

Johannes

A bűn története*

AZ ENSZ DOKUMENTUMA A SZÁMÍTÓGÉPES BŰNÖZÉSRŐL ÉS AMI MÖGÖTTE VAN

TARTALOM

I. rész: Honnan indult a szerzői jog?

1. Ki támad miért támad?
2. A gépek kihívása
3. Szolgáltatáslopás vagy valami más?
4. A számítógépes bűnözés: A szerzői jog mint új (?) jogfelfogás

II. rész: A számítógéppel elkövetett bűnök és a magánélet

5. Valaki figyel... A számítógépes kommunikáció és a lehallgatás
6. A magánélet tulajdona: magán vagy köztulajdon?
7. A számítógép és az egyén magánélete
8. Nyom nélkül? Hol a bizonyíték?
9. Egymás ellen vagy együtt? Kinek higgyünk?

* A cikket megjelenése idején a Computer Panoráma lap közölte folytatásokban, de utána több konferencián kivonatos formában elhangzott. Megállapításai mai is igazak és időszerűek. A szöveg annak idején a lapba szánt anyag húzás és rövidítés nélküli változata.

I. rész: Honnan indult a szerzői jog?

2002. április 29. 17:38

A korábbiakban sok szó volt erről a tanulmányról, amely a **Bűn története** címmel jelent meg a Computer Panoráma magazinban, majd később sok-sok helyen. A témája azért érdekes a mostani világban, mert éppen azokat az elméleti alapokat feszegeti: Miért ember és kultúraellenesek a szerzői jogvesztők diktátumai és vajon miért nem képesek a nem konzumer-idióta társadalmakkal elfogadtatni azt. A tanulmány hosszú, ezért két részletben közöljük. De mondanivalója megszívlelhető. **A legnagyobb baj a politikusok nem tudják, vagy valami - mondjuk anyagi érdekek - miatt nem akarják megérteni: kulturális holocaustban segítkeznek. A kultúra kiirtásában, tönkretételében.**

1. Ki támad miért támad?

1992 október 9-én Würzburgban megrendezték az ENSZ égisze alatt egy ad hoc szakértői ülést, amelyen a fő téma a számítógépes bűnözés volt. A kanadai igazságügy-minisztérium által összeállított kézikönyv egyre több országban vált zsinórmértékké a számítógépes bűnözéssel kapcsolatos gyakorlat kialakításában és információink szerint a magyar rendőri gyakorlatban is alapműnek fogják tekinteni ajánlásait. (Sajnos nem ez történt, azóta a BSA és egyéb jogvesztő szervezetek ajánlása vált zsinórmértékké.)



Érdemes megismerni ezt a dokumentumot, mert már most látható, hogy a számítástechnikai termékek, de különösen a szoftverek forgalmazói igyekeznek nemcsak élni, hanem visszaélni a helyzettel. Mint az egyik, a fordításban és az értelmezésben segítő jogász kolléga említette: Magyarországon, ha nem vigyázunk, kialakulhat az a példátlan helyzet, hogy a rendőrség nem törvénykezési, hanem törvényesnek álcázott cégérdekeket képvisel. (Sajnos most ez a helyzet...) Az USA számítástechnikai törvénykezésének korai időszakában pár esztendeig szabályos önkényuralmi helyzet volt ezen a téren, míg az ottani demokrácia, meg a bírói és szakértői apparátus beletanulása jelentősen csökkentette ennek lehetőségét. A piaci diktátumaikat törvényes paragrafusok félreértelmezésével, sőt a törvénykezés megfelelő alakításával mindaddig könnyű képviselni, amíg a bírói és rendőri apparátusban nem alakultak ki azok a szakemberek, akik valóban értenek a témához. (Vagy, mint nálunk, ezt eleve kicsukják, mert a szakértőket, rendőröket maguk az érdekeltek képzik.)

A Scotland Yard felállított egy célnak megfelelően és törvényesen működő alosztályt. A forgalmazók saját játékaik során nem is számíthattak erre, hanem létrehoztak egy sajátos szervezetet F.A.S.T. néven. (Nem ismerős: a BSA ősképe...) Ezek feljelentést tesznek és polgári perekkel próbálkoznak. Az előkészítendő perekhez az információkat a legváltozatosabb úton szerzik be, a legtipikusabb: fejpénzt fizetnek - múlt évben (1992-ben) 1000 adómentes angol fontot - a feljelentőnek, aki a perekhez szükséges bizonyítékokat szolgáltatja.

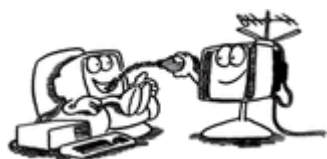
Az ENSZ dokumentumok között sikerült fellelnünk az eredeti szöveget, és annak alapján most ismertetni szeretnénk fontosabb megállapításait. A normarendszer megismerése és a nemzetközi gyakorlathoz való alkalmazkodás része a számítástechnikai kultúrának. A kézikönyvet Kanadából Donald Piragoff, Larissa Easson, John Nelly, Németországról Ulrich Sieber, Belgiumról pedig Bart De Shutter állította össze.

A legfontosabb kérdés: miként alkalmazkodhatnak az egyes államok jogrendszerei a számítástechnika kihívásához. Elsősorban azzal, hogy bűncselekményeket a megfelelő súllyal értékelik. Nyilvánvalóan jóval kisebb a veszélyessége a játékprogram-másoló diáknak, mint egy ezt iparszerűen űző vállalkozónak, a saját célra szoftvermásoló veszélyessége nulla ahhoz képest, mint aki komoly minisztériumokat és apparátusokat működtet illegálisan másolt szoftverpéldányokkal.

A számítógépes bűnözés, mint jelenség (computer crime) egy új kategória. Viták vannak arról, hogy ez szinonim fogalom-e a számítógéppel kapcsolatos bűnözéssel (computer related crime), és az angol szakirodalom éppen ezért ezeket mint homonim fogalmakat alkalmazza.

A bűn elkövetésének alapvető feltétele a bűnös szándék. Ezt kell a jogrendszereknek bizonyítani, mert ellenkező esetben csak gondatlanságról beszélhetünk, ami jóval enyhébb kategória. (A szabálysértési és gondatlan alakzat hiányzik a magyar hackertörvényből, éppen úgy, mint a szerzői jogi törvényből. Ezért a törvény nem konform a nemzetközi gyakorlattal.) Egy számítógépes rendszerrel való visszaélés egy olyan alkalmazott részéről, aki kapott egy jelszót munkaadójától egy adatbázisban való hozzáféréshez, de nem kapott utasítást arra nézve, mit tehet és mit nem, nem tekinthető bűnösnek (szintén hiányzik a büntethetőséget kizáró véttelen elkövető alakzat...), ha belép az adatbázisba és esetleg ott kárt, kavarodást okoz. Maximálisan gondatlanul járt el, miként főnöke is vétkes abban, ha nem oktatta ki kellőképpen. Azonban, ha ezt a jelszót valaki ettől a kollégától ellopja, akkor megvan a szándékosság a jogosulatlan hozzáférésre.

Különbséget kell azonban tenni, mi a jog szerint etikátlan - de a jog betűjébe beleférfő - és mi az illegális tevékenység, s a jogi válasznak, a megtorlásnak ezzel kell arányosnak lennie. **VÁDEMELEÉSNEK CSAK AKKOR SZABAD BEKÖVETKEZNI, HA BEIGAZOLÓDOTT A BÜNÖS SZÁNDÉK.**



E sorok szerzője szakértői munkája során zsinórmértékül használja Richard H. Baker Computer Security Handbook című munkáját. Ebben olvasható az az adat, hogy az ismertté váló számítógépes bűncselekmények a valóban elkövetetteknek mintegy 1-10 százalékát teszik ki. Az ENSZ kézikönyve egy korábbi, 1987-es adatot idéz. E szerint a The American Bar Association 1987-ben lefolytatott egy vizsgálatot, mely szerint akkor mintegy 300 vállalat panaszkodott arról, hogy számítógépes bűncselekmény áldozata lett. Erre a 12 hónapos időszakra az elszenvedett károk mértékét 145-700 millió USD közé teszik. Ez a számítógépes bűnözés egyik érdekessége, hogy a kár mértékét sokszor maguk a károsultak sem képesek felbecsülni.

A kriminológia egy bűncselekmény hátterének tanulmányozása során mindig a potenciális áldozatok és a potenciális elkövetők csoportját igyekszik meghatározni. Potenciális áldozat mindenki lehet, aki számítógépes rendszert üzemeltet. A sima BBS üzemeltetőjétől a multinacionális vállalatok és katonai hálózatok üzemeltetőjéig. A rendszer ugyanis ismertté válásától van kitéve annak, hogy betörjenek abba. Érdekes a potenciális bűnelkövetők listája is: diákok, terroristák, gengszterek vagy bosszúra éhes alkalmazottak.

Ami megkülönbözteti őket, az az elkövetett cselekmény természete. Az a diák, aki bűnös szándék nélkül lép be egy rendszerbe, egészen más megítélés alapján áll, mint az a pénzintézeti alkalmazott, aki ezen a módon pénzt lop. Érdekes következménye ennek a dolognak, hogy a rendszereket önmagukért, a kihívás miatt feltörő, legyőző hackereket az intelligens társadalmak minden jogellenes tevékenységük ellenére nem üldözik, hanem a biztonsággal foglalkozó cégek, vagy maguk az intézmények megveszik őket 'aranyáron' azaz a biztonságtechnikai ipar legjobb szakértőivé teszik őket. Izrael, USA, Anglia és újabban a német cégek egyre több ilyen szakembert alkalmaznak, míg a franciák igyekeznek megalkuvás nélkül üldözni őket. Ezért a franciaországi rendszerek veszélyeztetettsége jóval nagyobb.

A számítógépes bűnözők intelligenciaszintje is viták témája. Minden híreszteléssel ellentétben - s a tíz-tizenkét évvel ezelőtti csoportokkal is - a jelen számítógépes bűnözője intelligens, briliáns átlátó-, szintetizáló-képességű elme. Még a terroristák között is vannak ilyenek, csak az erkölcs az, ami defektes többségükben.

A számítástechnikai cégek gyakorlatából kiderült, hogy az adatbázisok és a pénzátutalások megdézsmálása tipikus belső bűnözés. Az elkövetők köre az alkalmazottak vagy a volt banki alkalmazottak köréből kerül ki. Egy nyugatnémet tanulmány szerint az ilyen cselekmények 90 százaléka alkalmazottak ténykedéséből ered. Észak-Amerikában és Európa más országaiban ez az arány 73 % körül van. A veszélyt az adatátviteli rendszerek összekapcsolása csak fokozza. Korábban volt lehetőség ugyanis arra, hogy ha az alkalmazottat a gép közeléből eltávolították, akkor az illegális beavatkozás veszélye is megszűnjön. Most azonban a kommunikációs vonalakon egy alkalmazott később is bármikor bekapcsolódhat a rendszerbe, ha annak idején telepítette vagy megszerezte a jogosultságokat biztosító azonosítóit.

A kommunikáció elterjedésével, az eszközrendszer fejlődésével a rendszerek sebezhetősége nő. Ez ellen megfelelő intézkedésekkel is csak akkor lehet fellépni, ha azok hatásosak. Tehát a rendszer csak annyit és úgy kommunikál, amennyit feltétlenül szükséges, és mindenki csak a számára feltétlenül szükséges jogokat kapja egy rendszeren belül. Ugyanakkor a rendszer-managereket úgy kell megválasztani és megfizetni, hogy ne legyen számukra kísértés a rendszer módosítása, adatainak áruba bocsátása.

2.A gépek kihívása

Az ENSZ kézikönyv külön fejezetet szentel annak megvizsgálására, milyen gépi rendszerek hívják magukra a bűnözést. Mindenképpen ismerni kell az új érték-definíciót. Azaz vajon miért érték az információ?



A történelmi jogfejlődés során gazdasági értéket a látható és kézzelfogható vagyontárgyaknak tulajdonítottak. Azonban az emberek igen korán felismerték, hogy az adatok is bírhatnak gazdasági értékkel. Így már azok vagyontárgyakká is válhatnak. Ezért lett a számítástechnikai környezetben a vagyon kettős értelmezésű. Egyszer megmaradt hagyományos módon, tehát a kézzelfogható javak pótlási értéke, azaz, ha tönkretettem egy berendezést, mennyiért kapom meg a piacon, mennyi pénzért hozhatom magam olyan helyzetbe, mint amilyenben a kár előtt voltam. De ott van a második érték: a benne tárolt információ. Sok esetben ezek nem pótolhatók, vagy mire pótoltam, már hatalmas veszteségeket szenvedtem el. Éppen ezért a számítástechnikai környezetben tárolt információ sebezhetőbb, mint a Top Secret irattárak mélyén rejlő.

Az információ ugyanis egy érdekes dolog. Úgy el lehet lopni, hogy fizikailag a helyén marad. De azzal, hogy a másik megtudja - például üzleti, gyártási titkokat képező anyagok esetén - és természetesen azt felhasználja, beláthatatlan károkat tud okozni. Az állam is él, sőt rendszeresen visszaél szinte mindenütt a világon ezzel, amikor a computer privacy-hez, azaz a számítástechnikai rendszerek saját tulajdonához való jogot szeretné korlátozni, ami sajnos a legtöbb szoftverforgalmazó igénye is lenne.

A computer privacy elvének sérelme az is, amikor az adóhivatal kíváncsi bankszámlánkra, könyvelési adatainkra, vagy a bank eképpen igyekszik máshol hitelképességünket megvizsgálni. A személyi nyilvántartó kódok, az egyes független nyilvántartások összekapcsolása már egészen más kategóriát, a személyiségi jog témakörét érinti.

A rendszerek csábítását fokozza a koncentráltág. Azaz: igen nagy számítási és adattárolási kapacitás összpontosul egyetlen egységen belül. Ugyanakkor a különböző, látszólag független információk összekapcsolása, minőségileg új és kíváncsú információk képződését eredményezi.

A rendszerhez való hozzáférés, mint az előző részben említettük, szintén komoly kihívást jelent, miként a rendszer komplexitása. Egyes behatolási technikák éppen ezt használják ki, azaz hogy egy ember vagy szervezet által végül a képződő komplex rendszer nem válik áttekinthetővé. Lukák, rések támadhatnak a biztonságtechnikai intézkedések hálójában. Például, ha egy telefonkártyát valaki primitív módszerrel, mondjuk egy érintkező leragasztásával módosít, a rendszer konstruktőrének lenne a feladata, hogy ezen kikaput becsukja. Így az eképpen keletkező kárért felelősséggel tartozik, amit a szolgáltatáslopás okozott. Az egyéni elkövető éppen a kár kis mértéke miatt nem büntethető, hiszen a szándékosság és az egy-két impulzusnyi szolgáltatáslopás még a szabálysértési kritériumokat is alig meríti ki. (Ezzel ellentétben a magyar jogban itt számítógépes csalás szerepel, értékhatár nélkül, bűncselekményi alakzatban. Hol itt a nemzetközi konformitás?)

