JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

A polgári célú rejtjelzés szabályozásáról

Dr. Jóri András (jori@mail.datanet.hu)

(Megjelent: Napi Jogász 2002/3., 21-23. o.)

Amióta az üzleti és a magánkommunikáció egyre nagyobb hányada új, digitális csatornákon bonyolódik, egyre jelentősebb szerepe van a magánszemélyek és szervezetek titkait védő technológiáknak. A digitális csatornán továbbított üzenet megfelelő védelem híján könnyen megismerhető, reprodukálható illetéktelenek által is. Az adatvédelmi jog mellett a múlt század utolsó évtizedeiben új, az adatok védelmét szolgáló technológiai megoldások jelentek meg – s e megoldások használatának jogi szabályozása pedig új kihívásként jelent meg a jogalkotók számára. Az alábbiakban hangsúlyozottan nem a teljességre törekedve adunk egy rövid vázlatot a polgári célú rejtjelzés jogi szabályozásával kapcsolatos egyes problémákról.

1. Az elektronikus aláírásról szóló törvény és a titkosítás szabályozása

Az elektronikus aláírásról szóló 2001. évi XXXV. tv. 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 aláírás létrehozó adatnak (magánkulcsnak) titkosítás céljából történő használatát". Ez a szakasz, mint az alábbiakban bemutatjuk, nem szerencsés szabályozási próbálkozás – lássuk mégis, mi van mögötte, mely az a jogalkotói szándék, amely a törvény e szakaszában testet öltött.

1.1. A kriptoanarchia veszélye

A titkosítóalgoritmusok fejlesztésévek, a rejtjelzés tökélyre vitelével sokáig kizárólag a kormányok alkalmazásában álló matematikusok foglalkoztak, azonban a 70-es évektől a 0már 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 eredményeképp jöhetett létre a szimmetrikus rejtjelzés szabványos algoritmusa, a DES. A szimmetrikus rejtjelzés lényege azonban az, hogy a küldő és a fogadó fél ugyanazt a kulcsot használja: a kulcs eljuttatása a másik félhez pedig problematikus – ez a módszer tehát még nem alkalmas arra, hogy egy számítógéphálózat nagyszámú, egymást nem ismerő felhasználója előzetes kulcscsere nélkül, biztonságosan kommunikálhasson. Erre a problémára keresett és talált megoldást Diffie és Hellmann: 1976-ban írták meg első cikküket a nyilvános kulcsú titkosításról, Rivest, Shamir és Adleman pedig nem sokkal ezután egy működőképes, nyilvános kulcsú titkosítást megvalósító eljárással álltak 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

1 A nyilvános kulcsú titkosítás feltalálásának és az azzal kapcsolatos politikai vitáknak a történetéről lásd : Steven Levy : Crypto ; Viking Penguin, New York, 2001. Érdekesség, hogy a nyilvános kulcsú titkosítás valódi feltalálója nem Diffie és Hellmann, hanem James Ellis, a General Communication Headquarters elnevezésű brit nemzetbiztonságú 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, Kluwer Law International, 1999

kulccsere nélkül is a másik fél számára titkosított üzenetet küldeni.

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, s – RSA algoritmus használata esetén – megfelelő hosszúságú köd 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 kifejlesztése és az Interneten való közzététele – e szoftverek közül az első és legismertebb a Phil Zimmermann által írt, ingyenesen elérhető Pretty Good Privacy (PGP)[3] – 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 magánszféra védelméhez, másrészt a bűnüldözéshez, nemzetbiztonsághoz fűződő érdek között fennállt a hagyományos kommunikációs csatornák esetén. Az új rejtjelzőtechnológiák használata mellett ugyanis még az állam rendelkezésére álló erőforrásokkal is lehetetlennek bizonyulhat a titkos információgyűjtés. Volt, aki üdvözölte ezt a fejleményt: a „kripto-anarchisták" apostola, Tim May kiáltványában így írt:

„Ahogy a nyomtatás megváltoztatta és csökkentette a középkori céhek hatalmát és a társadalom hatalmi rendszerét, úgy fogják alapjaiban megváltoztatni a titkosítóalgoritmusok 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 postázta – névtelenül - az Internetre 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 tetszoleges 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 szájbertérben elfoglalt helyünk számít. Elsodleges címünk a "BlackNet" PGP-kulcsos cím. […] A BlackNet névleg ideológiamentes, de a nemzetállamokat, exportjogszabályokat, szabadalmi törvényeket és a nemzetbiztonsági szempontokat a szájbertér elotti korszak relikviáinak tartjuk. 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

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. és köv. o ;

4 Tim May : Crypto Anarchist Manifesto, idézi Levy : i.m. 210. o.

5 Tim May : Bemutatkozik a Blacknet (holist fordítása). Köszönet CCFZ-nek a fordítás megküldéséért ; az eredeti az Interneten számos helyen elérhető.

rendszer bármire használható, legyen az jogszerű vagy jogszerűtlen. A May által leírt rendszer persze – bár sokan komolyan vették – nem létezett. Hamar elterjedtek azonban az ún. „anonim remailerek": ezek olyan szerverek, amelyeken keresztül a felhasználó úgy küldhet és kaphat üzenetet, hogy személyazonossága ismeretlen marad a fogadó fél előtt. Egy több remaileren keresztülküldött levél küldője nehezen azonosítható, ha minden szerver más országban van.

