GYARAKI RÉKA

A SZÁMÍTÓGÉPES KÖRNYEZETBEN ELKÖVETETT GAZDASÁGI BŰNCSELEKMÉNYEK

A PIN kód megadása sikeres vagy biztonságos az internet?!

I. Bevezetés

A számítógépes környezetben elkövetett bűncselekmények a számítógép, valamint az internet terjedésével fokozatosan alakultak ki. Térhódításuk egyre szélesebb sávban mozog. Az egyszerű felhasználótól a profi alkalmazón át bárkiből lehet áldozat és bárki válhat elkövetővé is. Mindennapi életünket áthatja akarva-akaratlanul a technika. Egyszerűbbé és gyorsabbá vált a kapcsolattartás, a banki tranzakciók intézése, a hírek-, információk áramlása.

A modern kor fejlődése, az informatika népszerűsége egyértelműen teret hódít, fontossága elvitathatatlan.

Az elmúlt évek kihívásai, a technikai fejlődés iránti igény szinte provokálja az embereket arra, hogy a hagyományos eszközök helyett a modern eljárást, technikai újításokat válasszák, úgy, hogy élvezzék annak minden előnyét, de közben sem az eszközök, sem a rajtuk tárolt adatok védelmére nem gondolnak, jelszavaikkal könnyelműen bánnak.

Egyszerűbben megfogalmazva, hatalmas összeget költenek arra, hogy minél szebb, jobb és gyorsabb notebook-t vagy okos telefont válasszanak, de az azok védelmét inkább az ingyen letölthető (megjegyzem ezek egyáltalán nem rosszak) vírusirtó programokra bízzák. Egy része rendeltetésének megfelelően működik, más fajtája viszont épp azért lett kitalálva, hogy azzal bejussanak a felhasználók gépére és onnan adatokat töltsenek le, módosítsák azokat, vagy épp használhatatlanná tegyék az egész rendszert.

A számítógépes bűnözés a számítógép megjelenésével indult meg és annak fejlődésével párhuzamosan „száguldott”.

A gyors fejlődéssel pedig a törvényhozók valamint a nyomozó hatóság nehezen tud lépést tartani.

I. 1 A számítógépes környezetben elkövetett bűncselekmények általános jellemzői:

- Anonimitás
- Gyorsaság
- Magas fokú látencia
- A sértettek nagy száma
- Nemzetközi, határokat átlépő bűncselekmények
- Nehéz felderíthetőség

Az anonimitás kedvez a bűncselekményt elkövetőknek. A világháló névtelenséget biztosít. Nincs olyan hazai- vagy nemzetközi jogszabály jelenleg, ami büntetné azokat, akik egyáltalán nem adják meg nevüket, adataikat, vagy fiktív névvel regisztrálnak. Ez az a jellegzetesség, ami miatt a számítógépen elkövetett bűncselekmények száma felfelé ível. A bűnözők így sokáig képesek névtelenek maradni, sőt ugyanaz a személy, vagy bűnözői csoport más-más hamis név alatt több bűncselekményt képes megvalósítani.

A gyorsaság miatt könnyű a bűnelkövetők helyzete és a nehéz a nyomozóhatóságok feladata. A gyorsaság nemcsak az adatok, információk sebességét jelenti, hanem a technika fejlődését is, mellyel lépést kell tartani. A bűnelkövetőket a haszon, a pénzszerzés, károkozás motiválja. De ugyanakkor a jogalkotókat és a jogalkalmazó hatóságokat is motiválnia kellene. Vagyis, a jogszabályokat, a bűnüldözésre használt eszközöket napi szinten szükséges fejleszteni. Lássuk be, ezt az anyagi erőforrások hiánya, valamint az emberi erőforrások hiánya miatt nehéz megvalósítani. Vagyis, kevés a szakember és kevés az a pénz, amit a fejlesztésre, oktatásra és megelőzésre tudnak fordítani. A gyorsaság miatt a sértettek vagy potenciális sértettek is veszélyben vannak, hiszen előfordulhat, hogy nem észlelik időben a sérelmükre elkövetett bűncselekményt, vagy annyi idő telt már el az elkövetés óta, ami a nyomozást megnehezíti.

A magas fokú látencia jellemzője többek között, a fentebb vázolt, vagyis a gyorsaság, de ugyanakkor többen kitértek már arra, hogy az esetek többségét nem jelentik a hatóságok felé. Azzal az állásponttal, hogy ez főleg a pénzintézetek esetébe jellemző, nem értek teljesen egyet, hiszen amikor a bankkártya hamisítás miatt több személy kártyájáról emelnek le az elkövetők kisebb-nagyobb összeget, akkor a bankok épp azért hozzák nyilvánosságra az esetet, valamint értesítik a hatóságot gyorsan, mert a kárt ők is viselik.

A sértettek nagy száma az internet népszerűségének köszönhető. Szinte megszámlálhatatlan sértettje lehet egy aukciós csalásnak, vagy egy pedofil hálózatnak, az adathalászatról már nem is beszélve. A sértetteket nem lehet jellemezni, sem életkor, sem iskolai végzettség alapján. Ugyanúgy sértett lehet egy idős ember, mint egy gyerek, egy magasan iskolázott vagy egy, mindenféle iskolai végzettség nélküli személy. Az internetes bűnözésre kimondottan jellemző, hogy az elkövetők célja éppen az, kevés kivétellel, hogy minél több ember sérelmére, minél több haszonnal hajtsák végre a cselekményt.

A nemzetköziség abból fakad, hogy az internet nem ismeri az országhatárokat. Az információ áramlását nem nehezíti meg, hogy az óceánon túlra kell eljuttatni, hiszen minden a virtuális térben történik. Nem szükséges, hogy az elkövető és az áldozat egy helyen tartózkodjon. Bármelyik bűncselekményt el tudnak olyan helyen követni, ahol a sértett még soha nem járt.