Ezzel elérkeztünk egy nagyon fontos kritériumhoz. A rendszerek elektronikus sebezhetőségéhez. Itt bele kell érteni a korábbiakban említett primitív módszereken kívül a komolyabb technológiát igénylő beavatkozásokat, a telefon- és az adatlehallgatást éppen úgy, mint a számítógépes rendszerek szórt elektromágneses teréből kinyerhető információk lefűléését.



A lehallgatási technikákból eredő információk segítségével nemcsak megfűjthetők a hozzáférési kódok, de hamis parancsok, felhasználó-szimulációk vihetők be a rendszerbe. Ugyancsak előnyt biztosít a manuális adatfeldolgozással szemben, hogy megfelelő szakértelem esetében ezek a beavatkozások azonnaliak és valóban nyom nélküliek. De az is bizonyíthatatlan, ha mondjuk X vesz egy szabadszoftvert, majd rámásol egy Y programot és illegális árusítás miatt perli az eredeti céges lemez eladóját. Ugyanis az nem bizonyítható, hogy a vétel előtt vagy után került rá valamilyen információ. Nem véletlen, hogy a nagy szoftvercégek a boríték felnyitása után nem vállalnak garanciát termékeikre...

Az elektronikus adatfeldolgozási rendszerek (angol jogi terminológiában EDP = Electronical Data Processing) sebezhetőek. A gépek - ha nem árnyékolják le és tervezik megfelelően őket - a működésük során keltette elektromágneses térrel kisugározzák a bennük zajló folyamatokat, ami megfelelő vevővel és értelmező programmal adatokká alakítható. De kívűlről, elektromágneses sugárással egyes gépek működése is befűyásolható.

E sorok írója is képes volt úgy maximális összegre rábeszélni az első német érmefelismerő telefonkészülékeket több mint tíz esztendeje, hogy piezo-elektromos öngyújtóval beszikráztatott az érmebedobó nyílásba. Ma már ezek a rendszerek védettek az ilyen primitív trükkökkel szemben.

Az adathordozók szintén érzékenyek. Például a szocialista országokban ezt ki is használták, amikor a külföldre küldött mágneses adathordozókat a csomag felbontása nélkül elektromágneses tekercseken tölték át - a kémkedést megelőzendő - minden információt törölve.

Az emberi tényező jelenti a legnagyobb kockázatot az adatfeldolgozó központokban. A dolog természeténél fogva a könyvtárosok, az operátorok, hardvertechnikusok a kivételes kedvénységezés állapota van, hiszen ahhoz férnek hozzá, amihez akarnak. A helyzet következménye, ha őket nem becsülik meg anyagilag, okkal vannak kitéve a kísértésnek.

A gondokat fokozza, hogy ezt a személyzetet nem tudják és nem képesek ellenőrizni. Nincsen jelszósabályzat, egyetlen emberre bízzák a rendszer generálását, alapjogok beállítását. Külön problémás a szoftverek kaotikus állapota. Gyakorlatilag egy forgalmazó vagy programozó azt tesz bele egy programba, amit akar, mert nem vállalják a költségeket, hogy valóban ellenőrzött forráskódú szoftverek kezeljék az adataikat. Az ellenőrzés lazaságát fokozza, hogy a főműszak utánra teszik a nem-folyamatos munkarendű számítóközpontban a rendszerkarbantartásokat, amikor az ellenőrzésre esetleg képes biztonsági személyzet (ha egyáltalán van ilyen) nincsen szolgálatban. Világos, hogy a rendszerprogramozók és az operátorok szabadsága nagyságrendekkel nagyobb, mintha egy hagyományos papír-alapú munkahelyről lenne szó.

Érdemes megnézni, melyek a számítógépes bűnözés gyakoribb típusai? Az ENSZ kézikönyv itt kifejti, hogy a számítástechnikai eszközökkel végzett műveletek szinte minden fázisukban ki vannak téve a bűnözés célpontjaiként. A bemenő adatok és adatfeldolgozó eszközök, a számítástechnikai adatok és adattárak, a számítógépes berendezések, az output, a kommunikáció mind-mind támadási felületet biztosít a bűnözés számára.

A leggyakoribb a számítógéppel támogatott csalás. Nem véletlen, hiszen a számlapénz-mozgásokkal viszonylag kis kockázattal igen nagy összegeket lehet elemelni. A Magyarországon eddig indult, 10 alatti számú, ilyen nyomozati eljárás is éppen ilyen bűncselekmény-gyanúik igazolására indult. (Ne feledjük, mikor is készült ez a tanulmány...)

A modern rendszerekben lévő hatalmas értéket képviselő számlapénz, munkaóra-elszámolás a leggyakoribb célpontjai az ilyen csalásoknak. A hagyományos vagyonokban megtestesülő értékkel szemben az adatformátumokban megtestesülő vagyon értéke nagyobb. Gondoljuk arra, hogy ahhoz, hogy valaki 90 millió forintot raboljon, milyen kockázatnak kell magát kitenni: esetleg le is lövik, míg ugyanezt adatátviteli rendszereken keresztül hozzáféréssel - akár egy tengerparti szállodából is - minimális kockázattal megteheti az elektronikus rendszerek használatával. Nem véletlen, hogy az adatok inputjának manipulációja a leggazdaságosabb és legnehezebben felfedezhető cselekmény. Példánkban elég, ha csak a töredék fillérkamatoztatjuk át egy számlára, majd onnan egy másikra, ahonnan fel lehet venni. Itt a beérkező adatokat vagy a kommunikációs csatornákat kell manipulálnia a bűnözőnek. Kissé nehezebb dió a programok módosítása, mondjuk: ha nem szerepel a fizetési listán X, akkor Y összeget utaljon egy másik bank fiktív számlájára. Ide mindenképpen bennfentesnek kell lenni, bár ezen módosítások is elvégezhetőek néhány rendszernél.



Külön műfaj a felhasználók zsarolása a forgalmazók részéről. Ezt természetesen nem ismerik el, sőt a törvénykezést igyekeznek (mint láthatjuk itthon is sikeresen) ezirányban manipulálni. Ilyenek például a határidős programok, másolásvédelmek, ahol a programot a működtető szoftvert újra és újra rákényszerítik egyenlőtlen szerződésekben a felhasználóra, mert különben nem fér hozzá adatbázisaihoz. Hasonlóan értékelhetők a másolásvédelmek is, hiszen mindegyikük csak a forgalmazók pénzügyi érdekeit képviseli.

A számítógépes hamisítás esetében adatokat hamisítanak meg, hogy eképpen jussanak előnyökhöz. Ennek klasszikus példája, amikor hitelkártyát hamisítanak, illetve eredetét többszöröznek azon célból, hogy a kommunikációs rendszer hiányosságait kihasználva, az egymással és a központtal off-line kapcsolatban levő (azaz nem összekötött) automatákból a számlán lévőnél lényegesen nagyobb pénzmennyiséget vegyenek fel. Elsősorban a rossz kommunikációs infrastruktúrával rendelkező országokban játszható el ez a módszer, Magyarország kiemelkedően veszélyeztetett e témában. (Na végre, egy dolog, amiben változás történt! Már itthon is on-line a legtöbb automata, sőt bolt is. A csalások száma radikálisan lecsökkent)

Kissé nehezebb a gépben lévő információ manipulálása. Nem véletlen, hogy például a szerencsejáték rendszerek esetében a szokásos védelmeket felülmúló extra védelmi rendszerek, egyedi megoldások teszik szinte lehetetlenné az adatok manipulálását.

Végezetül, csak említés szintjén, de fontos ide sorolni a számítógépes programok, adatbázisok megrongálását vírusokkal vagy trójai programokkal, esetleg másolásvédelmi büntető rutinokkal. Itt az elkövető névtelenségbe burkolózik, a jelenség felderítése, de különösen a tettes felkutatása igen nehéz, a cselekedet a legritkább esetben bizonyítható a jog kívánta igényességgel.

3. Szolgáltatáslopás vagy valami más?

A Kanadai Igazságügyi Minisztérium szakértői csoportja az ENSZ 1992-ben megtartott Würzburgi tanácskozására összefoglalást készített a számítógépes bűnözésről. Ennek a dokumentumnak az ismertetését már korábbi számunkban elkezdjük. Most folytatjuk a számítógépes eszközökkel elkövethető, és később esetleg a büntető törvénykezésbe átemelhető cselekményfajták ismertetését.

A számítástechnika egyik nagy problémája a rendszerek jogosulatlan használata. Itt sok esetben azt is felvetik egyes szakértők: valamit NEM HASZNÁLNI, nem bűncselekmény, használni pedig igen? Hiszen sok esetben ilyen rendszerek használatával lényegében nem károsít meg senki semmit, miként az adatlopással sem. Az adatok nem tűnnek el eredeti helyükről. Legfeljebb lemásolódnak.

A számítástechnikai rendszerekhez, programcsomagokhoz való jogosulatlan hozzáférés széles skálát foglal magában. A kémkedéstől a szabotázsig, a sima szolgáltatáslopástól a zsarolásig, minden hagyományos jogi tényállással rokonítható. Ugyanakkor ilyen magatartást az valósíthat meg, aki a tulajdonos engedélye nélkül - és ez lényeges momentum - egy védett rendszerbe behatol, ott adatokat tulajdonít el, programot, adatokat módosít, károsít.



Egy ilyen behatolással azután majd alkalom nyílhat nem szándékos károkozásra, rendszerösszeomlás okozására éppen úgy, mint vírus gondatlan bejuttatására, vagy éppen adatok véletlen módosítására. Ennek a hozzáférésnek nem kell a gép rendszeroperátori munkahelyéről történnie, ez lehet akár adathálózaton keresztül, vagy akár aképpen, hogy a szállítás során 'véletlenül lemásolódnak' egy rendszer elmentett adatai, programjai. Ez a módszer különben mind a mai napig eléggé általános. Ide azonban a szállítást végző személy együttműködése is szükséges. Igen nehezen bizonyítható, de bizonyítás esetén a legtöbb állam jogrendszerében találhatóak rá tételes jogi paragrafusok (lopás, szolgálati-, állam-, üzleti-titoksértés köre, illegális verseny stb.)

A behatolók hasznot húznak a rossz biztonsági intézkedésekből. Ilyen a jelszóvédelem, ha rosszul alkalmazzák. Nem véletlen, hogy a nagy rendszerek gyári biztonsági rendszere is tartalmaz úgynevezett BAD WORD file-okat, amelyekbe azokat a gyakran használt szavakat írják be, melyek használata jelszóként triviális. Például az USA történetének az egyik legnagyobb számítógépes behatolása a NASA védett rendszerébe is ilyen gondatlanságon alapult. A rendszer login neve ismert volt: ALLAH, és mi is lett volna a mindent kinyitó kulcs? Mi más, mint MOHAMED, az ő prófétája.

A jelszóvédelmet a laikusok gyakran úgy jellemzik, mint az illetéktelen hozzáférés megakadályozásának kulcsát. Ez ellen a jelszó-kezelés bonyolultságának növelésével lehet védekezni, de csak részben. A gyári operációs rendszerek bárhogy is igyekeznek titkosítani a jelszó-továbbítást, egy komoly szakember előtt kevés akadályt jelentenek. Ugyanis hiába kódolja el akárhogy, ha ezeket az algoritmusokat viszonylag kis erőfeszítéssel meg lehet szerezni bármelyik gépre a számítógépes kommuna rejtett ösvényeiről. Titok nem lehet, legfeljebb ideig-óráig. Ilyenkor sok esetben egyetlen megoldás van: bizonyos funkciókat csakis a gép mellől, a rendszerkonzolon lehet vezérelni. Ez látszólag visszalépés a korábbi őskőkori állapotokba, de legalább a rendszerkonzol egy hely, és ráadásul ennek az egy pontnak biztonsági személyi és számítástechnikai védelme jól megoldható.

A másik eljárás, amellyel a jelszó megtörésén kívül bejuthatnak a rendszerbe, egy magas privilégiumú felhasználó azonosítójának megszerzése. Erre a rendszergazdák szokott felületessége ad alkalmat. Magyarországon is ismert, hogy sokan külföldi ösztöndíjuk után évekig-évtizedekig használják azt az egyetemi rendszert, ahol ösztöndíjukat töltötték, mert elfelejtették megvonni ottani jogaikat a munkahely elhagyása után. Ha ez egy olyan esetben történik, amikor valaki egy vállalati rendszerben volt felelős pozícióban és esetleg elmegy a konkurenciához, akkor az bizony kemény következményekkel járhat a cég üzleti titkaira.

Sajnos az így adódott helyzetet egyre inkább dramatizálják is az egyes monopóliumok. Arra akarják kihasználni az egész szituációt, hogy a jogos felhasználók érdekeit is semmibe véve, maguk diktálhassák és alakíthassák a jogrendszert. Ilyenek a szoftverek másolási joga, a szoftverhasználati jog, a felhasználók megzsarolása másolásvédelmekkel, szoftverekbe beépített határidőkkel, úgynevezett bérleti joggal. Mindennek alakulása csakis azon múlik, hogy a felhasználók kisnyúlként viselkednek, vagy képesek olyan szervezetet létrehozni, amely egyenlő erejű félként tud bekapcsolódni abba a folyamatba, amit nemzeti és nemzetközi jogalkotásnak nevezünk. (Magyarországon itt győzött a szerzői jogilag informálatlan gombnyomogató honatyák butasága. A magyar jog kirívóan durva, semmibe veszi a felhasználói érdekeket. Ráadásul a hatóság is a szoftverforgalmazók érdekeit képviseli, rendelkezésükre bocsátva a rendőrséget és egyéb államhatalmi szervezetet.) Itt még egy probléma adott: a bírói kar, az ügyészi kar és a jogalkotók általában garantáltan nem értenek a számítástechnikához.

Azt írják, kodifikálják, sőt mérlegelik, amit a szakértők mondanak. Ez a jog egyetlen olyan területe, ahol éppen a szakma kasztjellege miatt, egyelőre nem lehet független cégektől és érdekektől független vélemény.

