

Számítógépes Bűnözés (2004)

Bevezetés

Napjainkban a számítógépek és szoftverek behatoltak az élet valamennyi területére és az emberi tevékenységek valamennyi szférájában jelentős szerepet játszanak. A tudományos - technikai haladásnak azonban káros mellékhatásai is vannak: új, a társadalomra egyre nagyobb veszélyt jelentő bűncselekményfajtákkal kell szembenéznünk. Az információtechnológia robbanásszerű fejlődése következtében a jogalkotás csak késve tudott reagálni a technológia kihívásaira. Az informatika által nyújtott előnyökkel visszaélő személyek ezt oly módon igyekeztek kihasználni, hogy olyan cselekményeket valósítottak meg számítógép segítségével, amelyeket a jog nem szancionált: megjelent a számítógépes bűnözés. A számítógép egyrészt eszközévé vált egyes már korábban ismert bűncselekményeknek, másrészt újabb, a társadalomra veszélyes cselekmények megjelenését is előidézte. A számítógép és az internet igencsak megkönnyíti a bűnelkövetők dolgát, hiszen anonimitást és az elkövetési hely megválasztásának szabadságát biztosítja számukra, megnehezítve a nyomozást. Az Internet 1990-es években való rohamos elterjedése új dimenziókat nyitott a számítógépes bűnözés előtt. Az Internetre kapcsolódott személyi számítógépek, szerverek mindegyike potenciális célponttá válik a számítógépes bűnözők számára, akik megfelelő szaktudás és szoftverek birtokában dollármilliók károkat okozhatnak egyes iparágaknak. Például a távközesi műholdak közötti adatforgalom zavarásával, megbénításával világméretű kommunikációs zavarokat idézhetnek elő.

Dolgozatom fő irányvonalát a számítógépes bűnözés és az Internet kapcsolatának bemutatása képezi, emellett kitérek olyan számítógépes bűncselekmények rövid ismertetésére is, amelyek a globális kommunikációs hálózaton kívül manifesztálódnak, nincsenek érdemi kapcsolatban az Internettel.

I. Fejezet

1. A számítógépek történeti fejlődésének általános bemutatása, az Internet létrejötte

A számolás nehézségeit az emberek a különböző történeti korszakokban különbözőképpen igyekeztek könnyíteni. Kezdetben kavicsok és földbe karcolt vonalak segítségével próbáltak számolni. A számolást segítő eszközök közül az első az abakusz volt, amely huzalokon mozgatható fagolyókból áll.

A skót Napier nevéhez fűződik a logaritmus felfedezése és kidolgozása. Wilhelm Shickard 1623-ban olyan eszközt épített, amely fogaskerekei és fogaslécei segítségével összeadott, kivont, szorzott, osztott.

Az első mechanikus működésű, digitális számítógépet Charles BABBAGE hozta létre 1822-ben, az angol kormány megbízásából.

Hermann Hollerith alkalmazta először a lyukkártyát statisztikai adatok tárolására 1890-ben, ezzel megalapozta a gépi adatfeldolgozást. Hollerith készüléke volt az első lyukkártyás számítógép.

A XX. század 30'-as éveiben Konrad Zuse fejlesztette ki a digitális programvezérelt számítógépet, amely már bináris számrendszert használt. A számítógépek gyors fejlődését gátolta, hogy a velük kapcsolatos kutatásokat titokban tartották, ezért a tudósok egymástól függetlenül dolgoztak.

1946 februárjában mutatta be a pennsylvaniai egyetemen John Mauchly és Presper Eckert az első elektroncsöves számítógépet, az ENIAC-ot. Ugyanebben az évben csatlakozott Eckertékhez a magyar származású Neumann János, aki azt javasolta, hogy a programot ne külső információhordozón, (lyukkártyán, lyukszalagon) hanem magában a gépben, annak központi tárolójában helyezték el. A mai, modern számítógép alapelvét tehát Neumann János dolgozta ki, aki elméletével megteremtette a számítógépek ipari méretekben történő gyártásának lehetőségét. 1958-ban az elektroncsövet felváltják a tranzisztorral, amelynek következtében lényegesen csökkenthető volt a gépek nagysága és energiafogyasztása.

