Jóri András

TÚLFÚTÖTT AMBÍCIÓK?

MEGJEGYZÉSEK A KORMÁNY INFORMATIKAI JOGALKOTÁSI PROGRAMJÁHOZ

Óriási ütemben halad az informatikai jogalkotás. 2001. szeptember 1-jével hatályba lépett az elektronikus aláírásról szóló 2001. évi XXXV. törvény. E sorok írásakor zajlik az elektronikus kereskedelemről szóló törvényjavaslat vitája, a Btk. pedig előreláthatóan a „számítástechnikai rendszer és adatok elleni bűncselekmény", valamint a „számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása" elnevezésű tényállásokkal egészül ki. A diktált ütem sok esetben a vita és az érdekegyeztetés hiányával jár együtt, ráadásul nem mindig egyértelmű, hogy vajon a szabályozást megelőző legfontosabb kérdést („kell-e szabályozni?") feltették-e maguknak az illetékesek. Az alábbiakban az elektronikus aláírásról szóló törvény, a tervezett Btk.-módosítás és az elektronikus kereskedelemről szóló törvény olyan rendelkezéseit vesszük számba, amelyek álláspontunk szerint méltók lehetnek a jogvédő szervezetek figyelmére.

AZ ELEKTRONIKUS ALÁÍRÁSRÓL SZÓLÓ TÖRVÉNY ÉS A TITKOSÍTÁS SZABÁLYOZÁSA

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény 13. § (4) bekezdése szerint „az aláíró az aláírás-létrehozó adatot kizárólag az aláírás létrehozására használhatja, betartva a tanúsítványban jelzett esetleges egyéb korlátozásokat is". A törvényhez kapcsolódó részletes miniszteri indokolásnak e szakaszhoz kapcsolódó szövege szerint „a (4) bekezdés nemzetbiztonsági érdekből nem teszi lehetővé az aláírást létrehozó adatnak (magánkulcsnak) titkosítás céljából történő használatát". Ez a szakasz nem más, mint a polgári célú rejtjelzés korlátozására történő „alkalmatlan kísérlet": inkább komikus, mint félelmet keltő, ám nem árt, ha a szabadság barátai már most számolnak azokkal az érvekkel, amelyek egy komolyabb szabályozási kísérlet esetén a titkosítás megregulázását lesznek hivatottak alátámasztani.

A KRIPTOANARCHIA VESZÉLYE

A titkosító algoritmusok fejlesztésével, a rejtjelzés tökélyre vitelével sokáig kizárólag a kormányok alkalmazásában álló matematikusok foglalkoztak, azonban az 1970-es években már felmerült a rejtjelzés polgári célú használatának igénye. A banki szektor által használt számítógéprendszereken folytatott kommunikáció biztosítására 1971-től folytak kutatások az IBM-nél. Bár az eredmények publikálását a National Security Agency kezdetben rossz szemmel nézte, végül e kutatások eredményeképpen létrejöhetett a szimmetrikus rejtjelzés szabványos algoritmusa, a DES. A szimmetrikus rejtjelzés lényege azonban az, hogy a küldő és a fogadó fél ugyanazt a kulcsot használja, márpedig a kulcs eljuttatása a másik félhez problematikus. Ez a módszer tehát még nem alkalmas arra, hogy egy számítógép-hálózat nagyszámú, egymást nem ismerő felhasználója előzetes kulcscsere nélkül biztonságosan kommunikálhasson. Erre a problémára keresett és talált megoldást Martin E. Diffie és Whitfield Hellmann: 1976-ban írták meg első cikküket a nyilvános kulcsú titkosításról, Ronald Rivest, Adi Shamir és Leonard Adleman pedig nem sokkal ezután egy működőképes, nyilvános kulcsú titkosítást megvalósító eljárással állt elő.[1] Ezzel megszületett a nyilvános kulcsú infrastruktúra, amelyben egymást nem ismerő felek is képesek a másik személyazonosságáról meggyőződni, ha az digitális aláírást használ, valamint képesek előzetes kulcscsere nélkül is titkosított üzenetet küldeni a másik fél számára.

