Szádeczky Tamás

# Az elektronikus írásbeliség és problémái

## 1. Bevezetés

Az írásbeliség fejlődésében az írás feltalálása után három forradalmat különböztethetünk meg.[1] Az első forradalom a fonetikus értéket hordozó alfabetikus írás feltalálása volt a Kr. e. 13. században, amely különválasztotta a szöveget a tartalomtól. A második a XV. században a Johannes Gensfleisch Gutenberg által feltalált könyvnyomtatás volt, amely lehetővé tette az írott művek elérhetőségét a nagy tömegek számára. A harmadik forradalom – melyet elektronikus írásbeliségnek nevezünk – jelenleg zajlik, és bár történelmi távlat híján nem tudjuk pontosan meghatározni a mibenlétét, azt kijelenthetjük, hogy jelentős mértékben megváltoztatta az írásbeli kommunikáció minden lényeges struktúráját, mindamellett, hogy az ezt megelőző forradalmak által elért vívmányokat is meghagyta. Ez jelenti a kulcsot a digitális kultúrához és az információs társadalomhoz.

Az elektronikus írásbeliség fejlődésével teret hódítottak a számítógépek a hagyományosan papírhordozót használó alkalmazásokban is. Ilyen alkalmazásnak tekinthetjük az iratkezelést, a számviteli bizonylatolást, valamint általában a köziratok, köz- és magánokiratok készítését. Az ehhez szükséges technikai feltételek már az 1990-es évek óta adottak, amióta a számítógéptechnikai és hálózati technológiák mellett kidolgozásra került az aszimmetrikus kulcsú titkosítás technológiája. Ez tette lehetővé az elektronikus aláírás megalkotását, majd a jogi kereteket meghatározó jogszabályok elfogadását. A nemzetközi gyakorlatban, illetve a magyar jogszabályi követelmények alapján a dokumentumok elektronikus hitelesítése elektronikus aláírással oldható meg.

**A harmadik forradalom – melyet elektronikus írásbeliségnek nevezünk – jelenleg zajlik, és bár történelmi távlat híján nem tudjuk pontosan meghatározni a mibenlétét, azt kijelenthetjük, hogy jelentős mértékben megváltoztatta az írásbeli kommunikáció minden lényeges struktúráját, mindamellett, hogy az ezt megelőző forradalmak által elért vívmányokat is meghagyta.**

Az Európai Unióban, illetve a Magyar Köztársaságban a jelenlegi politikai, illetve jogalkotói törekvések e területek igen gyors fejlesztését tűzték ki célul.

A tanulmány során a követelményekkel, az elért vívmányokkal és az ezekből fakadó kockázattal foglalkozom.

## 2. Az elektronikus írásbeliség kialakulásának feltételei

Az elektronikus írásbeliség kialakulásához szükséges műszaki követelmények három részre oszthatók: a számítógépre, a hálózati kapcsolatokra és az írásbeliség követelményeinek gyakorlati megfelelést biztosító adatbiztonsági eljárásokra.

A Zuse Z3-at, az első Turing-teljes digitális számítógépet Konrad Zuse alkotta meg 1941-ben. A tranzisztor megalkotása 1947-ben William Bradford Shockley, John Bardeen, és Walter Houser Brattain által forradalmasította az addig kezdetleges elektromechanikus számítógépek világát.[2] 1958-ban elkészült az integrált áramkör, az egy lapra szerelt tranzisztorok tömege. Az első személyi számítógép (IBM PC) megjelenésével 1981-ben lehetőség nyílt arra, hogy az emberek otthonába, illetve munkaasztalára kerülhessen az addig csak a számítóközpontokban, illetve azokhoz kapcsolódva elérhető számítási teljesítmény.

A számítógép-hálózatok fejlesztése 1962-ben kezdődött, amikor az Advanced Research Projects Agency (ARPA) Intergalactic Network néven kutatócsoportot állított fel J. C. R. Licklider vezetésével, amely csoport kifejlesztette az időosztásos rendszert, ami lehetővé tette a fent említett ún. *mainframe* szolgáltatásainak nagyszámú felhasználó közötti megosztását telexhálózaton.[3]

1969-ben szintén az ARPA keretein belül a Leonard Kleinrock vezette amerikai kutatócsoport megalkotta az első csomagkapcsolt számítógépes hálózatot, az ARPANET-et. A hálózat ekkor még csak pár egyetemi és katonai pontot kapcsolt össze. A hálózat polgári, és főleg szélesebb körű alkalmazása egészen a hetvenes évek végéig váratott magára, ekkor azonban robbanásszerű fejlődésnek indult, majd a katonai eredetet jelző ARPANET név 1998-ban Internetre változott.

A World Internet Project 2007-es adatai szerint a magyar háztartásoknak már 49%-ában, tehát közel kétmillió háztartásban van számítógép, valamint harmadában (35%) van internetkapcsolat.[4]

Még egy igen jelentős, de általában kisebb hangsúlyt kapó követelmény merül fel az elektronikus írásbeliség kialakulásával kapcsolatban: a humán erőforrás: az állampolgárok, ügyfelek hajlandósága az információs társadalomban való aktív részvételre, hajlandóságuk és képességük az elektronikus írásbeliség vívmányainak használatára. E kérdés, valamint a gazdasági aspektus értékelését jelen cikk korlátozott terjedelme miatt nem tartalmazza.

A fejezet további részében műszaki feltételként az adatbiztonsági eljárások és a jogi-politikai feltételek kialakulását ismertetem, mint a témakör jelen megközelítése szempontjából kiemelt jelentőségű területeket.

### 2.1. Adatbiztonsági eljárások

Az elektronikus írásbeliség kialakulásának igen fontos része az írásbeliség követelményeinek megfelelést biztosító adatbiztonsági eljárások kialakulása és nyilvános használata. Az adatok logikai biztonságának eléréséhez szükséges azok bizalmasságának, hitelességének és eredetiségének igazolása. Ez matematikai módszerekkel valósítható meg, amellyel a kriptográ-

A szerző okleveles biztonság- és védelempolitikai szakértő, mérnök és a PTE ÁJK ösztöndíjas doktorandusz hallgatója.

fia (titkosítás) tudománya foglalkozik. Az információ titkosítása gyakorlatilag az írással egyidős, hiszen amióta üzeneteket papírra (vagy agyagtáblára) vet az emberiség, felmerül az igény arra is, hogy ezt mások ne tudják elolvasni. Az ókortól napjainkig három generációját különböztetjük meg a titkosítást és visszafejtést lehetővé tevő logikai-matematikai eszközrendszereknek, melyeket kriptorendszereknek nevezünk. Ez a három generáció történeti előzménye a mai kriptorendszereknek, amelynek robbanásszerű fejlődését a számítástechnika fent vázolt eredményei tettek lehetővé.

