A magánszféra és a szerzői jogok védelmének egyes szabályozást igénylő kérdéseiről

GYENGE ANIKÓ, TÉNYI GÉZA
gyengea@im.hu, tenyi@mkab.hu

Kulcsszavak: adatvédelem, információs önrendelkezési jog, személyes adatok felhasználása és védelme, digitális jogkezelés

Az információs társadalom kialakulása számos jelentőséggel bíró szabályozási kérdést vet fel. A digitalizáció és az Internet elterjedésének jelensége a jog számos területén új szabályozási formák kialakítását tette szükségessé, s ezen túlmenően a hagyományos jogi kategóriák újraértelmezését is igényli. A cikk ezen jelenség két példáját, így a névtelenség és álnév használata által biztosított adatvédelem, valamint a digitális jogkezelés egyes, szabályozást igénylő kérdéseit kívánja bemutatni.

Az adatvédelem központi kérdését az információs önrendelkezési jog gyakorlása jelenti, a személyes adatok védelméhez való jog konkrét esetben az adatkezelés szükségességének és arányosságának, egyszóval célszerűségének vizsgálatát követeli meg.[1] Az államnak a mindenütt jelenlevő adatkezelés világában leszűkülnek azon lehetőségei, amelyekkel polgárainak az információs önrendelkezési jog minél markánsabb jogi hátterének megteremtésére irányuló intézményvédelmi kötelezettségét teljesíteni tudja. A jogi szabályozás által nyújtott lehetőségek kimerítése után az információs társadalomban fellépő adatvédelmi problémák megoldási lehetőségeként az úgynevezett „önadatvédelem" jelentkezik.[2]

Ez az önadatvédelem ugyanakkor nem jelentheti azt, hogy az egyes személyek egyéni felelőssége lesz a rendelkezésére álló adatvédelmi eszközök igénybevétele. Sokkal inkább kiegészítő védelmi lehetőséget nyújthat a jogi szabályozás és a technológiai lehetőségek kimerítése után. Ennek egyik legfontosabb szegmense a névtelenség megőrzése, vagy a pszeudonim, azaz az álnéven történő részvétel lehetőségének biztosítása.

Az anonimitás és az álnevek használata nem ismeretlen terület, a mindennapjainkban tömegesen kötött szerződéseink megkötése során névtelenül járunk el, a személyes adatok megadása felesleges, valamint a gazdaság hatékonyságával és a józan ésszel is ellentétes lenne.[3] Ez a lehetőség az Internet világában nem magától értetődő, hiszen önmagában minden cselekvés technikai szükségszerűségként „nyomot" hagy a hálózaton.[4]

Minél jobban eltűnik annak a lehetősége, hogy „nyom nélkül" vehessünk részt az Internet világában, annál inkább megnő az anomimitás jelentősége. Mivel a hálózatokon történő adatfeldolgozás az érintett személy számára ténylegesen szinte egyáltalán nem ellenőrizhető, és ezen adatok törlése a gyakorlatban nehezen kivitelezhető,[5] így döntő szerepet játszik a személyes adatok megelőző védelme.[6]

Ha tehát az Internet világában történő adatkezelés a klasszikus szabályozás keretei között csak nagy nehézségek árán érvényesíthető, úgy a személyes adatok védelmének központi elemét jelentő információs önrendelkezési jog fokozott érvényesítésére van szükség, így az adatvédelemhez való jog részeként meg kell, hogy jelenjen a meghatározott keretek között történő névtelenség, valamint az álnevek használata. Ez a követelmény, illetve lehetőség megjelenik az elektronikus hírközlési adatvédelmi irányelvben is, amely az anonim vagy álnéven szereplő adatok használatának ösztönzésére, azaz ilyen irányú technikai-gazdasági-jogi környezet kialakítására hív fel.[7] Érdemes itt megemlíteni a német szektoriális adatvédelmi szabályozást, amely az előbb említett közösségi irányelv átültetésének eredményeként a névtelenséghez fűződő jog biztosításával kíván az információs önrendelkezési jog követelményének eleget tenni.[8]

Egyes szerzők az ilyen típusú önadatvédelmi megoldásokat gyakorlati jelentőségüket tekintve az állam által biztosított adatvédelmi rezsim elé helyezik, mintegy az információs önrendelkezési jog hozadékaként.[9]

1 *Természetesen az adatvédelem normatív céljai sokkal cizelláltabb követelményrendszert írnak elő, így a az adatvédelem célhoz kötöttségén túl annak szükségességét, az önrendelkezési jog biztosítását, az érintettekkel fennálló kapcsolat lehetséges mellőzését, valamint az érintett jogainak érvényesítését. Lásd: 15/1991. (IV. 13.) AB határozat, ABH 1991.*