Az elkövetői oldalt jellemezni ugyanúgy nehéz, mint a sértetti oldalt. Az elkövetők számát tekintve lehet egy személy is, de akár többen is elkövetethetik ugyanazt a cselekményt, akár egymás tevékenységéről tudva és összehangoltan, akár pedig egymástól függetlenül. Általánosan szokás őket ún. „fehérgalléros” bűnözőknek nevezni. Mivel a számítógép- és az internet használata olyan széles körben elterjedt, ma már nem jellemző feltétlenül, hogy csak magasan kvalifikált, tanult –esetleg informatikus végzettségű- személyek követnék el ezeket a cselekményeket. Természetesen sok eset volt már, ahol az elkövetők valamelyik műszaki egyetem hallgatói vagy felsőfokú végzettséggel rendelkező informatikusok voltak, de talán gyakoribb, hogy pusztán szórakozásból vagy egyszerűen csak önszorgalomból, saját maga sajátította el az informatika csínját és követett el így

bűncselekményeket.[404] Ahhoz sem kell senkinek szakembernek lennie, hogy illegálisan töltsön fel a világhálóra filmet, zenét, szoftvert és azokat díj ellenében engedje letölteni mások számára. Már ahhoz, hogy olyan honlapot készítsen valaki, ami hasonló egy bankéhoz és így megszerezze a bank ügyfeleink adatait, majd pénzét, már inkább kell szakértelem. Bár sok esetben buktak meg azon, hogy a helyesírással problémájuk volt az elkövetőknek, de amíg ez senkinek nem tűnt fel, addig is hatalmas károkat okoztak.

A nyomozó hatóság munkáját nehezíti a fent felsorolt valamennyi jellemző akár együttesen, akár pedig külön-külön is. Jelenleg a hatóságnak nincs annyi képzett szakembere, amennyi ahhoz kell, hogy szakszerűen fel tudjon lépni. Vagyis, nem elég, hogy kijelölnek egy-egy nyomozót arra, hogy végezze ő a számítógéppel kapcsolatos bűncselekmények nyomozását, hanem minden egyes hivatásos állományú tiszthelyettes és tiszt számítástechnikai képzését legalább minimális mértékben biztosítani kellene. Így megelőzhető lenne, hogy ne szakértő módon történjen egy házkutatás, lefoglalás, ami során bizonyítékok semmisülhetnek meg.

Összefoglalva: az elmúlt években nőtt a számítógéppel elkövetett bűncselekmények száma, ami köszönhető többek között, annak, hogy a háztartásokban viszonylag nagy arányban (egy tavalyi felmérés szerint kb. 53%-ban található legalább egy számítógép[405]) van jelen az informatika. De véleményem szerint ma egyetlen egy vállalkozás, kormányhivatal sem képzelhető el anélkül, hogy ne jelennének meg a weben. Így a hagyományosnak mondható bűncselekmények mellett, vagy inkább azokat felváltva, egyre gyakrabban jelennek meg a számítógépen elkövetett bűncselekmények.

Ha abból indulunk ki, hogy a „hagyományos[406]" bűncselekményeknek is még most is nagy számban vannak sértettjei, akkor a modern, interneten elkövetett deliktumok még nagyobb, szélesebb körben szedik áldozataikat.

II. A számítógépes bűncselekmények jogszabályi háttere

Az Egyesült Államok mellett, az Európai Unió és Magyarország is szükségesnek vélte, hogy a megszaporodott számítógépes bűncselekményekre egy egységes szabályozást találjanak ki. Az OECD 1989-es ajánlása alapján nevesítettek

Az interneten elkövetett bűncselekményeket az Európa Tanács 89. számú ajánlása, minimum listája nevesítette,[407] mely egy ajánlást tartalmaz a tagállamok felé a számítógépes bűncselekmények egységes értelmezéséhez. Az Európa Tanács minimum listája, mely a szándékosan elkövetett bűncselekményeket tartalmazza:

- a számítógépes csalás,
- a számítógépes hamisítás,
- a számítógépes adatokban és programokban történő károkozás,
- a számítógépes szabotázs,
- a jogellenes behatolás: a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén,

[404] pl.: Elender-ügy, amelyben egy gimnazista fiú törte fel az Elender informatikai hálózatot 1999-ben.
[405] Forrás: http://einclusion.hu/2011-01-27/szamitogepek-otthon-2010/ (Letöltés ideje: 2012. 08. 06.)
[406] Hagyományos bűncselekménynek tartom például, amikor az elkövető magát valamelyik közüzemi szolgáltatónak kiadva becsönget emberekhez, és azoktól pénzt csal ki, vagy lop el. A többi vagyon elleni, életellenes, stb. bűncselekményről már ne is feledkezzünk meg, amely elkövetéséhez nem volt szükség a komputerekre.
[407] 2001. november 12-én Budapesten aláírt számítástechnikai bűnözésről szóló Egyezmény

- a jogellenes titokszerzés,
- védett számítógépes programok jogellenes másolása.

Az ET fakultatív listája, amely csak ajánlásokat tartalmaz, nem kötelező formában:
- A számítógépes adatok és/ vagy programok megváltoztatása
- A számítógépes kémkedés
- A számítógép jogellenes használata
- Védett programok jogellenes használata

A 2001 novemberében Budapesten aláírt „Számítástechnikai Bűnözésről Szóló egyezmény"[408] már újabb jogi normákat fogalmazott meg:

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

2. cikk: A jogtalan belépés
3. cikk: A jogtalan kifürkészés
4. cikk: Az adatok sértetlensége elleni cselekmény
5. cikk A rendszer sértetlensége elleni cselekmény
6. cikk: Visszaélés eszközökkel

II. cím: A számítástechnikai bűncselekmények

7. cikk: A számítástechnikai hamisítás
8. cikk: A számítástechnikai csalás: mindegyik aláíró fél vállalta, hogy megteszi azokat a jogalkotási lépéseket, amelyek szükségesek ahhoz, hogy a belső jogukkal összhangba bűncselekménynek minősüljön a másnak jogosulatlanul és szándékosan történő vagyoni károkozás.

