Menyhárt Gabriella

# AZ ELEKTRONIKUS ALÁÍRÁS SZABÁLYOZÁSA A ROMÁN JOGRENDSZERBEN

**1.** A beköszöntő „digitális évezred" számos tehnológiai vívmányának meghonosítása és, ezzel egyidőben, az információs társadalom megvalósítása érdekében, a román jogalkotó, az E.U. irányelveinek[1] eleget téve, megalkotta az elektronikus aláírást szabályozó 2001. évi 455. számú törvényt[2], majd 2002-ben a 365. számú elektronikus kereskedelmet szabályozó törvényt[3]. Addig míg az elektronikus szerződéses viszonyok nagyrészt ***BtoB*** (business to business) formában történtek az EDI[4] keretében, nem volt szükség az elektronikus aláírás használatára az elektronikus nyilatkozatok jogi elismerhetősége céljából, mivelhogy a felek zárt láncot alkottak, állandó kapcsolatban voltak és megvolt a kölcsönös bizalom a kereskedelmi ügyletek elektronikus úton történő lebonyolításához. Az Internet elterjedése azonban megváltoztatta a kereskedelmi viszonyokat, ugyanis nyílt hálózaton a szerződéses kapcsolatok ***BtoC*** (business to consumer) formában jelentkeztek, a felek nem ismerik egymást, a kapcsolat nem állandó és hiányzik a kölcsönös bizalom is. A ***BtoC*** kereskedelmi viszonyokban, a ***BtoB*** viszonyoktól eltérően, hiányzik a felek közötti egyensúly, mivelhogy az előbbi (***BtoC***) szerződéses jogviszonyokban a kereskedő egyértelmű előnyben van mind technikai, mind jogi szempontból a fogyasztóval szemben, míg az utóbbi (***BtoB***) esetén mindkét fél értesült a technikai és jogi feltételekről. A ***BtoC*** jogviszonyokban az elektronikus jognyilatkozatok hatályának, vagyis jogi elismerhetőségének problémájára nyújthat jogi megoldást az elektronikus aláírás, mely igazolni képes az aláíró személyének azonosságát az elektronikus iratban szereplő egyénével és az irat integritását.

**2.** Míg a hagyományos, emberi kézzel papírra írt írás és különösen a hagyományos értelemben vett aláírás jogi jelentősége közismert, addig az elektronikus aláírás viszonylag új és, főleg Romániában, kevésbé elterjedt és használt aláírási eszköz.

A hagyományos, tehát az elektronikus kereskedelmet figyelembe még nem vevő szabályozás, a magánokiratok hitelességének[5] megállapítása céljából az emberi kézírást veszi alapul és a kézíráshoz köti a magánokirat bizonyítási erejét. Ennek függvényében, a kézi aláírás bizonyítja,

1 A 2000. évi 31. számú Direktíva, amelyet az Európai Közösségek 2000 évi 178. számú Hivatalos Naplójában hirdettek ki és amely az elektronikus kereskedelmet szabályozza.

2 Kihirdetve a 2001. o7. 31. évi 429. számú Hivatalos Közlönyben.

3 Kihirdetve a 2002. o6. o5. évi 483. számú Hivatalos Közlönyben.

4 ***Electronic Data Interchange*** (Elektronikus Adatcsere), vagyis az elektronikus kereskedelem az Internet elterjedése előtt főleg zártláncú elektronikus hálózatokon folyt, mint amilyen az ***EDI*** is.

5 A magánokiratoktól eltérően, a Ptk. 1171. szakaszának megfelelően, a hiteles iratok kompetens köztisztviselő előtt kötetnek a törvény által előírt formalitások betartásával és ennek következtében a hitelesség és érvényesség vélelmével bírnak, bizonyítás nélkül is. Vagyis valóban azoktól a személyektől ered, akik az iratban megneveztetnek, tehát, nem hamis az irat. Ugyanakkor, ha a hiteles iratot hamisítottnak nyilvánítjákaz iratba foglalt kötelmek és jogok teljesítésének felfüggesztése a Ptk. 1173 szakaszának értelmében a bíróság döntésére van bízva.