Negyedik generációs kriptorendszereknek a XX. század végén kifejlesztett, teljesen matematikai alapú és számítógépet használó titkosítási módszereket nevezzük, amelyeknek két fajtája van: a szimmetrikus és az aszimmetrikus titkosítás. Elsődleges különbség köztük az, hogy szimmetrikus titkosítás esetén ugyanaz a kulcs használható titkosításra és visszafejtésre is (ezért egy kulcsosnak is nevezik ezt a módszert), míg aszimmetrikus esetén a titkosítási és visszafejtési folyamatot külön kulccsal kell végezni.

**Az aszimmetrikus titkosításhoz egy közös „titokból" kell matematikai úton két kulcsot (egy kulcspárt) generálni. Ezután a közös „titok" megsemmisítésre kerül. A kulcspár egyik tagja lesz a kriptográfiai magánkulcs, amely semmilyen körülmények között nem kerülhet ki a tulajdonos ellenőrzéséből. A kulcspár másik tagja a nyilvános kulcs, amely közzétehető az Interneten, illetve bármely nem biztonságos csatornán továbbítható. A két kulcs a használat szempontjából ekvivalens, tehát amit az egyik kulccsal titkosítottunk, azt a másik kulccsal lehet visszafejteni. Így lehetővé válik az eltérő irányok alkalmazása (titkosítás és elektronikus aláírás).**

A szimmetrikus titkosítás az 1970-es években került kifejlesztésre. A titkosításhoz invertálható (visszafordítható) függvények alkalmazására, majd blokkonként (általában 64-256 bit) keverésre és behelyettesítésre kerül sor az adott nyílt szövegen. Ezek az eljárások megegyeznek az első generációs kriptorendszereknél alkalmazottal, a különbség csak az, hogy ezeket a titkosítást biteken kell végezni, másrészt pedig ez a műveletsor többször megismétlődik. (iterálás). Így a viszonylag egyszerű eljárások kombinálásával, illetve nagyszámú ismétlésével igen jó biztonság szint érhető el. Ezek a blokkok alapesetben nincsenek kapcsolatban egymással (ez az *Electronic Code Book*), de a biztonság növelése érdekében a blokkok különböző módokon kapcsolatba hozhatók egymással (ilyenek a *Cypher Block Chaining*, *Cipher Feedback* és *Output Feedback* módok).[5] E megoldást használja a népszerű szimmetrikus kriptorendszer, a *Data Encryption Standard (DES)*, amelyet ma már a kulcshossz rövidsége miatt (56 bit) a szakemberek nem tartanak biztonságosnak, de még több helyen használják. A DES titkosításra kiírt törési versenyek[6] alapján kijelenthető, hogy megfelelő hardver alkalmazásával akár órák alatt feltörhető bármely titkosított üzenet. Magából a szimmetrikus titkosítás elvéből fakadóan a titkosított szöveg minden esetben feltörhető, csak idő kérdése. A titkosítás biztonságát csak az alkalmazott matematikai algoritmus minősége, illetve a kulcs hossza határozza meg, tehát az algoritmus titkossága nem. Ettől függetlenül egyes esetekben a biztonság növelése érdekében (DES), vagy szerzői jogi okokból kifolyólag (IDEA) az algoritmus maga is titkos lehet. A ma már leginkább elterjedt és alkalmazott módszer a századfordulón kifejlesztett *Advanced Encryption Standard* (AES), amely 128-256 bit kulcshosszal és az eddigi kísérletek alapján megfelelő algoritmusválasztással (eddig senki nem talált rajta gyenge pontot) a világ összes számítógépével évmilliók alatt lenne feltörhető.[7] Megjegyzendő ugyanakkor, hogy a kriptográfia jelenlegi tudományának teljes felborítását jelentené a kvantumszámítógépek kifejlesztése, amelyekkel igen rövid időn belül visszafejthető lenne a jelenlegi legerősebb szimmetrikus kulccsal titkosított szöveg is.

A modern kriptográfia másik ága a hasonlóan 1970-es években kifejlesztett nyilvános kulcsú, vagy aszimmetrikus kulcsú kriptográfia. Itt a matematikai alapokat már más problémák jelentik. Ilyenek többek között a nagy prímszámok szorzását és még nagyobb számok prímtényezőkre bontását jelentő faktorizációs probléma (*RSA*, *Rabin*, *Blum-Goldwasser* sémák alapulnak ezen), a diszkrét logaritmus problémája (*Diffie-Hellmann* és *ElGamal* kriptorendszerek), valamint a részhalmaz-összeg probléma (*Merkle-Hellman knapsack*, *Chor-Rivest knapsack* sémák).[8] Ezek megoldása egy bizonyos „titok" (magánkulcs) ismeretében egyszerű, míg annak hiányában igen nehéz matematikai feladat.. Az aszimmetrikus rendszerek alkalmazásánál nagyobb kulcsot kell használni (1024-4096 bit) és több időt vesz igénybe a kódolási és dekódolási folyamat is, de az elért biztonság megegyezik a szimmetrikus kriptorendszereknél elérhetővel. Mindez mégis forradalmasította a kriptográfiát mivel kiküszöbölte a kulcscsere problémáját. Először Diffie, Hellman és Merkle publikálták az aszimmetrikus titkosításon alapuló biztonságos kulcscsere elméletét, amely szerint a kommunikáló partnereknek az üzenetváltás előtt nem szükséges titkosított csatornán megosztania a kulcsot. Ezzel a módszerrel vált lehetővé a titkosítás széles körű publikus alkalmazása az elektronikus aláírás és a nyilvános kulcsú infrastruktúrán (PKI) alapuló rendszerek által. Az aszimmetrikus titkosításhoz egy közös „titokból" kell matematikai úton két kulcsot (egy kulcspárt) generálni. Ezután a közös „titok" megsemmisítésre kerül. A kulcspár egyik tagja lesz a kriptográfiai magánkulcs, amely semmilyen körülmények között nem kerülhet ki a tulajdonos ellenőrzéséből. Ha ez mégis megtörténne, az kompromittációnak minősül és a kulcspárt többé nem szabad használni, illetve ha infrastrukturálisan lehetséges, azt vissza kell vonni. A kulcspár másik tagja a nyilvános kulcs, amely közzétehető az Interneten, illetve bármely nem biztonságos csatornán továbbítható. A két kulcs a használat szempontjából ekvivalens, tehát amit az egyik kulccsal titkosítottunk, azt a másik kulccsal lehet visszafejteni. Így lehetővé válik az eltérő irányok alkalmazása (titkosítás és elektronikus aláírás).