Ez a vagyoni károkozásnak:
- vagy számítástechnikai adatok bevitelével, megváltoztatásával, törlésével vagy megsemmisítésével
- vagy a számítástechnikai rendszer működése ellen bármilyen más cselekménnyel anyagi haszonszerzés saját vagy más részére jogosulatlanul megszerzésére törekvés, melynek szándékosan kell megtörténnie.

III. cím: A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények:

9. cikk: A gyermekpornográfia
10. cikk: Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények

Az Egyezménnyel összhangban Magyarország a büntető törvénykönyvében a 300/C. § a Számítástechnikai rendszer és adatok elleni bűncselekmény tényállását felvette, valamint egyéb más törvényi tényállásokat kiegészített a meghatározottak szerint.
Az egyezményhez harminc ország csatlakozott.

Az egyik legfontosabb ilyen, az aláírókat kötelező jogszabály a Conviction on Cyber-crime, amit 2001-ben Budapesten írtak alá és a 2004. évi LXXIX törvénnyel hirdették ki.

[408] 2004. évi LXXIX. tv.

Az Egyezményben deklarálták, hogy „*minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek meghatározott bűnügyi nyomozás vagy büntetőeljárás érdekében… a jogkörök és eljárások megteremtéséhez szükségesek.*"[409]

Természetesen a fent említett, az ET minimum listája előtt, mely 1989-ben lett kidolgozva és a 2001-es Cyber Crime Egyezmény előtt és után, történtek még kísérletek a számítógépes bűnözés megállítására, az elkövetők szankcionálására. 2005-ben történt egy kiegészítése az Egyezménynek, amelyben többek között pontosan megfogalmazták, hogy mi a számítógépes bűnözés, ezzel összefüggésben a számítógépes bűncselekmények fellépésének eszközei és a tagállamok feladatai is meghatározásra kerültek.[410] Így tavaly, amikor Magyarország látta el az Európai Tanács soros elnökségi feladatait, nagy hangsúlyt kapott a szervezett bűnözés, és ezen belül a számítógépes bűnözés elleni fellépés.[411] Ennek keretében Magyarország belügyminisztere, dr. Pintér Sándor úr hangsúlyozta többek között, hogy a tagállamon belül együttműködésre és gyors reagálásra van szükség.

Az igazságügy-miniszterek 2011. április 12-i, luxembourgi hivatalos ülésén előterjesztették a Az informatikai rendszerek elleni támadásokról szóló COM(2010) 517 számú irányelvtervezetet, melynek célja, hogy korszerűsítse a 2005/222/IB kerethatározatot. Ez az iránytervezetben már szerepel, hogy bűncselekménynek minősítenék az eszközhasználatot, valamint kiterjed a lopott személyazonossággal való elkövetésre is, továbbá bűncselekménynek minősíti a számítógépes adatok ellopását. Valamint a gyermekek szexuális kizsákmányolását és a gyermekpornográfiát tartalmazó honlapokkal kapcsolatos teendőkre- így az ilyen tartalmú honlapok blokkolására, eltávolítására, vonatkozó szabályok megalkotását sürgetik

III. Ez elment vadászni, ez meglátta… az interneten elkövetett bűncselekmények és a szervezett bűnözés kapcsolata

A fentiek tükrében talán fölösleges is újra leírni, hogy a számítógép, az internet megjelenésével a szervezett bűnözés is terjeszkedni kezdett. A bűnözői csoportoknak is sikerült kihasználnia a nemzetköziséget, az anonimitást és minden egyéb, olyan jellemzőt, amely megkönnyítette a szervezettséget.

A szervezett bűnözés jellemzője többek között, hogy a legalább három személy bűnszövetségben áll egymással, de nem szükséges, hogy mindegyik tevékenyen részt vegyen az elkövetésben.[412]

A bűnözés e típusára jellemző még[413] a magasan szervezettség, így ezen belül az alá-fölérendeltség, a magasan képzett szakemberek bevonása, részvétele, érdekeltté tétele anyagilag, valamint a csúcstechnika igénybevétele.

Most csak nagyvonalakban fejteném ki a szervezett bűnözés és az interneten elkövetett bűncselekmények kapcsolatát, hiszen már maga a téma is, jellegéből adódóan akár külön tanulmányt érdemel.

A számítógépes bűncselekményeket az elkövetők elsősorban[414] anyagi haszonszerzési célzatból valósítják meg. Kis befektetéssel, ráfordítással hatalmas bevételre

[409] 2001. november 23-án kelt és Budapesten aláírt Számítástechnikai Bűnözésről szóló Egyezmény
[410] Forrás: http://eur-ex.europa.eu (Letöltés ideje: 2012. 08. 06.)
[411] Forrás: http://www.eu2011.hu/hu/hir/kiberbunozes-gyors-reagalasra-van-szukseg (Letöltés ideje 2012. 06. 22.)
[412] Btk. 137. § 13. pontja
[413] Forrás: http://bunmegelozes.uw.hu/szervezett.pdf (Letöltés ideje: 2012. 08. 06.) Dr. Szabó Henrik r. őrnagy

tehet szert, aki az interneten keresztül követ el illegális cselekményét. Sokszor elég, ha az elkövetőnek egyetlen számítógépe és egy normál sebességű internet hozzáférése van. Anélkül, hogy kimozdulna otthonából, irodájából képes lehet a világ bármely táján bűncselekményt elkövetni.