Amikor egy perben, ahol egy floppyt be lehet adni, és azt komolyan veszik, hogy XYZ-től vették, és szakértők a címke valódiságán, a dátumokon vitatkoznak, akkor a bírónak eszébe sem jut: Mivel bizonyítja valaki, hogy azok az adatok először és éppen attól kerültek oda, akit ezzel okoltak, vagy hogy a lemezen mi volt egyáltalán? Nem véletlen, hogy jelenleg csak a sokszorosított, gyárilag préselt CD az az egyetlen média, amelynek az eredetisége, ha a gyártó ismert - többé-kevésbé - bizonyítható. Ezért van a világon mindenütt - és bármennyire kellemetlen, a felhasználó számára jogos önvédelemből a borítékszerződésen, hogy annak kibontása után semmilyen garanciát nem vállalnak a termékre. Ki tudja, mikor módosíthatta. Az már megint más kérdés, hogy ezzel alaposan visszaélnék, mint mindennel, ahol a jog alkalmazása nem kiforrott, vagy mint nálunk, kifejezetten rosszhiszemű.

Mindezen ismeretek birtokában joggal tehetnénk fel a kérdést: milyen büntetőjogi szabályozás védi meg az információ birtokosát? Itt megint egy klasszikus római jogelv csődjének vagyunk tanúi. Ugyanis a klasszikus büntető és polgári jog jogtárgyakat és jogalanyokat ismer. Szintén klasszikus definíció szerint a jogtárgy valami kézzelfogható anyagi dolog, amelynek a tulajdonlása, a felette való rendelkezés jelenti a jog tárgyát, ahol a birtokló és a felette rendelkező egy és ugyanaz a természetes, majd későbbiekben jogi személy. Innen egy lépéssel előbbre ment a jogfejlődés, amikor a tárgy birtoklási és a felette való rendelkezési jog különválasztódott.

Gondoljunk bele: A lakásnak van egy birtokosa és van egy hasznélvezője, és mindkettő egy tárggyal, a lakással kapcsolatos. Innen már csak egy lépés a kézzelfogható jogtárgy nélküli rendelkezési jog megjelenése, ami rögtön különvált formában jelentkezik a szabadalmi jogban, ami a jogfejlődésben legkorábban jelent meg és a szerzői és kiadási jogoknak, majd várhatóan az informatikával kapcsolatos jogágnak is az alapja lesz.



A szabadalmi jog is két részből tevődik össze, miként a szerzői jog. Van egy személyhez fűződő része. Ez azt jelenti, hogy XYZ feltaláló. Ő találta fel a lépegető zöldbékát. Ezt senki el nem vitathatja, ezt a jogot el nem adhatja. Ugyanakkor ennek a hasznosítási jogát szabadon értékesítheti, rossz esetben akár, ha annyira jó, akár

ingyen, akár névleges összegért - nem véletlen az az USA gyakorlat, hogy a nagy cégek így veszik meg a kutatóintézeteikben foglalkoztatott feltalálóktól 1 USD-ért találmányuk minden jogát, hogy a feltaláló minden rendelkezését elvesztse saját szellemi terméke felett. A szabadalmi joggal teljesen analóg fejlődési pályát járt be a világon a szerzői jog is.

Itt immár nem tárgyat, hanem információt, ismeretet védenek, és nem véletlen, hogy a számítógépes programok, információk jogvédelme is a szerzői jogok kitaposott csapásirányát vette fel. Ehhez azután a számítástechnikai területen is bejöttek mindazok a kiegészítő argumentumok, amelyek a szabadalmi jogban már mindennaposak: titkosság, kizárólagosság, azonosság, reprodukálhatóság és a saját célra történő használat. (Szabadalom tárgya saját használatra, nem jövedelemszerző céllal reprodukálható. A szoftver a magyar jog szerint NEM, miként újabban a digitális DVD-másolást és egyes helyeken a digitális másolásvédett zenét is annak veszik. A rendőrség, a bíróság a jogvesztők nyomására fokozatosan terjeszti ki a törvény értelmezését.) Mindezeket a különböző jogrendszerek megspékelték nemzetbiztonsági megfontolásokkal. Ezzel kialakult az a vegyes mixtúra, amiből várhatóan az ezredév végéig letisztul a szerzői jog ezen új ága, ami már részben a maga önálló életét éli. (Nos nem tisztult le. Inkább egy szerzői jogi fasizmus kiinduló pontjává vált...)

Az információ - lett legyen az programforrás, programkód, adatbázis, videó vagy egyéb formában megjelenő információ - birtokosa vagy tulajdonosa érdekeinek figyelembe vételekor a törvényalkotás két fő szempontra koncentrál: Először is jogi precizitással meghatározza, hogy az információ kizárólagos használatát titkosságát kell-e védeni, s ha igen milyen körben, illetve melyek azok a területek, ahol ez a védelem semmilyen szempontból sem indokolt? Utána ehhez kell igazítani a büntetőjogi tényállásokat, lehetőleg megnevesítve a leginkább súlyosnak és veszélyesnek ítélteteket, konkrét elrettentő tarifákat adva. Ad absurdum például a kémkedés esetén - amit most már számítástechnikai eszközökkel ugyanúgy el lehet követni, mint régen a minifényképezőgéppel, hiszen mindkét esetben információt loptak, tulajdonítottak el, szereztek meg illegitim úton - akár halálos ítéletet is ki lehet osztani. Például ilyen eset volt az USA-ban annak idején a Rosenberg-házaspár kémkedési ügye.

Miként lehet biztosítani törvényes keretek között ezeket a szabályozásokat? Nyilván ezt tenné fel minden jogász és büntetőbíró. Nos jelenleg ezeket nagyjából a kereskedelmi titkokról, az üzleti titkokról szóló paragrafusok alá sorolják be az egyes jogrendszerek, és minősített esetben gazdasági kémkedésről is beszélnek, például ha YXZ cég ellopja HQZ cég ügyfél-listáját, tényleges forgalmi adatait. De sok esetben elnéző, ha ezt a vám- vagy az adóhatóság teszi... A másik nagy szabálycsoport, amivel sok helyen a forgalmazók a felhasználói oldal képviseletének hiányában oroszlánszerződés jellegűen visszaélnék, a szerzői jogi törvénykezés keretébe való elhelyezés, pontosabban annak számítógép-specifikus ágának a megteremtése.

A jogalkalmazó bíró ekkor kitaposott ösvény és szakmai hozzáértés hiányában áll és csak néz. Könnyű dolga van, ha a cselekmény anyagi információhordozó ellopásával valósul meg. Például kinyomtatott listákat, streamer-szalagokat léptettek olajra. De mit tegyen akkor, amikor az eredeti anyag ott is, itt is megvan, anyagi dolgok lopása nem történt meg??? Ezért merül fel a kérdés, milyen mértékben lehet ezeknek a nem anyagi információknak a jogosulatlan megszerzését fedni ezekkel a rendelkezésekkel? A legtöbb ország nem véletlenül nem alkalmazza a lopásra és sikkasztásra vonatkozó rendelkezéseket a titokban tartandó információk jogosulatlan megszerzőire. A jogosulatlan felhasználásra vonatkozó törvények azt igénylik - mint a bevezetőben emlegettük - hogy a vagyontárgyat elvigyék, elbirtokolják eredeti tulajdonosától.

Ez a korlátozás jogos is a világ fejlődésének szempontjából. Ugyanis a fejlődés megkívánja az információk szabad vagy korlátozottan szabad áramlását. Abban az esetben, ha ezeket drákói szigorral védenék az egyes jogrendszerek, a fejlődés teljesen megállna, mert mindenkinek mindent újra és újra ki kellene találnia, kutatnia. (Sajnos a világ mégis ebben az irányban halad.) Ugyanakkor felvetődik a másik kérdés.

Ha Nyergelj Szergej korábban egy atomkísérleti központ vezető tudósa volt, akkor egész életében nem léphet ki annak falai közül, csak a sírba, hiszen fejében olyan ismereteket hordoz, amik a legszigorúbb állami, szolgálati stb. titkot képezik. Nem véletlen volt az egyik közelmúltban megrendezett biztonságtechnikai konferencián az egyik ismert szoftveres cég vezetőjének kifakadása: az orvosok igazán feltalálhatnák már az emberi agy szelektív törlését, milyen kevés szívinfarktus lenne azután a nyugdíjas szakemberek körében. Ezt a kijelentését ugyan szeszközi állapotában tréfának szánta, de ez a megfogalmazás fedi, hogy a társadalmi kontroll miért védi az ilyen informatikai 'bűncselekmények' kivitelezőit, és miért csak a számítógépes rendszerekben elkövetett adatkárosítást, módosítást és sabotázst ítéli el.

4. A számítógépes bűnözés: A szerzői jog mint új (?) jogfelfogás

Korábban már említettük, hogy a tulajdonjog a klasszikus jogfelfogás szerint a kézzelfogható anyagi javakra vonatkozott, és a jog furcsán, kurtán nézett bármit, aminek nem volt fizikai megtestesülése. Ezért a hasonlót a hasonlóval jogi elv alapján nagyon gyorsan megjelent korunkban a szellemi tulajdonjog, mely a szabadalmi, írói szerzői és előadói jogban, s a jogfejlődés jelenlegi szakában a számítógép programok területén csúcsosodott ki. A szellemi tulajdon ezen felfogásban a természetes jogok származéka.

Az ENSZ általunk ismertetett würtzburgi dokumentuma leszögezi, hogy a félvezetők áramköri rajzának, azaz topológiájának védelme és a szoftverekhez fűződő szerzői jogok, a szabadalmi jogokhoz hasonlóan bizonyos helyzeti előnyt biztosítanak másokkal szemben az eredeti alkotónak.



A számítógépes rendszerekben azonban az információ tagolódik. Tagolódik a hardver félvezető topológiájára, tagolódik az operációs rendszer hardverbe épített szoftverelemeire, tagolódik magára az operációs rendszerre, a programfejlesztő programokra és végül az alkalmazói programokra. Legvégül, de nem utolsó sorban a gépben tárolt információra, melynek értéke és érzékenysége lehet nagyobb, mint a fentiekben emlegetett részek értéke.

A számítógépi programokra tekintettel a kereskedelmi titkokra vonatkozó jogelvek azonban nemcsak a számítógépben tárolt adatra vonatkoznak, hanem a szerzői és kereskedelmi jogok védelmének eszközei is jelenleg annyiban, hogy a programokat lefordított, futtatható formában és nem forráskód formájában forgalmazzák. Ezen programkódok azonban úgy átvihetők, hogy nem is kell tartalmukat tisztázni (azaz másolhatóak). A jogosulatlan másolatok azonban az eredeti termék forgalmát olyannyira csökkentik, hogy jogi kényszerítő eszközökkel próbálnak a forgalmazók fellépni saját, kevésbé kelendő, drága termékeik eladásának érdekében.

Az elmúlt években igen sok országban vita folyt arról: mire terjedhet ki a klasszikus szabadalmi jog, mi az, amit a szerzői jog szabályaival lehet védeni, és mi az, ami ezen túlnyúlik és alapján új szabályozást igényel? Sajnos itt egy érdekes jogfejlődési iránnyal kell szembenéznünk, aminek csirái a magyar jogon belül is megtalálhatóak.

Klasszikus elv, hogy a bűnüldözésnek és az igazságszolgáltatásnak pártatlannak és minden céges érdeken felül állónak kell lennie. Ugyanakkor a bűnüldöző szakemberek, jogászok, ügyészek sem itthon, sem pedig külföldön nem felkészültek ezen problémák kezelésére. Ilyenkor a tanácsadó-szakértői team-ek óhatatlanul a nagy vagy kis szoftverforgalmazó-fejlesztő cégek munkatársaiból kerülnek ki. Magyarországon is létezik egy tanácsadó testület a rendőrség mellett, melyben a nagy szoftveres cégek emberei találhatók meg és témája a számítógépes bűnözés. Nos, ezen testületek gondolkodásában, még a legnagyobb jószándék mellett is, elsősorban a céges korporatív szellem, a saját érdekek védelme érvényesül, és csak másodsorban az, ami az igazságszolgáltatás alapvető feladata lenne, és amit a bekötött szemű Justitia képvisel.

A jelenség nem új, csak napjainkra válik igencsak szembeszökővé. Már korábban a távközlés területén volt az USA-ban hasonló helyzet, amikor bírósági perekben a távközlési vállalatoknál vastagon érdekelt szakemberek voltak a törvényszéki szakértők, bírósági konzultánsok. Ezért ott napjainkra egy független testület: az FCC jött létre, hasonlóképpen Angliában is. Érdekes módon ez mindjárt magával vonta a távközlési monopóliumok törvénykezésén alapuló szétverését, fellazítását. Európa sajnos ugyanezt az utat az első betűtől az utolsóig kénytelen végigjárni. Magyarországon, Németországban a helyzet a korai amerikai állapotokat tükrözi.

Ha hiszünk az analogikus fejlődés tanának, akkor a szoftverjogi fejlődésnek is ugyanezt az utat kell - talán gyorsabban - végigjárni, de ezt a fejlődést itt is várhatóan nagyon sok, jogi eszközzel indokoltnak tűnő jogtalanság fogja kísélni.

A szerzői jog büntetőjogi védelmének a szerepét is különbözőképpen értékelik a különböző országokban. A múltban a közjogi rendszerekben a szerzői jog ritkán folyamodott büntető jogágbeli szankciókhoz. Mármint, ha ezt egyáltalán megtette és nem polgári peres úton érvényesítette vélt vagy valós érdekeit. A polgári jogág viszont ezt hagyományosan enyhe szankciókkal büntette. Az elmúlt években a zene-, videó-, könyv-, program-, és védjegykalózkodás azonban megszüntette a különbségeket az egyes polgári és közjogi rendszerek között, mivel néhány ország igyekszik hatékony szabályokat és elrettentő büntetési tételeket hozni a fentiek megakadályozására.

Az állam illetően kiterjedése sajnos a fejlődés során igencsak komolyan felveti az Orwell 1984 című művében olyannyira plasztikusan ábrázolt gondolat-rendőrség szerepét, amit mondjuk ezentúl szoftver-rendőrségnek vagy éppen szerzői jogi-rendőrségnek fogunk nevezni. (MÁRA MEGVALÓSULT. MŰKÖDIK: ITTHON IS) Egy ilyen típusú intézkedés sorozat, amennyiben a kereskedelmi forgalmon túlmenő ellenőrzési és szankcionálási jogosítványokat vív ki magának, jelentősen sérti azt a jogot, amit a magánélet sérthetetlenségének neveznek. Hiszen a jogellenőrzés illetően gyakorlásához jelentősen be kell hatolniuk abba a szférába, ami az emberi magánélet része.

Itt kell egy új fogalommal megbarátkoznunk, amit már sorozatunk elején érintettünk. Mégpedig az olyan régi-új szabadságjogot, melynek tiszteletben nem tartása esetén a szerzői joggal kapcsolatos szabályok nem igazság-, hanem jogszolgáltatást, a humánus jogelveken alapuló jogtalanságot és az emberi jogok megsértését fogják eredményezni. Miként e sorozat írása során az egyik jogász-konzultáns fogalmazott:

„- Ha egy állam mondjuk a szőke, kékszemű és kopasz embereket alkotmányában nem-embereknek nyilvánítja, akkor azok büntetlenül lecsukhatók, megölhetők, sőt még az Alkotmánybíróság is jogszerűnek fogja ítélni mindezt, annak ellenére, hogy az elemi jogi elvek és normák szerint ez abszolút jog és emberellenes.”