A felhasználó a nyilvános kulcsú rendszerben két kulcsot használ: egy nyilvánosat és egy titkosat. A nyilvános kulcsot közzéteszi, míg a titkos kulcsot rajta kívül senki nem ismerheti meg. Elektronikus aláírás generálásakor a felhasználó az üzenetet (vagyis annak egy meghatározott módon képzett lenyomatát) titkos kulcsával aláírja, a címzett pedig a küldő nyilvános kulcsa segítségével ellenőrizheti, hogy az üzenet nem változott, s azt valóban a küldőként megjelölt személy írta alá. Rejtjelzésnél a folyamat fordított: az üzenetet a küldő a címzett nyilvános kulcsával titkosítja, majd ezután azt kizárólag a címzett képes

visszafejteni saját titkos kulcsával.[2] A nyilvános kulcsú rejtjelzés igen hatékony, és – RSA algoritmus alkalmazásával – megfelelő hosszúságú kód használata esetén az üzenet megfejtésére a jelenleg rendelkezésre álló számítógépes kapacitás mellett nincs mód addig, ameddig nem ismeretes a prímtényezőkre bontást megkönnyítő matematikai eljárás.

A nyilvános kulcsú rejtjelzést felhasználóbarát módon megvalósító, bárki által egyszerűen kezelhető szoftver- és hardvereszközök – mely szoftverek közül az első és legismertebb a Phil Zimmermann által írt, ingyenesen elérhető Pretty Good Privacy (PGP)[3] – kifejlesztése és az interneten való közzététele a magánszféra és az üzleti titkok védelmének lehetőségét bármely digitális technológiát használó kommunikációs eszköz használatakor lehetővé tette. A folyamat azonban veszélyezteti azt az egyensúlyt, amely egyrészt fennállt a hagyományos kommunikációs csatornák esetén a magánszféra védelméhez, másrészt a bűnüldözéshez, nemzetbiztonsághoz fűződő érdekek között. Az új rejtjelző technológiák használata mellett ugyanis lehetetlennek bizonyulhat a titkos információgyűjtés, még az állam rendelkezésére álló erőforrásokkal is. Volt, aki üdvözölte ezt a fejleményt; Tim May, „kriptoanarchisták" apostola így írt kiáltványában: „Ahogy a nyomtatás megváltoztatta és csökkentette a középkori céhek hatalmát és a társadalom hatalmi rendszerét, úgy fogják alapjaiban megváltoztatni a titkosító algoritmusok a kormányok és a tőkés társaságok befolyását az üzleti tranzakciókra. A kialakuló információ-piacok és a kriptoanarchia együttesen virágzó piacot teremt majd minden árunak, amely szavak és képek formájában megjelenhet."[4]

Ugyancsak Tim May közölte – névtelenül – az interneten a BlackNet nevű szervezet képzeletbeli felhívását. A BlackNet identitása csupán egy az interneten elérhető nyilvános kulcs, amelynek segítségével titkosított üzenetet küldhetünk számára. S hogy mivel foglalkozik ez a hálózat? „A BlackNet tetszőleges formájú információ vásárlásával, eladásával és kereskedelmével foglalkozik. Az információt nyilvános kulcsú kriptográfiai rendszer segítségével adjuk és vesszük, amely vásárlóinknak tökéletes biztonságot biztosít. Ha nem mondja meg nekünk, hogy Ön ki (kérjük, ne tegye!), és véletlenül sem árul el magáról olyasmit, ami elvezethet Önhöz, nekünk nem áll módunkban azonosítani Önt, és Ön sem tud azonosítani minket. Fizikai térbeli pozíciónk nem fontos. Csak a cybertérben elfoglalt helyünk számít. Elsődleges címünk a »BlackNet« PGP-kulcsos cím. […] A BlackNet névleg ideológiamentes, de a nemzetállamokat, exportjogszabályokat, szabadalmi törvényeket és a nemzetbiztonsági szempontokat a cybertér előtti korszak relikviáinak tartja. Az export- és szabadalmi törvényeket gyakran használják bevallottan a nemzeti hatalom és az imperialista, kolonialista államfasizmus érdekében."[5]