A pénzmozgatások, a pénzmosások leggyorsabb módja az interneten keresztül történik. Az ezt elvégzőnek nem kell elutaznia, ahhoz, hogy a bűncselekményből származó pénzt megmozgassa, eltüntesse vagy legálissá tegye.

Felismerték a bűnözők, hogy egy jól megszervezett csapattal, vagyis a mennyiség ne menjen a minőség rovására- sokkal jobban koordinálni lehet egy szervezetet.

A gazdasági bűncselekmények egyik jellemzője, a haszonszerzési célzat. A fehérgalléros bűnözők így a világhálón meg tudják találni számításaikat, azokat a személyeket, akikkel a bűncselekményt elkövetik és főleg azokat az embereket, akiket meg tudnak károsítani.

A lebukás veszélye kicsi, hiszen nem feltétlenül kell a személyes találkozás, a kilétük felfedése. Az anonimitás így nemcsak a hatóság előtt maradhat meg, hanem egymás előtt is, ami csökkenti a lebukás veszélyének kockázatát.

A fejezet címének adott gyermekmondókát épp a szervezett bűnözés, az interneten elkövetett bűncselekmények lehetséges kapcsolódása, egymás elősegítése miatt tartom ideillőnek.

III. 1. Ez elment vadászni…, a phising vagy adathalászat

Az *adathalászatnak* valamennyi számítógép felhasználó, használó, de még az azt nem használó is ki van téve. Az adathalászatnak 4 módszerét különböztetjük meg:

- VoIP- csalás, amikor telefonon keresztül kérnek meg úgy adatokat, hogy a telefonáló valamelyik pénzintézet alkalmazottjának adva ki magát technikai problémára hivatkozik és annak rendezéséhez szükséges.[415]
- Phising vagy adathalászat, amikor emailben kérik el a felhasználóneveket jelszavakat. Ezzel a cselekménnyel tudják megszerezni a bankok, szolgáltatók ügyfeleinek személyes adatait, bankszámla számukat, pénzforgalmukat. A legegyszerűbb és leghétköznapibb formája még a spamek[416] küldése, melyben, a pénzintézet nevében személyes adatokat, de néha még PIN kódokat, felhasználóneveket kérnek. A pénzintézetek hiába teszik közzé saját honlapjaikon, hogy sem emailben, sem telefonon keresztül nem kérnek adatokat, az ügyfelek a határozott fellépésnek vagy a pénzintézet honlapjának megtévesztésig külsőleg hasonlító üzeneteire gondolkodás nélkül kiadják a kért információt. Egy konferencián[417] a francia rendőrség arról számolt be, hogy egy hosszabb nyomozást követően Franciaországban olyan elkövetőt sikerült kézre keríteniük, aki egy éven keresztül a közösségi honlapokat felhasználva, arról adatokat gyűjtött (név, cím, születési adatok, esetleg még a jelszót is sikerült kitalálnia) és nevükben bankszámlákat nyitott vagy bankszámlájukhoz fért hozzá.

[414] Az anyagi haszonszerzés mellett még előfordulhat, hogy bosszúból, szexuális vágyak kielégítésére, vagy tudatlanságból követik el a bűncselekményeket, bár ezek kevésbé fordulnak elő.
[415] Nagy Zoltán: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009. 262. o.
[416] Kéretlen üzenetek, levelek
[417] Nemzeti Nyomozó Irodán 2010. november 16-17-18. tartott konferencia, melyet a bankkártya hamisítással kapcsolatban tartottak

- A harmadik módszer a spamek vagy kéretlen levelek küldése, melyben különböző kereskedelmi tevékenységekre hívják fel a figyelmet, vagy illegális oldalt reklámoznak, pl. filmek, zenék illegális letöltését.
- A kémprogramok, vagy spyware-ek a negyedik módja az adathalászatnak. Ezeket a programok a számítógépre telepítve a felhasználók internet használatát rögzíti, így többek között a felhasználó neveket, jelszavakat, melyek megszerzését követően, azokkal visszaélnek vagy eladják bűnözőknek.

A magyar büntető törvényünkben adathalászattal kapcsolatos tényállás nincs, de ha nevet, címet, felhasználónevet, jelszót illetéktelenek megszereznek, akkor elsősorban személyes adattal való visszaélésnek[418] minősíti a törvény. Ha, a megszerzett adatokkal élnek vissza, azzal belépnek jogosulatlanul mások rendszerébe, akkor a Btk. 300/C. § (1) bekezdése szerint minősülő, a számítástechnikai rendszer és adatok elleni bűncselekményt követi el a magyar Btk. szerint.

III/2. Ez meglátta… a piramisjáték szervezése

A Büntető Törvénykönyv 299/C. §-a szerint „*aki mások pénzének előre meghatározott formában történő és kockázati tényezőt is tartalmazó módon való összegyűjtésén és szétosztásán alapuló olyan játékot szervez, amelyben a láncszerűen bekapcsolódó résztvevők a láncban előttük álló résztvevők számára közvetlenül vagy a szervező útján pénzfizetést vagy más szolgáltatást teljesítenek…*”

A piramisjáték, vagy pilótajáték szervezője az, aki a játékot bővíti, szervezi. Ennek legegyszerűbb eszköze az internet.

De a bűncselekmény elkövetőjének minősül-e az is, aki a népszerű közösségi oldalakon megosztja a játékot, ajánlatot? Erre nézve nem lehet biztosan állítani sem azt, hogy az a felhasználó, aki megoszt egy „kedvező’ ajánlatot, tudatában volt azzal, hogy ez által a piramisjáték szervezője lesz. Viszont az ellenkezőjét már - esetleg a hatóság előtt - épp neki kell majd bebizonyítania.

