözés. Net

Rebecca Crootoof, Philip Levitz: Law of Cyber-Attack, California Law review, Vol. 100, Issue 4 (2012)

Ron Plesco, Phyllis Schneck: Criminal Public-Private Partnerships: Why Can't We Do That. Georgetown Journal of International Affairs, Vol 11. special issue (2011)

Simon Ernst: Internetkriminalität- Gefahren für die Wirtschaft, GRIN

Sütő János: Spamtelenül, Szak Kiadó, 2008.

Szabó Imre: Internetes bűncselekmények, 2003. <http://www.ajk.elte.hu/file/SzaboImre-InternetesBuncselekmenyek.pdf>

Szentkúti Dániel/ Szűts Márton: Az internet és a büntetőjogi felelősség egyes kérdései, <http://jesz.ajk.elte.hu/szentkuti15.html>

Thomas J. Primig: Internationales Strafrecht und das Internet,

Wolfgang McGavran: Intended Consequences: Regulating Cyber Attacks, Tulane Journal of technology and intellectual Property, Vol. 12. Issue 1 (2009)

William C. Banks, Elizabeth Rindskopf Parker: Cybersecurity Symposium: National Leadership, Individual Responsibility- Introduction, Journal of national security Law & Policy, Vol. 4, Issue 1 (2010)

http://rechtsprobleme.at/doks/primig-1-internationales_strafrecht.pdf

www.ptext.at/nachrichten/symantec-sicherheitsbericht-signifikanter-anstieg-qualitaet-volumen-schadcode-166105

www.cert-hungary.hu/sites/default/files/news/cert_2012_quart_2.pdf

www.computerworld.hu

www.scientificamerican.com

www.darkgovernment.hu

<http://www.acunetix.com/websitesecurity/cross-site-scripting.htm>

http://www.us-cert.gov/nav/report_phishing.html

<http://tarhely.eu/ugyfeladmin/knowledgebase/94/virus-hack-hackelesek--spamek-.html>

<http://www.slideshare.net/krasznay/hackactivity2007-krasznay>

<http://facebookhirek.hu/2012/03/11/facebook-adathalaszat/>

http://itcafe.hu/hir/viragzik_az_internetes_adathalaszat.html

<http://krono.inaplo.hu/index.php/component/content/article/439>

<http://www.interpressmagazin.hu/index.php?page=archivum&cid=491>

<http://www.webbeteg.hu/cikkek/egeszsleges/10742/a-kozossegi-oldalak-veszelyei>

<http://tech.cert-hungary.hu/tech-blog/120827/alkalmazas-keresi-a-kozossegi-oldalakon-terjedo-spam-et-es-karos-szoftvert>

http://www.infoter.eu/cikk/likejacking_a_spamerek_elertek_a_kozossegi_oldalakat

<http://pcworld.hu/tamadas-erte-a-linkedint-tobb-millio-jelszo-szivaroghatott-ki-20120607.html>

http://www.fzolee.hu/framework/a_facebook_es_a_nyilvanos_kozossegi_portalok_veszelyei

Bűnözés. Net

<http://krono.inaplo.hu/index.php/inter/8-networkstudies/582-adathalaszat-adatvedelem-es-spam>
<http://nonstopuzlet.hu/zsakutcaban-a-kozossegi-oldalak-20100203.html>
http://www.mfor.hu/cikkek/Vilagszerte_csokkennek_az_adatbiztonsagi_kiadasok_a_gazdasagi_valsga_nyoman.html#
<http://hu.spam.wikia.com/wiki/Phishing>
<http://internetdetektiv.hu/>
<http://pcforum.hu/hirek/8810/Rohamosan+no+az+internetes+csalasok+szama.html>
<http://www.hwsz.hu/hirek/40113/buntetojog-es-az-internet.html?oldal=2>
<http://www.internetrecht.at/intern.recht.html>
<http://www.dikri.de/>
<http://www.stern.de/digital/online/betrug-den-ganzen-tag-lang-auf-einen-link-klicken-536615.html>
<http://www.bmvit.gv.at/telekommunikation/Internet/spam.html>
http://www.krone.at/Oesterreich/Kriminalstatistik_mit_weniger_Anzeigen_dafuer_Cyber-Boom-Sorgenkind_Internet-Story-241272
http://www.info-graz.at/ausbildung-beratung-fortbildung-familie-gesundheit-tipps-ernaehrung-freizeit/news/3740_wer_profiziert_bei_uns_von_phishing/
<http://blogs.technet.com/b/gerhardg/archive/2007/05/22/bankomarkarten-phishing-letztes-jahr-in-sterreich-heuer-in-den-usa.aspx>
http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2006/03_04/files/Phishing.pdf
<http://goo.gl/Ty7Cu>
<http://goo.gl/dA6cZ>