Ennek veszélye fennáll. Nem véletlen, hogy az USA-ban polgári jogi mozgalmak indultak az úgynevezett Computer Privacy, azaz a saját számítógépes rendszerek titkainak magántitokká való minősítésére, és egészen addig - ez a dolog másik oldala - hogy adataink egy nagy részét csak tudtunkkal és beleegyezésünkkel tarthassák nyilván. Ott már nyilvánvaló az, amit itthon - érdekes módon - mindig az érdekeltek hangsúlyoznak csak, hogy a magánszemély szuverenitásának egy részét fel kell áldozni a közösség érdekében.... Ez pedig már az orwelli jogállam. Az államnak joga van mindenre. Az állampolgárnak meg meghalni, ha ezt nem tiltja a törvény.

Az új törvények igyekeznek kriminalizálni - éppen a konszernek nyomására - a szerzői jogi termékekkel való - úgymond - jogosulatlan cselekményeket. Itt mindenképpen a jogi oldal tiltakozásával lehet számolni, ezért elsősorban a polgári jogon keresztül igyekeznek ilyen szabályozást kiharcolni. Különösképpen veszélyes, hogy a magán célra, nem haszonszerzés céljából történő másolást is igyekeznek megakadályozni, szankcionálni. Ez pedig az analóg jogterületeken - videó, hangzó anyagok, könyvek, újságcikkek, hírügynökségi anyagok stb. - természetes és megszokott dolog, amit a jog is engedélyez a civilizált országokban. Ott ugyanis korábban tudomásul vették, hogy az írott és hangzó anyag, majd később a kép is az emberiség kollektív memóriája és a kereskedelmi vonatkozásai mellett az idő előrehaladtával megőrzését és hozzáférhetőségét kell biztosítani. E célt szolgálja a szerzői jogi védetség

korábban már emlegetett időhöz kötöttsége. A számítógép programok esetében ez az idő azonban hihetetlenül hosszú, nem mérhető a rendszer technikai élettartamához.



Nem csak számítógép programok azok az új gazdasági értékek, melyeket ez a technológia hozott magával. A miniaturizálás, a félvezetők struktúrájának, topológiájának tervezése is komoly szellemi értékek forrása. Az új technikával már egy chip is lemásolható.

A legtöbb országban teljesen tisztázatlan, milyen jogi módon - a kereskedelmi ipari titok védelmének körében, a szerzői jogvédelem körében, mint sajátos művészeti alkotást - próbálják védeni a hagyományos jogi értelmezésen belül. Az USA 1984-ben a japán és távolkeleti chipmásolás elleni védekezésül új utat választott. Egy „sui generis”, azaz alapjában szóló szabályozást hozott létre: a Semiconductor Chip Protection Act törvényt, aminek megfelelője a magyar jogrendszerben is él nem is olyan régen.

Az egyes országokban azonban a jelen törvénykezéssel kapcsolatos szankciók igencsak különböznek. Az USA, Kanada, Olaszország ilyenkor kártérítési igényt és a jogsértő tevékenység megszüntetését, a jogsértő termék elkobzását illetve megsemmisítését alkalmazza szankcióként. E tárgyban a holland, finn, német, japán és svéd szabályozás már büntetőjogi klauzulákat alkalmaz. Ezen eljárások azonban csak ritkán működnek, hiszen botrány csak ritkán van, mert egy ilyen eljárás lefolytatásához szükséges bizonyítási eljárás majdnem olyan komoly apparátust igényel, mint amilyet egy-egy új chip kifejlesztése. Hiszen ki kell tokozni, vissza kell fejteni az inkriminált struktúrát, majd bizonyítani kell az eredetivel való azonosságát, illetve részbeni azonosságát. Nem véletlen, hogy a perek nagy részében az Intel perli X vagy Y utángyártót, hiszen ő rendelkezik azzal a tőkével, ami kell arra, hogy a konkurens termékeket folyamatosan figyelje és visszafejtsse.

Mint egy német jogász fogalmazott e tárgyban: A jog kicsúszik az igazságszolgáltatók és a rendőri szervek hatóköréből, és előbb-utóbb high-tech ügyekben csak sima végrehajtókká válnak, sőt egyes cégek leszámolásának eszközeivé. (Na, ez van most...)

Mint látható, a Computer Privacy egy igencsak új polgári jogi követeléssé kezd válni a fejlett országokban. Az embereknek meg kell adni a magánélethez való jogot éppen úgy, mint a gépnek tartalmához való jogot. Nagy a kísértés, hogy visszaéljenek a forgalmazók a lehetőségekkel. Az Egyesült Államokban, Németországban kezdenek megjelenni olyan címkék, ahol a felirat azt kérdezi: „Lehet hogy az Ön gyermeke bűnöző?” Ugyanis az első rendőri fellépések célpontjai Németországban iskolai játéklukok, BBS-rendszerek voltak. Az első eljárások pedig játékprogramokat másoló diákok ellen folytak, hiszen ott nem kellett komoly ellenállással számolni a megtámadottak részéről.

A hatás az ellenkezőjére vált, és egyre kevésbé folytatnak az állampolgárok ott jogkövető magatartást ezen a téren, minden egyéb híreszteléssel ellentétben. Ott is azonban a nagy cápák, akik valóban illegális programterjesztésből élnek, ha nem is vígan, de élik világukat.

Itt szeretnénk eloszlatni két tévhitet: az egyik, hogy Magyarországon nem rosszabb a helyzet, de nem is jobb mint Ausztriában vagy Németországban a programok forgalmában. Az viszont már más kérdés, hogy Magyarországon az USA programverziókat és nem a sokszor butított vagy másolásvédt európai verziót keresik, ami eredeti szoftver, csak éppen a kibocsátott nem mindig ismeri el jogos példánynak. A másik, hogy Magyarországon szívesebben használnak angol-amerikai verziót, mint magyar nyelvűt, míg német nyelvterületen szinte kizárólag csak német parancsnyelvű szoftvereket lehet vásárolni. A másik probléma szintén német tapasztalat, hogy a valós helyzet eltúlzása megfelelő polgári jogi mozgalmak hiányában főként nagy cégek érdeke.

II. rész: A számítógéppel elkövetett bűnök és a magánélet

2002. május 1. 8:54 rovat: Szerzői jog

A bűn története című tanulmányunk második részében folytatjuk a számítógépes és természetesen a szerzői jogi bűncselekmények körbejárását a nemzetközi ajánlások fényében. Emlékeztetni szeretnénk: e tanulmány írása óta sok esztendő telt el, de megállapításai ma is érvényesek. Vannak kommentárok, amit nem tudott megállni e sorok szerzője, azt zárójelben találhatják a szövegben.

5. Valaki figyel... A számítógépes kommunikáció és a lehallgatás

Már több szakanyagban megjelent, hogy a hatalom sanda figyelme a bűnözők mellett igencsak gyorsan megindult a számítógépes adatkommunikáció irányában is. Sok országban az 1980-as évek óta ezt törvények szabályozzák, bár a kereskedelmi titokról szóló törvényeket senki sem tartja elegendőnek a számítógépes kommunikáció titkosságának védelmében. Hihetetlenül nagy a kísértés, hogy az adatkommunikációs rendszereket lehallgatva az állami érdekeltségek olyan ismeretek birtokába jussanak, amit felhasználhatnak politikai nyomás gyakorlására éppen úgy, mint az adók behajtására, zsarolásra vagy éppen állami méretű ipari, gazdasági kémkedésre. Erre nagyon jó ürügyet szolgáltat a bűnözés és a pénzmosás elleni harc érve, melyet laikusok első hallásra elfogadnak.

Sok ország kormányrendeleti vagy alacsonyabb szinten éppen ennek a nyomásnak a hatására olyan rendeleteket adott ki, amelyekben védik ezt a területet, a titkosság formális szféráját. Mindez közel áll ahhoz, amelyet az USA-ban Computer Privacy-nak neveznek, és ami ellen az ottani sikertelenségek láttán egyes felbátorodott forgalmazók Magyarországon megpróbálnak fellépni. (A Windows XP és az AutoCAD regisztrációs aktiválásával bemutatták, képesek a győzelemre, ha a hatalom bamba birkaként asszisztál mindehhez.) Ahol a computer privacy-t védő rendeletek érvényben vannak, ott a magán adatbázisokban való jogellenes kutakodást ezek kriminalizálják. Mindez a gyakorlat azért vált szükségessé, mert egyes ipari konglomerátumok és államok iparrá fejlesztették az adatokkal való visszaélést, és a hagyományos büntető jog értetlenül állt ezen jelenségek előtt.

Ami a számítógépekben tárolt adatok lecsapolását, a kommunikációs lehallgatását illeti, a legtöbb jogrendszer lehallgatással foglalkozó jogi - nyilvános és nem publikus - szabályozása csak és kizárólag a levélcenzúrára és a hagyományos telefonbeszélgetések - tágabb értelemben vett analóg és digitális telefonbeszélgetések, némi jogi csúrcsavarral a faxok - megfigyelésével és regisztrálásával foglalkozik. Így érthető a hatalom azon törekvése, hogy törvényesítsék a lehallgatást, az adatlopást, azaz a megfigyelés kiterjedhessen a számítógépes kommunikációk és rendszerfunkciók minden formájára. Fontosnak tartják, hogy az új törvénykezés terjedjen ki a minden lehetséges közvetlen behatolással történő, a kommunikációs utak eltérítésével és megcsapolással történő, valamint az elektromágneses kisugárzás útján történő lehallgatás eseteire, igen nagy mozgásszabadságot engedve ezzel az állami szférának. Itt a hatalom képviselői előnyben vannak, hiszen a közvetlen döntéshozók - a szenátus és a képviselőházi emberek - nem látják át egy ilyen törvény következményeit. Egyszerű gombnyomogatók. Miként külföldön, Magyarországon is probléma, hogy a bírói és ügyészi kar gyakorlatilag

képtelen a számítástechnikai problémák kezelésére. Így óhatatlanul cégekhez kötődő vagy a hatalmi struktúrában résztvevő szakembereket alkalmaz szakértőként és tanácsadóként, ami viszont enyhén szólva megkérdőjelezi a semlegességet....

A dolgot jelentősen bonyolítja, hogy nem alkalmazhatóak a hamisításokra vonatkozó rendelkezések sem ezekre az esetekre, miként az OTP mágneses hitelkártya másolóit, a telefonkártyák módosítóit is csak akkor lehet ennek alapján megfogni, ha a kártya küllemét is leutánozta, nemcsak funkcióját. (Erre a magyar jog talált egy gumiparagrafust: a számítógépes csalást, abba a hazai értelmezés szerint MINDEN belefér, ami mágneses térrel működik, vagy legalább egy elektron helyet változtat....)

Ugyanakkor sok egyéb jogi momentum is terheli és bonyolítja a számítógéphálózatokkal kapcsolatos felállást. Például, ha jogosult személy követ el adatlopást, az bűncselekmény-e? Ezt a legtöbb ország jogrendszere azzal kerüli meg, hogy csak a külsők által elkövetett ilyen eseteket kriminalizálja, az ilyen dolgokat a cég belső ügyévé, illetve polgári kártérítési per tárgyává teszi.

Igencsak érdekes az USA California szövetségi államának e tárgyú szabályozása. A szolgáltatás- és információ-lopás nem bűncselekmény, de nem is szabálysértés abban az esetben, ha a rendszert alkalmazási körükön belül használták, például egy tőzsdei rendszert használó alkalmazott onnan magán célra információkat fejt le, vagy ha az alkalmazás körén kívül van ugyan, de nem okoz kárt, vagy ha kárt okoz, akkor a szolgáltatás-lopás értéke nem több, mint 100 USD.

Mint látható, a legtöbb országban a szolgáltatás lopása a hardver illegális használatára vonatkozik. Ezt a római jogban alkalmazott megnevezéssel furtum usus-nak nevezik. Ez valamilyen tulajdon ideiglenes kölcsönvételét és használatát jelenti, a tulajdonos beleegyezése nélkül. Ilyen, ha valaki elköt egy gépkocsit, használja, majd valahol otthagyja. Ilyenkor ő nem lopott, csak jogtalanul használta más járművét. Ezt sok polgári jogrendszerű ország, mint általános érvényű jogelvet, elveti, csak néhány speciális esetben, mint például a gépjárműlopások esetében alkalmazza. Így nem valószínű, hogy a computer információkkal kapcsolatban valaha is ez fog történni. Ugyanakkor vannak olyan skandináv országok, ahol ennek a jogelvnek a használata tradicionális, így a számítógépes rendszerek jogtalan használatát, az információk jogtalan kölcsönvételét is kriminalizálják.

A klasszikus polgári rendszerű országok, mint például USA és Kanada a bevezetőben említett kormányérdekek védelmének elve alapján a jogtalan használatot és az információhoz való jogtalan hozzáférést átmossa - jogi kifejezéssel élve subsumálja - és ezzel ezen tényállások összevonásából létrejön egy olyan harmadik változat (egyszerűen lopásnak neveztetik), amely laikus fejjel felfogható, és nagyobb esélye van a laikus törvényhozásban egy ezt szankcionáló törvény elfogadásának. Hiszen a lopás magával vonja a kártérítést és a büntetést.

Ennek a jogi csúrcsavarnak van egyetlen racionális indoka is. Ugyanis egy rendszerben lévő információ felhasználásához meg kell történnie a rendszerhez való jogosulatlan hozzáférésnek. Más országok egy analóg szabályozást választanak: ha a számítástechnikai rendszer szolgáltatásai pénzért elérhető szolgáltatások, akkor analóg módon ugyanazokat a szabályokat kell rá alkalmazni, mint például, ha valaki vezetékes gázt, elektromos energiát vagy éppen telefont lopna a szolgáltatótól. (Nálunk is hasonló a helyzet: szolgáltatás-lopásról van szó)



Ugyanakkor kérdés az, hogy az állam miként tekinthet bele ebbe, a feje felett is működő kommunikációs rendszerbe. Nagy felzúdulást váltott ki Belgiumban, Hollandiában és a német nyelvterület országaiban egy olyan szabályozás, mely teljesen megtiltja magán személyeknek és cégeknek a kódolt, titkosított kommunikációt. Bankok és arra indokoltnak látszó, és erre engedélyt megkapó szervek jogosultak csak titkosítást használni, de csakis olyan eljárást és kulcsot, amelyet előzetesen leadtak egy arra illetékes állami hivatalnak, hogy a lehallgatók meg tudják fejteni a kódolt üzenetek tartalmát. Az USA-ban ez kicsit másként működik. Ott ugyanis a polgári és nemzetközi kereskedelembe nem árusítható olyan rejtjelező eszköz, melynek kódját az NSA, azaz az USA nemzetbiztonsági ügynöksége egy adott időn belül ne lenne képes megfejteni. (Ezt a szabályozást a hidegháború megszűntével feloldották. Most a terrorizmus elleni harc ürügyén inkább a rendszerek felpuhításával, hátsó ajtók beépítésével kísérleteznek, de e kemény kriptográfiai eljárásokat is megpróbálják ellenőrzésük alá vonni.)