Az elektronikus aláírás készítése a következőképp történik: az adatból (dokumentumból) egy ún. hash-függvénnyel ujjlenyomat (digitális lenyomat) képződik. Ez a függvény egy csapóajtó függvény, amely azt jelenti, hogy a függvény elvégzése az egyik irányba egyszerű, a másik irányba pedig bonyolult matematikai feladat. Ez a függvény tetszőleges mennyiségű adatból egy állandó méretű (128–256 bit) adathalmazt generál. A bemeneti adathalmazban egyetlen bit megváltozása legalább a kimeneti bitek 50 százalékát meg fogja változtatni (lavinahatás). A kimenetként kapott adathalmazt ujjlenyomatnak nevezzük, mivel közel egyedi módon jellemzi a bemeneti adathalmazt. A kimenetből a bemenetet előállítani nem lehet. A gyakorlatban az SHA-1, RIPEMD-160, *Whirlpool* algoritmusok használatosak, mivel a több éve gyanús MD5 algoritmust 2008 decemberében feltörték, így használata többé nem biztonságos.[9] Az aláírandó dokumentumon ezt a folyamatot végrehajtva kapott ujjlenyomatot a kriptográfiai magánkulccsal kell titkosítani. Így létrejön az elektronikus aláírás, amely a bemeneti dokumentumtól független, külön fájl lesz. Az aláírt dokumentum és az aláírás együtt, egy nyilvános csatornán, például e-mailben elküldhető a címzettnek. A címzett az elektronikus aláírást az aláíró nyilvános kulcsával megfejti, így megkapja azt az ujjlenyomatot, amely az eredeti dokumentumból az aláíró készített. Ezalatt az átküldött dokumentumból a címzett is elkészíti az ujjlenyomatot, és ezt a kettőt összehasonlítja. Amennyiben ezek megegyeznek, biztosan állíthatjuk, hogy az aláírt dokumentumban nem történt változtatás, valamint azt, hogy egy meghatározott kulccsal történt a dokumentum aláírása. Nem bizonyítja viszont azt, hogy ez ténylegesen a feladónak a magánkulcsa volt, azt, hogy ezt nem vonták vissza, és nem állapítható meg belőle a feladás ideje sem. Ezek bizonyítására más, kiegészítő funkciókat kell alkalmazni. A kulcsok személyhez kötése, a hitelességi probléma kétféle módon oldható meg: egyrészről a bizalmi háló (*web of trust*) módszerével,[10] amelyet a PGP használ. Ezen módszer szerint az egymásban megbízó személyek egymás kulcsait aláírják, így ha a címzett megbízik a feladó kulcsát aláíró bármelyik személyben, vagy vissza tudja vezetni az aláírásokat egy megbízható személyig, akkor ez biztosítékot jelent számára a feladó megbízhatóságára is. Ennek a módszernek a hátránya, hogy igen nagy bizalmi hálókat követel meg az, hogy két ismeretlen ember közös ismerőssel rendelkezzen. Másik módszerként a nyilvános kulcsú infrastruktúra (*Public Key Infrastructure*, PKI) használatos. Itt a felek megbízhatóságát egy mindenki által megbízható harmadik személy tanúsítja. Az általa kiadott tanúsítvány egy elektronikus adathalmaz, amely általában tartalmazza a nyilvános kulcsot is. A harmadik személy az állam által megbízhatónak tartott hitelesítés szolgáltató (*Certificate Service Provider*, CSP), aki a tanúsítvány kiadása előtt ellenőrzi a kulcsbirtokos és a kulcs összetartozását (például személyigazolvány kérésével). A hitelesítés szolgáltatók tanúsítási láncot alkotnak, amelynek a tetején a legmagasabb szintű hitelesítés szolgáltató (*Certificate Authority*, CA) áll. Ezek a CA-k mindenki által elfogadottak és ebből kifolyólag a tanúsítási lánc többi eleme is megbízhatóvá válik. Az aláírás idejének hiteles megállapítása időbélyeg szolgáltató (*Timestamping Authority*, TSA) segítségével történik, aki a pontos időt látja el saját elektronikus aláírásával, amit a feladó beépít a dokumentum elektronikus aláírásába. Az időbélyeg

igénylése alapvetően Interneten keresztül, on-line történik. A TSA megbízhatóságát a tanúsítványa biztosítja, amely a tanúsítási lánc mentén visszavezethető egy CA-hoz. Az elektronikus aláírások, illetve tanúsítványok használati köre korlátozott. Egy kulcspárt csak elektronikus aláírásra, vagy titkosításra, vagy biztonságos kapcsolat kiépítésére (SSL) lehet használni. Amennyiben ezek közül több funkciót is használni kíván a felhasználó, több kulcspárra, illetve tanúsítványra van szüksége.

Az ismertetett fejlődési folyamat a bemutatott két évezred során szerves fejlődéssel elért oda, hogy bizonyítottan alkalmas legyen az elektronikus írásbeliség kiszolgálására. Ez a tény persze közel sem elegendő e cél eléréséhez.

### 2.2. Szabályozási háttér és gyakorlat

Az elektronikus aláírás algoritmikus és műszaki infrastrukturális megvalósítása után a tényleges gyakorlati használathoz szükséges volt az, hogy ezt a jogalkotó is elfogadja, és így ki lehessen váltani a papír alapú aláírást elektronikus aláírással az írásba foglalást megkövetelő minden területen. Az elektronikus aláírás, mint a hagyományos aláírást több jogterületen kiváltó aktus jogi elfogadására Európában először Németországban 1996-ban (*Gesetz zur digitalen Signatur*), majd az Egyesült Királyságban 1999-ben (*Building Confidence in Electronic Commerce – A Consolidation Document*), az Európai Unió szintjén 1999-ben (az elektronikus aláírás közösségi keretéről szóló 1999. december 13-ai 1999/93/EK európai parlamenti és tanácsi irányelv), az Egyesült Államokban 2000-ben (*Electronic Signatures in Global and National Commerce Act*) megszületett jogszabályok teremtettek lehetőséget.

A magyar jogalkotásban az első lépés az elektronikus aláírásról szóló 2001. évi XXXV. törvény (Eat) elfogadása volt. A törvény alapelveit a Kormány az elektronikus aláírásról szóló törvény szabályozási alapelveiről és az ezzel kapcsolatban szükséges intézkedésekről szóló 1075/2000. (IX. 13.) Korm. határozatban határozta meg. A főbb alapelvek a technológiafüggetlenség, a joghatály meg nem tagadhatósága, a hitelesítés-szolgáltatás szabályozottsága és a szolgáltató felelőssége, a minősített elektronikus aláírással ellátott elektronikus irathoz teljes bizonyító erejű magánokirati, illetve közokirati minőség elrendelése, az alkalmazás önkéntessége, az állami alkalmazás és a külföldi szolgáltatók feltételhez kötött elfogadása.