A kiáltvány folytatásában a szervezet közli, hogy mi érdekli – üzleti titkok, találmányok, bármely értékes információ –, majd leírja a fizetés menetét. A képzeletbeli szervezet még belső fizetőeszközzel is rendelkezik, az anonimitás az üzleti tranzakciók során végig biztosított, s a rendszer bármire használható, legyen az jogszerű vagy jogszerűtlen. A May által leírt rendszer persze – bár sokan komolyan vették – nem létezett. Hamar elterjedtek azonban az úgynevezett anonim remailerek, vagyis azok a szerverek, amelyeken keresztül a felhasználó úgy küldhet és fogadhat üzenetet, hogy személyazonossága ismeretlen marad a fogadó fél előtt. Egy több remaileren keresztül küldött levél feladója nehezen azonosítható, ha minden szerver más országban van.

LEHETSÉGES VÁLASZ: KULCSLETÉT?[6]

A „kriptoanarchia" lehetőségét értékelve az amerikai kormányzat igen gyorsan lépett: a National Security Agency bábáskodásával kifejlesztett Clipper chip olyan hardvereszköz volt, amely számítógépekbe, telefonokba építve erős titkosítást valósított meg, ám biztosította a bűnüldöző és nemzetbiztonsági szervek hozzáférési lehetőségét is: minden egyes kulcshoz tartozott a visszafejtést lehetővé tévő kulcs is, amelyet a chip gyártója két részre osztott, s a két rész két kormányzati szervhez került „letétbe". A nemzetbiztonsági és bűnüldöző szervek szükség esetén a megfelelő engedélyek birtokában a két szervtől beszerezhették volna a két kulcsrészt, majd az azokból összeillesztett kulcs segítségével visszafejthették volna az üzenetet.[7] Ez az úgynevezett kulcsletét rendszere.[8] Az elképzelés tetszetős,[9] hiszen kellő garanciák mellett biztosítja a bűnüldözők számára a hagyományos kommunikációs csatornák esetén megszokott eszközök használatát – a Clipper chip mégis csúfos bukásnak bizonyult. A Clinton-kormányzat által 1993 tavaszán tett bejelentés után, amely szerint támogatják a kulcsletét – önkéntesen igénybe vehető – rendszerét (nagy összegű kormányzati megrendeléseket is kaptak a chippel felszerelt eszközök gyártói), emberi jogi szervezetek és az informatikai ipar lobbistái összetüzet zúdítottak a programra.

Számos ellenérv fogalmazható meg: a kulcsletét technológiája fenyegeti a titkosítás biztonságát (a Clipper chip megvalósításában nem sokkal a program meghirdetése után biztonsági hibát találtak), az eszközzel felszerelt berendezések nem lennének

exportálhatók, mert a külföldi piac nem fogadná el a kizárólag az amerikai szervek számára nyitva álló „hátsó kaput". A kulcsletéti rendszer üzemeltetése természetesen nagy költségekkel járna. A legnagyobb probléma azonban, hogy a titkosított üzenetforgalom ellenőrzése a kulcsletét mellett sem megoldható: a kulcsok beszerzésével visszafejtett üzenet talán egy további rejtjelzett üzenetet takar; de az is lehetséges, hogy a kódolt üzenet maga is el van rejtve valamely kép- vagy hangfájl meghatározott szabályok szerint módosított bitjeibe. A rendszer tehát feleslegesen gyengítené a biztonságot – szóltak az ellenérvek. Az amerikai kormányzat a javasolt rendszer módosításával kísérletezett: a későbbi tervek szerint kormányzati szervek helyett magáncégek is lehettek volna a kulcsokat őrző „letéteményesek", ám a kulcsletét rendszerén alapuló infrastruktúra megteremtése az 1990-es évek végére – miután az USA sikertelenül próbálta meggyőzni európai szövetségeseit egy nemzetközi kulcsletéti rendszer szükségességéről[10] – lekerült a napirendről.