A számítógépek tömeges elterjedése a 60'-as évek végére tehető amikor már olyan számítógépeket építettek, amelyekben integrált áramkörök is voltak, ezek nagyságának csökkenése és összeépítésük eredményezte 1971-től a mikroprocesszorok - chipek - megjelenését.

1.1 Az Internet

Az Internet nem más, mint kisebb kiterjedésű számítógépes hálózatokból (LAN) álló globális, bolygónk mintegy kétszáz országára kiterjedő hatalmas rendszer, világméretű számítógépes hálózat.

A rendszer magva a hatvanas évek elején az USA-ban alakult ki, ahol a Védelmi Minisztérium anyagi támogatásával indított ARPA kutatási program keretében az egymástól távoli számítógépeken keresztül történő adattovábbítás lehetőségeit vizsgálták. A fejlesztők a digitális adatok rendszeren belüli átvitelére csomagkapcsolt átviteli rendszert használtak. Ez azt jelenti, hogy az adatok szabványos csomagokra bontva jutnak el az egyik géptől a másikig. A csomagok mindegyikének elejére egy fejrész kerül, amely a feladó és a fogadó címét, a csomag sorszámát és néhány járulékos információt tartalmaz. A gépek közötti út lehet a hagyományos telefonkábel, de ma már inkább üvegszál kábel és földi vagy műholdas mikrohullámú távközlési csatorna.

Az Internet születését általában akkortól számítják, amikor 1969-ben a Los Angelesi Egyetem Network Measurement Center részlegének számítógépét összekötötték a Stanford Research Institute számítógépével, az ARPANET hálózat segítségével. Az ARPANET egyes egyetemek, tudományos intézetek, és katonai kutatólaborok összeköttetésével megteremtette a tudósok részére az adat- és véleménycsere lehetőségét. A potenciált felismerve más egyetemek is létrehoztak ilyen alapon működő, de egymással még össze nem kötött hálózatokat. Ezeket kötötte össze végül 1988-ban a National Science Foundation és magáncégek segítségével készült NFSNET 13 nagy sebességű

gerincvezetéke. Az ARPANET katonai részét elkülönítették és egyesítették a Defense Data Network-kel, a maradékot pedig beolvasztották az NFSNET-be. Így jött létre a ma ismert Internet alapja, amelynek költségeit kezdetben az Egyesült Államok viselte, majd fokozatosan átvették a kereskedelmi szolgáltatók.

Az Internet felépítéséből következően a világméretű hálózat kisebb, regionális hálózatok (WAN) halmaza, amelyek pedig maguk is még kisebb kiterjedésű hálózatokból (LAN) épülnek fel.

Az Internet maga nem jelenik meg olyan egyértelmű szolgáltatási formában a felhasználónak mint a telefon vagy a rádió, többféle felhasználási lehetőség alakult ki. Ezek közül a lényegesebb szolgáltatások a következők:

- Archie - szoftverkereső szolgáltatás
- E-mail - elektronikus levelezés
- Finger - hálózati felhasználók adatszolgáltatása
- FTP - távoli gépek közötti állománycsere
- Gopher - menürendszerű adatforrás tallózó
- IRC - többcsatornás, többirányú párbeszédéses kapcsolat
- Talk - kétirányú párbeszédéses kapcsolat
- WWW - hypertext és multimédia alapú Gopher

Az ezen szolgáltatásokkal kapcsolatos bűncselekmények sorolhatók tehát az internetes bűnözés tárgykörébe.

Mivel az Internet hatalmas kiterjedésű, központi gép nélküli önszerveződő rendszer, ma már gyakorlatilag nincs lehetőség arra, hogy bármilyen kormány vagy szervezet a rajta folyó tevékenységet lehetetlenné tegye, korlátozza, vagy cenzúrázza. Ennek következtében az információs szabadságjogok megtestesítőjévé vált és általa leomlott minden fölrajzi akadály az információk szabad áramlása, a távollevők közti kapcsolattartás, a különböző ügyletek lebonyolítása, a szolgáltatások nyújtása és igénybevétele előtt.

1.2 A számítógép fogalmi ismérvei, a jelenlegi számítógépkategóriák

A számítógép információfeldolgozó gép, amely lényegét tekintve három rendszer összessége: információs rendszer, hardver rendszer, és szoftver rendszer.