2 *Roßnagel, A.: Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger. Zeitschrift für Rechtspolitik 1997/1, p.26.*

3 *Még a bankkártyával történő fizetések nagy részénél is csak a PIN kód használatával azonosítjuk magunkat, az általános üzleti gyakorlat szerint csak meghatározott összeghatár túllépése esetén igénylik a kereskedők a közvetlen személyazonosítást.*

4 *A szolgáltatók egyben kötelesek is a használat „nyomainak" rögzítésére a naplófájlok megőrzéseként.*

5 *Roßnagel, A.–Bizer, J.: Multimedia und Datenschutz. Datenschutz und Datensicherheit, 1996/4, pp.209–217. közölt cikkükben a médiaarchívumokat illetik hasonló jelzőkkel.*

6 *Roßnagel, A.–Scholz, P.: Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung von anonymen und pseudonymen Daten. Multimedia und Recht 2000, p.721.*

7 *Az Európai Parlament és a Tanács 2002/58/EK 2002. július 12-én meghozott irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről. L 201, 2002. július 31., pp.37–47.*
Az irányelv külön is megemlíti az anonimitás elősegítésének példájaként a hívókártyát, vagy a hitelkártyával történő fizetést.

8 *A hírközlési szolgáltatásokhoz kapcsolódó, 2001. december 14. napján kihírdetett törvény 4. § (6) bekezdése*

9 *Hoffmann–Riem, W.: Informationelle Selbstbestimmung in der Informationsgesellschaft. Archiv für öffentliches Recht, 1998/4, p.532.*

A személyes adatok felhasználásától való eltekintés példájaként egyrészt az elektronikus aláírásról szóló törvényt említhetnénk, amely az álnév használatát minden különösebb gond nélkül szabályozza.[10] A névtelenség követelménye ugyanakkor már a hatályos magyar adatvédelmi szabályozásnak is része, amikor is az adatkezelő az adatkezelés célszerűségéhez mérten nemcsak az adatkezelés megszüntetésével teljesítheti törvényi kötelezettségeit, hanem az adatok anonimitásának (végleges) megteremtésével is. Ekkor megfosztja az adatokat az érintett személlyel való kapcsolatától és ha ennek helyreállítása sem lehetséges, úgy az adatkezelő tevékenysége már nem tartozik az adatvédelmi törvény hatálya alá, ami egyben gazdaságilag is előnyös megoldás a hírközlési piac szereplői, és az adatkezelők számára is.[11]

Az adatkezelő ezen kötelezettségét egyúttal az érintett személynek a névtelenséghez, vagy pszeudonimitáshoz való joga kell, hogy kiegészítse. Ezt a jogot természetesen korlátozni kell a harmadik személyek érdekeinek megóvása, valamint a közérdek érvényesítése szempontjából. A közérdekből történő azonosítási kötelezettségeket természetesen egy ilyen lehetőség nem szüntetheti meg. Ahhoz, hogy az önadatvédelem lehetőségeiként az Interneten a névtelen és álnéven történő részvétel elterjedjen, önmagában a technikai megoldások, így az identitás-menedzsment-biztosító szoftverek elterjedése nem elegendő. Jelen esetben a közszféra aktív szerepvállalására van szükség több síkon is. Így az egyéni és több oldalról történő önadatvédelem jogi kereteinek biztosításán túl szükséges az esetleges panaszok és jogsérelmek esetére szóló „leleplezési-felderítési eljárás" szabályozása, a felhasználók széleskörű és részletes tájékoztatása, valamint az egységes technológiai megoldások érdekében a köz- és magánszféra fejlesztéseinek összehangolása.

A digitalizáció és az Internet megjelenése, az informatika térhódítása a szerzői jogi eszköztár módosulását is magával hozza. A legújabban fellángolt vita során a Digital Rights Management System (digitális jogkezelési rendszer – DRMS) megjelenésével kapcsolatban több, a jogosításra vonatkozó kérdés merül fel.

Egy teljes DRMS[12] a mű azonosítása mellett képes a felhasználás biztosítására, a jogsértő felhasználások bizonyos keretek között történő megakadályozására, sőt, a felhasználásért járó ellenérték elszámolására is. Ez a multifunkciós jelleg lehetővé teszi, hogy a DRMS-t a szerzői jogi iparban érintett valamennyi szereplő alkalmazza, a saját igényeihez, illetve feladataihoz adaptálva azt. Ebből következik, hogy a DRMS a szerzői jogi iparban új üzleti modellek kialakulását teheti lehetővé, illetve egy teljes elektronikus kereskedelmi láncolat műszaki hátteréül szolgáló eszközként is definiálható. Ennek az eszköznek azonban nem minden eleme tartozik a szerzői jog alá, hiszen a mű továbbítását végző szolgáltató felelősségét, az elektronikusan kötött szerződés okirati hitelességét, illetve a jogsértésért érvényesíthető szankciók rendszerét egyéb jogszabályokban találjuk meg.