Európában szintén felmerült az amerikaihoz hasonló rendszer megteremtése, azonban az Európai Bizottság 1997-es, A digitális aláírás és a titkosítás európai kereteinek megteremtéséről szóló közleménye[11] óta nem merült fel uniós szinten olyan kezdeményezés, amely a kriptográfia használatának korlátozására irányult volna. A tagállamokban is a titkosítás belső használatának mellőzése a tendencia: a német kormány által 1999-ben elfogadott kriptográfiai politika szerint az erős titkosítás használatát kifejezetten ösztönözni kell, Franciaország pedig 1999-ben feloldotta a korábbi jogszabályi korlátozásokat a titkosítás használatát illetően. Nagy-Britannia szabályozása sem ismeri a kulcsletét rendszerét, azonban a 2000-ben elfogadott Regulation of Investigatory Powers Act szerint az a személy, akinek valamilyen titkosító kulcs a birtokában van, meghatározott feltételek szerint kötelezhető annak kiadására.[12]

KIS MAGYAR KRIPTOGRÁFIA-VITA

Magyarországon 2001 februárjában Majtényi László adatvédelmi biztos az internettel kapcsolatos, adatvédelmi kérdésekkel foglalkozó ajánlást bocsátott ki. Az ajánlásban az adatvédelmi biztos hangsúlyozta: „A nemzetközi példák nyomán arra az álláspontra jutottam, hogy a polgári célú kriptográfia jogszerű használatának korlátozása káros, a bűnüldözés hatékonysága szempontjából előnyei kétségesek, viszont a személyes adatok védelme szempontjából hátrányai kétségtelenek." Az ajánlás különösebb visszhangot nem keltett, ám az elektronikus aláírásról szóló törvény fent idézett szakasza válaszként is értékelhető: a kormányzat nem osztja Majtényi álláspontját. A szándék kifejezésén túl az elektronikus aláírásról szóló törvény 13. § (4) bekezdésének szövege másra nem alkalmas: értelmetlen ugyanis a feladó magánkulcsával történő titkosítást megtiltani a nyilvános kulcsú infrastruktúrában, ahol a titkosítás a címzett nyilvános kulcsával történik. Csak remélhető, hogy mire a jogszabály-előkészítők a kormányzati szándékot megfelelőbb formába öntik, a személyes adatok védelmét, a hazai e-kereskedelem és információs társadalom fejlődését zászlajukra tűző jogvédők és érdekképviseleti szervezetek is megfogalmazzák majd álláspontjukat: a 13. § (4) bekezdéséről ugyanis sem az Országgyűlésben, sem azon kívül nem esett szó az elektronikus aláírásról szóló törvény vitája során.

Ez év végén Budapesten tartották az Európa Tanács égisze alatt született számítástechnikai bűnözésről szóló egyezmény „aláíró ünnepségét".[13] Az egyezmény 18. cikke szól a „közlésre kötelezés" szabályozásáról: a szerződő fél ennek értelmében „megteszi azokat a jogalkotási és egyéb intézkedéseket, amelyek ahhoz szükségesek, hogy feljogosítsa illetékes hatóságait, hogy kötelezhessék a területén tartózkodó személyt a birtokában vagy az ellenőrzése alatt lévő és egy számítástechnikai rendszerben vagy egy számítástechnikai adattároló egységen tárolt meghatározott számítástechnikai adatok közlésére, és a területén szolgáltatást nyújtó szolgáltatót a birtokában vagy az ellenőrzése alatt lévő, az előfizetőre vonatkozó és a szolgáltatást érintő adatok közlésére". Az egyezményhez fűzött magyarázat (Explanatory Memorandum) 176. pontja alapján a szerződő felek meghatározhatják, hogy az információt a kötelezett a közlésre kötelezést elrendelő határozatban meghatározott módon – vagyis, mint maga a magyarázat is utal rá, akár titkosítatlan formában – köteles szolgáltatni. Bár az egyezmény nem ír elő kulcsletét megvalósítására irányuló kötelezettséget a tagállamoknak, az előkészítés szakaszában az ötlet felmerült,[14] s nem lehetetlen, hogy a 2001. szeptember 11-i események nyomán megváltozott hangulatban újra előtérbe kerül a kulcsletét mint lehetséges megoldás, akár Magyarországon is.[15]