hogy a magánokirat aláírója valóban az iratban szereplő egyén. Ez a feltevés abból a tudományos tapasztalatból származik, hogy az ember saját aláírását másvalaki azonos módon nem képes megismételni, vagyis a kézi aláírás egyedi. A másik feltevés az irat integritására vonatkozik, vagyis a magánokirat tartalmának meg nem változtatására az aláírás pillanatától számítva, mely igazolja hogy az irat nem hamisított. A fentebb elhangzottak alapján, magánokirat hitelessége alatt azt értjük hogy az irat nem hamis, vagyis aláírója az iratban megnevezett személy és azt hogy az irat nem hamisított, vagyis az irat tartalma az aláírás pillanatától számítva nem volt megváltoztatva. Következésképpen, hogy bizonyos technikai megoldás, jelen esetben, az elektronikus aláírás, alkalmas-e a kézi aláírás helyettesítésére, eldönthető az alapján, hogy képes-e önmagában, papíralapú aláírás és magánokirat nélkül, a hitelességet[6] biztosítani.

**3**. A 2001. évi 455. számú törvény[7] 4. szakaszának 4. alpontja meghatározza az elektronikus aláírás fogalmát. ***Elektronikus aláírás*** alatt elektronikus irathoz[8] azonosítás céljából kapcsolt vagy ahhoz logikailag hozzárendelt elektronikus adatot értünk. Más szavakkal, az elektronikus aláírás fogalom általános, tehnológia független aláírási eszközökre vonatkozik és magába foglalja mindazokat a módszereket, melyekkel valaki aláírni képes egy elektronikus adatot. Ennek értelmében, elektronikus aláírás az elektronikus levelek, adatok végére írt név, a kézi aláírás képének elektronikus képként szövegekhez csatolása, melyek azonban nem biztonságosak technikai szempontból, vagyis bárki által létrehozhatóak vagy módosíthatóak. A törvény 4. szakaszának 4. alpontja szabályozza a ***fokozott biztonságú elektronikus aláírást***[9], amelynek, a törvény értelmében, a hitelesség biztosítása céljából egyidőben a következő jellemzőkkel kell rendelkeznie: *kizárólag egy aláíró személyéhez kötődjék, az aláíró személyét egyértelműen azonosítsa, úgy kapcsolódjon az elektronikus adatokhoz, hogy az aláírást követő minden utólagos-szándékos vagy véletlen- változás egyértelműen kimutatható legyen és az aláírás ténye utólag le nem tagadható legyen, vagyis kizárólag az aláírást kibocsátó jogos tulajdonos által felügyelt technikai eszközökkel hozzák létre az aláírást*[10]. A törvény és a 2001 évi 1259. számú kormányhatározat[11], mely az elektronikus aláírást szabályozó törvény metodológiai jogi szabályait tartalmazza, szentesítik a ***hitelesítést szolgáltató szerv*** fogalmát és jogi létét és az ezek által kibocsátott ***tanúsítvány*** és ***minősített tanúsítvány12*** fogalmát. A törvény 4. szakaszának 11. alpontja értelmében tanúsítvány alatt elektronikus adathalmazt értünk mely bizonyítja az aláíró személy azonosságát és az elektronikus aláírás és az aláíró személy közötti tulajdonjog viszonyt. Ugyanazon törvény és szakasz 12. alpontja értelmében minősített tanúsítvány alatt olyan tanúsítványt ért, amely a törvény 18. szakaszának feltételeit[13] teljesíti és amely egy olyan hitelesítést szolgáltató szerv bocsájt ki, mely a törvény 20 szakaszának feltételeit teljesíti. Titkos kulcs alatt a kormányhatározat értelmében olyan

6 A hitelesség problémája mellett, elektronikus aláírás esetében, feltevődik az aláírás **titkosításának** kérdése is mivelhogy nyilvános kommunikációs csatornák (például az Internet) használata esetén, felmerülhet a nem jogosult személyek által való használata is.

7 Továbbiakban, *„a törvény”*.

8 Elektronikus irat a 2001. évi 455. számú értelmében olyan elektronikus adathalmazt jelent, melyek között logikai és funkcionális kapcsolatok állnak fenn, melyek betűket, számokat vagy bármilyen más érthető kommunikációs jeleket tartalmaznak és melyek informatikai programok segítségével olvashatóak.

