JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Az új magyar adatvédelmi törvény elé

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

(Megjelent: Jogtudományi Közlöny, 2003/12. 393-408. o.)

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény megalkotása egy évtizede óriási jelentőségű volt Magyarországon: az adatvédelmi jog – nem utolsósorban a törvény alapján működő, annak rendelkezéseinek megtartásán őrködő adatvédelmi biztosok tevékenysége nyomán – széles körben ismertté, a gyakorlatban érvényesülő joganyaggá vált. A törvény jogharmonizációs célú módosítása régen napirenden van: 2001-ben megszületett az első tervezet is. Az alábbiakban a hatályos adatvédelmi törvény, a 2001-es tervezet, az EU irányelv, és egy tagállam törvényének elemzésével a hatályos törvénnyel kapcsolatos egyes jogalkalmazási problémákra, ill. egyes új, az európai adatvédelmi jogban megjelent intézményekre kívánjuk felhívni a jogalkotó figyelmét[1].

Előzetesen megjegyezzük: csalódást okozott, hogy a 2001-ben megfogalmazott tervezet az EU adatvédelmi irányelvének implementálásán túl nem volt figyelemmel az adatvédelem új fejleményeire, s az irányelv rendelkezéseinek – sokszor szószerinti – fordításán túl nem mutatott arra, hogy a jogalkotó egyáltalán megvizsgálta volna az adatvédelmi szabályozás területén az EU tagállamaiban megjelent új intézményeinek adoptálásának lehetőségét. A tervezetből ezen túl kimarad számos, a hatályos törvény alkalmazói számára nyilvánvaló jogalkalmazási probléma megoldása. A 2001. évi tervezet álláspontunk szerint az információs önrendelkezési jog számos ponton történő áttörése, az egyén személyes adataival való rendelkezési jogának a jelenlegi helyzethez képest – akár gazdasági érdekekre tekintettel történő – jelentős korlátozása mellett nem tartalmazott olyan megoldásokat, amelyek akár a szankciórendszer reformjával, akár más módon a védelmi szint csökkentését korrigálták volna[2].

---

1 2002 végén és 2003-ban újabb tervezeteket bocsátott közigazgatási egyeztetésre az Igazságügyi Minisztérium. A korábbi tervezet a jelen tanulmányban elemzettekhez hasonlóan implementálta volna az EU adatvédelmi irányelvét. A 2003. februári tervezet bevezetője szerint azonban „a beérkezett észrevételek terjedelme alapján azonban meg kellett állapítanunk, hogy azok egyeztetése, egy teljesen új törvényi szabályozás országgyűlési tárgyalásra alkalmas szövegének kidolgozása olyan hosszabb időt és nagy munkát igénylő feladat, amit megfelelő módon nem lehet elvégezni az uniós jogharmonizációs kötelezettség teljesítéséhez rendelkezésünkre álló határidőn belül". Új törvény elfogadása helyett az IM olyan megoldást dolgozott ki, amely a hatályos 1992. évi LXIII. tv. rendelkezéseit módosítja, csupán a jogharmonizációhoz szükséges terjedelemben. Tanulmányunk gondolatmenete szempontjából érdekes, hogy a tervezett módosítás nem „relativizálja" az információs önrendelkezési jogot, hanem fenntartja a védelmi szintet, ám álláspontunk szerint aggályos módon. Tézisünk szerint ugyanis a megfelelően elvégzett EU-harmonizáció *szükségeszerűen* járna az adatvédelmi szint csökkenésével, amelyet a szankciórendszer átalakításával kell kiküszöbölni. A várhatóan elfogadásra kerülő tervezet a védelmi szinten nem változtat (ezzel tézisünk szerint nem ülteti át teljeskörűen a magyar jogba az irányelv rendelkezéseit), ám a szankciórendszert sem alakítja át megfelelően, ezen túl az Avtv. számos, tanulmányunkban elemzett hibáját elmulasztja kiküszöbölni. A szöveg lezárása óta az adatvédelmi jog szankciórendszerét tovább károsította 2003. március 1-ével hatályba lépett módosítása, amelynek nyomán csak „jelentős érdeksérelem" esetében valósul meg a jogosulatlan adatkezelés helyébe lépett visszaélés személyes adattal elnevezésű tényállás. E tényállás alkalmazása oda vezetett, hogy a nyomozó hatóság máris legalább egy, az adatvédelmi jogot súlyosan sértő, és álláspontunk szerint a társadalomra veszélyes cselekmény kapcsán szüntette meg a nyomozást (az ún. OEP megfigyelési ügyben). A törvény elfogadása után szándékunk szerint külön tanulmányban elemezzük majd a módosítás következményeit, s igyekszünk alátámasztani tézisünket.

2 A szakmai vita sajnos e kérdések helyett olyan jelentéktelen kodifikáció-technikai kérdésekre összpontosult, hogy

Jelen cikk írása idején újabb törvénytervezet áll közigazgatási egyeztetés alatt[3]. Reméljük, tanulmányunkkal még hozzájárulhatunk az új törvény sikeréhez.

Az alábbiakban az egyes rendelkezések ismertetése során összehasonlítjuk a hatályos magyar jog és a visszavont tervezet szabályozását az EU adatvédelmi irányelvének tervezetével, valamint az 1998-ban elfogadott brit adatvédelmi törvény adott kérdést szabályozó rendelkezésével. Az EU irányelv szabályozásának ismertetése a jogharmonizációs kötelezettség miatt indokolt, a brit törvény pedig azért érdekes, mert az az EU irányelv implemetálásaként született tagállami jogszabály – ráadásul, mint arról később részletesen szólunk, elfogadásának körülményei miatt az implementálandó szabályok „minimumaként" is vizsgálható.