A bűncselekmény elkövetési magatartása a játék szervezése. A bűncselekmény lényege mások pénzének összegyűjtés és újraosztása. A „játékban” résztvevők akkor részesülnek a beszedett pénzből, ha vagy a legelsők között csatlakoztak a rendszerhez vagy pedig az ismeretségi körükből minél több embert tudtak-, ahogy ők mondják- maguk alá szervezni, akiknek a befizetett pénzéből magas jutalékban részesülnek.

A bűncselekmény bizonyítása azért nehéz, mivel annak kitalálója, az ún. MLM rendszerhez hasonlóan építi fel a játékot. A kockázati tényezők fontos szerepet játszanak, amikről szó esik, akkor, amikor népszerűsítik, ajánlják a játékot.

A piramisjáték szervezése bűncselekmény vizsgálatára, nyomozására a Nemzeti Adó-és Vámhivatal (NAV) jogosult. Mégis sokszor nehéz annak elhatárolása, hogy egy adott bűncselekmény csalásnak vagy pedig piramisjátéknak minősül-e. A piramisjáték úgy épülhet fel, hogy a cég egy törzsvásárlói programot hirdet, amelyhez ingyenesen lehet csatlakozni. Ezt főleg a cég honlapján teheti meg. Itt a nevét vagy felhasználó nevet, valamint egy személyes azonosítót kell megadni. Ezt követően üzletekben, benzinkutaknál kedvezményt kap a vásárló. A vásárlásait, kedvezményeit egy ún. webirodán keresztül

[418] Btk. 177/A.§ (1) bek.

követheti nyomon. Amennyiben a belépő is ajánl valakit, úgy már az újonnan belépő után jutalékot kap.

Ahhoz, hogy esetleg a „piramisban" még fentebb kerüljön az szükséges, hogy minél több embert/ saját tagot vonjon be, valamint ezek az újonnan belépő személyek szintén vásároljanak. A belépőket és a beszervezőket érdekeltté teszik abba, hogy minél inkább egy nagy kiterjedésű hálózatot építsenek ki maguk alá, valamint abban is, hogy pénzért jogokat vásároljanak a belépők, ami által ők maguk alá is be tudjanak léptetni embereket.

Szükséges annak megállapítása a bűncselekmény bizonyítása érdekében, mivel a piramis játék kockázati tényezője egyértelműen az, hogy a törzsvásárlók nagyobb része a rendszerben nem vásárol, amiből keletkeznek a jogai és a jutalékai, hanem a jogokat ún. „foglalózással" szerzi meg, amiből azonban nem kerül bonusz és a jutalékok levonásra.

A hálózat építésének az a célja, hogy a kevés munkával minél több pénzt lehessen keresni, ám beígért meggazdagodás csak a felsőbb szinteken állóknak lehetséges. A rendszerben felhalmozott pénzeket, amiből a jutalékok és a bonusz jogok teljesíthető, csak vásárlás során keletkező kedvezményből lehet vissza osztani (mivel a rendszer felépítése a pénzek begyűjtése és újraosztása), így a vásárlás során származtatott jogoknak nem lesz fedezete és az új belépők és a törzsvásárlók külső forrás híján nem juthatnak a pénzükhöz.

Bizonyos esetekben egy-egy ilyen hálózatépítésre épülő rendszer esetében indul nyomozásnál bizonyítani kell, hogy a játék szervezőjének célja, hogy ha a rendszer eléri azt a szintet, amikor több lesz a foglalózó, mint a tényleges vásárló, nem generálódik jutalék és így csak akkor lehetne pénzt kivenni a rendszerből, ha a foglalózók vagy elkezdenek vásárolni, vagy újabb vásárlókat szerveznek be a rendszerbe.

A piramis játék szervezését tovább erősítheti az a tény is, hogy a gazdasági vállalkozásban természetes személy nem szerepel, hanem csak újabb offshore cégeket lehet fellelni, és amely cégek felé mindig nagyobb összegű kiutalásokat lehet találni.

Mind a két cselekményt haszonszerzési célzattal követik el, több sértett sérelmére ugyanúgy el lehet követni csalást is, mint a piramisjátékot. Ám a Btk. 299/C. §-ba ütköző cselekmény, mint ahogy a neve is elárulja, egy piramisszerűen felépített hálózat kiépülését célozza meg, ahol a szervezeti szinten alul állók pénzbeli hozzájárulásából finanszírozzák a szervezet fentebb, vagy épp a piramis tetején álló játékosokat. Azaz, a rendszer addig lehetne működőképes, amíg vannak új belépők, illetve a befizetések folyamatosak.

A rendszer addig működőképes, amíg újabb és újabb emberek lépnek be és érdekelté válnak a hálózat építésben.

A pilótajáték, vagy piramisjáték, annak ellenére, hogy évről-évre buknak meg a szervezőik, és mindig nagy tömegeket károsítanak meg, a mai napig fellelhető és sikeres a hiszékeny emberek között.

III/3. Ez meglőtte… a (számítógépes) csalás – SCAM

Az egyre kedveltebb, és egyre népszerűbb az online kereskedelem. Az egyszerű e-ügyintézés miatt az interneten elkövetett csalások száma is megsokasodott, hiszen az ügyfélkapukba történő belépéshez meg kell adni a felhasználóknak személyes adataikat, elérhetőségüket. Mivel a technikára igen, de a védelemre már kevesebb pénzt költenek a felhasználók, valamint adataikat is felelőtlenül adják ki, így a csalóknak mindig zöld utat engednek, hogy elkövessék a cselekményüket.