9 Gyakorlati szempontból az egyik legbiztonságosabb a két – nyilvános és titkos – kulccsal operáló digitális aláírás.

10 Elektronikus aláírás és fokozott biztonságú elektronikus aláírás fogalmak közötti különbség jogi szempontból az elektronikus irat bizonyító erejében nyilvánul meg.

11 Kihirdették a 2001. évi 847. számú Hivatalos Közlönyben. Ezt a szabályozást a továbbiakban „kormányhatározat” néven fogjuk említeni.

12 A tanusítvány és a minősített tanusítvány jogi jelentősége hasonló a ***tanúk*** jogi jelentőségével. Értjük alatta azt, hogy a tanúk jelenléte magánokirat megkötésénél arra hivatott, hogy, bizonyos, a törvény által megkövetelt, alaki feltételek nem teljesítése esetén, mely a magánokirat bizonyítási erejének megfosztásával járna – mint például a felek számával megegyező példányszám kérelme – a bizonyítási erőt biztosítsa.

13 A törvény 18. szakasza a minősített tanusítvány kötelező tartalmára, a hitelesítést szolgáltató szerv által az aláírónak kötelező módon biztosított személyes kódra és a tanusítványt azonosító kódok létrehozását szabályozó intézkedésekre vonatkozik. A személyes kódot oly módon kell megalkotni, hogy kizárólag az aláírás tulajdonosának személyét lehessen vele azonosítani.

egyedi digitális kódot értünk, melynek segítségével ugyancsak egyedi elektronikus aláírás hozható létre. Nyilvános kulcs alatt, a kormányhatározat értelmében olyan digitális kódot értünk, mely a titkos kulcs párja és a titkos kulcs által létrehozott aláírás ellenőrzésére használható.

**4.** Az általános fogalmak bemutatása után, azt kell megvizsgáljuk, hogy a kézi aláírás mely jellemzőit képes a minősített elektronikus aláírás fogalomkörbe tartozó digitális aláírás kiváltani. Az a tény, hogy a digitális aláíráson[14] keresztül vizsgáljuk meg, hogy képes-e biztosítani az irat hitelességét, nem kell úgy érteni, hogy csak a digitális aláírás tudja technikailag biztosítani a hiteleséget és csak a digitális aláírás bírhat bizonyítási erővel. Ennek értelmében bármely technikai megoldás, amely az elektronikus aláírás fogalomba tartozik felhasználható, mint bizonyítási eszköz, ám ennek eldöntését a bíróság mérlegeli. A törvény 5. szakasza[15] szentesíti azt a vélelmet mely szerint a fokozott biztonságú aláírást tartalmazó, fel nem függesztett vagy vissza nem vont minősített tanúsítvánnyal ellátott elektronikus irat bizonyító ereje megegyezik a magánokiratokéval. A vélelem összefügg azzal a ténnyel, hogy a két kulcsos digitális aláírás biztosítani tudja az irat hitelességét, vagyis azt, hogy nem hamis és hogy nem hamisított az irat. Mindkét kulcsot a környezet egyes véletlen elemeinek felhasználásával (véletlen számalkotással) hozták létre, így biztosítva az egyediséget. Sőt, a kormányhatározat a 35. szakaszban szabályozza a digitális aláírás titkos kulcsának paramétereit is. A titkos kulcs segítségével a tulajdonos képes csak a rá jellemző elektronikus aláírást létrehozni, illetve adatokat titkosítani[16]. A nyilvános kulcsot – amelyet mint neve is mutatja – széles körben el lehet terjeszteni a rendszerben[17], és segítségével bárki képes a titkos kulcs által létrehozott aláírást ellenőrizni és a titkos kulcs birtokosa számára adatokat titkosítani. Az irat integritásának védelmében olyan (ú.n. Hash-code) algoritmusokat használnak, amely az aláírás és titkosítás után minden utólagos – szándékos vagy véletlen – változást egyértelműen kimutat. Következtetésképpen, a digitális aláírás is, akárcsak a kézi aláírás, képes biztosítani az irat hitelességét.