A két legfontosabb kérdés, amely felmerül a DRMS és a szerzői jog viszonyában: az engedélyezési rendszer esetleges átalakulásának módja, valamint az engedélyköteles és a szabad felhasználások viszonyának megváltozása a technikai eszközök fejlődésének hatására.

Tekintettel arra, hogy a szerzői felhasználási szerződések érvényességének feltétele a jelenlegi szabályozás alapján az írásbeliség, ennek azonban a digitális világban csak a fokozott biztonságú elektronikus aláírással ellátott dokumentumok felelnek meg,[13] felmerül a kérdés: nem kellene-e oldani az írásbeliség béklyóján, hogy segítsük a DRMS-sel biztosított kommunikáció terjedését és vele a biztonságos tartalomátvitelt a hálózatokon. Addig ugyanis, amíg az írásbeliség és a fokozott biztonságú elektronikus aláírás érvényességi feltételek, addig ez az üzleti modell csak igen lassan tud terjedni, hiszen a felhasználók többsége nem rendelkezik ezzel az aláírástípussal. Mindenesetre a rendszer biztonsága, pótolhatja az írásbeliségben rejlő garanciákat is.

További probléma, hogy a művek DRMS-mel védett példányai legtöbb esetben nem teszik lehetővé, hogy az arra jogosult az analóg szabad felhasználásokat (magáncélú másolás, archiválás) érvényesítse, azaz hozzájusson a művek példányaihoz. A szerzői jogi törvénybe már beépített, a nemzetközi és a közösségi szabályozásban is elismert szabályozói technika afelé mutat, hogy a szabad felhasználások szabályozásának struktúrája fel fog lazulni.[14]

Az analóg világban a szabad felhasználást (legalábbis a kontinentális szabályozásban) a törvény konstituálja és határozza meg feltételeit. Ehhez a digitális világban a szerző aktívabb részvétele járul: amennyiben hatásos műszaki intézkedés (adott esetben DRMS) védi a művet, akkor egyes szabad felhasználások kedvezményezettje követelheti, hogy a szerző biztosítson számára hozzáférést. Elképzelhető az, hogy ez a modell válik általánossá az ily módon védett művek esetében: a szabad felhasználás is egyfajta, a szerző jogi és technikai engedélyétől függő cselekménnyé válik. Ebben a konstrukcióban azonban mindenképp biztosítani kell, hogy az engedély ne legyen megtagadható, ha a szabad felhasználás kedvezményezettje igazolja jogosultságát.

10 az elektronikus aláírásról szóló 2001. évi XXXV. törvény, 4. sz. melléklet f) pontja

11 Az adatvédelem írott malaszt marad, ha a hatékony, kockázatarányos és közérthetően szabályozott védelem nyújtása mellett nem elég vonzó az adatkezelést végző gazdasági társaságok nagy része számára, akik a jogszabályok betartását marketingelőnnyé változtathatják.

12 Az egyes DRMS-típusok részletes elemzését lásd: Gyenge A.: A digitális jogkezelés és a szerzői jog, Infokommunikáció és Jog 2004/2, p.50.

13 2001. évi XXXI. törvény az elektronikus aláírásról 2. § 15. pont; 1952. évi III. törvény a Polgári perrendtartásról 197. §

14 Szjt. 95/A. § – (1) A reprográfiával történő magáncélú másolás, továbbá a 34. § (2) bekezdésében, a 35. § (4) és (7) bekezdésében és a 41. §-ban szabályozott szabad felhasználási esetek tekintetében a szabad felhasználás kedvezményezettje követelheti, hogy a jogosult a műszaki intézkedések megkerülésével szemben a 95. § alapján biztosított védelem ellenére tegye lehetővé számára a szabad felhasználást, feltéve, hogy a szabad felhasználás kedvezményezettje a műhöz jogszerűen férhet hozzá. Ha a felek között nem jön létre megállapodás a szabad felhasználás lehetővé tételének feltételeiről, a felek bármelyike kezdeményezheti a 105/A. § alapján történő eljárást.
(2) Az (1) bekezdés nem alkalmazható, ha a művet szerződés alapján teszik úgy a nyilvánosság számára hozzáférhetővé, hogy a nyilvánosság tagjai a hozzáférés helyét és idejét egyénileg választhassák meg.