A magyar adatvédelmi jog fejlődésének tendenciái: EU-harmonizáció, az információs önrendelkezési jog relativizálása, korlátozás üzleti érdekek alapján

Az Alkotmánybíróság 15/1991 (IV.13.) sz. határozatát vezérfonalként követő jogalkotó 1992-ban olyan adatvédelmi törvényt fogalmazott, amely rendkívül szigorú követelményeket támasztott az adatkezelővel szemben, Európában szokatlanul radikális megoldással szerzett érvényt az információs önrendelkezési jognak. Ebből a szempontból a törvény legjelentősebb rendelkezése az, amely az érintett (adatalany) hozzájárulásához vagy törvényben (törvény felhatalmazása alapján kiadott önkormányzati rendeletben) foglalt felhatalmazáshoz köti az adatkezelést. Vagyis az önrendelkezési jogot (amelyet az érintett valamely adatkezeléshez történő hozzájárulása fejez ki) csak olyan esetekben lehet korlátozni, amikor a korlátozást széleskörű – a jogforrási hierarchia csúcsán álló jogi normában kifejezett – társadalmi konszenzus indokoltnak (és az esetleges alkotmánybírósági normakontroll esetén a testület alkotmányosnak) fogadja el. A törvény alapján – bár csak 1995-ben - megválasztott adatvédelmi biztos a következő években szilárdan érvényt is szerzett ennek az előírásnak.

Ilyen környezetben olyan érvek, mint egyes cégek költséghatékony működése, bizonyos társadalmi költségek csökkentése (pl. az ún. hitelinformációs rendszerek kapcsán) – a biztos részéről nem is kerülhettek elfogadásra: az adatkezelésnek csak abban az esetben lehetett helye, ha a mögöttes indokot a törvényhozó is elfogadta, s a kérdést valamely szektorális törvényben rendezte. Ha ez nem történt meg, akár egész üzletágak magyarországi működése kerülhetett veszélybe az adatvédelmi jog miatt. Érdekes ebből a szempontból áttekinteni három olyan gazdasági tevékenység magyarországi jogi kereteit, amelyek esetében ezt a jogi keretet döntő – az üzleti sikert meghatározó – mértékben az adatvédelmi jog jelenti. E három terület a direkt-marketing üzletág, a hitelreferencia-szolgáltatás, valamint az ún. követeléskezelő tevékenység.

Ami a direktmarketing-szakmát illeti, az a hatályos adatvédelmi törvény 1993. május 1-i hatálybalépését követően rendkívül hátrányos jogi környezetbe került. Nem volt ugyanis a közvetlen üzletszerzést szabályozó törvény Magyarországon, vagyis az Avtv. fent idézett rendelkezései szerint e társaságok is csak az érintett hozzájárulása esetében küldhettek volna üzenetet a címzettek számára (hiszen az adatok felvétele, tárolása, amely a címlista összeállításához és felhasználásához szükséges, az Avtv. szerint adatkezelésnek minősül). A potenciális ügyfelek hozzájárulása csak azok előzetes megkeresése esetében

szükséges-e a személyes adatok védelmének és a közérdekű adatok nyilvánosságának külön törvényben történő szabályozása, vagy az a továbbiakban is egy törvénnyel történjen.

3 A jogharmonizációs programról és a program végrehajtásával összefüggő feladatokról 2099/2002. (III. 29.) Korm. határozat szerint az új törvény 2002. II. félévében kellett volna megalkotni.

lett volna kikérhető, amely azonban jogszerűtlen adatkezelést feltételezett volna. A helyzetet a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. tv. (a továbbiakban: direktmarketing-törvény) oldotta fel. Ez a törvény meghatározott adatgyűjtéseket lehetővé tesz a direktmarketing-cégek számára, bizonyos kötelezettségek megfogalmazása mellett. A felhatalmazás igen széleskörű: a közvetlen üzletszerző szerv kapcsolatfelvétel céljából felhasználhatja annak a személynek az adatait, akivel korábban kapcsolatban állt, gyűjthet ilyen adatokat a jogszerűen nyilvánosságra hozatal céljából készített, és nyilvánosságra hozott adatállományból, ha az érintettet figyelmeztették az eredetitől eltérő célra történő adatfelhasználás lehetőségére, vehet át adatot más, ugyanazon tevékenységet végző személytől vagy szervtől, ill. igényelhető adat direktmarketing-tevékenység céljára a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló törvény hatálya alá tartozó nyilvántartásból is; újabban pedig a közúti közlekedési nyilvántartásról szóló 1999. évi LXXXIV. törvény szerint pl. e nyilvántartásból is igényelhető adat közvetlen üzletszerzés céljára[4].

A direktmarketing-törvény tehát az ott meghatározott esetekben az érintett hozzájárulása nélkül hatalmazza fel a hatálya alá tartozó szervezeteket személyes adatok kezelésére. Az Alkotmánybíróság már hivatkozott 15/1991. (IV. 13.) sz. döntése szerint „az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel az Alkotmány 8. §-ában megkövetelt feltételeknek”[5] – vagyis mindenekelőtt nem korlátozza az alapvető jog lényeges tartalmát. Az Alkotmánybíróság állandó gyakorlata szerint az ilyen – tehát a lényeges tartamot nem érintő – korlátozás is csak akkor jogszerű, ha elkerülhetetlenül szükséges és a korlátozás céljára tekintettel arányos. Ezt a tesztet az AB számos határozatában kifejtette és alkalmazta, az információs önrendelkezési joggal kapcsolatban például a 29/1994. (V. 20.) AB határozatban. Álláspontunk szerint lehetséges, hogy a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. tv. ill. a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. tv. azon rendelkezései, amelyek nem az érintett előzetes hozzájárulásával, csak tiltakozási jogának biztosítása mellett (opt-out rendszerben) tesznek lehetővé egyes direktmarketing-célú adatkezeléseket, nem állnának ki egy alkotmánybírósági próbát, hiszen üzleti érdekből korlátozzák az információs önrendelkezési jogot. (Megjegyzendő, hogy a jogalkotó egyik törvény miniszteri indokolásában sem érvel a szabályozás alkotmányossága mellett, ill. e kérdésre egyáltalán nem tér ki.) A direktmarketing-törvény tehát az információs önrendelkezési jog korábbi felfogásához képest egyfajta elmozdulást jelent a hazai jogban, megjelenik az első olyan jogszabály, amely – legyen bár alkotmányos vagy sem – az üzleti érdekhez méri az információs önrendelkezési jog korlátozását, s a mérlegelés után, bizonyos garanciák mellett lehetővé tesz meghatározott üzleti célú adatkezeléseket.