Az elektronikus kormányzati szolgáltatások részben e törvény alapján indultak el. Az elektronikus adóbevallás a '90-es évek végétől több fázisban vált elérhetővé; a folyamatnak 2002-ben és 2006-ban voltak fordulópontjai.[11] 2003-ban indult a TakarNet, a földhivatali elektronikus adatszolgáltató rendszer, 2005-től az Ügyfélkapu, 2006-ban megszülettek az elektronikus iratkezelésre vonatkozó jogszabályi követelmények, elindult az elektronikus közbeszerzés, 2007-ben az elektronikus cégeljárás, majd 2008-ban az APEH elektronikus árverése, az ügyvédek számára a jogügyletek biztonságának erősítése céljából hozzáférhető adatellenőrzés, valamint megtörtént a számviteli szabályok változtatása az elektronikus számlák tárolásának egyszerűsítése irányában (annak tömeges elterjedése ezt követően várható).

A magyar elektronikus aláírási törvény az 1999/93/EK irányelvvel megegyezően a műszaki háttértől függetlenül az elvi működést figyelembe véve három szintet különböztet meg. A legalsó szint az „egyszerű" elektronikus aláírás, amely mindennemű biztonsági követelmény nélkül az elektronikus dokumentumokba leírt nevet jelenti (például az aláírás egy e-mail végén). Ehhez a jogalkotó különös jogkövetkezményt nem fűz, szabad mérlegelés tárgyává teszi ennek bizonyítékként való elfogadását és súlyát, azzal, hogy az Eat. egyértelművé teszi, hogy elektronikus aláírás, illetve dokumentum elfogadását – beleértve a bizonyítási eszközként történő alkalmazást – megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni nem lehet kizárólag amiatt, hogy az aláírás, illetve dokumentum elektronikus formában létezik.[12] A második biztonsági szint a fokozott biztonságú elektronikus aláírás, amellyel szemben törvényi követelmény, hogy alkalmas legyen az aláíró azonosítására, egyedül csak az aláíróhoz legyen köthető, olyan eszközökkel kerüljön létrehozásra, amelyek kizárólag az aláíró befolyása alatt állnak, és a dokumentum tartalmához olyan módon kapcsolódjon, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető legyen.[13] Jogkövetkezményként – meghatározott területeket kivéve[14] – az írásba foglalás követelményeinek való megfelelést nevesíti a törvény. Az elektronikus aláírások közül a legbiztonságosabb, illetve a legmagasabb követelményeket kielégítő típus a minősített elektronikus aláírás. A minősített elektronikus aláírás olyan fokozott biztonságú elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.[15] Az ezzel szemben kitűzött követelmények igen szigorúak és további jogi szabályozás tárgyát képezik az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendeletben foglaltak szerint.[16] A minősített elektronikus aláírással ellátott dokumentum teljes bizonyító erejű magánokirat, ezért annak hitelessége és az aláíróhoz való egyértelmű tartozása annak ellenkezőjének bebizonyításáig kétségbe nem vonható. Ez utóbbi két szint esetében mind az előállítás módjára, mind pedig a szolgáltató működésére vonatkozóan tanúsítást, illetve hatósági felügyeletet követel meg a jogszabály. A tanúsítást az informatikáért felelős miniszter által kijelölt, független tanúsító szervezetek[17] (jelenleg a HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. és a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft.) végzik, míg a hatósági felügyeletet a Nemzeti Hírközlési Hatóság látja el.[18] Ezekkel az eljárásokkal biztosítható a szolgáltatók és így az elektronikus aláírási rendszer működésének biztonsága és minősége. A Magyar Köztársaságban hitelesítés szolgáltatóként jelenleg a NetLock Kft., Microsec Kft., MÁV Informatika ZRt., Magyar Telekom Nyrt. és az EDUCATIO Kht. működnek. A hitelintézetek közötti elszámolás-forgalom lebonyolításának biztosításában vezető szerepet betöltő GIRO Zrt. 2001 óta hitelesítés-szolgáltatóként működött, de érdektelenség miatt 2005 óta nem bocsátott ki tanúsítványokat, majd 2008 áprilisában határozott, úgy, hogy megszünteti hitelesítés-szolgáltatói tevékenységét. Nyilvántartásait a NetLock Kft. vette át, ami az első ilyen szolgáltatás-átadási eset volt Magyarországon.

Magyarországon jelenleg elektronikus aláírás igénylése a gyakorlatban úgy történik, hogy az állampolgár felkeresi a hitelesítés szolgáltatót, akitől személyazonossága igazolása mellett e-mail címéhez elektronikus aláírást és tanúsítványt igényel. A személyazonosság igazolása a személyazonosság igazolására alkalmas okmány (személyazonosító igazolvány, útlevél, jogosítvány) illetve a cégkivonat másolatának elküldésével, vagy annak személyes bemutatásával történhet. Ezeket a hitelesítés szolgáltatók külön biztonsági kategóriába sorolják (például *Class C* és *Class B*). A közigazgatásban alkalmazható elektronikus aláírás igényléséhez elengedhetetlen a személyes megjelenés is.[19] A minősített aláírások esetében közjegyző általi hitelesítés történik.

A kulcspárt a birtokos a tulajdonában lévő biztonságos aláírást létrehozó eszközzel (BALE, pl. smart card, USB token) vagy szoftveres eszközzel állítja elő, amelynek nyilvános kulcsát a tanúsítvány elkészítéséhez átad a hitelesítés-szolgáltatónak. A tanúsítvány és a kulcsok így valamely biztonságos adathordozón vagy szoftveres kulcstárban kerülnek tárolásra. A megfelelő szoftvereket a számítógépre telepítve a felhasználó a kártyaolvasó segítségével alá tudja írni e-mailjeit, illetve bármely egyéb elektronikus dokumentumát. Különleges alkalmazásokban is lehetőség nyílik az elektronikus aláírás használatára, ilyen például az elektronikus cégeljárás, amely nem sokban különbözik egy dokumentum aláírásától, mindössze formalizáltan és a Cégbíróság által feldolgozhatóan teszi lehetővé azt.