Annak ellenére, hogy több európai uniós ország is a büntető törvénykönyvében megkülönbözteti a „hagyományos" csalás tényállását az internetes csalásokétól, valamint a már említett ET 89. számú ajánlása és a Számítógépes Bűnözésről szóló Egyezmény is meghatározza a számítógépes csalás fogalmát, a magyar büntetőjog külön nem nevesíti a tényállást, ám a Btk. 300/C.§ (3) bekezdése szerint:

„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.…"[419]

Ezt a szakaszt sokan az „új" számítógépes csalásnak is nevezik. Álláspontom szerint és a következőkben leírtak alapján nehezen, de végeredményben megállhatna egy gyanúsításban. Ennek a tényállásnak a jogi tárgya a számítástechnikai rendszerben tárolt, továbbított, feldolgozott adatok megbízhatóságához fűződő jogi érdek, vagyoni, gazdasági értelemben. Az elkövetési tárgy a számítógépen tárolt valamint feldolgozott, továbbított adat. Az elkövetőnek valamilyen speciális szaktudással vagy ismerettel kell rendelkeznie ahhoz, hogy a cselekményt szándékosan elkövesse.

Viszont, ami miatt hétköznapiasan szólva kilóg a lóláb, az az, hogy amikor felsorolásra kerülnek a csalások típusai, akkor egy-két esetet leszámítva nem valósul meg a 300/C. § (3) bekezdése. Hiszen ahhoz, hogy valaki a későbbiekben nevesített „nigériai levelet" küldjön, vagy telefonos csalást kövessen el, nem kell, hogy jogosultsággal rendelkezzen számítástechnikai rendszer felett, és abban bármilyen adatot megváltoztasson.

Így amennyiben a rendőrséghez olyan feljelentés érkezik, amelyben nem valós aukciós oldalon vagy piactéren vásároltak, vagy pénzt, adományt kértek, úgy a kárértéktől, az elkövetők számától függően a Bt. 318.§-ba ütköző csalás bűncselekménye miatt indul meg a nyomozás.

A számítógépes csalások fajtái:

- Telefonkártyás csalások: az elkövető(k) felhívják a sértettet a telefonszolgáltatójuk vagy más társaság nevében nyerési lehetőséget kínálva úgy, hogy ha azonnal vásárolnak feltöltő (telefon)kártyát és annak a hátoldalán lévő kódot beolvassák nekik. Természetesen a megadott kód után a nyereményt nem kapja meg a játékos.
- Spanyol vagy holland lottó: telefonon vagy e-mailben értesítik a „szerencsés" személyt egy nyereményről vagy külföldi örökségről, amelyben személyes adatokat, számlaszámot kérnek, amire majd a pénzt át tudják utalni. A bankkártya adatain kívül kérik az ahhoz tartozó PIN kódot, személyigazolvány fénymásolatot is stb.. A gyanú elkerülése érdekében egy esetleg létező (külföldi) ügyvédi iroda nevében történhet mindez. Az így megszerzett adatokkal jobb esetben az áldozatuk számláján lévő pénzt leemelik, de előfordulhat, hogy adatival visszaéléseket követnek el.
- Spamek (kéretlen levelek, levélszemét) küldésével, amely esetében sokszor úgy tűnik, mintha egy véletlenül félrement e-mailt kapna az áldozat, melyben valamilyen nyerési lehetőségre, illegális tartalmú weboldalra hívják fel a figyelmet. Az adathalászatnál is megemlítettem a spameket. Tulajdonképpen ez a Jolly Joker, melyet valamennyi bűncselekményhez fel tudnak használni.

[419] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=97800004.TV

- Sokszor kihasználják a magányos, társkereső embereket, akiket az általuk feladott partnerkereső hirdetésekből választanak ki. Esetleg arra, hivatkozva, hogy szeretnének találkozni az illetővel, de pénzt kérnek az utazáshoz, amit természetesen a „találkozás" létrejötte alkalmával azonnal visszafizetnek. Előfordulhat azonban az is, hogy a sértett bizalmába férkőzve, magányosságát kihasználva még több pénzt kérnek.
- Aukciós csalások: a csalók hirdetéseket adnak fel az interneten, melyben ingóságot- pl. autót, mobiltelefont, órát…stb. –vagy ingatlant kínálnak megvételre igen kedvező áron. Néhány esetben az ár jóval a piaci alatt van, ennek ellenére az érdeklődőben nem kelt gyanút és felveszi a kapcsolatot az eladóval illetve licitál rá. A csalás kétféle módon történik meg, még vagy az áruért előre fizetett összeg átutalása vagy átadása után a dolgot nem kapja meg a vevő vagy pedig ha meg is kapja, akkor az nem az, amiért fizetett (pl.: totálkáros az autó, vagy hamis vagy hamisított értéktárgy illetve a minősége messze elmarad a feltüntetettől.) [420]
- Nigériai levelek (SPAM-419[421]): Afrikából, főleg Nigériából érkező emailek (korábban levelek, faxok voltak), amelyben egy menekült táborban élő személy segítséget kér, ahhoz, hogy a jelenlegi rendszer által zárolt külföldi számláján lévő pénzéhez hozzájusson. Mivel a segítséget kérő az országában dúló harcok miatt nem tud elutazni, így a megkeresett személyt kéri meg arra, hogy ezt tegye meg helyette és ezért cserében a bankszámlán elhelyezett pénz bizonyos részét megtarthatja. De azért bizonyos összeget, egy megadott külföldi bankszámlára el kell helyeznie a sértettnek, hogy úgymond érdekében álljon a majd felvett összeget a szegény sorsú fogolynak átadni. Ezek a nigériai csalások sokszor annyira kecsegtetőek és a segítséget kérők annyira meggyőzőek, hogy nehéz ellenállni. A nigériai csalásokat olyan alapossággal készítik elő, hogy egy valós személy nevét használják fel, így a sértett még ha, ellenőrzi is az interneten a történetet, az állítások igaznak fognak tűnni.
- Adománygyűjtések: beteg, egyedül élő, szegény sorsú emberek nevében vagy egy segítő alapítványként adományokat gyűjtenek. Ezek az adomány-kérések lehetnek pénzbeli vagy valamilyen, főleg nagy értékű tárgyra irányulóak. A közösségi oldalak a legmegfelelőbbek arra, hogy „népszerűsítsék" tevékenységüket. A képek vagy valós személyt ábrázolnak, vagy pedig egy reklámfotót, kampányfotót használnak fel.
- Hamis vírusellenőrző programok: az internet történő munkavégzés közben a felhasználót arról értesítik, hogy vírust található a gépen. Ennek ellenőrzése során a rendszer egy kis részében tényleg megtalálja a felhasználó. Az ellenőrző program ezt követően egy 60-80 euróért megvásárolható programot kínál, ami kiírtja a vírust. Ebben az esetben két dolog történhet, vagy a gép az adott vírustól tényleg mentes lesz vagy pedig egy újabb vírust juttat a számítógépre.