A számítógépeket teljesítőképességük-rendeltetésük alapján lehet csoportokba sorolni:

- házi számítógép - egyszerűbb, játékprogramok futtatására alkalmas gép
- személyi számítógép - PC- egy személy használatára szolgáló asztali vagy hordozható gép. Ebben a kategóriában kisebb és nagyobb teljesítményű gépek egyaránt előfordulnak.
- munkaállomás - workstation- nagy teljesítményű asztali gép, amely hackerek célpontja lehet a merevlemezen tárolt információk jellegétől függően.

- Nagygép -mainframe vagy szerver- nagyobb méretű gép, amely egyszerre több(száz)ezer felhasználó kiszolgálására képes. Szintén hackercélpont lehet.

2. A számítógépes bűnözés története és ismérvei

2.1. Jelentősebb számítógépes bűncselekmények kronológiája

Az egyik első számítógéppel elkövetett bűncselekmény az egyesült államokbeli Walston and Co. alelnöke által elkövetett sikkasztás, aki - nem kevés fizikai munkával - hamis lyukkártyákat készítve 50 000 dollárt szerzett az ötvenes évek végén. Ebből az időből származik a az egyik legtetemesebb kárt okozó csalássorozat, amelyet 1963-74 között követtek el. Az Equity Funding Corporation számítógépeivel a cég munkatársai hamis kötvényeket készítettek, amelyekre fiktív kifizetéseket eszközöltek. Hatvannégyezer fiktív biztosítási kéresetért kétfélmillió dollárt fizetettek ki a társasággal.

Az Amerikai Egyesült Államokban a távadat-átviteli hálózatok elterjedéséig évente csak néhány esetet regisztráltak, azok is belső személy által elkövetett számítógépes csalások voltak. A jelentősebb növekedés a hetvenes évektől volt tapasztalható, Európában a nyolcvanas évek közepétől vált általánossá. Mindez természetesen összefügg a számítástechnikai alkalmazások rohamos elterjedésével.

1971-ben a Turner-Curtis banda néven ismert amerikai alvilági szervezet komputerszakembereket helyezett el hamis néven több banknál, akik egy sor komputer-bűncselekményt követtek el. A kaliforniai Newport National Bankot például 200 000 dollárral károsították meg.

1978-ban egy Stanley Mark Rifkin nevű számítástechnikai tanácsadó az egyik ügyfélszámlaszámról a hozzárendelt kódszám azonosításával 10.2 millió dollárt utaltatott át magának.

1985 márciusában a Los Angeles-i víz-és energiaügyi részleg számítógépeit a vírusok egyik fajtája, egy logikai bomba bénította meg.

1988-ban egyetemi hallgatónak sikerült behatolni az USA Védelmi Minisztériumának kommunikációs, ún. Arpanet állomásába. A rendszerbe beültetett vírus szaporodott, és több mint hatezer számítógépet bénított meg.

1989-ben indították útjára az egyik legismertebb számítógépes vírust, a Péntek-13-at, amelynek az volt a feladata, hogy törölje a számítógépek merevlemezének boot szektorát, s ezáltal működésképtelenné tette a komputert. Szintén ebben az évben német hackerek hatoltak be amerikai, angol és más külföldi számítógépes rendszerekbe, és az így szerzett információkat eladták a KGB szovjet titkosszolgálatnak.

Vlagyimir Levin az orosz maffia megbízásából 1994-ben Szentpétervárról negyven alkalommal tízmillió dollárt hívott le az egyesült államokbeli Citibank számláiról, és a pénzeszegeket holland, finn, stb. bankok számláin helyezte el.

A '90-es évek elejétől a számítógéppel kapcsolatos bűncselekmények köre kibővült, az elkövetések száma - mind a mai napig kitartó emelkedést mutat. A bűnözés palettáján megjelentek a számítógépes adatbázis adatainak manipulálásával megvalósított csalások,

a számítógépes hamisítások, a számítógépes rendszerek biztonsági-védelmi falának feltörésével és a tárolt adatok jogtalan megszerzésével megvalósított támadások, a szoftverek illegális másolása és terjesztése, a számítógépek adatszállító vezetékének és elektromos berendezéseinek lehallgatása, hamis bankkártyák és telefonkártyák készítése és felhasználása, a mobil telefonkészülékek "klónozása".