**A magyar közigazgatásban több, nem PKI rendszerre alapuló azonosítási rendszert is alkalmaztak, illetve alkalmaznak. Ilyen az Adó- és Pénzügyi Ellenőrzési Hivatal által 2004 és 2006 között[22] elektronikus adóbevallás hitelesítésére használt chipkártyás megoldás. Másik – szintén nem PKI alapú – megoldás a Miniszterelnöki Hivatal Elektronikuskormányzat-központ által üzemeltetett Ügyfélkapu rendszere, amelynek biztonságát és megbízhatóságát több szakember vitatja. A felhasználó azonosítására kétségtelenül gyenge az Ügyfélkapuban alkalmazott módszer, ugyanis nem írja elő valamely biztonságos eszköz birtoklását (például chipkártya) az azonosításhoz, amely lehetőséget biztosítana a kétfaktoros azonosításhoz.**

A közigazgatási hatósági eljárásokban használható tanúsítványokra vonatkozó szabályokat a 194/2005. (IX. 22.) Korm. rendelet határozza meg, mely alapján az ilyen aláíró tanúsítványokat kibocsátó hitelesítés-szolgáltatói tanúsítványokat legfelsőbb szinten a Közigazgatási Gyökér Hitelesítés-szolgáltató (KGYHSZ) bocsátja ki. Az ily módon kiépített infrastruktúra ellenére a magyar közigazgatásban több, nem PKI rendszerre alapuló azonosítási rendszert is alkalmaztak, illetve alkalmaz-

nak. Ilyen az Adó- és Pénzügyi Ellenőrzési Hivatal által 2004 és 2006 között[20] elektronikus adóbevallás hitelesítésére használt chipkártyás megoldás. Másik – szintén nem PKI alapú – megoldás a Miniszterelnöki Hivatal Elektronikus-kormányzat-központ által üzemeltetett Ügyfélkapu rendszere, amelynek biztonságát és megbízhatóságát több szakember vitatja. A rendszerbe való első bejelentkezés, illetve a személyazonosság igazolása Okmányirodákban történik, majd egy felhasználó név – jelszó páros alkalmazásával lehet belépni a rendszerbe és azon keresztül különböző hatósági eljárásokat illetve egyéb tevékenységeket végezni. A felhasználó azonosítására kétségtelenül gyenge az Ügyfélkapuban alkalmazott módszer, ugyanis nem írja elő valamely biztonságos eszköz birtoklását (például chipkártya) az azonosításhoz, amely lehetőséget biztosítana a kétfaktoros azonosításhoz.[21] Maga a kapcsolat titkosított csatornán (SSL) történik.

## 3. Az elektronikus írásbeliség problémái

Az elektronikus aláírással hitelesített dokumentumok hosszú távú megőrzése komplex feladat. Egyrészről magát az elektronikus adatot, illetve annak fizikai leképezését meg kell védeni a megsemmisüléstől. Az elektronikus aláírás hosszú távú bizonyító erejét a tanúsítási lánc tárolásával meg kell oldani, valamint biztosítani kell az adott dokumentum megnyitását lehetővé tevő alkalmazás tetszőleges időben történő elérését.

Az elektronikus adatok épségének hosszú távú megőrzése fizikai, logikai és üzemeltetési biztonsági feladatok összessége. Mindenképpen szükséges hozzá az adattároló rendszer redundanciája és az adattároló eszközök biztonságos hosszú távú tárolása.

### 3.1. Túlzott gyorsaság

A Kormány minden téren igyekszik az állampolgárok, illetve az egyéb ügyfelek eddigi papíralapú tevékenységeit elektronikus mederbe terelni. Ez a gyakorlatban a kizárólag elektronikus dokumentumok készítését és felhasználását jelenti. E törekvés egyes esetekben túlzottan előremutatónak tűnik.

A jogalkotó gyakorlatilag nem biztosítja az időt a papír alapú folyamatokról az elektronikusra történő átállásra. Így történt például az elektronikus adóbevallás, elektronikus iratkezelés, illetve az elektronikus cégeljárás esetében is. Az elektronikus adóbevallásra való átállásra a gazdasági társaságok többségének kevesebb, mint egy év állt rendelkezésére, az iratkezelés esetében másfél év, a cégeljárás tekintetében pedig félévnyi átállási időt kapott a kötelezett. Ha ezt tekintjük az elektronikus írásbeliségre való áttérésnek a hagyományos írásbeliségből, amelyet több ezer éve gyakorlunk, ezzel szemben az analfabéták száma Magyarországon eléri a százezer főt,[23] meggondolatlanságnak tűnik egy ilyen léptékű paradigmaváltás megvalósítása pár év távlatában. Más, nálunk fejlettebb ország, amely már korábban bevezette azokat a lépéseket, amelyeket mi is megtettünk ebben a pár évben, fenntartja a lehetőséget a papíralapú dokumentumok használatára. Konkrét példaként Ausztria említhető, ahol az elektronikus cégeljárást már a nyolcvanas években lehetővé tették telefonhálózaton összekötött gépek segítségével, a kilencvenes években a polgári- illetve büntetőeljárások számottevő részét elektronizálták, ebben az évtizedben pedig – tovább finomítva az igazságszolgáltatásban alkalmazott informatikai lehetőségeket – bevezették az elektronikus fizetési meghagyást. Mindezen nagyfokú és folyamatos fejlődés ellenére mindmáig lehetősége van, sőt bizonyára a jövőben is lehetősége lesz az ügyfélnek papír alapú dokumentumok használatára a fenti cselekményekben, amelyeket az igazságügyi tárca honlapjáról letölthet.

### 3.2. A formátumok különbözősége

Jelentős nehézségeket okozott eddig is, és az elkövetkezendőkben is valószínűleg problémát fog jelenteni a dokumentumok formátumbeli különbözősége, és az ebből adódó feldolgozási és alkalmazási különbségek.[24]

Jól ismert és több-kevesebb ideje széleskörűen használt elektronikus dokumentum állományok az egyszerű szövegfájl (*plaintext,* TXT) a *Microsoft Rich Text Format* (RTF), és a *Portable Document Format* (PDF). Jelenleg Magyarországon az elektronikus ügyintézési eljárásban a TXT, RTF 1.7, PDF 1.3 dokumentumok értelmezési kötelezettség alá esnek a közigazgatási szervek által.[25] Ezen formátumok elsődleges hátránya, hogy nem strukturáltak, ezért nehézkesen dolgozhatóak fel automatikus rendszerrel. Ezeknél is szélesebb körűen használt a *Microsoft Word dokumentum* (DOC), amely ráadásul zárt, egyedi formátum, annak pontos felépítése a Microsoft üzleti titka, ezzel lehetetlenné téve bármely nem-Microsoft szoftver teljes kompatibilitását. Ezen generációs hibák javítására születtek meg mindkét fejlesztői oldalon (*Microsoft* és *OpenDocument Foundation*) az XML-re épülő formátumok. A Kiterjeszthető Leíró Nyelv (*Extensible Markup Language*, XML) általános célú leíró nyelv, speciális célú leíró nyelvek létrehozására. Az 1986-ban ISO által szabványosított SGML nyelv[26] továbbfejlesztése, 1998-ban vált W3C ajánlássá.[27] Az XML célja az adatok strukturálása, licenszmentesen, platform-függetlenül és széleskörűen támogatva. Egy XML dokumentum akkor helyes, ha helyesen formázott, vagyis megfelel az XML nyelv szintaxisának és érvényes, vagyis megfelel a felhasználó által definiált tartalmi szabálynak, amely meghatározza az elfogadott értéktípusokat és értékhelyeket. Ez utóbbi követelményhez szükséges a szabályok meghatározása, amely Dokumentum Típus Definícióval (*Document Type Definition*, DTD) vagy XML Séma Definícióval (XML *Schema Definition*, XSD) történhet.