HACKEREK ÉS CRACKEREK A BÜNTETŐ TÖRVÉNYKÖNYVBEN

Az Eric Raymond szerkesztette New Hacker's Dictionary[16] szerint hacker „az a személy, aki élvezi a

programozható rendszerek részleteinek felfedezését, lehetőségeik végletekig történő kihasználását, a legtöbb olyan felhasználóval ellentétben, akik csak a szükséges minimumot szeretik tudni azokról". Ez azonban csak az első jelentés; jelent a hacker gyors programozót, lelkes programozót, valamely rendszer szakértőjét, valamint bármiféle szakértőt, s jelent olyan személyt is, „aki élvezi azt az intellektuális kihívást, amely a korlátok kreatív módon történő megkerüléséhez, áthágásához fűződik". A hacker utolsó jelentése „rosszindulatú személy, aki érzékeny információkat próbál megszerezni" – a helyes szó erre a jelentésre a szótár szerint a cracker. Cracker az, „aki megsérti egy rendszer biztonságát – 1985 körül alkották a hacker szó újságírói félreértelmezésére válaszul". A hackerek, a szabad szoftver mozgalom önkéntesei, a Linux operációs rendszer és számos más csodálatos alkotás karbantartói azonban nem tudták elérni, hogy megváltozzon a szóhasználat: a világ máig a hacker szó hetedik jelentését használja. Pedig hacker és cracker között nagy a különbség: ugyanazt teszik – tesztelik, feltörik[17] a rendszereket –, azonban más céllal.

A Büntető törvénykönyv tervezett módosításának[18] elfogadása után büntetendő lesz az a személy, „aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad" (vétség, büntetése egy évig terjedő szabadságvesztés, közérdekű munka), vagy aki „számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz, illetve adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza". A törvény minősített esetként szabályozza azt, ha az elkövető „jogtalan haszonszerzés végett" vagy kárt okozva követi el a cselekményt. Ez a számítástechnikai rendszer és adatok elleni bűncselekmény. A „számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása" tényállást pedig az valósítja meg, aki az előzőleg ismertetett cselekmény elkövetése céljából „az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot készít, megszerez, forgalomba hoz, azzal kereskedik, vagy más módon hozzáférhetővé tesz". Büntetendő az is, aki az előbbi cselekmény „megvalósításának céljából az ehhez szükséges vagy ezt könnyítő számítástechnikai program, jelszó, belépési kód, vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit másnak a rendelkezésére bocsátja". Nem büntethető az elkövető, ha – mielőtt cselekménye a hatóság tudomására jut – „tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását".