Itt a magyar szabályozás abszolút mértékben eltér ettől, és a józan önvédelem eszköze. (Sajnos ennek amerikanizálása várható, ami az informatikai öngyilkosság sajátos, és jól definiált formája a szerzői jogi rendelkezések következetes átvételével együtt...) Ugyanis minősített információk továbbítására csakis olyan kódolás alkalmazható, amelynek megfejtése a benne lévő információ elavulásánál jóval hosszabb időt igényel. Tehát nem a maximális, hanem a minimális titkossági fokot írja elő. Ennek elbírálására a Belügyminisztériumon belül működik a Rejtjelfelügyelet, amely megvizsgálja és titkossági szempontokból minősíti a forgalomba, illetve alkalmazásba kerülő titkosító eszközöket és eljárásokat. Ezt a szabályozást mindenképpen meg kellene őrizni a későbbiek folyamán is. Ugyanakkor a magyar rejtjeltörvény nem tiltja magánszemélyek és vállalkozások kódolt kommunikációját. Csak a Magyar Posta nem vesz fel, csak kizárólag arra jogosult testületektől - követségek, külképviseletek - rejtjeltáviratokat. Ennek oka első sorban a nemzetközi postai szabályozásban rejlik.

Ugyanakkor az USA és a Cebit egyik szemináriumán kiderült: Németország igyekezik elérni, hogy a számítógépes rendszerek, de még az ISDN és digitális hálózatok lehallgatásának szabályozása is maradjon ki a törvénykezésből. Ez érthető, hiszen a spontán kommunikáció állandó és elektronizált megfigyelése a gazdaság és az egyén állapotáról, az eltitkolt jövedelmekről és sokmindentől naprakész tájékoztatást nyújt aképpen, hogy egyes szervek csak ülnek és figyelnek. (Magyarországon a Nemzetbiztonsági Szakszolgálat teljesen törvényesen végezhet általános célú, preventív lehallgatásokat, megfigyeléseket az Interneten és a telefonhálózaton. Ügyészi felhatalmazás csak egyes egyének konkrét kommunikációjának tartalmi feldolgozásához kell. Magyarán: minden gyűjthető, kivéve hogy a levél csak felhatalmazással olvasható el...) Egyik előadó említette, hogy az USA-ban a telefonbeszélgetéseknél a digitális központok teremtették meg az adat-, a fax-forgalom és a beszélgetés szelektív szétválasztásának és regisztrálásának lehetőségét. A telefonközpontok log-állományait, amelyek azt tartalmazzák, hogy ki kit és milyen átviteli úton hívott, immár harminc évig megőrzik. Ugyanakkor a közelmúltban készítettek olyan kiegészítő áramköröket, amelyek egy beszélgetésben mintegy 50-100, úgynevezett hívószót képesek felismerni. Ha például ezeket vagy ezeket egy adott előfordulásnál nagyobb számban találják a beszélgetésben (például háború, LSD, terrorizmus stb.), akkor a beszélgetést az elektronikus átmeneti tárolóból utólag kiteszik az értékelőkhöz. Ez a kulcsszó állomány dinamikusan változtatható.



Az előadó - aki hacker körökben is eléggé jól ismert - újra kifejtette azon véleményét, hogy a digitalizálás egyre inkább átok, mint áldás lesz az emberek számára. A törvényhozók nem értik egy-egy rendelet veszélyeit, ugyanakkor a szakértői testület egyre inkább képes maradéktalanul saját elképzeléseit érvényesíteni. (Azaz saját törekvéseik érdekében orruknál fogva vezetni a törvényhozókat. Az állami törvények és erőszakszervezetek egyre inkább egyes cégek, cégcsoportok saját érdekeit szolgálják.) Márpedig a finansziális államigazgatási szférából éppen úgy, mint a hírszerzési és egyes bűnüldözési körökből igen nagy nyomás nehezedik egy ilyen típusú, totálisan ellenőrzött társadalom megvalósítására. Ott mutattak be egy olyan rendszert - hazai megvalósítása is ismert - amelyik egy autópálya mellett elhelyezve, optikailag leolvassa az elhaladó kocsik rendszámát, és azt egy központi adatbázisba viszi be. Ezt állítólag a majdan bevezetendő fizető autópálya adatok nyilvántartására akarják felhasználni, de egy rendőr-szakértő szerint a lakosság gépkocsi mozgásának regisztrálásával már több illegális fuvarozót, embercsempészt, terroristát lepleztek le. Ehhez viszont a biztos, ami biztos elve alapján egy teljes tartomány kulcsútvonalainak gépkocsi-mozgását tárolják és regisztrálják. (Németországban. Itthon az autópálya ellenőrző kamerarendszere kezd ilyen feladatokat betölteni) Ennek kapcsán említettek meg egy USA jogesetet, amikor egy kéjgyilkost úgy lepleztek le, hogy egy egész település minden lakosáról ujjlenyomatot vettek. Később bírósági döntések során kellett köteleznie az FBI-t az eképp képződött archívum megsemmisítésére és a lakók ma sem biztosak benne, hogy valahol nem lapulnak ezen kartonok másolatai. (Másik ügy kapcsán kiderült, nekik van igazuk...)

Hasonló megoldás ismert, és várhatóan nagyon rövid időn belül az NSZK-ban polgárjogot is nyer. Itt egy elektronikus rendszerrel előállított személyi igazolványról van szó. (Már nálunk is ez a módi...) A kép egy elektronikus kamerával készül, amit rögtön digitalizált formában tárolnak. Van olyan rendszer, amelyik ennek alapján - például egy tüntetés-videóról - azután képes azonosítani az ott résztvevőket. Hasonlóan érdekes a beszélő személyi igazolvány koncepciója. Ezt már, mint katonai és polgári objektumokon belüli mozgás ellenőrző eszközt, két-három éve mindennapos gyakorlatként alkalmazzák. Itt az igazoló kártyában elhelyezett passzív áramkör, ha egy lekérdező induktív hurok felett vagy mellett halad el a tulajdonosa, le tudja kérni a kártya azonosítóját. Ezzel embereket lehet ugyanúgy nyomon követni, mint a rendszám leolvasó rendszerrel az autókat. (Amerikában a bőr alá ültethető azonosító rendszeren dolgoznak. Természetesen az állampolgár saját érdekében...)

Sajnos a számítógépes bűnözés szabályozása sok esetben az állampolgár helyett egyre inkább a forgalmazók, illetve az államapparátus érdekeit védi. Erre lehetősége van, mert a számítástechnika ilyen alkalmazásának veszélyeit vajmi kevésbé lehet felmérni. Ezzel kapcsolatosan még az sem mindegy, ki milyen adatokat és hogyan tárol rólunk.

Töredékes jellege miatt a büntetőjog nem alkalmas az adatok helyességének, illetve a gyűjtési-felhasználási körnek, az egyes adatok összekapcsolhatóságának szabályozására. Erre más jogi eszközöket kell alkalmazni, amelyekre sorozatunk következő részében fogunk majd kitérni.

6. A magánélet tulajdona: magán vagy köztulajdon?

Mielőtt továbblépnénk, vajon hogyan kezelik az egyes szervezetek a számítógépes bűnözés problémakörét, érdemes még egy pár mondat erejéig az adatoknál maradni. Az egyes adatok már önmagukban is a személy tulajdonát, magánéletének részét képezik. Ugyanakkor ezen adatrendszerek összekapcsolása lehetővé teszi az egyes személyek magánéletének korábban sohasem látott teljességű átvilágítását.

Nem szakmai, hanem erkölcsi etikai probléma, hogy egy társadalom olyannyira feláldozza az ártatlan állampolgárainak emberi jogait, a kisebbség megfegyelmezése érdekében.

Tipikus megnyilvánulása ennek a magyar személyi szám problémakör. Annak ellenére, hogy a Magyar Köztársaság Alkotmánybírósága megállapította, hogy használata sérti alapvető állampolgári jogainkat, a belügyi, rendőri szervek és - ami viszont még inkább jogsértő - az APEH, a Vám és Pénzügyőrség, és emellett másodlagosan a Társadalombiztosítási és Nyugdíj Önkormányzat mai napig ezt használja az adatok összeillesztéséhez. Ezen a jelenlegi helyzetben mit sem segítene, ha kiváltanák egy másik személyi jellel, hiszen megfelelő translációs táblák készítése, karbantartása és egyeztetése a mai számítástechnikai és hírközlési eszközökkel egyszerű. (Jelenleg ugyan ezek a szervek a napi gyakorlat szerint külön azonosítókat alkalmaznak, de egy percig sem titkolják - elvileg ügyészi engedéllyel - ezek a rendszerek, a benne nyilvántartott adatok éppen a személyi számmal összekapcsolhatóak. Azaz a hatalom képtelen lemondani játékszeréről.) Nagyon hiányzik a mai magyar társadalomból egy olyan erős polgári jogi mozgalom, amely a számítástechnikai alkalmazásokban nem érdekelt szakembereket fogja össze a számítástechnikai eszközökkel való visszaélés csökkentése érdekében. Ez az USA-ban fejlett, míg az Európai Közösségben csak most kezdi szárnyait bontogatni. (Viszont minden hatalom összefogva a céges lobbykkal mindent elkövet ezen csoportok jelentőségének csökkentésére, illetve ellehetetlenítésére, A fő szállóige a terrorizmus elleni harc, aminek érdekes módon már részévé vált a szerzői jogi szervezetek igénye is.)



A számítógépes bűnözés büntetőjogi problémaival foglalkozó első nemzetközi kezdeményezés az OECD - azaz a Gazdasági Együttműködési Fejlesztési Szervezet - kezdeményezésére jött létre. 1983-1985 között működött egy ad-hoc bizottságuk, mely a nemzetközi számítógépes bűnözés elleni harc összehangolásának első lépéseként a tényállások megfogalmazását és közelítését tartotta fontos célnak. Ők igen tisztán láttak, az ebben rejlő visszaélés veszélyeit is megfogalmazták. Ez a korábban vázolt szituáció alapján abból áll, hogy a jog eszközeivel a szoftverforgalmazók saját üzleti érdekeiket, stratégiájukat erőltetik rá a társadalomra, ugyanakkor az állam sok területen a polgári demokratikus társadalmakban nem kívánt elő- és erőjogi eszközökhöz jut. Olyanokhoz, amelyek korábban a totalitáriánus diktatúrákban sem igen léteztek, mert azoknál az eszközöknél jóval hatékonyabbak. Mint egy magyar jogász-professzor előadásában az ilyen szituációt megfogalmazta:

‘Kérem, ilyenkor hol van az igazság? Az igazság, az emberi jog az halott! Itt jogszolgáltatás történik!’

Az ad-hoc bizottság éppen ezért kérte a tagországokat, fontolják meg, milyen mértékig kellene kriminalizálni a tudatosan elkövetett cselekményeket a számítógépes visszaélés területén és milyen mértékben kellene foglalkozni ezzel az egyes nemzetek egyéni büntető törvénykezésének?

A lényeges törvények komparatív elemzése alapján az OECD 1986-ban javasolta az alábbi tényállások nevesítését:

- A számítógépi adatok és /vagy számítógépi programok szándékos bevitele, módosítása, törlése, és/vagy visszatartása, amelynek a célja a pénzek vagy egyéb értékek illegális transzferének elkövetése.

Ezen pontban a pénzügyi és egyéb értékhozó rendszerek vírusokkal, trójai programokkal, másolásvédelmi rendszerekkel történő megtámadását próbálja ezzel a megfogalmazással kivédeni a nemzetközi ajánlás. Hasonló megfontolás alapján született a következő két pont is...

- A számítógépi adatok és/vagy számítógépi programok szándékos bevitele, módosítása, törlése és /vagy visszatartása, melynek célja a hamisítás elkövetése.

- A számítógépi adatok és/vagy számítógépi programok szándékos bevitele, visszatartása vagy módosítása vagy a számítógépes rendszerekkel való egyéb szándékos interferencia (például külső elektromágneses térrel történő szándékos zavarás), amelynek célja a számítástechnikai és/vagy telekommunikációs rendszer működésének akadályozása.
- Védett (és itt KIZÁRÓLAG JOGI ESZKÖZÖKKEL, például szabadalommal vagy szerzői joggal védett programokról van szó. A Védett szó minden esetben a jogi védettséget jelöli és nem például annak technikai megvalósítását, például másolás-védelmet, licence managert stb.....) számítógépi program tulajdonosának kizárólagos jogának megsértése azzal a szándékkal, hogy a programot kereskedelmileg kiaknázzák és piacra dobják.

Ezen ajánlás mint látható CSAK a kereskedelmi célú másolást rendeli a jog hatálya alá. A kereskedelmi fogalom viszont igencsak egyértelműen definiált, miként az áru is az egyes országok jogi-törvénykezési rendszerében.

- A számítógépes és/vagy telekommunikációs rendszerhez való tudatos hozzáférés vagy annak lehallgatása a rendszerért felelős személy felhatalmazása nélkül, vagy a biztonsági intézkedések megsértésével vagy egyéb tisztességtelen káros szándékból.

Ezen megfogalmazás érdekessége, hogy elvben ezen rendszereket teljes körűen igyekszik védeni. Ezzel szemben vannak olyan törekvések, amelyek az államhatalmi, hírszerző és pénzügyi szervek részéről éppen a kommunikációs szféra számukra történő teljes átvilágíthatóságára törekszenek. E két irányzat közül - mármint a privacy védelme és az állam totális ellenőrzése -, sajnos az utóbbi látszik felülkerekedni. Ezt mutatják a nyugati országokban a rejtjelezést korlátozni akaró rendelkezések, és az a törvénycsomag, amit hazánkban a pénzmosás tilalma néven emlegetnek, és amely gyakorlatilag megszünteti, az állam számára átláthatóvá teszi - egyéb kiegészítő rendelkezésekkel kapcsolva - a bank- és üzleti titkot az államhatalmi és adó-, vám-, TB-szervezetek számára.