**5.** A digitális aláírás, sajátos technológiai jellemzőiből fakadóan, számos új, a kézi aláírásra nem vonatkoztatható jogi következményekkel jár. A kézi aláírástól eltérően, mely nem idegeníthető el, nem változtatható meg, a digitális aláírás titkos kulcsa ellopható, elveszthető, sérthető (feltörhető)[18]. Az ebből eredő egyik fontos jogi következmény, hogy az ellopott digitális aláírás használata nem szolgál az illegális használat bizonyítására, – ez a letagadhatatlanságból ered – míg a kézi aláírás esetében az illegális használatot az írásszakértő az esetek nagy részében be tudja bizonyítja. Vagyis a digitális aláírás használata egyértelműen kimutatja és rámutat a kibocsátó személyére is. Következésképpen, az illegális használatot más bizonyítási eszközökkel kell kimutatni.

Másik fontos jogi következmény a minősített tanúsítványok törvény által biztosított visszavonhatósága, amelyet a 23. szakasz szentesít. A 23 szakasz 2. alpontja felsorolja azokat az eseteket amikor a hitelesítést szolgáltató szerv köteles visszavonni a tanúsítványokat. Ez esetek között szerepel a digitális aláírás titkos kulcsának bizalmas jellegének megsértése (vagyis jogtalan személyek birtokába került, lopás vagy elvesztés során). Éppen azért mert a digitális aláírás elveszthető, ellopható, módosítható, a tanúsítványok érvényességi ideje sem haladhatja meg az egy évet.

A törvény legfontosabb jogi következménye az elektronikus iratok és nyilatkozatok jogi hatályának és bizonyítási eszközként való felhaszná-

14 A törvény az elektronikus aláírás és a minősített elektronikus aláírás fogalmakat használja, mely általános fogalom, magába foglalva a digitális aláírást is. A kormányhatározat azonban nagyrészt digitális aláírásra vonatkozó metodológiai normákat ír elő.

15 A törvény 5. szakasza értelmében azon elektronikus iratok melyek fokozott biztonságú elektronikus aláírással vannak ellátva és mely aláírás kibocsátója le nem tiltott vagy érvénytelenített minősített tanusítvánnyal rendelkezik ugyanolyan bizonyító erővel bír mint a magánokiratok.

16 Mivelhogy nyílt csatornás kommunikációs rendszerről van szó, az aláírási funkció mellett, jelentkezik egy másik funkciója is a digitális aláírásnak, a titkosítási funkció. A hitelesség tekintetében azonban a titkosítás kérdése irreleváns.

17 A kormányhatározat 3. szakaszának értelmében a titkos kulcsot, annak ellenére, hogy kulcspárt képez a nyilvános kulccsal, nem lehet kikövetkeztetni, megfejteni a nyilvános kulcsból.

18 Éppen ezért szükséges szigorúan titokban tartani, a fizikai hordozót pedig biztonságos helyen tárolni.

lásának szentesítése. A törvény 5. szakaszának értelmében azon elektronikus iratok amelyek fokozott biztonságú elektronikus aláírást tartalmaznak és az aláírás kibocsátója le nem tiltott vagy érvénytelenített minősített tanúsítvánnyal rendelkezik ugyanolyan bizonyító erővel bír, mint a magánokiratok. A Ptk. 1177 szakaszának értelmében egy aláírással szembesített személy köteles elismerni a magánokiratot vagy az aláírást, mint sajátját vagy letagadni. Ha összevetjük a fentebb említett törvény 5. és a Ptk. 1177 szakaszát, tudván azt is hogy a fokozott biztonságú elektronikus aláírás a 4. szakasz 4. alpontjának értelmében egyértelműen azonosítja az aláíró személyét – a letagadhatatlanság elve szerint- arra a következtetésre jutunk, hogy a törvény 8. szakaszának 1. alpontja[19] az 5. szakaszra nem vonatkozik. Vonatkozhat tehát olyan esetekre, mikor nem fokozott biztonságú elektronikus aláírásról van szó, melyet le nem tiltott vagy érvénytelenített minősített tanúsítvány igazol, hanem bármilyen elektronikus aláírásra mely a 4. szakasz 3. alpontja által leírt meghatározásnak eleget tesz.[20] Vagyis az 5. szakasz egy relatív vélelmet szentesít, olyan értelemben hogy az általa leírt esetben nem szükséges a bizonyítási erő igazolása, vagyis az irat hitelességének igazolása[21]. Bizonyítási eszközként nem csak a fokozott biztonságú elektronikus aláírást lehet felhasználni, hanem bármely más elektronikus iratot és aláírást[22], de ezek esetében bizonyítani kell, ha a mások fél nem ismeri el, az irat hitelességét bármilyen bizonyítási eszközzel.