A hitelreferencia-szolgáltatás szintén egy olyan üzletág, amelynek sikerét, lehetőségét alapvetően befolyásolja az adatvédelmi jog. A hitelreferencia-szolgáltatás fogalmának meghatározásához idézzük a törvényi definíciót: a hitelintézetekről és pénzügyi vállalkozásokról szóló 1996. évi CXII. tv. (Hpt.) 2. számú melléklet I. rész 4. pontja szerint „hitelreferencia-szolgáltatások: bankinformáció díjazás ellenében történő – a banktitkot nem sértő – nyújtása”.

1998. január 1-ével lépett hatályba a Hpt. azon módosítása, amelynek alapján - a törvény 54. § (1) bek. c) pontjában ill. az 54. § (2)-(7) bekezdéseiben foglalt rendelkezései szerint - mód van arra, hogy a pénzügyi intézmények és a befektetési társaságok az „általuk működtetett központi hitelinformációs rendszernek” (54. § (1) bek. c)) meghatározott adatokat adjanak át a természetes személy hiteladósokról, amennyiben ezek szerződésben vállalt kötelezettségeiknek kilencven napot meghaladóan, összegszerűségében pedig a minimálbért meghaladóan nem tesznek eleget (54. § (3) bek.). A magyar központi hitelinformációs rendszer tehát valójában adósnyilvántartás: pozitív, a jó adósokra vonatkozó információkat nem tartalmaz. A rendszer elnevezése Bankközi Adós- és Hitelinformációs Rendszer (BAR), s azt egy a hazai hitelintézetek által alapított részvénytársaság

4 Lásd az idézett törvény 21. §-át.
5 15/1991. (IV. 13.) AB. hat.

üzemelteti.

A központi hitelinformációs rendszerek mellett azonban "üzleti alapon működő hitelinformációs rendszerek" is feltűntek a 90-es évek végén[6]. E cégek a Hpt. 51. § (1) bekezdése alapján kívánták igazolni az adatszolgáltatók és a rendszer közötti adatszolgáltatást; e törvényhely szerint banktitok kiadható harmadik személynek, ha a pénzügyi intézmény ügyfele, annak törvényes képviselője a rá vonatkozó kiszolgáltatható banktitokkört pontosan megjelölve közokiratba vagy teljes bizonyító erejű magánokiratba foglaltan kéri, vagy erre felhatalmazást ad. Az adatalany ezekben az esetekben a hitel- vagy hiteljellegű szerződésben adná meg hozzájárulását. Az ügyben az adatvédelmi biztos által 1998. augusztusában írt levélre az ÁPTF (a PSZÁF jogelődje) akkori elnöke a felügyelet álláspontjáról azt a tájékoztatást adta, hogy „csupán egy központi hitelinformációs rendszer működhet állami elismeréssel, de annak nincs akadálya, hogy a hitelintézetek hitelezési kockázatuk csökkentése érdekében üzleti alapon más hitelinformációs rendszert is kiépíthessenek".

Az adatvédelmi biztos ezt követően levélben fordult a pénzügyminiszterhez. Levelében kifejtette, hogy a központi hitelinformációs rendszer hiteladat-szolgáltatóitól eltérően a többi rendszerhez kapcsolódó adatszolgáltatókat nem kötik a Hpt. 54. §-ának (3) bekezdésének rendelkezései, amelyek a polgárok személyes adatokhoz fűződő alkotmányos jogát érő korlátozás arányosságát biztosítják azzal, hogy csak meghatározott súlyú szerződésszegés esetén teszik lehetővé a hiteladat-szolgáltató számára, hogy a természetes személy hiteladós adatait a rendszer számára továbbítsa. Az e rendszerekhez csatlakozó társaságok az általuk használt általános szerződési feltételekben az adattovábbítás feltételeit szabadon határozhatják meg. Így a Hpt 54. §-a által meghatározott korlátok funkciójukat vesztették (hatásuk annyi, hogy a központi hitelinformációs rendszer versenyhátrányba kerül általuk), s adatvédelmi szempontból igen veszélyes helyzet állt elő.

Az adatvédelmi biztos a Hpt. olyan módosítását ajánlotta a miniszter figyelmébe, amely a törvény 54. § (3) bekezdésében foglalt korlátozásokat valamennyi hitelinformációs rendszerre kiterjesztené, ám pozitív választ javaslatára nem kapott[7].

A közelmúltban olyan hírek láttak napvilágot, amelyek szerint a központi hitelinformációs rendszer pozitív – vagyis a „jó adósok" hiteladatait is tartalmazó – rendszerré történő alakítását kezdeményezte a Magyar Bankszövetség[8]. Bár a pozitív listás hitelnyilvántartó gondolata a Hpt. 2002-es módosítása során végül nem valósult meg, a hitelinformációs rendszerek esetében is megfigyelhető, hogy az információs önrendelkezési jogot a jogalkotó bizonyos egyéb (akár a hitelezők üzleti, akár a biztonságosabb hitelkihelyezés előnyeihez társítható össztársadalmi) érdekekre tekintettel egyre jobban korlátozza.

Harmadik példánk a követeléskezelő üzletággal kapcsolatos. A követeléskezelő cégek nagy tömegű, ám viszonylag kis mennyiségű követelésnek a hitelező helyetti beszedésével foglalkoznak. Az adatvédelmi biztos által 2000. június 19-én kiadott „Adósság- és követelésbehajtással foglalkozó gazdasági társaságok személyes adatok kezelésének gyakorlatával kapcsolatos adatvédelmi biztosi ajánlás" szerint magánszemély ügyfelek adatait az adatkezelő követeléskezeléssel foglalkozó társaságoknak csak az érintettek hozzájárulásával továbbíthatja.

A szóban forgó ügyben a követeléskezelő társaságoknak az adatkezelőként szereplő távközlési cég mint adatfeldolgozónak továbbította a személyes adatokat, s a követeléskezelők e cég nevében és javára eljárva voltak kötelesek a behajtást és az attól elválaszthatatlan adatkezelési műveleteket végezni. A követeléskezelő cég tevékenysége abban állott, hogy az ügyféllel telefonos kapcsolatot létesített, ill. ha

6 Lásd pl. Tevan Imre: Adóshivatal, HVG 1998. július 25

7 Az adatvédelmi biztos levelének szövegét lásd: Az adatvédelmi biztos beszámolója 1998, Adatvédelmi Biztos Irodája, Budapest, 1999, 286. o.