1.2. 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 kulcs is, amelyet a chip gyártója két részre osztott, s 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 ún. „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 össztüzet zúdítottak a programra.

Az ellenérvek számosak: a kulcsletét technológiai megvalósítása 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 nyitvaálló „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 a kilencvenes 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 a 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 1999-ben oldotta fel a korábbi jogszabályi korlátozásokat a titkosítás használatát illetően. Nagy-Britannia szabályozása

6 Jelen írásban nem érintjük a titkosítótechnológiák 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. és köv. o.

8 Jelen írásban nem különböztetjük meg a „key escrow" és „key recovery" rendszereket.

9 A kulcsletét rendszerét jónevű független szakértők is támogatták , pl. a Georgetown University professzora, Dorothy Denning. Lásd pl. Dorothy Denning : The Future of Cryptography, in : The Governance of Cyberspace, Routledge, 1997, 175-189. o.

10 Az USA a végleges vereséget a fegyverek és kettős használatú termékek (polgári és katonai célokra is használható termékek ; ilyennek minősülnek a titkosítóeszközök 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)

sem ismeri a kulcsletét rendszerét, azonban a 2000-ben elfogadott Regulation of Investigatory Powers Act szerint az a személy, akinek valamely titkosító kulcs a birtokában van, meghatározott feltételek szerint kötelezhető annak kiadására[12].

1.3. A 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 kifejezte azt a véleményét, hogy „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 válaszképp 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, amely esetén a titkosítás a címzett nyilvános kulcsával történik. Csak remélhető, hogy mire a jogszabályelőkészítők 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) bekezdésről ugyanis sem az Országgyűlésben, sem azon kívül nem esett szó az elektronikus aláírásról szóló törvény vitája során.

2001. 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 felek ennek értelmében „megteszik azokat a jogalkotási és egyéb intézkedéseket, amelyek ahhoz szükségesek, hogy feljogosítsa az 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 valamely, 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 való kötelezettséget a tagállamoknak, az előkészítés szakaszában az ötlet felmerült[14], s nem lehetetlen, hogy a szeptember 11-i események nyomán megváltozott hangulatban újra előtérbe kerül a kulcsletét mint lehetséges megoldás, akár Magyarországon is[15].

12 A titkosítás szabályozásának fejleményeiről lásd Bert-Jaap Koops fél évente frissített, a Föld 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 : http://www2.epic.org/reports/crypto2000.

13 Az Egyezmény szövege magyarul : http://www.stopcybercrime.net/2_2.php; a hozzá kapcsolódó Expanatory Memorandum szövege angolul : http://conventions.coe.int/Treaty/EN/cadreprojets.htm

14 Lásd Bert-Jaap Koops összefoglalóját : http://cwis.kub.nl/~frw/people/koops/cls2.htm#coe

15 A World Trade Center épületében röviddel azelőtt elkövetett merényletek Levy beszámolója szerint hozzájárultak ahhoz, hogy a Clinton-adminisztráció a nemzetbiztonsági szolgálatok mellé állt a 1993-ban a Clipper-chippel kapcsolatban : lásd Levy : i.m. 244. o.

Első Magyar Jogi Portál
és online Ügyvédi Szaknévsor

JOGI FÓRUM

jogi hírek

interjúk

publikációk

vitafórum

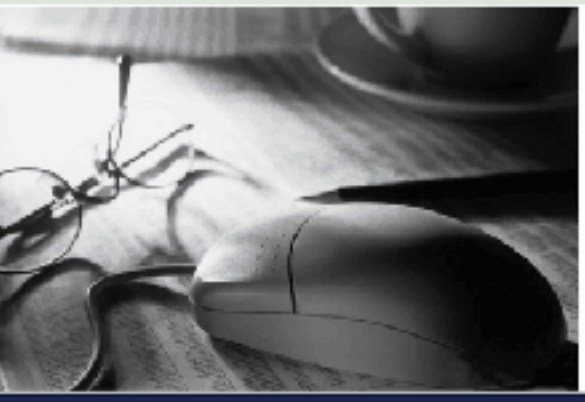
szaknévsor

jogi szakkönyv-katalógus

jogi állásbörze

szakmai rendezvények

heti hírlevél



országos ügyvédi szaknévsor

magyar, angol és német nyelven

ügyfél keres ügyvédet szolgáltatás

www.jogiforum.hu