2.2 A számítógépes bűnözés általános jellemzői

A számítógépes bűnözés meghatározásával kapcsolatban a szakemberek körében még ma is létezik egy definíciós dilemma, és a létező megfogalmazások sem rendelkeznek tiszta körvonalakkal. A jogirodalom egy szűkebb és egy tágabb meghatározást alkalmaz a számítógépes bűnözés fogalmára vonatkozóan. A tágabb értelmezés szerint minden olyan büntetendő cselekmény, amelynek célja vagy eszköze az elektronikus adatfeldolgozás. A szűkebb értelmezés szerint olyan jogellenes vagyoni károkozást, jelent, amelynél elektronikus adatfeldolgozási adatokat szándékosan megváltoztatnak, megsemmisítenek, jogosulatlanul megszerzik és felhasználnak, vagy elektronikus adatfeldolgozó eszközzel együtt jogosulatlanul használnak. Egy másik definíció szerint a számítógépes bűnözés fogalma úgy határozható meg, mint azon bűncselekmények összessége, amelyek információtechnológiai eszközök, rendszerek, illetve rendszerelemek ellen irányulnak, vagy információtechnológiai eszközöket, rendszereket használnak a bűncselekmény elkövetésének eszközeként⁷.

A számítógépes bűncselekmények legjellemzőbb tulajdonsága a rendkívül változatos elkövetési módok. Az adott bűncselekmény a régi maradt, - lopás, csalás stb - csupán új formát öltött a technikai eszközök révén.

2.2.1 A latencia

A latencia igen magas ennél a bűncselekményformánál egyfelől jellegéből adódóan - elkövetési mód stb. - másrészt az elkövető mindent megtesz, hogy tevékenységét leplezze nemcsak a nyomozhatóságok, hanem a sértett előtt is. A számítógépes bűncselekmények láthatatlansága számos tényezően alapul. Az ismertté vált számítógépes bűncselekmények a valóban elkövetett cselekményeknek mintegy 1-10 százalékát teszi ki.

A fejlett technika biztosítja, hogy a számítógépes bűnözést nagyon nehéz felderíteni. Előfordulhat olyan eset, amikor csupán néhány másodpercet vagy századmásodpercet vesz igénybe az elkövetési magatartás kifejtése. Egyetlen billentyű lenyomásával olyan adatok törölhetőek vagy módosíthatóak, amelyek vagyoni értéket testesítenek meg, vagy bizonyító erővel bírnak. Ezekben az esetekben az áldozatokat gyakran a bűnüldöző szervek tájékoztatják arról, hogy számítógépes bűncselekményt követtek el velük szemben.

A latenciát az is erősíti, hogy a bűncselekmény elkövetője és a bűncselekmény megvalósulásának helyszíne térben és időben is különválhat. Az elektronikus betörő nem jelenik meg fizikai valójában az elkövetés helyszínén, nem azonosíthatja tanú. Ezen

tényezők nagymértékben megnehezítik a bűncselekmény felderítését, bizonyítását. A latenciához hozzájárul az a körülmény is, hogy az elektronikus támadással érintett pénzügyintézetek - bankok biztosítók, nyugdíjpénztárak - a támadások felderítésében nem mindig együttműködőek a nyomozó hatóságokkal. Jó híréket féltve általában be sem jelentik, ha bűncselekmény érte őket.

A latencia oka a számítógépes programok, szoftverek engedély nélkül történő másolása, használata, forgalmazása is, amely egyre inkább társadalmi méreteket ölt.

2.2.2. Az elkövetői oldal

A számítógépes bűncselekmények elkövetői általában magas szakértelemmel bíró, nemegyszer foglalkozásuknál, beosztásuknál fogva valósítják meg a bűncselekményt, tipikus fehér galléros (white collar) bűnözők. A fehérgalléros bűnözésen belül a szakirodalom különbséget tesz foglalkozási (occupational) és szervezeti (corporate) bűnözés között. Foglalkozási bűncselekményekről beszélünk abban az esetben, amikor az elkövető munkakörét felhasználva saját magának szerez vagyoni előnyt, vagyoni hasznot számítógép felhasználásával. Erre példa a magyar büntető-törvénykönyvben a dematerializált értékpapírra elkövetett lopás (Btk. 333.§) lopás (Btk. 316.§), a sikkasztás (Btk. 327.§), a számítógépes csalás (Btk. 300/C.§) stb. Szervezeti bűncselekményeket a szervezet érdekében, a szervezet számára biztosítandó előny, vagyoni haszon eléréseért követnek el.