Ezen a technológiai keretrendszeren alapul az *OpenDocument Foundation* által kifejlesztett *OpenDocument Format* (ODF) formátumcsomag[28] és a Microsoft által kifejlesztett *Office Open* XML (OOXML) fájlformátum.[29] Ezek képezhetik az alapját a jövőbeni, széles körben alkalmazható dokumentumformátumoknak Az ezen technológián alapuló egyedi, szigorú megkötésekkel rendelkező XSD-jű űrlapok (form-ok) automatikusan feldolgozhatóak.

Szakmailag partikuláris, de a közigazgatási informatikában jelentős kérdés az általános, illetve az iratkezelési metaadat-probléma, miszerint az adatokat leíró adatok (metaadatok) pontosan milyen formában, értékben és egyedekkel áll elő. E kérdés megoldására született több kezdeményezés, mint a *Dublin Core Metadata Initiative* (DCMI), a *Managing Information Resources for e-Government* (MIREG), GovML és a PSI *Application Profile*.[30]

### 3.3. On-line adatbiztonság

Amennyiben valamely számítógép rendszerben őrizzük az adatokat, a rendszert a fizikai biztonság tekintetében védeni kell az elemi károktól (tűz-, és vízkár, akár a közüzemi ivóvízellátás illetve csatornázás tekintetében, földrengés, illetve az objektum megsemmisülése egyéb okokból), a műszaki követelmények hiányából bekövetkező incidensektől (áramellátás hiánya, áramellátási zavarok, klimatikus körülmények romlása, amely eredhet a hőmérséklet, illetve a páratartalom változásából, informatikai hálózati probléma), az elektromágneses zavaroktól (akár szándékos károkozás esetén is), és a műszaki megbízhatósági problémák ellen (a gyártási hiba, elfáradás, egyéb műszaki hiba). A logikai biztonság felöleli a szoftverelemek megbízhatóságát (operációs rendszer, alkalmazói programok) a szándékos károkozás elleni védelmet (vírusok, férgek, rosszindulatú programok, hálózati támadások, hacker tevékenység), a hálózati protokollok biztonságát és a hozzáférés-menedzsmentet.

### 3.4. Off-line adatbiztonság

A digitális adatok tárolása – amennyiben az adat nem változik, illetve ha a költségek szempontjából ez a megoldás mutatkozik előnyösebbnek – valamely optikai, vagy mágneses adathordozón is történhet. Az optikai adathordozón való tárolásnak elsődleges médiuma jelenleg a DVD lemez. A közhiedelemmel ellentétben ez sem örökéletű adattárolási megoldás: a lemez minőségétől függően legfeljebb 10 évig bízhatunk az adatok fennmaradásában, de a szerző saját tapasztalata alapján a 2 év utáni adatvesztés is előfordulhat. Ebből adódóan az optikai adattároló eszköz alkalmazása esetén is feltétlenül szükséges a periodikus regenerálás, amely a gyakorlatban a DVD lemezek lemásolását jelenti. Az optikai adattárolás előnye az elektromágneses terekre való érzéketlenség, de a megfelelő hőmérsékleti, páratartalmi és mechanikai viszonyokat fenn kell tartani tároláskor. A másik, mindmáig működő, nagyobb történelmi múltra visszatekintő adattárolási mód mágnesszalagos egységek használata. Ez a videokazettához hasonló, igen hosszú, általában végtelenített mágnesszalagos kazettát takar. Ennek tároló kapacitása máig meghaladja az optikai tárolók kapacitását, akár a terabájtos nagyságrendet is elérheti kazettánként.[31] A szalag tárolási környezetével kapcsolatban az optikai eszközök igényein felül felmerül az elektromágneses terek, illetve zavarok elleni védelem szükségessége is. Regenerálás a tárolási eljárás miatt mindenképpen szükséges, ugyanis a mágneses hordozó idővel demagnetizálódik.

Különösen nagy jelentőséggel bír az a követelmény – amelyet egyébként a felhasználók és az üzemeltetők is hajlamosak elfelejteni – hogy az elektronikus dokumentumok megnyitásához szükséges környezetet biztosítani szükséges.[32] Ez egy rosszabb esetet feltételezve azt is jelentheti, hogy a teljes számítógép architektúra változás ellenére mondjuk 100 év múlva meg kell nyitnunk egy olyan dokumentumot, amelyet egy garázsban működő szoftverfejlesztő cég szövegszerkesztő-alkalmazásával készítettek 1992-ben, a dokumentum formátuma nem követ semmilyen szabványt, de a jogi szabályozás nem teszi lehetővé a dokumentum selejtezését. Ebből a – természetesen erősen sarkított – lehetőségből adódik, hogy el kell tárolni az archivált dokumentummal együtt az azt megnyitni képes alkalmazást, az alkalmazást futtatni képes operációs rendszert, esetleg az ezeket futtatni képes teljes hardver konfigurációt. Ennek egyszerűsített formája lehet a megjelenítésre képes rendszer emulációja vagy az emuláció és a migráció együttes megvalósításával működő ún. Univerzális Virtuális Számítógép (UVC).[33] Ez a probléma Magyarországon a rendszerváltás után az állambiztonsági iratok kutatásakor már felmerült, mikor az adatokat tároló mágnesszalag leolvasására csak azért nem volt lehetőség, mert a megfelelő olvasó már nem szerezhető be és nem utángyártható.[34] Az eset kapcsán természetesen kérdésként felmerül, hogy valamely érdekcsoportoknak szándékában áll-e ezen információk titokban tartása.

**Különösen nagy jelentőséggel bír az a követelmény – amelyet egyébként a felhasználók és az üzemeltetők is hajlamosak elfelejteni – hogy az elektronikus dokumentumok megnyitásához szükséges környezetet biztosítani szükséges. El kell tárolni az archivált dokumentummal együtt az azt megnyitni képes alkalmazást, az alkalmazást futtatni képes operációs rendszert, esetleg az ezeket futtatni képes teljes hardver konfigurációt. Ennek egyszerűsített formája lehet a megjelenítésre képes rendszer emulációja vagy az emuláció és a migráció együttes megvalósításával működő ún. Univerzális Virtuális Számítógép (UVC).**