Az 1989-ig ülésező bizottság - neve: Az Európa Tanács Számítógépes bűnözéssel foglalkozó Válogatott Szakértői Bizottsága - kapcsolódva a Bűnözés Problémaival foglalkozó Európai Bizottság munkájához, elkészítette az R. (89). 9. számú ajánlást, melyet az Európa Tanács 1989 szeptember 13-án elfogadott, és ezzel európai alapszabálynak jelölt ki. Ezen nyilatkozat:

‘Ajánlja a tagállamok kormányainak, hogy vegyék figyelembe, amikor áttekintik törvényeiket vagy új törvényeket kezdeményeznek....’

A nemzeti törvényhozások számára készült irányelvek tartalmazzak egy olyan minimum listát, mely tükrözi a bizottság tagjainak konszenzusát a számítógépes bűnözésre vonatkozóan, amelyekkel a számítógépes bűncselekményekkel kapcsolatos törvények megalkotása során feltétlenül foglalkozni kell, ugyanakkor egy opcionális listát, ahol a korábbiakban kifejtett aggályait hangoztatták az egyes meghívott szakértők, és ahol fennáll a joggal való visszaélés veszélye is.

Érdemes megismerkedni ezen minimum lista tartalmával és definícióival:

1. Számítógépes csalás

Számítógépes adatok vagy számítógépi programok bevitele, módosítása, törlése vagy visszatartása vagy egyéb interferencia az adatfeldolgozás során, amely befolyásolja az adatfeldolgozás eredményét, és ezáltal más személynek gazdasági vagy tulajdoni vagyoni kárt okoz, (Itt megjelöltek egy alternatív szöveget is: azzal a szándékkal, hogy jogellenesen megfossza azt

személyi tulajdonától) abból a célból, hogy jogellenes gazdasági hasznot szerezzen magának vagy más személynek.

2. Számítógépes hamisítás

Számítógépi adatok vagy számítógépi programok bevitele, módosítása, törlése vagy visszatartása vagy egyéb interferencia az adatfeldolgozás során olyan módon, vagy olyan feltételek közepette, ahogyan a nemzeti jogrendszer a hamisítás fogalmát megtestesíti, ha elkövetik az ilyen bűncselekmény hagyományos tárgya tekintetében. (Ennek a jogi ajánlásnak a hazai próbája a közeljövőben lesz az OTP pénzautomatáit megcsapoló egyetemisták ügyében....) (Megvolt. Azóta Lex MATÁV címen is ismerik, hiszen a MATÁV telefonkártya klónozókkal szemben ennek alapján lépnek fel. Ebből is a magyar gyakorlatban gumiparagrafus lett.)

3. Számítógépi adatokkal vagy számítógépi programokkal szembeni károkozás

Számítógépi adatok vagy számítógépi programok törlése, rongálása vagy visszatartása jog nélkül. (Ezen paragrafus kompromisszum eredménye, és mint ilyen, sajnos visszaélésre ad alkalmat. A „Jog nélkül” klauzula elhagyása lett volna a normális megoldás. Mert itt, ha egy másolásvédelem törli a programot, adatokat, akkor annak forgalmazója a jogaira hivatkozhat. Szakemberek ez másolásvédelmi paragrafusként is idézik.) (A jelenlegi hang CD védelmek kiagyaloí is erre hivatkoznak, nekik jogaik vannak, és a felhasználóknak-vásárlóknak pofa súlyba!)

4. Számítógépes szabotázs

Számítógépi adatok vagy számítógépi programok bevitele, módosítása, törlése vagy visszatartása vagy egyéb interferencia számítógépes rendszerekkel azzal a szándékkal, hogy akadályozzák egy számítógépes vagy telekommunikációs rendszer működését. (Másik ismert neve: Vírusellenes paragrafus.)

5. Jogosulatlan hozzáférés

Számítógépes rendszerhez vagy hálózatokhoz való hozzáférés jog nélkül, a biztonsági rendszabályok megkerülésével. (Magyar megfelelője: Szolgáltatáslopás.)

6. Jogosulatlan lehallgatás

Számítógépes rendszer vagy hálózat felé, vagy abból vagy azon belül történő lehallgatás jog nélkül, technikai eszközök igénybevételével. (Ez szinte hallgatólagosan két dolgot mond ki:



- a.) Az államnak mindenhez mindig joga van, mert ha mégsincs joga, akkor hoz olyan törvényi szabályozást, hogy joga legyen rá.
- b.) A véletlen áthallás, műszaki hiba eredetű ilyen probléma természetesen nem számít bűncselekménynek, még akkor sem, ha valaki ezt a lehetőséget tudatosan kihasználja.)

7. Védett számítógép program jogosulatlan másolása

Törvény által védett számítógépi program másolása, terjesztése vagy kommunikációja a köz felé jog nélkül. (Legtöbb vitára és visszaélésre lehetőséget adó ajánlás, buktatóit korábban már tárgyaltuk.)

8. Topográfia jogosultan másolása

A félvezető termékek törvény által védett topográfiájának (maszkrajzainak) jog nélküli másolása, vagy annak a topográfiának az azon topográfia felhasználása által gyártott félvezető termékeknek a kereskedelmi felhasználása vagy importálása kereskedelmi célra jog nélkül.

A határozat tartalmaz egy igencsak vitatott részt, az úgynevezett opcionális listát, melyet a tagállamok saját ízlésük szerint implementálhatnak, mivel e tárgyban konszenzus nem született. Az aknák, és a jogi eszközökkel alkalmazott jogtalanság veszélye ezen tényállásoknál jóval nagyobb, mint az eddigiekben ismertetett tényállások esetében.

1. Számítógépi adatok és/vagy számítógépi programok módosítása

Jog nélküli módosítása az adatoknak vagy a programkódnak. (Kriminalizálhatóvá teszi a programok trójaivá történő alakítását éppen úgy, mint a hibák kijavítását (patch) vagy éppen akár a másolásvédelem leszedését. E veszély ez utóbbiban rejlik, amiért eddig még senki sem kriminalizálta ezen tényállást, vagy az ajánlottnál szűkítettebb mértékben adatokra korlátozva, mint például Svédország, Anglia.) (A tanulmány írása óta Magyarország a jogvesztői lobby nyomására a szerzői jogi törvény részeként kodifikálta. A paragrafus csúfneve Lex UPC. Érdekessége, hogy még olyan ISMERET, DOKUMENTÁCIÓ, eszköz, TUDÁS, KÉPESSÉG birtoklását is tiltja, amellyel egy technikailag levédett információ a szerzői jog tulajdonosának beleegyezése és tevőleges közreműködése nélkül felfedhető. Az EU új jogértelmezése alapján így tiltott a rendszerhibák felfedése, dokumentálása és természetesen javítása, tesztelése is...)

2. Számítógépes kémkedés

Kereskedelmi titok vagy egyéb jogilag védett dolog jogosulatlan megszerzése, felfedése továbbítása vagy jog nélküli felhasználása azzal a céllal, hogy gazdasági veszteséget okozzanak annak a valós vagy jogi személynek akit megillet az a titok, vagy azzal a céllal, hogy jogellenes előnyt szerezzen valaki saját maga vagy egy harmadik személy számára. (A paragrafus ezen megfogalmazása veszélyt jelent a számítógépes kultúra egészére nézve. Ugyanis kimondatlanul tiltja a program visszafejtés a reverse engineering minden fajtáját, ugyanakkor elméletben büntethetővé teszi azt, ha valaki leleplezi egy forgalmazó programokba beépített praktikáit, büntető rutinjait, mert egyrészt a visszafejtéssel megsértette az ipari titkot, másrészt kárt okozott annak, aki ezt alkalmazta. Ezen megfogalmazásában kifejezetten életveszélyes jogi megoldás....)

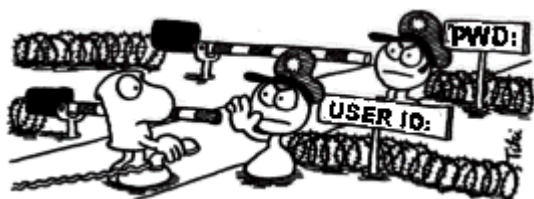
3. Számítógép jogosulatlan használata

A számítógépes rendszer vagy hálózat jog nélküli használata, amelyet vagy:

- a.) abban a tudatban követnek el, hogy jelentős veszteségi kockázatot okoznak annak a személynek, akit megillet a rendszer használata, illetve kárt okoznak a rendszerben és/vagy annak működésében
- b.) azzal a szándékkal követnek el, hogy jelentős kárt okozzanak annak a személynek, aki jogosult a rendszer használatára, illetve kárt okoznak a rendszerben és/vagy annak működésében
- c.) kárt okoz a használatra jogosult személynek vagy a rendszernek, vagy annak működésében.

4. Védett számítógépi program jogosulatlan használata

Egy számítógépi program jogosulatlan használata, amelyet a törvény véd, és amelyet jog nélkül lemásoltak vagy abból a célból használják, hogy jogtalan gazdasági hasznot szerezzen valaki magának vagy másik személynek vagy a jog birtokosainak.



Mint láthatóak, ezen ajánlások nagy része létkérdés egy ipari informatikai társadalom számára. Ugyanakkor látszik az állampolgári polgári jogi kontroll teljes hiánya, amely nagyon sok emberi, etikai, gazdasági problémát fog okozni az informatikai társadalmak számára. Ezen törvényeket a nyugati országokban emberi tragédiák, az emberi igazságérzettel ellenkező bírósági ítéletek sora kíséri. (NÁLUNK IS!!!!) Ugyanakkor a polgári jogi mozgalmak képtelenek még - az USA kivételével - felfogni az egyes polgárookra, a Privacy-ra leselkedő veszélyeket, az államrezon fokozódó túlhatalmát, amit cégek érdekei motiválnak sok esetben. (Az USA-ban a terrorizmus elleni harc ürügyén a polgári jogi szervezetek száját hatalmi szóval befogták.)

Ugyanakkor az ENSZ is megpróbált valamiféle jogi zsinórmértéket állítani ezen a téren. Ezért a nyolcadik kubai kongresszusán 1990-ben Kubában, majd később is foglalkozott ezzel a kérdéssel. A Bűnözésmegelőzésről és az Elkövetőkkel való Bánásmódról Szóló VIII. ENSZ kongresszus határozata ezt részben pontosítja.

Erről szólunk sorozatunk következő részében.

7. A számítógép és az egyén magánélete

Az 1990-es évek végén a Bűnmegelőzésről és az Elkövetőkkel való bánásmódról szóló Nyolcadik ENSZ Kongresszuson Kubában majd azt követő, a Számítógépes Bűnözés Megelőzéséről és a Törvénykezésről című szimpóziumon, melyet a Foundation for Responsible Computing szervezett, megvitatták a számítástechnikával kapcsolható bűnözés jogi szempontjait is. A kanadai delegáció határozott fellépése alapján a kubai ENSZ kongresszus egy határozatot fogadott el, amely kimondja a következőket:

Felhívja a tagállamok figyelmét, hogy a már elvégzett munkára való tekintettel lépjenek fel hatékonyabban a számítógépes bűnözés ellen, mégpedig azokkal a visszaélésekkel szemben, amelyek büntető szankciók alkalmazását igénylik. Itt elsősorban a hagyományosan köz-törvényes bűncselekmények számítógéppel megvalósított variánsai kerülnek szóba: például a bankátutalásokkal kapcsolatos műveletek.

Fontolóra kellene venni szerintük szükség esetén a következő intézkedések megtételét:

- a.) Biztosítani, hogy a már meglévő kriminalizált - azaz bűncselekménynek elfogadott és jogilag szankcionált - cselekmények esetében a bizonyítékok a bírói eljárásokban elfogadhatóak legyenek. Ha szükséges ehhez a Btk és a Ptk és a PP megfelelő szabályaiban illetve a jogrendszerben szükséges törvényi változtatásokat el kell végezni.
- b.) Ha hiányoznak a törvények, melyek a megfelelő bizonyítékokra illetve a nyomozati cselekményekre vonatkoznak, azt meg kell hozniuk és kialakítaniuk az alkalmazáshoz szükséges egységes jogi gyakorlatot.
- c.) Biztosítani a számítógépes bűncselekmények révén szerzett vagyonok elkobzását és az eredeti állapot helyreállítását.

(Sajnos, mint láthatjuk, ezek nagyon szép elvek. Ugyanakkor ezen gyakorlat tekintettel arra, hogy itt csak és kizárólag az államrezon és a mögötte meghúzódó gazdasági és politikai hatalom hozza ezen rendelkezéseket, anélkül hogy a megfelelő ellensúly, azaz a polgári és civil szféra, a védőügyvédek és egyéb érdekképviselői csoportok hangsúlyosan képviselnék a hatalomtól független érdekeiket, egyre inkább a joggal való visszaéléshez vezet. Gazdaságilag

mintha a korábbi helyzet lenne...)

- h.) Intézkedések elfogadása a számítógéppel kapcsolatos bűncselekmények áldozatai számára, összhangban az ENSZ-nek a Bűnözés és a Hatalommal való Visszaélés Áldozatainak Igazságtétele Alapvető elveiről szóló 40/34 számú közgyűlési határozat alapján, beleértve az illegálisan megszerzett vagyonok eredeti gazdájuknak való visszaszolgáltatását, és az áldozatok bátorítását szolgáló intézmények megszervezését, és azt, hogy az ilyen bűncselekményeket a károsultak bejelentsék.



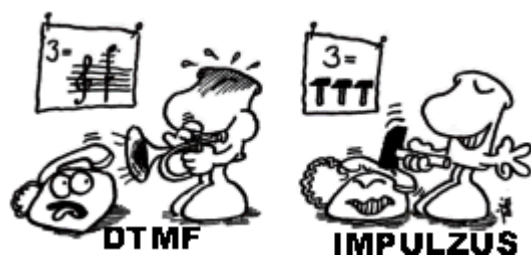
Az ENSZ Közgyűlése 1990 december 14-én elfogadott határozatában felszólította a tagországokat, hogy kulturális hagyományuknak és jogrendszerüknek megfelelően tegyenek lépéseket a számítógépes bűnözés megelőzésével illetve szankcionálásával kapcsolatos törvények és direktívák kidolgozására.

lémát vetnek fel. Az anyagi tárgyakra vonatkozó jogszabályoktól eltérően az információs jog (eképpen nevezi a szakirodalom a számítástechnikával kapcsolatos törvénykezési és jogi szakágat) birtokosa vagy tulajdonosa nemcsak a gazdaság érdekeit nézi. Figyelembe kell vennie azon személyek érdekeit is, akiket az információ tartalma érint. A számítástechnika elterjedése előtt igencsak korlátozott volt azoknak a jogi védelme, akiket az információ tartalma érintett. A büntetőjogban a panaszokra vonatkozó rendelkezések kivételével szinte semmi sem volt, ami erre vonatkozott volna, azon rendelkezéseket is éppen általánosságuk tette erre a területre alkalmazhatóvá, némi jóindulattal.