A számítógépes bűnözők fontosabb jellegzetességei:

- életkorukat tekintve főleg a fiatalabb korosztályhoz tartoznak, legtöbbször 18-35 év közötti,
- rendkívül kevés közöttük a nő,
- kvalifikált, jól képzett személyek, gyakran amatőr bűnözők,
- legtöbbször cég alkalmazottja, akinek módjában áll bizalmas értesüléseket szerezni a működtetett számítógépes rendszerről, a rendszerhez való hozzáférés lehetőségeiről, (rendszergazdai, operátori munkakört betöltő személyek)
- az elkövetők általában első büntényesek

II. Fejezet

A számítógépes bűncselekmények szabályozási rendszere

1. A számítógépes bűnözésel szembeni nemzetközi fellépés, a számítógépes bűncselekmények osztályozására tett kísérletek

Nemzetközi téren a számítógépes bűnözéssel szembeni első jelentős lépésnek az OECD (Gazdasági Együttműködési és Fejlesztési Szervezet) kezdeményezése tekinthető, mely szervezetnek az erre a célra alkult ad hoc bizottsága 1983 és 1985 között széles körű felméréseket végzett az európai államok joggyakorlata területén és tapasztalataikat összegezve közzétette a büntetőjogi reformokat sürgető jelentését "Computer related Crime: Analysis of legal Policy" címmel. A cél a számítógépes környezetben elkövetett bűncselekmények kodifikálásához való iránymutatás volt.

A következő komoly előrelépést az Európa Tanács 1989-ben elkészült szakértői jelentése⁸ (The Select Committee of Experts on Computer-related crime of the Committee of Crime Problems), majd az ugyanebben az évben elfogadott ajánlása jelentette (R89/9), mely dokumentumok a számítógéppel kapcsolatos bűncselekmények egy minimum - nemzeti törvényhozók által feltétlenül büntetendő - és a minimum listát kiegészítő fakultatív lajstromot tartalmaznak.

1.1. Az Európa Tanács minimális listája 1989-ben

- a, A számítógépes csalás.
- b, A számítógépes hamisítás.
- c, A számítógépes adatokban és programokban és programokban történt károkozás .
- d, Az illegális belépés.
- e, A jogellenes titokszerzés.
- f, A védett számítógépes programok jogellenes másolása.
- g, A félvezető topográfiák jogellenes másolása.

1.2. A fakultatív lista

- számítógépes adatok vagy számítógépes programok jogosulatlan megváltoztatása
- számítógépes kémkedés
- a számítógép kizajkosulatlan használata károkozási szándékkal
- a védett programok jogosulatlan másolása és használata

1.3. Az Európa Tanács Informatikai bűnözéssel kapcsolatos egyezménye

Az Európa Tanács 1997-ben hozta létre a Büntetőjogi kérdésekkel Foglalkozó Szakértői Bizottságot, amely felhatalmazást kapott egy, az informatikai bűnözéssel kapcsolatos nemzetközi egyezmény kidolgozására, melyet 2001. novemberében Budapesten fogadott el. Az egyezmény több részből épül fel, az egységes jogalkotást, jogalkalmazást megkönnyítendő büntető anyagi, eljárás- és nemzetközi jogi javaslatokat, megoldásokat fogalmaz meg. Meghatározásokat nyújt nemcsak az egyes cselekményeket, eljárásjogi intézkedéseket illetően, hanem a számítástechnikai rendszer egyes elemi fogalmát is igyekszik tisztázni.