A fent nevezett csalások még feltehetőleg meg sem közelítik valamennyi módszert, melynek köszönhetően pénzünktől vagy adatainktól fosztanak meg az elkövetők.

[420] Nagy Zoltán András: i. m.
[421] A SPAM-419 a nigériai büntetőtörvénykönyv 419.§-áról kapta a nevét, amely a csalás tényállása

Az említett csalások jellemzői összefoglalva: a technika kínálta lehetőségeket az elkövetők maximálisan kihasználják. Az általuk kínált árukat, szolgáltatásokat fényképekkel, okiratokkal dokumentálják.

- jóval több sértettet érint, mint a hagyományos csalások esetében
- a cselekmények és a sértettek felderítése nehezebb, mint a hagyományos csalásoknál
- az elkövetők beazonosítása nehéz, hiszen az internet szabadságot és anonimitást biztosít
- az állandó, hatósági figyelmeztetések ellenére is, a könnyelműség, figyelmetlenség miatt még mindig sok ember adja meg személyes adatait (nevét, email címét, lakcímét), amelyeket a csalók fel tudnak használni

Mivel úgy tűnik, hogy jelenleg a jogalkotók megelégednek azzal, hogy nem kívánják külön nevesíteni valamint eltérően büntetni a csalást és az internetes csalást, így az elkövetés módszerében az *interneten* szóval a nyomozó hatóság révén a gyanúsítás szövege alapján kerül megkülönböztetésre a hagyományos csalástól.

III/4. Ez hazavitte… a bankkártyával való visszaélés, bankkártya hamisítás

Az utóbbi években egyre inkább terjed a bankkártyák[422] népszerűsége. Mind a bankok, mind az állam egyre inkább ajánlja, támogatja azok használatát. Mára már nemcsak pénzfelvétel alkalmával, hanem kereskedelmi, szolgáltató egységekben, valamint az interneten történő vásárláskor, szállodai szobafoglaláskor is egyre többször vesszük kezünkbe a kis plasztikkártyánkat.

A bankkártyával való visszaélés bűncselekménye a Btk.-ban a Készpénz-helyettesítő fizetési eszközzel való visszaélés.[423] A bankkártya adatainak és a felhasználó adatainak megszerzése:

- bankkártya ellopását követően, amely mellett sokszor megtalálható annak PIN kódja, használták fel
- hamis, vagy hamisított kártya használata, amely esetben például egy, a banki terminálon (POS terminál) elhelyezett igen kisméretű eszköz segítségével szerezték meg az eredeti kártya adatait- ún. skimming módszerrel lemásolják
- internetes vásárláskor szerezték meg a bankkártya adatokat.
- email-en vagy spaman keresztül az áldozatoktól beszerzik a felhasználó nevüket és jelszavukat, a bankkártya PIN kódját
- telefonon keresztül szerzik meg az áldozatok adatait

A bankkártya hamisítás illetve az azzal való visszaélés olyan mértékben vált bűncselekménnyé, hogy a bankok, épp azért mert sokszor viselték ők az okozott kárt, a rendőrséggel összefogva, őket segítve küzdenek a bűncselekmény ellen.

A bankkártyával való visszaélés bűncselekményének jellegzetességei:

- az elkövetők főleg bűnszervezetben dolgoznak

[422] Mi is az a bankkártya? Ez egy olyan, a nemzetközi szabványnak megfelelő 85x54 mm-es műanyag kártya, mellyel a hátoldali mágnescsíkon vagy újabban az előlapi mikrochipen tárolt adatok segítségével, a kártyabirtokos (elektronikus vagy okmánnyal igazolt) azonosítását követően bankszámlaműveletek, tipikusan fizetés végezhető (Forrás: http://www.bankkartya.hu/?oldal=alapok_def, letöltés ideje: 2012. 06. 13)

[423] Btk. 313/C. § (amelyet az 1994. évi IX. törvény 27.§-a iktatta a Büntető törvénykönyvbe)

- a nemzetköziség, vagyis sokszor nem az adatlopás helyén követnek el visszaéléseket, hanem akár másik országból, vagy kontinensről kap értesítést a sértett, hogy visszaéltek bankkártyájával
- a sértetteknek nagyobb kárt okoznak, mint a hagyományos vagyon elleni bűncselekmény elkövetésénél
- az adatok megszerzését követően akár hosszabb idő is eltelhet, mire észreveszik az elkövetést
- az előző pont miatt a rendőrségi felderítés sokkal nehezebb, speciális szaktudást és türelmet igényel az elkövetők kézre kerítése
- az elkövetéshez használatos eszközök akár interneten keresztül is, megvásárolhatóak
- az elkövetés módja változatos, vagyis a bankkártya ellopásától és felhasználásától kezdve a skimming-gel történő kártyamásoláson át egészen a hamis honlapokon keresztül.