Az 1970-es évek óta azonban az új technológiák kiterjesztették az adatok tárolásának, gyűjtésének és értékelésének módszereit. Az adatok összekapcsolása, továbbítása, visszakereshetősége és e formában történő tárolása, az egyes, korábban nem összekapcsolt rendszerek automatikus és asszociatív jellegű összekapcsolása nagyobb fenyegetettséget jelent a magánszférának, mint korábban bármilyen titkosszolgálati nyilvántartás vagy besúgóhálózat bármikor a történelmi fejlődésünk eddigi menetében. Ez viszont fokozottabban szükségessé teszi a magánszféra védelmét az egyéni magánélethez, az otthon tárolt adatokhoz (computer privacy) való jogát az egyénnek. Aki ismeri az államigazgatási gyakorlatot, az tudja, hogy érvényes alkotmánybírósági döntések sorozata ellenére sem sikerült Magyarországon kiirtani a személyi szám használatát igen sok területről. Az USA törvénykezése, annak ellenére, hogy van ilyen egységes nyilvántartó számuk, a Social Security Number, mégis személyi igazolvány bevezetését fontolgatja. A Nagy Testvér kíváncsisága határtalan.....

A magánszféra védelmére a különböző jogi hagyományokkal rendelkező országok különböző típusú szabályozást hoztak. Ezek legtöbbször nem foglalkoznak speciálisan az informatikai eszközökkel, hanem egy elvi és generális szabályozási szisztéma részét képezik. Legtöbb országban ezen alapokon a bíróságok is kidolgozták annak joggyakorlatát, hogy mi az, amit magánszférát ért sérelemnek nevezünk. A nemzeti törvénykezési elvek analízise, valamint a vonatkozó jogszabályok vizsgálata azt mutatja meg, hogy a különböző országok joggyakorlatában jelentős mértékű azonosság figyelhető meg a privacy megítélésében.

A legtöbb nemzeti törvény tartalmaz olyan rendelkezéseket, amelyek szabályozzák az adatgyűjtést, vagy lehetővé teszik, hogy az egyén az engedélyezett rendszerben róla gyűjtött adatokhoz hozzáférhessen. Ennek ellenére szinte mindenhol az állami szféra saját törvényeinek megsértésével vagy éppen rugalmas alkalmazásával egyre több és több adatot gyűjt be, úgymond a kriminális viselkedés és a biztonsági kockázat csökkentésére saját-, és az országban megforduló idegen állampolgárokról. Itt elsősorban a vám- és adóügyi szervek járnak az élen, de ezeket szorosan követik a különböző nemzeti információs szolgálatok és más, államrezon részét képező nyílt vagy legtöbbször titkos szervezetek. Így e nyilvántartások létéről legtöbbször az állampolgároknak sincsen tudomásuk, és ezek adatait - éppen a lelepleződés elkerülése végett - mindig csak közvetetten használják fel. Erre bizonyítható példa a keletnémet STASI hatalmas archívuma, vagy éppen Franciaországban az egyik bulvárlap leleplezés sorozata az állami titkos(piszkos)szolgálatok működéséről.



Éppen ezért, bár a tendencia pozitív (már régen nem az, de optimista voltam, amikor írtam mindezt), jelentős különbségek vannak az egyes országok rendelkezéseiben, melyek az alkalmazás hatályát érintik. Jogi személyek jogait legtöbbször igencsak szabadosan, vagy például az USA-ban szigorúbban kezelik, mint a természetes személyekét. A különbségek az egyes nemzeti jogokban a különböző típusú adatok gyűjtésének és felhasználásának tiltásában keresendők.

Melyek a Privacy ellen az egyes jogrendszerekben elfogadott és üldözendő cselekmények? Ezzel foglalkozunk sorozatunk következő részében. Ugyanakkor azonban azt is le kell szögezni, hogy a titkos eszközökkel történő adatgyűjtés eseteit gyakorlatilag ellenőrizhetően eddig még egy ország sem szabályozta, annak ellenére, hogy a titkosszolgálati és rendőrségi törvényekben erre utalások találhatók.

8. Nyom nélkül? Hol a bizonyíték?

A számítástechnika igen sok specifikus eljárásjogi és nyomozástechnikai problémát vet fel. Mindezek azonban nem vizsgálhatóak a nélkül, hogy ne vizsgálánánk az ezzel a hatóság illetve a feljelentő részéről a vád javára történő visszaélés lehetőségét. Ugyanis a számítástechnika csábítása nem csak a hagyományos értelemben vett bűnözőket vonzza. Vonzza a programok kereskedőit, akik a kriminalizálás révén kényszeríteni szeretnék a felhasználót szükségletein túlmutató vásárlásra, túlköltekezésre.

(Tőlem került át a mindennapok használatába a police aided sales - PAS, azaz rendőrileg segített eladás -, illetve Dr Simai Endre számítástechnikai újságírótól a LAS - azaz a Lawyer aided sales , magyarul ügyvédekkel segített eladás - gúnyos, de igaz definíciója.)

Mi tarthatja vissza a hatalmat vagy pedig egyes cégeket, hogy a számukra kellemetlenné vált személyektől cégektől egy számítógépes eszközökkel elkövetett bűncselekmény kreálása révén szabaduljanak meg? A magyar gazdaságban már vannak jelek, hogy ezen negatív irányzatok igencsak hamar elsődlegessé válnak a valódi számítógépes bűncselekmények felett. A konkurrenciaharc és a hatalmi harc eszközeként züllesztik le a jogot, amellet, hogy a felhasználókat szükségleten felüli vásárlásokra és magánéletük feladására kényszerítik. Ugyanakkor a magyar gazdaságban e miatt újra beállt a csengőfrász állapota.

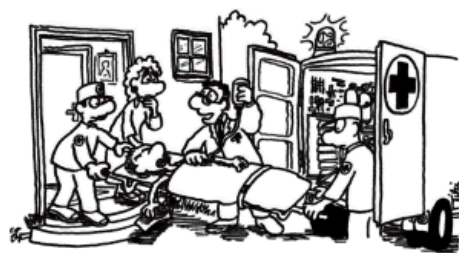
A jog fejlődésnek azonban valamiképpen követnie kell a technikai fejlődést. Ugyanis egyre több esetben a számítástechnikai bizonyítás az egyetlen, amely rendelkezésre áll. A mikrofilm helyét kezdi átvenni a papírmentes iroda (tévedtem, ismét működik a papír), ahol a CD-ROM-ra rögzített dokumentum. Ilyenkor egyre inkább az eredeti tárolása helyett annak megsemmisítése kerül előtérbe. Ugyanakkor egyre több dokumentum kizárólag gépben létezik és képződik, meg akkor is, ha esetleg a végén ott a kibocsátó hagyományos aláírása - ami szintén fotóról került oda.

Így a számítástechnikai eljárásjogban alkalmazott kényszerintézkedések nagy része éppen a hagyományos jogban ellentétes szerepet kaphat, ugyanis ahelyett, hogy a vádlott bűnösségének bizonyítására szolgálhatna, éppenséggel ellentétesen, lehetőséget ad arra, hogy egyik oldalon a vádlott terhére róható dolgokat viszonylag kényelmesen, kívánság szerint gyarapíthassák, másik oldalon pedig komoly emberi jogi aggodalomra ad okot. Ugyanakkor ez a lehetőség - amennyiben az emberi jogok tiszteletben tartásával konform jogrendszerekkel van dolgunk - a vádlott számára is megfelelő jogilag és számítástechnikailag képzett védelem és bíróság esetén megadhatja a védekezés lehetőségét. (Ez nálunk a Holdban...)

Itt a jog története során először állunk szemben egy olyan kihívással, hogy bizonyos dolgokat HINNI kell. Vagy HINNI kell a vádlottnak, hogy nem bűnös, vagy HINNI kell a vádlónak, hogy a terhelt elkövette a terhére rótt cselekményt. Ugyanis a számítástechnikai eszközökkel tárolt dokumentumok az elsők a világ történelme során, amelyeknél a bennük kellő szakértelemmel végzett változtatások utólag soha és semmilyen eszközzel nem bizonyíthatók a bizonyítás klasszikus jogi értelmében.

Az eljárásjogi szakértők tudják, hogy a nyomozati cselekmény során a bizonyítékokat keresési (például házkutatás, könyvvizsgálat, vagyonleltár) illetve megszerzési cselekményekkel (foglalás, hatósági zár alá történő helyezés) lehet begyűjteni. Ugyanakkor ezen megszerzési jogosítványok problémát okozhatnak abban az esetben, ha a szükséges bizonyítékot nem tárolják hagyományos adathordozón, azaz papíron vagy újabban mikrofilmen.

A klasszikus kérdésre: kinek áll érdekében még viszonylag könnyen tudunk válaszolni, de az ezzel kapcsolt kérdésekre többnyire már kevésbé. Kellő szakértelemmel egy dokumentumban olyan változtatások eszközölhetők, amik utólag már ne igazolhatóak. Vagy akár csak azt a kérdést tesszük fel: ki vette fel a nevezett adatokat vagy programokat egy többször írható-olvasható adathordozóra, például mágneslemezre, akkor már megáll a tudomány. És a bíróságoknak a kétes illetve bizonytalan bizonyítékokat éppen az emberi jogi aspektusok miatt mindig a vádlott javára kell(ene) mérlegelniük. (A magyar szerzői jogvesztői szoftverpererek alapján nem így tetszik a helyzet. Hiszen hisznek a rendőrségnek és az eljárás kimenetelében, de leginkább a magas szakértői díjban érintett szakértőknek. Nem vizsgálják a hátteret, de nem is értenek hozzá.)



-MEGKAPTA A TELEFONSZÁMLÁT!

Ezen esetekben az ENSZ dokumentumot készítő jogász-csoport felvet egy nagyon érdekes kérdést: A pusztán adatok vagy az információ, a megszerzés szempontjából tekinthető e hagyományos értelemben tárgynak? Ugyanez igaz - és ezzel a problémával már a magyar rendőrségnek és ügyészségnek is szembe kell néznie, amikor a szoftverjog területén tesz lépéseket - hogy a minimum kényszerítés (azaz kényszerítő eszközöket csak és kizárólagosan az eljárás szempontjából a legnélkülönözhetet-

lenebb mértékben alkalmaznak) és az arányosság elve (mely szerint a kényszerintézkedéssel okozott hátránynak összemérhetőnek kell lenni, éspedig jelentősen kisebbnek, mint maga a bűncselekmény által okozott kár) jogellenessé és az emberi jogokkal ellentétessé teszik a adathordozók illetve számítógépes installációk megszerzését, egy bizonyíték megszerzése céljából.

Így például, ha a hatóság egy gazdasági bűncselekmény bizonyítása céljából lefoglalja a bank archívumát, akkor jelentősen sérti az ártatlanok jogait azzal, hogy az ő adataikban és magánéletükben kutakodik. Egy ilyen tevékenység igencsak súlyosan sértheti az üzlet érdekeit, de ennél is súlyosabban más személyek a magánélethez, a privacy-hoz fűződő jogait. Bizonytalanságok keletkezhetnek, amikor a tárolókat nem lehet lefoglalni, hanem a kérdéses számítógéprendszer használatával kell kiértékelni. Ekkor fontolóra lehet venni, hogy lefoglalási jogosítványok helyett keresési jogosítványokat kell alkalmazni - a hagyományos értelmezés kiterjesztésével, mondjuk olyformán, mint amikor operatív eszközökkel (rejtett figyelés lehallgatás stb.) szereznek információt egy tényről, majd utána az ekképpen megkapott outputra - nyomtatás, adathordozó - érvényesíteni a hagyományos foglaltatás technikáját. Hogy érthetőbb legyen a helyzet:

Z úr ellen nyomozás folyik nagyoösszegű banki számítógépes csalás miatt. Ezért nem foglalható le a bank teljes számítógépes rendszere, nem fagyaszthatók be az ügyfelek adatai. Ilyenkor a banki rendszerből ki kell keresni a csalással kapcsolatos tételeket, és azok ellen-tételeit, ki kell nyomtatni és utána a nyomtatást lefoglalni. A bizonyítás innen már hagyományos papír és számszaki feladat. De.... mi bizonyítja, hogy Z úr tényleg csalt, és az adatokat nem utólag vagy éppen más vitte be hamisan Z úr nevére. Ez a lehetőség fennáll, hiszen a belső alkalmazottak által elkövetett csalások nagy része ilyen technikát alkalmaz.

Azonban maga a keresés is felvet igencsak komoly jogi problémákat: A keresésre és a megszerzésre vonatkozó jogosítványok egyáltalán - ha igen akkor milyen mértékben - foglalják magukban azon technikai berendezések és szerzői joggal védett programok használatára vonatkozó jogosítványt, mely a gyanúsítottak vagy egy tanú tulajdonát képezik, hogy a számítógépes adatokat kikeressék és/vagy rögzítsék. Csak néhány, mégpedig nagyon kevés

ország jogrendszere állítja azt, hogy meg lehet tenni „minden szükséges intézkedést” -, a többi ország jogrendszerében törvény nem biztosítja a „puszta adatok és az információ” hatékony kutatását. Ezen országok jogrendszere eddig gyakorlatilag a törvénytelenséget törvényesített gyakorlattá tette azzal, hogy az ilyen operációkat a hírszerzés eszköztárának megfelelő szabályozással és elbírálással kezelte. A Német Alkotmányvédő Hivatal, az FBI és az amerikai NSA egyértelműen ezt az utat követi, míg Svájc inkább a törvényes rendezés útját próbálja meg járni.



Különleges problémák vetődnek fel az ilyen kutatással azzal, ha egyáltalán igénybe is vehető egy számítógéprendszer speciálisan információk keresésére, ezen keresés joga magában foglalja-e azon jogosítványokat, hogy e rendszerrel kapcsolatban lévő, de mások tulajdonában lévő, máshol levő rendszerekben is kutakodjanak. Ez nem olyan elméleti jellegű probléma, mint gondolnánk.

Olaszországban pusztán azon gyanú alapján csukták le 600 BBS üzemeltetőjét, hogy rendszereik egymással kapcsolatban vannak, tehát ha egy valaki valami törvénybe ütközött követett volna el, akkor azt mindegyik vele kapcsolatban lévő rendszer is elkövette...

Ennél nagyobb közjogi problémák vetődnek fel, ha a nemzetközi telekommunikációs rendszerbeli kapcsolatokat nézzük. Amennyiben egy ilyen nyomozati cselekmény során adatvonalon történik behatolás egy másik ország területén levő adatbázisba, akkor ez megtestesíti a tároló állam szuverenitásának megsértését, ami nemzetközi jogi retorziókat von maga után. Itt is lehet néhány kivétel, amikor a kölcsönösség elve alapján két ország, illetve adatbázis-rendszer kezelői megállapodnak egymással és segítik egymás számára a bizonyítékok beszerzését. Ez banki gyakorlatban hitelkártya csalások esetén szinte természetes, míg más területeken érthetően élénk ellenállást tanúsítanak.