8 Lásd: Végre indulhat a hitelnyilvántartó? Magyar Hírlap, 2002. október 13.

ez nem sikerült, akkor legfeljebb két alkalommal tértivevényes levélben kereste meg őt. A követeléskezelő a megbízó nevében részletfizetési lehetőséget ajánlhatott fel. Az adatvédelmi biztosi ajánlás szerint „az adósságbehajtó társaságok nem tekinthetők adatfeldolgozónak, mivel a birtokukba került személyes adatokkal nem adatkezelési végrehajtási technikai műveleteket hajtanak végre, hanem azokat felhasználják és azokra támaszkodva a szerződés keretei között döntéseket hoznak, a polgárral szerződésben álló gazdasági társaság tevékenységébe tartozó feladatot látnak el. Az adatkezelő nem adhat át rendelkezési-döntési jogot az adatok felett." Ez az értelmezés – amelyre lentebb, az adatfeldolgozás fogalmának tárgyalásakor még visszatérünk – a hatályos törvény fogalomrendszerének gyengéire mutat rá, ám egyben annak is példája, hogy a hatályos törvény szerint még jogos érdek fennállta sem igazolhat adatkezelést. (A három üzletág különböző helyzete pedig megmutatja a szektorális szabályozás egyik súlyos veszélyét: azt, hogy a szektorális szabályozás által meghatározott feltételrendszer alakításában nem a tevékenység valós veszélye, az azzal kapcsolatos össztársadalmi érdek játszik szerepet, hanem az, hogy az adott üzletág milyen erős lobbitevékenységre képes).

A fenti három példa azt mutatja, hogy ha vannak is még olyan gazdasági szereplők, amelyek tevékenységét az adatvédelmi jog hátráltatja, az utóbbi évtizedben az információs önrendelkezési jog mégis „relativizálódott" (lásd a direktmarketing-cégek széleskörű adatkezelési felhatalmazását). Mint az alábbiakban bemutatjuk, a jogharmonizációs folyamat tovább erősíti majd ezt a tendenciát[9], hiszen az EU adatvédelmi irányelve, ill. az annak alapján született 2001-es magyar törvénytervezet üzleti érdekből is lehetővé tesz meghatározott adatkezeléseket. A folyamat álláspontunk szerint nem káros, hiszen összetettebb, a valós társadalmi viszonyokat jobban tükröző szabályozás jön létre a korábbi, sok szempontból életidegen, ezért betarthatatlan szabályozással szemben. Álláspontunk szerint azonban e tendencia egy fontos követelményt állít a jogalkotó elé. Ha a szabályozás komplex, tekintettel van az adakezelők egyes – akár üzleti – érdekeire, akkor a végrehajthatóság, a kikényszeríthetőség legyen követelmény. A korábbiakhoz képest olyan mechanizmust kell teremteni, amelyben az adatvédelmi jog követelményeire nem csak abban az esetben ébred rá az adatkezelő, ha ellene azok megsértése miatt esetleg már büntetőeljárás folyik; biztosítani kell az adatvédelmi joganyag folyamatos érvényesülését. Álláspontunk szerint ennek eszközei lehetnek az önkéntes magatartáskódexek, a legjobb gyakorlatok meghatározása és cseréje, az adatvédelmi audit intézményének meghonosítása, és esetleg az adatvédelmi szabványosítás. A 2001-es törvénytervezet csalódást kelt, hiszen az EU-irányelv implementálásán (döntően az információs önrendelkezési jognak a korábbiakhoz képest erősebb korlátozásán) túl nem tartalmaz új megoldásokat, amelyek a megmaradó védelmi szint valós érvényesülését segítenék elő.

A hatályos magyar adatvédelmi törvény, a 2001-es tervezet, az EU adatvédelmi irányelve és a brit törvény elemzése

A fent idézett AB határozat szellemében született meg a ma is hatályos magyar törvény, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. tv. A törvény először meghatározza a jogszerű adatkezelés főbb feltételeit (célhozkötöttség elve[10], szükségesség elve[11], adatok kezelésére vonatkozó követelmények[12], az adatalany számára a tájékoztatás, helyesbítés és törlés jogának biztosítása[13], adatbiztonsági követelmények[14]). A törvény központi rendelkezése, hogy személyes adat csak az érintett hozzájárulása vagy törvényi – annak felhatalmazása esetén, az ott meghatározott körben önkormányzati rendeleti – felhatalmazás esetén kezelhető[15]; az átlátható adatkezelés biztosítása

9 Ezzel a megállapítással kapcsolatban lásd az 1. jegyzetben írtakat.
10 Avtv. 5. § (1) bek.
11 Avtv. 5. § (2) bek.
12 Pl. Avtv. 7. §
13 Avtv. 11., 12. és 13. §§
14 Avtv. 10. §
15 E – Reidenberg és Schwartz által az átláthatóság biztosítása körében tárgyalt – követelmény talán a hazai adatvédelmi jog legfontosabb rendelkezése : a 3. § (1) bekezdésben jelenik meg az információs önrendelkezési jog. *Kizárólag* az érintett hozzájárulása vagy a törvényben kifejeződő közmegegyezés esetén van lehetőség személyes adat kezelésére – más érdek

érdekében a törvény létrehozza az adatvédelmi biztos által vezetett Adatvédelmi Nyilvántartást[16]. A törvény ismeri a különleges adat fogalmát, s az ilyen körbe tartozó adatok kezelésével szemben szigorúbb követelményeket határoz meg, mint általában. Végül a törvény szabályozza az adatvédelmi joganyag érvényesülése felett őrködő intézményként az adatvédelmi biztost.

A hatályos magyar – és európai – adatvédelmi jog egy olyan korból maradt ránk, amelyben kevés számú adatkezelő által működtetett nagy – elsősorban állami kezelésben lévő – adatbázis transzparenciáját kellett biztosítani az adatkezelést szabályozó jogi rendelkezésekkel, valamint az adalanyok számára biztosított jogokkal. Megjegyzendő, hogy álláspontunk szerint a magyar Avtv. – bár úttörő szerepe nem vitatható, tekintettel arra is, hogy elfogadása idején Európában egyedüliként együtt szabályozta a személyes adatok védelmét a közérdekű adatok nyilvánosságával (az információszabadsággal) – nem csak az információs társadalom fogalmával jellemezhető folyamat nyomán vált anakronisztikussá, hanem már meghozatalakor sem volt rá jellemző a megfelelő dogmatikai kidolgozottság, s a helyzet a szöveg egyes módosításaival csak romlott.