Az utóbbi tényállás tekintettel van a célzatra: csak az büntethető, aki az elkövetési magatartást az előbbi tényállásban leírt cselekmény elkövetése céljából tanúsítja. Ugyanakkor problematikus, hogy a „számítástechnikai rendszer és adatok elleni bűncselekmény" elkövethető célzatra való tekintet nélkül is. A biztonságtechnikai szakemberek körében ismert gyakorlat, hogy valamely sokfelhasználós rendszer (például az ismert Hotmail levelezőrendszer, vagy valamely operációs rendszer, szerveroldali szoftver) gyengeségeit feltérképezik, majd értesítik a gyártót a rendszer hiányosságairól. A gyártó sok esetben nem válaszol; ekkor az a szokás, hogy a hibát annak felfedezője nyilvánosságra hozza a megfelelő fórumokon.[19] Mindez hasznos, hiszen a jó rendszergazda olvassa ezeket a fórumokat, és felkészíti rendszerét a várható támadásokra. A hibák nyilvánossága nem csökkenti, hanem növeli a biztonságot, míg a gyártó érdeke sok esetben a hibák titokban maradása lenne. Azonban a magyar Btk. tervezett módosítása célzatra való tekintet nélkül rendel majd büntetendőnek a védelmi intézkedések megsértésével, kijátszásával történő bármely belépést, bennmaradást. A javaslat nem ismeri a különbséget a hacker és a cracker között: a cél nem számít. Bár valószínűtlen, hogy a biztonságtechnikával kapcsolatos, nemzetközileg elismert levelezőlisták működését a magyar javaslat befolyásolja majd, de itthon veszélyeztetheti azt, aki biztonsági hibákat tár fel, hiszen a hibákat szükségszerűen bűncselekmény elkövetésével lehet csak megismerni és felfedni. A javaslat nyomán a társadalomra nem veszélyes cselekmények minősülnek majd tényállásszerűnek, s csupán a jogalkalmazó jóindulatán múlik majd a jó szándékú biztonsági szakemberek sorsa is.

Érdekesség, hogy az Európa Tanács keretében született, fent említett egyezmény nem követeli meg az ilyen szabályozást: a büntető anyagi jogról szóló I. cím „jogosulatlan belépés" nevű cselekményt szabályozó 2. cikke szerint „a Fél kikötheti, hogy a bűncselekményt a biztonsági intézkedések megsértésével vagy a számítástechnikai adatok megszerzésére irányuló, illetőleg más bűnös szándékkal vagy egy másik számítástechnikai rendszerhez kapcsolódó számítástechnikai rendszerre vonatkozóan kövessék el".

ÉRTESÍTÉSI-ELTÁVOLÍTÁSI ELJÁRÁS AZ ELEKTRONIKUS KERESKEDELEMRŐL SZÓLÓ TÖRVÉNY TERVEZETÉBEN

Az elektronikus kereskedelemről szóló törvény tervezetében[20] felbukkant „értesítési és eltávolítási eljárás" az Egyesült Államokban 1998-ban elfogadott Digital Millennium Copyright Actből származik. A magyar törvényjavaslatban foglalt eljárás lényege, hogy az a személy, akinek a szolgáltató által elérhetővé tett valamely tartalom bármely jogát vagy jogos érdekét sérti, felhívhatja a tárhelyszolgáltatót, illetőleg a keresőrendszert vagy a gyorsítótárat üzemeltető szolgáltatót, hogy az általa kifogásolt tartalmat távolítsa el. A szolgáltató köteles a tartalmat a tartalomszolgáltató (a törvényjavaslat sajátos fogalomhasználata szerint „érintett igénybevevő") egyidejű értesítése mellett eltávolítani, és a jogosult rendelkezésére bocsátani a tartalomszolgáltatóra vonatkozó adatokat. A tartalomszolgáltató nyolc napon belül kifogással élhet az eltávolítás ellen. Ekkor – hacsak az eltávolítást nem bíróság vagy hatóság kérte – a tartalmat újra elérhetővé kell tenni. Az eljárás végső stádiuma a jogosult által a tartalomszolgáltató ellen indított eljárás jogerős lezárása után következik: ekkor a jogosult köteles haladéktalanul értesíteni a szolgáltatót a jogerős befejezés tényéről. Amennyiben a bíróság vagy hatóság úgy dönt, a szolgáltató köteles véglegesen eltávolítani a tartalmat, amennyiben pedig az előzőleg eltávolított tartalom még nem került vissza (például mert az eltávolítást maga a bíróság vagy hatóság kérte), s a jogerős döntés ez, akkor vissza kell helyezni az eltávolított tartalmat.