Az egyezmény II. fejezete határozza meg azokat a cselekménytípusokat, amelyeket kriminalizálni javasol a részes államoknak. Ezek a következők:

1. alcím: A számítógépes adatok és rendszerek titkossága, integritása és elérhetősége ellen elkövetett cselekmények.
2. cikkely: Az illegális hozzáférés.
3. cikkely: Jogtalan kifürkészés.
4. cikkely: Beavatkozás az adattartalomba.
5. cikkely: Beavatkozás rendszerek működésébe.
6. cikkely: Visszaélés eszközökkel.
2. alcím: a számítógéppel kapcsolatos bűncselekmények
7. cikkely: A számítógépes hamisítás.
8. cikkely: A számítógépes csalás.
3. alcím. A tartalommal kapcsolatos bűncselekmények.
9. cikkely: A gyermekpornográfiával kapcsolatos bűncselekmények,
4. alcím. Szerzői és szomszédos jogok megsértésével kapcsolatos esetek.
10. cikkely: Szerzői és szomszédos jogok megsértésével kapcsolatos esetek
5. alcím. Mellékes felelősség és szankciók.
11. cikkely: Kísérlet, segítségnyújtás, felbújtás.
12. cikkely. Vállalati felelősségi kérdések.
13. cikkely: Szankciók, és fogalmak.

1.3.1 Az egyezmény fogalomrendszere

”Számítástechnikai rendszer”

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 biztosítják.

”Forgalomra vonatkozó adat”

Forgalomra vonatkozó adat minden olyan számítástechnikai rendszeren átmenő és a számítástechnikai rendszer által, mint a kommunikációs lánc egyik eleme által létrehozott kommunikációra vonatkozó adat, amely jelzi a kommunikáció származási helyét, rendeltetési helyét, útvonalát, napját, óráját, terjedelmét és időtartamát vagy a szolgáltatás típusát.

”Szolgáltató”

Minden olyan közjogi és magánjogi alany, amely a szolgáltatást igénybe vevőknek biztosítja azt a lehetőséget, hogy egy számítástechnikai rendszer által érintkezzen, b) minden más olyan alany, amely kommunikációs szolgáltatás vagy az azt igénybe vevők részére feldolgoz vagy tárol számítástechnikai adatokat.

2. A számítógépes bűncselekmények hazai szabályozása

2.1. A számítógéppel kapcsolatos bűncselekmények osztályozása

A hazai jogirodalom a számítógéppel kapcsolatos deliktumokat alapvetően két nagy csoportra osztja: az egyikbe azok a bűncselekmények tartoznak, amelyeknek elkövetési eszközét jelenti a számítógép, a másikba pedig azok, amelyek magát a számítógépet, annak adatfeldolgozását, és a szoftvereket támadják. (a számítógépes bűncselekmények osztályozásának ezen módjára az elsők között Dr. Polt Péter mutatott rá 1983-ban írt munkájában. Dr. Polt Péter: A számítógépes bűnözés) A két fő csoporton belül a Btk.-t alapul véve további alcsoportokat lehet megkülönböztetni:

1. abban az esetben, ha a számítógép az elkövetés eszköze:
 - a) az adatbiztonság sérelmével és a titoksértéssel megvalósuló bűncselekmények,
 - b) a nagy nyilvánosság, illetve mások előtt elkövethető bűncselekmények,
 - c) a számítógépes hamisítások,
2. amennyiben a számítógép az elkövetés tárgya:
 - a) a számítástechnikai rendszer és adatok elleni bűncselekmény,
 - b) a bankkártyával kapcsolatos bűncselekmények,
 - c) a szerzői és iparjogvédelmi jogokat sértő bűncselekmények,
 - d) egyéb, a számítógép ellen irányuló bűncselekmények között tehető különbség.

2.1.1. A számítógép mint az elkövetés eszköze

Az adatbiztonság sérelmével és a titoksértéssel megvalósuló bűncselekmények

Az Alkotmány 59. (1) bekezdése szerint a Magyar Köztársaság területén mindenkit megillet a magántitok és a személyes adatok védelméhez való jog.

Az 1992. évi LXIII. törvény (a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról) kimondja, hogy az adatokat -kiemelten az államtitokká és az állami titokká minősített személyes adatot -védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen. A törvény 17. biztosítja az érintettek azon jogát, hogy a személyes adataik megsértése esetén az adatkezelő ellen bírósághoz forduljanak és az ezzel összefüggésben felmerült polgári jogi igényüket peres úton érvényesítsék.

Az ide sorolható bűncselekmények a következők: magántitok megsértése Btk. 177.§, jogosulatlan adatkezelés 177/A.§, különleges személyes adatokkal visszaélés 177/B.§, levéltitok megsértése 178.§, magántitok jogosulatlan megismerése 178/A.§,

államtitoksértés 221.§, szolgálati titoksértés 222.§, üzleti titok megsértése 300.§, banktitok megsértése 300/A.§ és az értékpapírtitok megsértése.