Az alábbiakban elemezzük a hatályos magyar adatvédelmi törvény (a továbbiakban: Avtv.), a 2001-ben közigazgatási egyeztetésre bocsátott, majd visszavont tervezet (a továbbiakban: Tervezet), az EU adatvédelmi irányelve (a továbbiakban: Irányelv) és az 1998-as brit adatvédelmi törvény rendelkezéseit. Az elemzés célja, hogy rámutassunk az Avtv. olyan pontjaira, amelyeket a jogharmonizáció során módosítani kell, ill. megvilágítsuk fogalomrendszerének egyes következetlenségeit, a jogalkalmazást nehezítő bizonytalan tartalmú rendelkezéseket. Az Avtv. megszületésének körülményeit fentebb már részletesen ismertettük: az az információs önrendelkezési jog német eredetű koncepcióján alapul, amely koncepció Magyarországon az Alkotmánybíróság határozataiban jelent meg, és alapjává vált az 1992-ben elfogadott adatvédelmi törvénynek.

Az Európai Unióban sorra elfogadott adatvédelmi törvények felvetették annak a veszélyét, hogy az egyes tagállamok által megállapított eltérő szabályok akadályozzák majd a személyes adatok szabad áramlását az uniós tagállamok között, így veszélyeztetve az egységes belső piac működését is. Ezért született meg az Európai Parlament és a Tanács 95/46/EC számú irányelve az egyénnek a személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról[17]. Az Irányelv és a két állam adatvédelmi joga közötti viszonyra az jellemző, hogy a nem tagállam Magyarország adatvédelmi joga általában többletkövetelményeket ír elő az EU-irányelvhez képest, addig az 1998-as brit adatvédelmi törvény előkészítése során kifejezetten szempont volt, hogy az Egyesült Királyság csak olyan mértékben implementálja az irányelv rendelkezéseit, amennyire feltétlenül szükséges ahhoz, hogy eleget tegyen a közösségi jog által előírt kötelezettségeknek[18].

Alapfogalmak

Személyes adat

Az Avtv. szerint személyes adat a meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható.

A magyar törvény által használt definíció lényeges elemei:

– pl. az adatkezelőé – az Irányelv előírásaival szemben nem lehet az adatkezelés jogalapja.

16 Avtv. 28-30 §§

17 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data

18 Idézi Rosemary Jay-Angus Hamilton : Data Protection Law and Practice, Sweet and Maxwell, London, 1998. 1-18

„meghatározott" természetes személy

Sem az adatvédelmi törvény, sem annak miniszteri indokolása nem ad iránymutatást arra, vajon mely természetes személy tekinthető „meghatározott"-nak. A „meghatározott" fogalom jelentését az adatvédelmi biztosi gyakorlat sem bontotta ki. Az Európa Tanács az egyének védelméről a személyes adatok gépi feldolgozása során szóló egyezménye (kihirdette az 1998. évi VI. törvény) – amelyre az Avtv. miniszteri indokolása mint „nemzetközi mércére" hivatkozik – szerint „személyes adat: bármely információ, amely egy azonosított vagy azonosítható egyénre vonatkozik". Jay és Hamilton szerint „azonosíthatónak az a személy tekinthető, amelynek különálló identitása felismerhető, de személye nem ismert. […] Javasoljuk azt a meghatározást, amely szerint valaki azonosítható, ha elég információ áll rendelkezésre hogy elkülönült létezésének, egyénként való létének tényét tükrözze, és akkor válik azonosítottá, ha elég információ áll rendelkezésre a vele történő kapcsolatfelvételhez vagy a másoktól való valamilyen módon történő megkülönböztetéséhez, felismeréséhez."[19]

„kapcsolatba hozható"

A kapcsolatba hozhatóság az adatvédelmi biztos gyakorlata szerint azt jelenti, hogy a kapcsolat akár többszörös áttétellel is megteremthető a személy és az adat között[20]. Az adatvédelmi biztos egyik állásfoglalása alapján „a magyar adatvédelmi törvény definíciója szerint […] minden olyan adat személyes adat, amely természetes személlyel kapcsolatba hozható. Az ilyen adat személyes adat tekintet nélkül arra, hogy a kapcsolat csak több lépésben építhető fel illetve arra, hogy a kapcsolat megteremtésére valamely adatkezelő önmagában nem képes".

Ettől az értelmezéstől eltérő bírói gyakorlatot látszik megalapozni egy újabb keletű eseti döntés[21], amely szerint „meghatározott természetes személlyel kapcsolatba hozható adatnak minősül a természetes személy lakáscíme, telefonszáma. Az az adat azonban, hogy az előfizető telefonvonaláról mikor, mely telefonszám hívásával és milyen időtartamban került sor telefonbeszélgetésre, meghatározott természetes személlyel már nem hozható közvetlenül összefüggésbe. A telefonbeszélgetések időtartama, irányultsága alapján meghatározott természetes személyre következtetés sem vonható le." Az eseti döntésből kiolvasható értelmezés alapján közvetlen kapcsolat esetén az adat személyes adat, ám közvetett kapcsolat esetén nem az.

„adat"

Az adat meghatározása az adatvédelmi törvényben nem szerepel. Az adatvédelmi biztos gyakorlata szerint személyes adatnak minősülnek pl. a következők:

- a természetes személy által olvasott művek, annak olvasási szokásai[22];

- képmás, az érintett azonosítására alkalmas képrészlet, hangfelvétel[23];

- grafológiai vizsgálat eredményeképp előálló véleményben szereplő következtetések[24];

19 Rosemary Jay-Angus Hamilton : i.m., 2-05

20 Csak így minősülhet pl. személyes adatnak a számítógép-hálózatban adott számítógépet azonosító IP-cím : Az adatvédelmi biztos beszámolója 1998, Adatvédelmi Biztos Irodája, 1999., 97. o.