A magyar jogszabály-előkészítő kezdetben bármely jogvita esetére alkalmazni rendelte az eljárást; azonban az időközben megváltozott, módosított javaslat formájában testet is öltött kormányzati akarat szerint az csak szerzői jogi viták esetén lesz alkalmazandó. Magyarországon nem váltott ki különösebb vitát a „notice and take down" ötlete, sőt a nagyobb hazai internetes tartalomszolgáltatók érdekeit képviselő, hat tagot számláló Magyar Tartalomszolgáltatók Egyesülete korábban hasonló eljárást magában foglaló megállapodást kötött a hazai szerzői jogvédő egyesületek képviselőivel.[21] Tény, hogy ez az eljárás jó a szerzői jogok jogosultjainak, hiszen könnyen, gyorsan távolíthatók el a valóban jogsértő anyagok, és jó a tartalomszolgáltatóknak, hiszen előírt eljárást követhetnek s meghatározott feltételek mellett mentesülhetnek a felelősség alól.[22] Kérdés, hogy a véleményszabadság szempontjából helyes-e az eljárás. Lawrence Lessig így ír erről a Foreign Policy legutóbbi számában: „Amikor egy internetszolgáltatót értesítenek, hogy az oldalán található valamely anyag szerzői jogot sért, akkor mentesülhet a felelősség alól, ha eltávolítja az anyagot. Mivel nincs, ami arra ösztönözné, hogy kitegye magát ennek, a szolgáltatók az értesítésre általában eltávolítják az anyagot. Az eljárást egyre több, a bíráló hangokat elnyomni akaró vállalat használja fel a kritika elhallgattatására. 2001 augusztusában egy brit gyógyszeripari cég használta a DCMA-t [az amerikai szerzői jogi törvényt, a Digital Millennium Copyright Actet – a szerk.] arra, hogy letiltasson egy az állatok jogaiért küzdő oldalt, amely bírálta a céget. A szolgáltató szerint »világos, hogy a cél az, hogy elhallgattassák őket, de a szolgáltatót semmi nem ösztönzi arra, hogy visszautasítsa a kérést«".[23]

Magyarországon különösebb aggály nélkül fogadott el a kormány egy olyan eljárást szabályozó törvényjavaslatot, amely kizárólag a szerzői jogsértések esetére alkalmazva is viták középpontjába került az Egyesült Államokban. Lehet, hogy a módosító javaslat nyomán az eljárás szabályozása már megfelelő, de a szólásszabadságért aggódók hangját ebben a vitában sem hallhattuk. A szabadságjogokat védeni hivatott szervezetek láthatóan nem érzékelik a probléma súlyát, a szolgáltatók érdekeit védő szervezetek pedig nem tekinthetők jogvédő szervezetnek, hiszen – egyébként érthetően – gazdasági érdekeket védenek. Legyen szó titkosításról, hackerekről vagy az értesítési-eltávolítási eljárásról, a tanulság közös: a jogvédőknek van mit tenniük a cybertér magyar sarkában.

JEGYZETEK

1. A nyilvános kulcsú titkosítás feltalálásának és az azzal kapcsolatos politikai vitáknak a történetéről lásd Steven LEVY: *Crypto,* New York, Viking Penguin, 2001. Érdekes, hogy a nyilvános kulcsú titkosítás valódi feltalálója nem Diffie és Hellmann, hanem James Ellis, a General Communication Headquarters elnevezésű brit nemzetbiztonsági szolgálat alkalmazásában álló matematikus volt, aki már 1969-ban megalkotta a modellt. A kriptográfia technológiájáról és a szabályozásával kapcsolatos jogi kérdésekről tudományos igénnyel ír Bert-Jaap KOOPS: *The Crypto Controversy. A Key Conflict in the Information Society,* The Hague, Kluwer Law International, 1999.
2. Valójában a – számítógépek által lassabban végrehajtott – nyilvános kulcsú rejtjelzési eljárást általában csak arra használják, hogy egy kulcsot titkosítsanak; a kulcs átvitele után maga az üzenet dekódolása és visszafejtése már az átküldött – kódolásra és visszafejtésre egyaránt alkalmazott – kulccsal történik.
3. A PGP megalkotásáról lásd: LEVY: *I. m.,* 188–.
4. Tim MAY: *Crypto Anarchist Manifesto,* idézi LEVY: *I. m.*, 210.