### 3.5. Elektronikus aláírás hitelessége

Az elektronikus aláírás hitelessége a létrehozásától számított kb. pár órától pár napos időintervallum után bizonyítható. Ennek oka az, hogy a hitelesség ellenőrzéséhez meg kell ismernünk az aláírás létrehozásakor aktuális visszavonási listát (CRL), amelyben az elektronikus aláírási szolgáltató az adott időpillanatban kompromittáltnak minősülő vagy egyéb okból visszavont tanúsítványokat közzéteszi. Ez az idő on-line tanúsítvány állapot ellenőrzés (OCSP) alkalmazásával jelentősen csökkenthető. Az elektronikus aláírás hitelessége ezek után folyamatosan bizonyítható, amennyiben a hozzáférési listák, illetve a teljes tanúsítási lánc hozzáférhető marad. Itt kap szerepet az elektronikus archiválási tevékenység, melynek keretében az archiválás pillanatában érvényes hitelesítési adatokat az elektronikus archiválási szolgáltató eltárolja, illetve felülhitelesíti saját kulcsával. Így az elektronikus archiválási szolgáltató által aláírt elektronikus dokumentum hitelessége csak az archiválási szolgáltató létének függvénye és nem befolyásolja a tanúsítási lánc valamely elemének kiesése, például úgy, hogy az adott tanúsítási szolgáltató befejezte tevékenységét, vagy saját kulcsa kompromittálódott. Ez az a pont, melyben az elektronikus archiválási szolgáltató tevékenysége felülemelkedik az egyszerű biztonságos adattárolás kérdésén.

### 3.6. Kockázat és védekezés

Ezekből a sokrétű követelményekből és széles körű problémaforrásokból adódóan az elektronikus dokumentumok tárolását és feldolgozását végző szervezet komoly nehézségekkel kell, hogy szembenézzen.

Az ismertetett problémákból fakadó kockázat különböző országokban eltérő mértékű. Abban az esetben, ha az elektronikus írásbeliség nagyfokú fejlődést mutat, a problémák kiküszöbölésére kevesebb idő jut, fokozva a probléma későbbi eszkalálódásának esélyét. Ebbe a kategóriába tartozik a kelet-közép-európai országok gyors közigazgatási informatikai fejlesztése. A szerző véleménye szerint nem történik meg a nyugat-európai államok tapasztalatainak kellő mértékű feldolgozása annak érdekében, hogy azzal kikerüljék az eredendő buktatókat. Ezek a problémák a későbbiekben akár komoly állami adatvesztéseket is okozhatnak.

A fenti nehézségekből közösen fakadó veszélyekkel és az ellenük való védelemmel a digitális megőrzés (digital preservation) foglalkozik. Az ezekből keletkező apokaliptikus végkifejlet a digitális sötét kor (digital dark age), melyben a fentiek miatt elvesznek a XXI. században keletkezett elektronikus dokumentumok, ami miatt erről a századról is – a sötét középkorhoz hasonlóan – kevés írásos emlék marad fenn – állítják ezen elmélet főbb képviselői, a *Getty Research Institute* több kutatója,[35] és Terry Kuny.[36] Ugyanakkor ezen gondolatokra cáfolat is született, miszerint az eddigi tapasztalatok csak az adat-visszaállítás hiányosságaira, nem pedig az adatvesztésre szolgáltak példaként.[37] A műszaki problémák megoldására átfogó jelleggel *Open Archival Information System* (OAIS) néven ISO referenciamodell készült.[38]

A túlzott gyorsaság problémájára a jobb politikaalkotás, a formátumproblémára és részlegesen az adatbiztonsági problémákra a jobb, illetve szigorúbb szabályozás nyújthat védelmet Magyarországon. Az elektronikus aláírási probléma, és részlegesen az adatbiztonsági probléma hatékony kezelője a piaci alapokon működő elektronikus archiválási szolgáltatók igénybevétele. Bizonyára e problémák bonyolultságából és a piaci igény hiányából kifolyólag nincsen jelenleg Magyarországon hatékonyan működő (megfelelő mértékben kihasznált) archiválás szolgáltató. Másrészről viszont az elektronikus dokumentumok megőrzésére kötelezettek igen nagy része úgy gondolja, hogy e kötelezettségének saját infrastruktúrájával, illetve humánerőforrásaival képes eleget tenni. A szerző saját tapasztalata alapján ide tartoznak a 10 fős községi önkormányzatok is, melyekről még nagy jóindulattal sem jelenthetjük ki, hogy ezen feladatuknak képesek lesznek eleget tenni.

## 4. Összefoglalás

A tanulmány ismerteti az elektronikus írásbeliség kialakulását, párhuzamot vonva a hagyományos írásbeliséggel, bemutatva annak kialakulását lehetővé tevő műszaki és jogi alapokat és az eddig elért vívmányokat. A műszaki alapok tekintetében ismerteti a számítástechnika és kiemelten a kriptográfia fejlődését és jelenlegi eredményeit. A jogi alapok tekintetében bemutatja az elektronikus aláírás és dokumentumok elfogadását lehetővé tevő jogi szabályozás kialakulását az Amerikai Egyesült Államokban, az Európai Unióban és egyes tagországaiban, beleértve Magyarországot is. A mű ismerteti az elektronikus írásbeliséghez szükséges részterületek, mint az elektronikus kereskedelem, elektronikus számlák, elektronikus iratkezelés, és egyes elektronikus kormányzati funkciók Magyarországon kialakult gyakorlatát. A tanulmány felhívja a figyelmet az elektronikus dokumentumokkal kapcsolatos problémákra és azok megőrzésének fontosságára, értékeli a kockázatokat és javaslatot tesz a védelemre.

## Jegyzetek

1 Sebestyén György: A Gutenberg-galaxis és a digitális kultúra szintézise: (Az elektronikus-virtuális könyvtár). Írás tegnap és holnap, I. évf. 1. sz., (1997. augusztus)

2 Köpeczi Béla (szerk.) et al.: Az embergéptől a gépemberig. Minerva, 1974. p. 206.

3 Kita, Chigusa Ishikawa: J.C.R. Licklider's Vision for the IPTO, IEEE Annals of the History of Computing, 2003/3. p. 65.

4 ITTK: Magyar információs társadalom jelentés 1998–2008. p. 38.

5 Bővebben lásd Horváth László – Lukács György – Tuzson Tibor – Vasvári György: Informatikai biztonsági rendszerek. BMF-E&Y, 2001. p. 111.

6 Lásd http://www.rsa.com/rsalabs/node.asp?id=2108

7 Virasztó Tamás: Titkosítás és adatrejtés. Biztonságos kommunikáció és algoritmikus adatvédelem. Netacademia, 2004. p. 50.

8 A. Menezes – P. van Oorschot – S. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996. p. 284.

9 Sotirov, Alexander – Stevens, Marc – Appelbaum, Jacob – Lenstra, Arjen – Molnar, David – Osvik, Dag Arne – Weger, Benne de: MD5 considered harmful today. Creating a rogue CA certificate. http://www.win.tue.nl/hashclash/rogue-ca/ [2009. 01. 03.]