21 BH 2001.269. sz.

22 Az adatvédelmi biztos beszámolója 1997, Adatvédelmi Biztos Irodája 1998, 277. o.

23 Az adatvédelmi biztos beszámolója 1999, Adatvédelmi Biztos Irodája 2000, 201. o.

24 Az adatvédelmi biztos beszámolója 1999, Adatvédelmi Biztos Irodája 2000, 247. o.

- szakmai szervezet etikai bizottságának egy taggal kapcsolatos elmarasztaló állásfoglalása[25];

- a természetes személy által egy vizsgateszten bármely kérdésre adott válasz, ill. az íráskép[26].

A személyes adatok köre tehát az adatvédelmi jog szerint igen széles, jóval bővebb annál, mint amit a köztudat annak minősít (név, lakcím, születési év, stb.). A törvény külön kiemeli, hogy "a személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható". A jogalkalmazás során további probléma a kapcsolat helyreállíthatóságának fogalma, amely alapján valamely információ igen távoli kapcsolat esetében is személyes adatnak minősülhet.

A brit törvény szerint *személyes adatok az az adatok, amelyek olyan élő személyre vonatkoznak, aki azonosítható ezen adatok, vagy ezen adatokból és más olyan információ segítségével, amely az adatkezelő birtokában van ill. valószínűleg az adatkezelő birtokába kerül.* A brit törvény az azonosított személyekre vonatkozó adatok mellett csak azon személyekre vonatkozó adatokat minősíti személyes adatnak, amelyek az *adatkezelő által* azonosíthatók[27]. A magyar törvény hatálya tehát jóval szélesebb, mint a brité[28].

Az Irányelv szerint „személyes adat bármely, azonosított vagy azonosítható természetes személyre („adatalany") vonatkozó információ; a személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – azonosító szám vagy egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet"[29]. Az Irányelv meghatározását kívánta átvenni a Tervezet is. Az Irányelv további fontos sajátossága, hogy annak – az értelmezés szempontjából jelentős – preambuluma az azonosítás feltételévé teszi az „ésszerűséget" is („minthogy annak megállapításához, hogy egy személy azonosítható-e, tekintettel kell lenni minden olyan módszerre, amelyek ésszerű alkalmazásával az adott személyt az adatkezelő vagy bármely más személy azonosíthatja"). A preambulum e szakasza alapján – bár a magyar csatlakozás után az adatvédelmi törvény rendelkezéseit az Irányelvvel összhangban kell értelmezni – megfontolandó az „ésszerű erőfeszítéssel" történő azonosíthatóság feltételének előírása. (A preambulum szövege azt is mutatja, hogy a brit törvény néhol még a minimumot sem éri el, ami az Irányelv követelményeit illeti.)

Adatkezelés

Az Avtv. szerint "adatkezelés az alkalmazott eljárástól függetlenül a személyes adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is".

A törvény egyes adatkezeléseket külön is meghatároz. Rendelkezései szerint adattovábbításnak minősül: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik (2. § 5. pont); nyilvánosságra hozatalnak minősül pedig, ha az adatot bárki számára hozzáférhetővé teszik (2. § 6. pont). Adattörlés, ha az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk nem

25 Az adatvédelmi biztos beszámolója 1999, Adatvédelmi Biztos Irodája 2000, 270. o.

26 Az adatvédelmi biztos 2002. július 23-án kibocsátott ajánlása, lásd : http://www.obh.hu/adatved/magyar/nyvaj.htm

27 A brit törvényben már az „adat" fogalma is meghatározott, s ez – a releváns iratrendszer fogalmával együtt – igen fontos szerepet játszik a törvény hatályának kijelölésében.

28 Jay és Hamilton példája szerint pl. valamely személynek egy magánnyomozó által kezelt adatai, pl. neme, magassága ill. ujjlenyomata alapján a személy akkor azonosítható, ha valamely adatkezelo - pl. a rendorség - által kezelt adatok segítségével megállapítható a kapcsolat a nyomozó által kezelt adatok és a személy neve és lakcíme (ill. egyéb olyan adatok, amelyek alapján a személy azonosítottnak minosítheto) között. Ha ez utóbbi feltétel fennáll, akkor a magyar törvény szerint a nyomozó által kezelt adatok attól függetlenül személyes adatok, hogy neki nincsenek birtokában az azonosításhoz szükséges adatok, s azokat a rendorség nem is bocsáthatja azokat a rendelkezésére: az azonosíthatóság fennáll. A brit törvény szerint azonban csak a nyomozó általi azonosíthatóság esetén minosülnek a birtokában lévo adatok személyes adatnak (Jay-Hamilton i.m. 2-05)

29 2. cikk. a). Ebben a fejezetben az Irányelvnek az adatvédelmi biztos megbízásából 1995-ben készíttetett fordítását használjuk (Adatvédelmi Biztos Irodája, OBH, 1995).

lehetséges (2. § 8. pont).

A jogalkotói szándék szerint bármely olyan cselekmény adatkezelés, amelynek tárgya személyes adat. Az adatvédelmi törvény indokolása úgy fogalmaz, hogy „az adatkezelés az adatokra alkalmazható minden elképzelhető műveletet felölel". A hatályos szöveggel kapcsolatos bizonytalanság, hogy abban – az EU irányelvével ellentétben – nem szerepel az adatok puszta megismerése, a betekintés, mint adatkezelési művelet. "az adatkezelés az adatokra alkalmazható minden elképzelhető műveletet felölel". Eleddig eltérő értelmezések születtek abban a kérdésben, hogy vajon adatkezelés-e valamely adat megismerése, az adatokba történõ betekintés; e ponton még az adatvédelmi biztos gyakorlata is ingadozó volt[30]. Igen veszélyes bármilyen értelmezési bizonytalanságnak teret adni e kérdésben, hiszen – tekintettel arra, hogy a Btk. 177/A §-ában foglalt jogosulatlan adatkezelés kerettényállás[31] - az adatkezelés fogalmának terjedeleme dönti el azt, hogy az adatokba jogtalanul betekintő, ám adatkezelést nem végző személy cselekménye büntetendő-e. Álláspontunk szerint az adatokba történő betekintés is adatkezelésnek minősül.

Az Irányelv szerint adatkezelés a személyes adatokkal végzett következő műveletek egyike vagy egy csoportja, függetlenül attól, hogy a műveleteket automatizálták-e vagy sem: felvétel, rögzítés, szervezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, továbbítás átadással, terjesztéssel, vagy a hozzáférés más módon való megteremtésével, összehangolás vagy összekapcsolás, zárolás, törlés és megsemmisítés. Az Irányelv angol szövege az adatkezelésre a „data processing" kifejezést használja (ennek jelentőségére visszatérünk az alábbiakban).