A bankkártya hamisítást elkövetői főleg orosz, ukrán, román, bolgár és magyar állampolgárok. A bankkártya hamisítókra a bűnszervezet jellegzetességei vonatkoznak. Megfigyelhető a hierarchia. A szervezeten belül munkamegosztás működik, vagyis, van aki, megszerzi a bankkártya adatokat. Vannak a szervezetben olyan személyek, akik beszerzik a hamisításhoz szükséges berendezéseket, eszközöket, és végrehajtják a hamisítást.[424] A szervezet legfelső szintjén pedig azok állnak, akik a hamisításhoz szükséges pénz biztosítják, a munkát felügyelik. Sajnos a bankkártya hamisításhoz szükséges eszközöket, berendezéseket, szoftvereket az internetről könnyen be lehet szerezni, meg lehet vásárolni. Főleg Kína ezeknek a lelőhellye.

III/5. Ez az ici-pici mind megette… a pénzhamisítás

A technika fejlődésével a pénzhamisítás is egyre jobban fejlődött, a forgalomba került hamis vagy hamisított pénzek felismerése is nehezebbé vált.

A színes fénymásoló használatával készült pénzek azonos sorozatszámuk miatt, vagy a vízjel hiánya és a papír minősége miatt könnyen felismerhető volt, a XXI. században az adatfeldolgozó egységgel kiegészített fénymásolók, szkennerek tökéletesítették a hamis pénzek nehezen felismerhetőségét, valamint a hamis okiratok készítését.

Gondot már „csak" az alapanyagok beszerzése okozhat, hiszen az eredeti pénz egy speciális alapanyagból, eljárással készül. De a világhálón erre is lehet igen nagy valószínűséggel megoldást találni.

A magyar Büntető Törvénykönyv a 304.§ (1) bekezdése alapján: *„aki:*
a) pénzt forgalomba hozatal céljából utánoz vagy meghamisít
b) hamis vagy meghamisított pénz forgalomba hozatal céljából megszerez, az országba behoz, onnan kivisz, az ország területén átvisz
c) hamis vagy meghamisított pénzt forgalomba hoz…"[425]

A pénzhamisítás jogi tárgya a pénz és az értékpapír forgalomba hozatala. A bűncselekmény elkövetési magatartása:

[424] P. Nagy Ferenc: A számítástechnikai bűnözés elleni harc. Belügyi Szemle 2004. 11/12. szám
[425] Btk. 304.§ (1) bekezdés a pénzhamisítás tényállása

- utánzás,
- meghamisítás,
- megszerzés,
- forgalomba hozatal.

Mivel a számítógépes környezetben elkövetett bűncselekményeket vizsgálom, így ki kell térni a pénzhamisítás kísérletére is. Vagyis, *aki pénzhamisításhoz szükséges anyagot, eszközt, berendezést vagy számítógépes programot készít, megszerez, tart, átad, forgalomba hoz, vagy azzal kereskedik...* [426]

Az elkövetés tárgya pénzhamisításhoz szükséges anyagok, eszközök, berendezések vagy számítógépes programok.

Tehát a kísérlete a pénzhamisításnak nagy valószínűséggel számítógépen vagy számítógéppel történik. Így ez a törvényi tényállás miatt, amikor pénzhamisítás gyanúja merül fel, akkor mindenképpen szükséges, hogy házkutatás alkalmával valamennyi számítástechnikai berendezést lefoglalásra kerüljön és azokat szakértői vizsgálatnak alá kell vetni. Ugyanakkor a Btk. kommentár szerint, amennyiben az átadás, forgalomba hozatal, kereskedés célzat nélküli, úgy az nem alkalmas a bűncselekmény megállapítására!

A pénzhamisítást főleg bankjegyekre követik el. Ilyen formában a címlet megváltoztatása fénymásoló, számítástechnikai eszköz vagy egyéb módszer segítségével. Sokszor annyira tökéletes másolatokat készítenek, hogy észrevenni is csak speciális eszközzel lehet.

IV. A rendőrség szerepe az interneten elkövetett gazdasági bűncselekmények nyomozásában

A számítástechnika ismerete elengedhetetlen követelmény a rendőri munkában. De, nemcsak az alapvető, felhasználói szintű ismeretre van szükség ahhoz, hogy sikeresen fel tudjuk venni a kesztyűt a számítógépes bűnözés elleni harcban, hanem akkora tudás elérése legalább, amekkorával a számítógépes bűnözők rendelkeznek. Mivel az internetes bűncselekmények nem csak Magyarországot, hanem a világ valamennyi államát érinti, így elengedhetetlen a rendszeres kapcsolattartás más országok szerveivel. A szoros, aktív és rendszeres együttműködésre, akár évente több alkalommal való konferenciák megtartására is szükség van. A konferenciákon a vezetőségen és a szakirányítást ellátó tiszteken kívül a végrehajtó állománynak is részt kellene vennie.

Az újabb és újabb elkövetési módszerek állandó ismertetése, valamint az Európai Unión bűnüldöző szervein belül is aktívabb kell, hogy legyen. Mivel a témaválasztásom a gazdasági bűncselekményeket érinti, így a hitel-és pénzintézetekkel és a Pénzügyi Szervek Állami Felügyeletével (PSZÁF) történő folyamatos kapcsolattartás, a felbukkanó hamis okiratok, bankkártyák, az elkövetésre irányuló kísérletekről szóló pontos dokumentálást is megemlíteném.

A gazdasági válság ma is érezteti hatását, az elkövetők nem feltétlenül bankrablással akarnak pénzt szerezni, hanem mára már a kifinomult módszerek élveznek előnyt.

[426] Btk. 304/A. § a pénzhamisítás elősegítése