10 Alfarez Abdul-Rahman: The PGP Trust Model. EDI-Forum, April 1997.

11 Jacsó Tamás: Az ügyfélkapu és az eBEV használata. Bp : Saldo, 2006.
12 Eat. 3. § (1)
13 Eat. 2. § 15.
14 Eat. 3. § (2)–(3) családjog és bírósági eljárások, kivéve, ha ezt az eljárástípusra vonatkozó jogszabály kifejezetten lehetővé teszi
15 Eat. 2. § 17.
16 További részletes iránymutatás található a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV. 26.) MeHVM irányelvben.
17 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
18 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól.
19 Előírja a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről szóló 194/2005. (IX. 22.) Korm. rendelet 7. §.
20 2006. május 2. óta az elektronikus adóbevallás az Ügyfélkapu rendszeren keresztül nyújtható be.
21 Hornák Zoltán: Felhasználó-azonosítás. http://www.biztostu.hu/mod/resource/view.php?id=451 [2009. április 29.]
22 2006. május 2. óta az elektronikus adóbevallás az Ügyfélkapu rendszeren keresztül nyújtható be.
23 UNESCO: UIS Statistics in brief. UNESCO, 2008.
24 A formátumproblémára külföldi példaként említhető az az eset, amelynek során,a Viking űrszonda 1976-os mágnesszalagon tárolt mérési adatait nem lehetett visszaállítani, mert az ismeretlen formátumban volt tárolva, ezért újra be kellett azokat gépelni a korábban kinyomtatott dokumentumokból. Wikipedia: Digital dark age. http://en.wikipedia.org/wiki/Digital_Dark_Age [2008.12.20.]
25 12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól (formátum r.) 1. melléklet
26 ISO 8879:1986
27 World Wide Web Consortium: XML Core Working Group Public Page http://www.w3.org/XML/ [2008.11.15.]
28 ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument) v1.0
29 ISO/IEC 29500:2008, Information technology – Office Open XML formats, valamint ECMA-376 Office Open XML File Formats – 2nd edition (December 2008)
30 Lina Bountouri, Christos Papatheodorou, Vasilis Soulikias, Mathios Stratis: Metadata Interoperability in Public Sector Information, Journal of Information Science, 7/2007, pp. 1–25
31 Lásd pl. http://www.ibm.com/systems/storage/tape/
32 Melléklet a 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelethez, 10.1.1. pontja: „Az ISZ-nek képesnek kell lennie az előírt formátumban rendelkezésre álló elektronikus iratok megjelenítésére olyan módon, ami megőrzi az iratokban foglalt információkat." Ez egyes jogalkalmazói értelmezések szerint a fenti követelményt takarja.
33 Lorie, Raymond: The UVC: a Method for Preserving Digital Documents – Proof of Concept. IBM Netherlands, Amsterdam : 2002.
34 Trócsányi Sára, az Adatvédelmi Biztos Hivatala főosztályvezetőjének szóbeli tájékoztatása alapján, Pécs, 2008. november 15.
35 MacLean, Margaret – Davis, Ben H. (Eds.): Time and Bits: Managing Digital Continuity. Getty Publications, Los Angeles, USA : 2000.
36 Kuny, Terry: A Digital Dark Ages? Challenges in the Preservation of Electronic Information. 63RD IFLA Council and General Conference, 1997.
37 Harvey, Ross: So where's the black hole in our collective memory? A Provocative Position Paper (PPP). http://www.digitalpreservationeurope.eu/publications/position/Ross_Harvey_black_hole_PPP.pdf [2008. 12. 28.]
38 Consultative Committee for Space Data Systems: Reference Model for an Open Archival Information System (OAIS). CCSDS Secretariat, Washington, DC, USA : 2002.

Gondol Daniella

# Honnan jövünk, kik vagyunk, hová megyünk[1] – gondolatok a szerzői jogi törvény módosításáról

Jelen cikk a szerzői jogról szóló 1999. évi LXXVI. törvény 2009. február 1-jétől hatályba lépett módosításaival kapcsolatos egyes kérdéseket kíván áttekinteni.[2] Célja azonban elsősorban nem a kommentárszerű magyarázat (hiszen ezt többek között maga a módosítás indokolása is megteszi), sokkal inkább azoknak a folyamatoknak, történéseknek a rövid ismertetése, amelyek magához a módosításhoz vezettek, illetve emellett a módosítás főbb elemeinek rövid bemutatása és az azokhoz kapcsolódó egyes kérdések vizsgálata.

A cikk írásakor maga a teljes jogalkotási folyamat nem tekinthető még lezártnak: a módosításhoz kapcsolódó miniszteri rendeletek közül eddig mindössze egy lépett hatályba, amely az árva művek egyes felhasználásainak engedélyezésére vonatkozó részletes szabályokról rendelkezik.[3] A többi (két új, illetve egy módosító) kapcsolódó rendelet még előkészítési fázisban van, ezért ezekkel kapcsolatosan nyilvános információ még nem áll rendelkezésre.

**2009. szeptember 1. napján lesz tíz éve, hogy hatályba lépett a jelenlegi szerzői jogi törvény. Tíz év egy törvény életében nem hosszú idő (más jogágak – pl. a társasági jog – esetében esetleg igen, az előző szerzői jogi törvény viszont, ha nem is változatlan formában, harminc évet szolgált ki, magában foglalva egy rendszerváltozást), azonban ennyi idő alatt már látszódnak a jogfejlődés és a változtatási igények irányai és az ezeket kiváltó mozgatórugók.**

## Ahonnan jövünk

2009. szeptember 1. napján lesz tíz éve, hogy hatályba lépett a jelenlegi szerzői jogi törvény. Tíz év egy törvény életében nem hosszú idő (más jogágak – pl. a társasági jog – esetében esetleg igen, az előző szerzői jogi törvény viszont, ha nem is változatlan formában, harminc évet szolgált ki, magában foglalva egy rendszerváltozást[4]), azonban ennyi idő alatt már látszódnak a jogfejlődés és a változtatási igények irányai és az ezeket kiváltó mozgatórugók.

Ha pusztán az elmúlt tíz év szerzői jogi módosításait vizsgáljuk, úgy tűnik, minden jelentősebb változás nagy mértékig „külső kényszeren" alapult: az EU-tagság eléréséhez szükséges, illetve a magából a tagságból fakadó jogharmonizációs kötelezettség hívta életre ezeket. Így volt ez pld. az Adatbázis, az ún. INFOSOC, a követő jogról és a jogérvényesítésről szóló irányelvek implementálása esetében is.[5] Ehhez képest átfogó jellegű, ám belső kezdeményezésű módosítás nem történt ez alatt az időszak alatt[6] (ennek okai akár egy külön vizsgálatot is megérdemelnének: akár annak a felettébb valószí-

A szerző az ELTE ÁJK-n végzett szerzői jogász, az Előadóművészi Jogvédő Iroda jogtanácsosa.