Mi történik abban az esetben amikor a tanúsítványt letiltották vagy érvénytelen? Ebben az esetben az 5. szakaszban felállított vélelem nem alkalmazható, de ez nem azt jelenti, hogy a bizonyítási erő nem eredhet más körülményből és hogy az iratot nem lehet felhasználni bizonyítási eszközként[23]. Tovább elemezvén az 5. szakaszt arra a következtetésre jutunk, hogy a minősített tanúsítvány feltétel a szakaszban nem helytálló[24], mert a minősített aláírás, a 4. szakasz 4. alpontja értelmében, egymagában képes az aláíró személyét igazolni, ugyanazt amire a minősített tanúsítvány hivatott. Ha figyelembe vesszük a 6. szakasz előírásait is, mely kimondja, hogy az az elektronikus irat, melyhez egy a 4. szakasz 3. alpontja értelmében vett elektronikus aláírást csatoltak és a szembesített személy elismerte, ugyanolyan bizonyítási erővel bír, mint a hiteles iratok és vonatkoztatjuk az 5. szakaszhoz és a letagadhatatlanság elvéhez[25], arra a logikai következtetésre jutunk, hogy az 5. szakasz teljes mértékben fölösleges. Véleményünk szerint, elegendő lenne csak a 6. szakasz előírása, mivelhogy ez magába foglalja az 5. szakaszt is, azért, mert az 5. szakaszban felállított vélelem olyan helyzetre vonatkozik amikor az aláíró nem tudja letagadni az aláírás tényét (ez a minősített elektronikus aláírás letagadhatatlanságából fakad). Vagyis, az 5. szakaszban leírt helyzetben, az elektronikus irat a hiteles irat bizonyító erejével kellene, hogy bírjon.

**6.** Az elektronikus aláírásra vonatkozó törvény elemzése nem kimerítő jellegű. Számos gyakorlati probléma felmerülése várható az elkövetkezendőkben, amelyek talán, idővel, leülepednek és tisztázódnak.

19 Abban az esetben ha az egyik szerződő fél nem ismeri el az elektronikus iratot vagy az elektronikus aláírást, a bíróság minden esetben elrendeli az irat vagy aláírás ellenőrzését szakvéleményezés útján.

20 Elektronikus aláírás alatt elektronikus irathoz azonosítás céljából logikusan elhelyezett elektronikus adatot értünk.

21 A 4. szakasz 4. alpontja a fokozott biztonságú elektronikus aláírást olyan technikai feltételekhez köti, melyek egyértelműen igazolják az irat hitelességét, vagyis a) egyedi kell legyen, b) az aláíró személyét egyértelműen kell igazolja c) kizárólag az aláíró által birtokolt eszközökkel legyen létrehozva d) olyan technikai megoldásokkal legyen felszerelve, melyek bármilyen utólagos tartalom módosítást egyértelműen kimutatnak.

22 A fent említett esetben, elektronikus aláírás fogalom alatt a 4. szakasz 3 alpontja által megadott meghatározást értjük.

23 Hasonló a helyzet, mint mikor a szerződés megkötettik tanúk nélkül, a szerződés érvényes a felek között, de bizonyítása nehézkessé válik, mert a tanú egyik jogi szerepe a szerződés megkötésének és a szerződő felek identitásának igazolása. Kereskedelmi szerződések esetén, ahol a jogviszonyokat az operativitás jellemzi, nem jellemző az írásos formában történő szerződéskötés, vagyis hiányzik az írásos bizonyíték. Éppen ezért hasznos és fontos a tanúk jelenléte, amelyek igazolni tudják, szükség esetén, a felek identitását és a szerződésbe foglalt jogokat és kötelmeket. A Ktk. engedélyezi a tanúkkal való bizonyítást olyan jogviszonyokban is amelyek meghaladják a Ptk.-ban előírt értékhatárt és amely felett a polgári jogvitákban nem lehet a tanúvallomáshoz folyamodni.

24 Lásd, T.G.Savu: **Consacrarea legală a semnăturii electronice**, *Revista de Drept comercial*, 7-8/2002, 226 o.

25 A letagadhatatlanság elve a fokozott biztonságú elektronikus aláírást jellemzi.