5. Tim MAY: *Bemutatkozik a Blacknet* (holist fordítása). Köszönet CCFZ-nek a fordítás megküldéséért; az eredeti az interneten számos helyen elérhető.
6. Jelen írásban nem érintjük a titkosító technológiák jogi szabályozásának a belföldi használat szabályozásán kívüli másik nagy területét: az ilyen technológiák exportjának szabályozását.
7. A Clipper chip fejlesztésének történetéről és a körülötte zajló politikai vitákról lásd LEVY: *I. m.*, 127–.
8. Jelen írásban nem különböztetjük meg a „key escrow" és „key recovery" rendszereket.
9. A kulcsletét rendszerét jó nevű független szakértők is támogatták, például a Georgetown University professzora, Dorothy Denning. Lásd Dorothy DENNING: *The Future of Cryptography*, in *The Governance of Cyberspace*, Routledge, 1997, 175–189.
10. Az USA a végleges vereséget a fegyverek és a kettős használatú termékek (polgári és katonai célokra is használható termékek; ilyennek minősülnek a titkosító eszközök is) exportjának ellenőrzésével kapcsolatos nemzetközi fórum, a Wassenaari Együttműködés 1998-as ülésén szenvedte el, lásd a német Gazdasági Minisztérium közleményét a http://www.kuner.com/data/crypto/wassenaar.html oldalon.
11. COM 97 (503).
12. A titkosítás szabályozásának fejleményeiről lásd Bert-Jaap Koops félévente frissített, a világ szinte minden országáról információkat közlő felmérését a http://cwis.kub.nl/(frw/people/koops/lawsurvy.htm oldalon; az Electronic Privacy Information Center 2000-ben készített felmérését lásd a http://www2.epic.org/reports/crypto2000 oldalon.
13. Az egyezmény szövege magyarul a http://stopcybercrime.net/2_2.php oldalon, a hozzá kapcsolódó magyarázat (Explanatory Memorandum) szövege angolul a http://conventions.coe.int/Treaty/EN/cadreprojets.htm oldalon olvasható.
14. Bert-Jaap Koops összefoglalóját lásd a http://cwis.kub.nl/~frw/people/koops/cls2.htm#coe oldalon.
15. A World Trade Center épületében röviddel azelőtt elkövetett merényletek Levy beszámolója szerint hozzájárultak ahhoz, hogy a Clinton-adminisztráció a nemzetbiztonsági szolgálatok mellé állt 1993-ban a Clipper chippel kapcsolatban. LEVY: *I. m.*, 244.
16. http://tuxedo.org/jargon/jargon.html.
17. Avagy a szubkultúra szóhasználatával: „megtörik".
18. http://www.mkogy.hu/irom36/5060/5060.htm.
19. A legismertebb fórum a Bugtraq levelezőlista, amelynek archívuma elérhető a http://www.securityfocus.com címen.
20. http://www.mkogy.hu/irom36/5141/5141.htm.
21. http://www.szamitastechnika.hu/hirek_hir.php?id=25117.
22. Arról, hogy e feltételek mennyiben felelnek vagy nem felelnek meg a mintául szolgáló EU-irányelvben foglaltaknak, lásd JÓRI András: *Megjegyzések az elektronikus kereskedelmi törvény tervezetéhez*, Napi Jogász, 2001. december.
23. Lawrence LESSIG: *The Internet under Siege*, Foreign Policy, November/December 2001; http://www.foreignpolicy.com/issue_novdec_2001/lessig.html.