A brit törvény az Irányelvhez hasonló, igen széles körű meghatározást használ. A Tervezet szerint adatkezelésnek számított volna a személyes adatok gyűjtése, felvétele, rögzítése, szervezése, tárolása, átalakítása vagy megváltoztatása, visszakeresése, megismerése (betekintése), felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, valamint olyan újszerű adatkezelési módok is, mint a fénykép-, hang-, vagy videofelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, írisz) rögzítése.

Álláspontuk szerint az Avtv. meghatározásával kapcsolatos értelmezési bizonytalanság ebben az esetben megfelelően elhárítható az Irányelv meghatározásának átvételével.

Adatkezelő, adatfeldolgozó, adatfeldolgozás

Az „adatfeldolgozó" és az „adatfeldolgozás" fogalma az Avtv. 1999-es módosításakor került be a törvénybe[32]. A módosítás nyomán az Avtv. azon személyt határozza meg adatfeldolgozóként, amely az adatkezelő megbízásából személyes adatok feldolgozását végzi; adatfeldolgozásnak pedig az „adatkezelési műveletek, technikai feladatok elvégzését" tekinti[33]. A jogalkotó célja az volt, hogy az Irányelvben foglaltakkal összhangban az adatkezelő mellett olyan alany is megjelenjen a törvényben, amely pusztán az adatkezelő által meghatározott célból, módon és keretek között kezelhet adatot. Az adatfeldolgozó által végzett jogellenes adatkezeléssel okozott kárért is az adatkezelő felel, mégpedig az Avtv. 18. §-ában foglalt, a veszélyes üzemi felelősségnek megfelelő szabály szerint.

30 Lásd a 440/K/1999 ill. 917/K/1998 sz. ügyeket (mindkettot lásd: az Adatvédelmi Biztos Beszámolója 1999, Adatvédelmi Biztos Irodája, 2000). Magunk a második állásfoglalásban foglaltakkal értünk egyet.

31 A tényállás a tanulmány lezárása óta változott: lásd az 1. jegyzetben írtakat.

32 1999. évi LXXII. tv. A törvény indokolásából az derül ki, hogy a jogalkotó szándéka az Irányelvhez történo közelítés volt – a megvalósítás sajnos nem igazán sikeres. Érdekesség, hogy ugyanez a tv. – szintén az adatfeldolgozó intézményére tekintettel – úgy módosította a Btk. jogosulatlan adatkezelésrol szóló tényállását, hogy az összes többi tényállásban használt „büntetendo" szó helyett „büntetheto" áll.

33 Avtv. 2. § 4. b) és 7. b) pontok.

A törvénymódosítás nem szolgálta a magyar adatvédelmi jog fogalomrendszerének átláthatóságát, ill. nem közelítette azt az Irányelvéhez. Az alábbi táblázatban összefoglaljuk, miképp feleltethetők meg egymásnak az Irányelv, az Avtv, a Tervezet, és a brit törvény kategóriái:

Irányelv	Avtv.	Tervezet	Brit törvény
data controller	adatkezelő	adatkezelő	data controller
data processing	adatkezelés	adatkezelés	data processing
data processor	adatfeldolgozó	adatfeldolgozó	data processor
-	adatfeldolgozás	adatfeldolgozás	-

Az Irányelv nem ismeri az „adatfeldolgozás" kategóriáját. Az abban használt fogalmak pontosan tükrözik azt a helyzetet, hogy *egy* tevékenységről van szó (data processing, melyet magyarul adatkezelésnek fordítunk), az e tevékenységet megbízás alapján végző személy a „data processor", az a személy pedig, amely az adatkezelés célját és módját meghatározza, a „data controller"[34]. Ezzel ellentétben a magyar törvény fogalomrendszere több értelmezésre is lehetőséget ad.

Az általunk helyesnek vélt értelmezés szerint az adatfeldolgozó *bármely* adatkezelési műveletet (a törvény szerint ilyennek minősül a személyes adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt is) és törlése) végrehajthat, adatkezeléssel kapcsolatos döntéseket azonban az Avtv. 2. § 7. a) pontja alapján nem hozhat. Az adatfeldolgozó tehát tulajdonképpen nem más, mint megbízott adatkezelő: mérlegelési joga az adatkezelésre vonatkozó döntések során nincs.

Az Avtv. fogalomrendszere azonban lehetőséget ad olyan értelmezésre is, amely szerint az különbség adatkezelő és adatfeldolgozó között nem csak abban áll, hogy az előbbinek van az adatkezelést illető döntési jogosultsága, míg az utóbbinak nincs, hanem az általuk végezhető adatkezelési műveletek köre is más – miért határozta volna meg egyébként a jogalkotó az adatfeldolgozó tevékenységét? Ilyen értelmezés olvasható ki az adatvédelmi biztos által 2000. június 19-én kiadott, s fentebb már idézett, „Adósság- és követelésbehajtással foglalkozó gazdasági társaságok személyes adatok kezelésének gyakorlatával kapcsolatos adatvédelmi biztosi ajánlás"-ból. A szöveg szerint „az adósságbehajtó társaságok nem tekinthetők adatfeldolgozónak, mivel a birtokukba került személyes adatokkal *nem adatkezelési végrehajtási technikai műveleteket* hajtanak végre, hanem azokat felhasználják és azokra támaszkodva a szerződés keretei között döntéseket hoznak, a polgárral szerződésben álló gazdasági társaság tevékenységébe tartozó feladatot látnak el. Az adatkezelő nem adhat át rendelkezési-döntési jogot az adatok felett."

Kiemelésre érdemes az ajánlásban foglalt azon értelmezés, amely szerint az adatfeldolgozó kizárólag „adatkezelési végrehajtási technikai műveleteket" végezhet, s nem „használhatja fel" az adatokat. Pedig ez utóbbi művelet sem más, mint egy adatkezelési cselekmény végrehajtása: vagyis ha a célt az adatkezelő határozza meg, ill. az adatkezelésre vonatkozó döntést (kit kell megkeresni, mikor, stb.) az adatkezelő hozza meg, magát a felhasználást (megkeresést) az adatfeldolgozó is végezheti.