A nagy nyilvánosság, illetve más személy előtt elkövethető bűncselekmények

Az idetartozó bűncselekmények közös vonása, hogy megvalósításukra kizárólag egy másik személy vagy a nagy nyilvánosság jelenlétében kerülhet sor. Ezt a jelenléte biztosítja az Internet, amelynek információs bázisa mindenki számára minden időben korlátlanul hozzáférhető.

A következő bűncselekmények sorolhatóak ide: rágalmozás 179.§, becsületsértés 180.§, kegyeletsértés 181.§, pornográf felvétellel visszaélés 195/A.§, törvény vagy hatósági rendelkezés elleni izgatás 268.§, közösség elleni izgatás 269.§, nemzeti jelkép megsértése 269/A.§, önkényuralmi jelképek használata 269/B.§, rémhírterjesztés 270.§, közveszéllyel fenyegetés 270/A.§, fogyasztó megtevesztése 296/A.§.

Számítógépes hamisítások

A számítógépes szövegszerkesztő- és grafikai programok, a színes lézer nyomtatók és az egyéb speciális eszközök dinamikus fejlesztésével egyre kifinomultabb technikai lehetőségek állnak az okirat- és pénzhamisítók rendelkezésére.

A számítógép felhasználásával elkövethető hamisítások tényállásai: közokirat hamisítás 274-275.§, magánokirathamisítás 276.§, pénzhamisítás 304-305.§, bélyeghamisítás 307-308.§ és a bankkártya-hamisítás 313/B.§.

2.1.2. A számítógép mint az elkövetés eszköze

Számítástechnikai rendszer és adatok elleni bűncselekmény

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, közérdekű munkával vagy pénzbüntetéssel 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, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(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, 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.

A számítástechnikai rendszer és adatok elleni bűncselekmény tényállását a 2001. évi CXXI. tv (a hackertörvény). 57.§-a iktatta be a Btk-ba, melynek következtében a számítógépes csalás tényállását hatályon kívül helyezte.

A bűncselekmény jogi tárgya egyfelől a számítástechnikai rendszerek megfelelő működéséhez és a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint titokban maradásához fűződő érdek., mivel a számítástechnikai rendszer zavartalan működése, illetőleg az adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények egyben a vagyoni, illetve a gazdasági viszonyok sérelmét is eredményezhetik. Nyilvánvaló tehát az, hogy szoros kapcsolatot lehet kimutatni a hagyományos gazdasági bűncselekményekkel is e tényállás kapcsán

.A törvényi tényállás sajátossága, hogy a törvény az adott bűncselekmény három alapesetét szabályozza, amelyek az elkövetési magatartások függvényében egymáshoz képest súlyosabban büntetendő cselekmények.

A (4) bekezdés szabályozza azokat a minősített eseteket, amelyek kizárólag a (3) bekezdésben írt bűncselekmény esetében állapíthatók meg.

Az elkövetési magatartás a számítástechnikai adatok jogosulatlan megváltoztatása, törlése vagy hozzáférhetetlenné tétele. Az elkövetési magatartás tehát ez esetben a jogosulatlan, illetve jogtalan programmanipulációban fogalmazható meg, amely gyakorlatilag egyrészt jelentheti a védelemben részesített adatok megváltoztatását, amely gyakorlatilag a programutasítások teljes vagy részbeni átírását, a program lefutásának megváltoztatását jelenti. A program a legcsekélyebb beavatkozás esetén is már nem az eredeti funkció szerint működik, így a számítástechnikai rendszerben tárolt adatok hitelességéhez, illetve megbízhatóságához kétségek férkőznek.

A számítástechnikai rendszerben tárolt, kezelt, feldolgozott adatok törlése lehet teljes, részleges, vagy akár szelektív is. Az adatfeldolgozási eredmény akár a program részbeni vagy teljes törlésével, akár az adatbázis törlésével is befolyásolható, ugyanis olyan adatok semmisülhetnek meg, amelyekre gyakorlatilag az adatfeldolgozási rendszer épült.

A törvény megfogalmazásából következik, hogy akár egyetlen adat törlésével is befejezett bűncselekmény valósul meg.