Értelmezési problémák is felmerülnek egyedi információk biztosítékai kiadhatóságának tekintetében. A hivatásos jogi tanácsadók, újságírók, orvosok, papok a legtöbb jogrendszerben fel vannak mentve - éppen a társadalom érdekében - az ilyen információk kiadására vonatkozó kényszer alól. Azonban a legtöbb helyen, ahol ez nem adott, saját tisztességük és egzisztenciájuk érdekében inkább vállalják a jogi következményeket, de nem adják ki a tudomásukra jutott információkat. Itt inkább már az a kérdés, hogy az elektronikus posta és a BBS mennyiben rendelkezik a sajtó ismérveivel, ezen kiváltságok mennyire alkalmazhatóak rájuk. Az általános álláspont egyre inkább az, hogy legalábbis a BBS rendszerek azonos ismérvekkel rendelkeznek, mint az újságok. Tehát a benne megjelentek tartalmáért szerkesztőségi anyagok esetében a főszerkesztő (sysop), míg levelek esetében, miként a lapok levelezési rovatában közöltekért is, a levél írója felel. Országos hálózatok esetében a hálózat gazdája a főszerkesztő, míg az egyes rendszerek sysopjai a rovatvezetőkkel analógok.

Néhány országban kísérletek történtek a joghézagok bestoppolására, mégpedig a hagyományos törvények mellé állított kiegészítésekkel. Az Egyesült Királyságban az 1984. évi Rendőrségi és Büntető Bizonyítékokról Szóló Törvény 19. paragrafusa egy olyan jogosítványt biztosít a nyomozó hatóságnak, hogy „bármit” megszerezhet, ami az „adott épületben” van, és némi korlátozás mellett biztosítja azon jogot, hogy „bármely információt megkereshessen, melyet a számítógép tartalmaz”.



Kanadában hasonló rendelkezéseket több törvény tartalmaz. Például a Versenytörvény 14. szakasza, valamint a Környezetvédelmi Törvény és a Kölcsönös Jogsegélyről szóló törvény megengedi a keresést „bármely adatra, amelyet a számítógépes rendszer tartalmaz, vagy rendelkezésre áll annak számára”. Ez utóbbi

fogalmazással azt fejezték ki, hogy nem csak az adott rendszerre, hanem az azzal kapcsolatos, abból elérhető rendszerekre is kiterjeszthető a keresés...

A Kanadai Jogi Reform Bizottság aképpen javasolja a törvénykezési gyakorlat megváltoztatását, hogy a „megszerzés tárgyai” jelenleg használt megfogalmazás immár a „dolgozat és információt” jelentik, melyekről ésszerűen feltételezik, hogy bűncselekményből származó haszon, csempészet vagy bűncselekmény bizonyítéka.

Az adatgyűjtés ilyenét sui generis (azaz eredendően, alapértelmezetten) történt felfogása a nyomozó hatóság számára bizonyos jogbiztonságot ad az elektronikus környezetben való hatékony nyomozásra, de az emberi jogi, jogpolitikai felfogás alapján alapulhat azon az érven, hogy az adatok másolása kevésbé súlyos tilalom, mint magának az adathordozónak a megszerzése, azaz magának az adatnak az eltüntetése, zárolása. Ezentúl ezzel az alap megoldással az adatok keresését és megszerzését képesek megoldani, kivédeni olyan vitás problémákat, mint a költségek kompenzálása az elektronikus rendszerek használatáért, vagy a keresésért a telekommunikációs hálózatokban.

Mindezen dolgok azonban csak írott malasztok maradnak, abban az esetben, ha nincsen a keresésben együttműködő beavatott személy. Ugyanis az információ természete alapján könnyen eltüntethető, módosítható. E sorok írója is tervezett már olyan rendszert, amely jogtalan behatolás esetén egy egészen más rendszer képét mutatja, és ezen jogtalannak tűnő behatolást akár a saját operátorok is elkövethetik, egyszerűen az úgynevezett vész-jelszavak használatával.... Eképpen, amennyiben egy rendszert kellőképpen körültekintően terveznek meg, együttműködő nélkül lehetetlen annak valós tartalmát felderíteni.

Sorozatunk következő részében azt vizsgáljuk, milyen együttműködések kell kialakítaniuk a bűnmegelőző nyomozóknak és az egyes rendszerek üzemeltetőinek, illetve melyek ezen együttműködés veszélyei?

9. Egymás ellen vagy együtt? Kinek higgyünk?

Korábban említettük, hogy a számítógépes bűnözés kriminalizálása esetében a hatóságnak valóban jogszerűen ki kell vizsgálnia és bizonyítania a kriminált eseményt. Ehhez azonban a sorozatban korábban említett, az adatok megszerzésének, rögzítésének és gyűjtésének általános (klasszikus jogi kifejezéssel élve: sui generis) jogosítványai szinte semmit sem jelentenek. A hagyományos hatóságok nem rendelkeznek a számítástechnikai rendszerekben bekövetkező eseményekkel, cselekményekkel szemben megfelelő szakmai-technikai ismeretekkel. Ugyanolyan ez a gond is, mint az egyszeri bűvészinásé. Aki tudta, hogy kell megigézni és vízholdásra bírni a seprűt, de amikor le kellett állítani, akkor már arra csak a Mester volt képes.

Itt a bíróságok és az igazságszolgáltatás függő helyzetbe kerülnek egy olyan csoporttól, akinek nem feltétlenül az objektív igazság érvényesítése a célja. A felkért szakértői, sőt értékelést végző testület az esetek igen nagy részében nem független, hanem nagy számítástechnikai és szoftveres cégek dolgozója, így annak érdekeit testesíti meg, sok esetben még akkor is, ha ő maga úgy tudja, teljesen pártatlanul ítélik. Eképpen felmerülhet a gyanú, hogy a törvény ez esetben a céges érdekek érvényesítésének eszköze. Az USA-ban a legutóbbi bírósági ítéletek (Microsoft kontra Stack Corporation vagy Microsoft kontra USA Monopóliumok Ellen Küzdő Bizottság stb.) a céges érdekek igazságszolgáltatásban történő megjelenésére utalnak.



Ez azért törvényszerű, mert a hatóságoknak nem is lehet ismeretük az esetleges cselekményben lévő szoftverekről, hardverekről, olyan ismeretek szükségesek, amik nagy része a szoftveres vagy hardveres cég legféltettebb ipari, kereskedelmi vagy éppen marketing titka. (Microsoft vs. Stack per és annak ellenpere a Stack vs. Microsoft éppen ilyen infókkal dobálódzott, ki lopott kitől, mit és mennyit, s mi ebből, ami nyilvános, és mi

nem....) Ezen problémákban az ENSZ szakértők optimisták, hiszen folyton azt hangsúlyozzák, hogy a nyomozótisztek jobb felkészítésével ezen problémák megoldhatóak. Ugyanakkor a fentiek miatt ez nem járható út. (Nagyon nem, különösen ha a rendőrség, a Vám- és az Adóhivatal szakembereit éppen az érdekeltek oktatják, jutalmazták, mint a világ számos országában.)

Járható útnak egy olyan számítástechnikai szakértő-nyomozói szerv felállítása látszik, melynek tagjai minden technikai információt megkaphatnak, megszerezhetnek, de ugyanakkor tudományos tevékenységen kívül sehol másutt semmilyen számítástechnikával kapcsolatos területen nem tevékenykedhetnek pályafutásuk során. Ez egy kicsit a magyar alkotmánybírói bíróság bírósági bírák jogállásához hasonló. Ez viszont, mivel ezen szakértők tartása igencsak költségigényes: fizetés, őrzés, technikai eszközök stb., hiszen egy ilyen ember tudása pénzben kifejezhetetlen, nagy teherterhelés arra a társadalomra nézve, aki ezt vállalja, hiszen egy ilyen ember tudása egy informatikai atombombával ér fel. (Ilyen atombombák azért szép számmal szaladgálnak szabadlábon, és nincs belőle gond, hacsak az illető nem kerül valamilyen céghez vagy a Hatósághoz dolgozni...)

A hozzáférés más problémákat is felvet. Különösen azoknál a rendszereknél, amelyeket aképpen terveztek, hogy idegen ne is férhessen hozzá. Ugyanakkor a számítógép rendszereken hatalmas adat- és információ-tömeget tárolnak, nem mindig minden van a rendszer számára látható formában. Például cserélhető háttértárakon van, amit csak alkalmasszerűen tesznek a rendszerbe. Ugyanakkor a nyomozó hatóság számára korlátozott idő és pénzmennyiség áll - szerencsére - rendelkezésre, és a vizsgálati, előzetes letartóztatási időket sok ország az emberi jogok figyelembevételével szigorúan meghatározza. A számítástechnikában ilyen vizsgálati idő nincsen, elvileg a vizsgálódás korlátlan ideig tarthat és korlátlan pénzmennyiséget emésztethet fel.

Ennek következményeként az állampolgárok bejelentési kötelezettsége (t. i. állampolgári bejelentés sok esetben hírszerzési vagy nem törvényes forrásból származó alapinformációt takar a világ legtöbb rendőrségének zsargonjában), itt jelentős szerepet kap, hiszen egy cselekmény akkor fogható meg, ha elsőre a nyomozó hatóság tudja, milyen kóddal, és hova kell nyúlni. Különben nem sok esélye van. Ugyancsak nem bizonyítható, hogy a nyomozó hatóság nem változtatta-e meg az adatokat, amire szintén nagy a veszély az eredményességre törekvő szervezeteknél (sok-sok gyanú van erre akár Európa, akár Amerika országaiban), vagy akkor, ha a szakértői céges érdekeket is képviselnek.

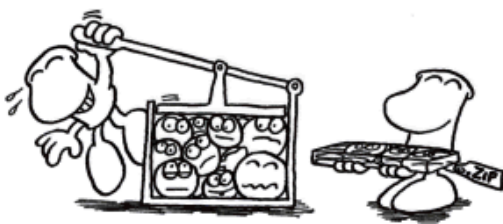
Két eszközt tartalmazott eddig minden ország jogrendszere ezen bizonyításhoz:

1. a megszerzett tárgyakat le kell foglalni és változatlan állapotban kell tárolni az eljárás befejezéséig. Ennek veszélye, hogy a legtöbb számítástechnikai adathordozó tartalma utólagos nyom nélkül módosítható.

2. A másik a tanúvallomási kötelezettség. Itt viszont ha a tanú tartja a száját, örök „nem tudom”-mal válaszol, akkor a tanú és a vádlott felmentéssel, vagy igen kis büntetéssel megúszhatja az ügyet. Minden ezen túlmenő intézkedés, amit egyes országokban fontolgatnak - büntetéssel, vagy egzisztenciálisan történő tönkretétellel, például vagyon-elkobzással vagy ezzel felérő büntetéssel történő fenyegetés - ellenkezik az emberi jogokkal és mint ilyen, nemzetközi fórumokon hosszabb távon eredményesen támadható.

Ha visszatekintünk a megszerzéssel lefoglalható tárgyakra, akkor annak párosulniuk kell a keresés és megszerzés jogosítványaival. Jó pár helyen - például nálunk - a megszerzendő tárgyat annak birtokosa köteles kiadni a hatóságoknak vagy a bíróságnak. Más országokban, bár a bíróság kötelezheti a kiadásra, de semmilyen jogi szankcióval nem jár annak megtagadása, megint más országokban pedig a bíróság sem kötelezhet senkit a tárgyak kiadására. Annak törvényes megszerzése a nyomozóhatóság feladata. Ez a jog azonban csak azt segíti, hogy a sokezer adathordozó közül kiválaszthassák a keresettet. Azonban, ha azt jól kódolták, és a központ tagjai bár ismerik a kódot, nem kötelezhetőek a megfelelő információ kikeresésére a kérdéses adathordozón, különösképpen nem annak dekódolására. Ugyancsak elfedhetőek a keresett adatok olyan valós adattömeggel, amikor egyes bankok hatalmas tömegű adatokat, amik ellenőrizhetően valódiak, kinyomtatnak, beadnak, hogy a pár kényes adat hiánya ne derüljön ki. Ez a nemzetközi gyakorlatban általános taktika minden hivatali szervezettel szemben - adóhivatal, nyomozó hatóságok, sőt hírszerzés - mindig eredményesen alkalmazható, és az is marad szinte mindörökké.

A másik probléma a tanú. Hagyományos jogrendszerek a tanút igazmondásra kötelezik. Mindaddig hisznek állításának, míg az ellenkezőjéről meg nem győződnek, amit bizonyos társadalmi aktusokkal (eskü), illetve súlyos büntetésekkel való fenyegetéssel (hamis tanúzás, mint kriminalizált cselekmény) próbálnak biztosítani. Itt nem alkalmazhatóak azon kötelezettségek, amiket az USA adó-ügyeiben alkalmaznak, hogy a tanút felkérjük, míg a dokumentumok rendelkezésre állnak, frissítse fel az ügyről szerzett ismereteit, és tanú volta csak ennek megtörténte után kerül nyilvánosságra. Itt a tanú azonban nem kötelezhető dokumentumok ellopására. Miként a számítástechnikai rendszerekben sem kötelezhető jelenleg információ ellopására, például arra, hogy mondja meg a dekódolás kulcsát, vagy információt nyomtasson ki.



Mindezen dolgoknál azonban figyelembe kell venni a 1966 évi nemzetközi megállapodást a Polgári és Politikai Jogokról. Ez kimondja: bármely bűnvád megállapításában mindenkit megillet azon minimális garancia, hogy „ne legyen kötelezhető arra, hogy saját maga ellen tanúskodjék, vagy bűnösnek kelljen vallania magát”. Ezt természetesen megteheti, ha úgy látja jónak, de semmiképpen sem kötelezhető erre.

Post Mortem: Jelen szöveg képekkel vagy anélkül a szerző jelen engedélyével - mint az Euroastra Internet magazin bármelyik publikációja - engedélye és külön hozzájárulás nélkül archiválható, tárolható közkönyvtári törvény hatálya alá eső és NON PROFIT elektronikus rendszerekben és publikálható, ingyenesen hozzáférhetővé tehető - pld MEK. Az egyéb publikációkban - hivatkozással felhasználható, de a szerzőt és a forrást jelölni kell. A profit-érdekelt kiadványokban csak a szerző engedélyével és szerzői jogdíj megfizetése ellenében közölhető. Ugyanez vonatkozik olyan adatbázisokra, ahol a hozzáférésért jogdíjat kérnek.