Az Avtv. által használt „adatkezelési műveletek, technikai feladatok elvégzése" fordulat álláspontunk

34 Lásd Irányelv 2. cikk (b), (d) és (e) pontok.

szerint megalapozatlanul változott az ajánlásban „adatkezelési technikai műveletek" elvégzésére[35]. A helyes nyelvtani értelmezés szerint az adatfeldolgozás lehet (a) adatkezelési műveletek elvégzése vagy (b) technikai műveletek elvégzése. Mivel a (b) körbe tartozó műveletek mindegyike egyben adatkezelés is, valójában az „adatfeldolgozás" fogalmának tartalma megegyezik az adatkezelésével, s annak használata a törvényben felesleges, hatása csupán annyi, hogy értelmezési bizonytalanságokhoz vezet. Célszerű lenne mielőbb az Irányelv által használt, a fenti táblázatban bemutatott fogalmi hármas átvétele, pl. felelős adatkezelő (data controller), adatkezelő (data processor), adatkezelés (data processing) fordításban, ám a Tervezetben továbbra is az Avtv. által ismert fogalmi négyes szerepelt.

Ezen a ponton jelentős különbség van a magyar és a brit törvény fogalomrendszere között; a brit törvény fogalomrendszere az Irányelvéhez hasonlít.

A brit törvény szerint adatkezelő (data controller)

az a személy, aki akár önmagában, akár más személyekkel együttesen (jointly) vagy közösen (in common) meghatározza azokat a célokat, amelyek végett és, azt a módot, amelyen valamely személyes adatot kezelnek vagy kezelni fognak.

Amennyiben a személyes adat feldolgozása kizárólag valamely jogszabály által előírt vagy alapján végzett célból kerül sor, a törvény szerint az adatok feldolgozására kötelezett személy az adatkezelő.

Adatfeldolgozó (data processor) személyes adat vonatkozásában

bármely (az adatkezelő alkalmazottján kívüli) személy, aki az adatkezelő nevében (on behalf of) adatot kezel.

Jay és Hamilton szerint „az adatkezelőnek nem kell minden esetben gyakorolnia ezt (az adatkezelés módjának meghatározásához fűződő) jogosítványát, és a lehetőségek bizonyos skálájának keretei között delegálhatja azt az adatfeldolgozó részére - ám az adatkezelő az a személy, akinek a hatalmában áll meghozni a végső döntést atekintetben, hogy az adatokat pl. visszatartsák vagy hozzáférhetővé tegyék."[36]

A brit törvény szerint az adatfeldolgozó (data processor) bármely adatkezelést (data processing!) végezhet, tehát valójában megbízott adatkezelőről van szó. Valójában a magyar adatvédelmi törvénybe az 1999-es módosítás nyomán bekerült "adatfeldolgozó" is megbízott adatkezelő lenne a helyes értelmezés szerint, hiszen a törvény 2. § (4) bekezdése szerint az "adatfeldolgozás" fogalma valójában az adatkezelések összességét valamint a technikai feladatok elvégzését jelenti.

A magyar törvénnyel kapcsolatban felmerülő további jogalkalmazási bizonytalanság, hogy az adatkezelő és az adatfeldolgozó közötti adatforgalom törvényen (magán az Avtv. rendelkezésén) alapuló adattovábbítás-e (a hatályos magyar szabályozás alapján, amely a harmadik személy fogalmát nem határozza meg, ez a védhetőbb elképzelés), vagy nem is minősül adattovábbításnak (az Irányelv és a brit törvény fogalomrendszere szerint ez így van, mivel az – a magyar törvénnyel ellentétben – mindkettő meghatározza a harmadik személy fogalmát, és abból kizárja az adatfeldolgozót). Amennyiben adattovábbításról van szó, úgy alkalmazni kell a külföldre történő adattovábbításra vonatkozó 9. §-t; amennyiben nem, akkor lehetséges olyan érvelés, hogy a külföldön történő adatfeldolgozás nem esik a

35 Az értelmezésre talán az 1995. évi CXIX. tv-ben foglalt meghatározás volt hatással: „Adatfeldolgozás: az adatkezelést érinto, érdemi döntést nem jelento technikai feladatok elvégzése" (2. § (1) bek. 9. pont)

36 Jay-Hamilton, i.m. 2-17

9. § hatálya alá, tehát az olyan országokban is végezhető, amelyek nem biztosítják a magyar jognak megfelelő védelmi szintet a személyes adatok számára. A kérdésnek óriási jelentősége van a multinacionális vállalalatok szervezetén belüli adatforgalom jogszerűségének megítélésekor[37].

További rendezendő kérdés ebben a körben a közös és együttes adatkezelés kérdése. A brit törvény szerint együttesen végzett (jointly) adatkezelésről van szó, amennyiben két adatkezelő együttesen határozza meg az adatkezelés célját és módját, míg közös adatkezelésről (in common) abban az esetben van szó, ha a személyes adatok megadott halmazán bármelyik adatkezelő végezhet műveleteket, s e műveleteket a másik adatkezelőtől függetlenül végzi. A gyakorlatban is felmerült már az a kérdés Magyarországon, vajon miképp alakul az adatkezelésért viselt felelősség, ill. egyes kötelezettségek viselése az utóbbi esetben[38]. A jogalkotónak ezen a ponton meg kellene fontolnia a brit meghatározásokhoz hasonlók meghonosítását.

Az adatfeldolgozással kapcsolatban kiemelendő még, hogy a magyar jog nemzetközileg egyedülálló, s kevéssé végiggondolt szabálya szerint az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót nem vehet igénybe. Ez azt jelenti, hogy ha pl. valamely magyarországon tevékenykedő multinacionális cég ügyféladatbázisát az anyacég szerverén tárolják (tehát az anyacég a magyarországi cég adatfeldolgozója), akkor az anyacég ezen adatbázis karbantartására, az azzal kapcsolatos bármely – adatkezelési műveletet magában foglaló – tevékenység ellátására nem vehet igénybe külső vállalkozót. Az outsourcing mindennapossá válásával ez a rendelkezés különösen életidegenné vált, s az adatfeldolgozó fogalmának felülvizsgálatával párhuzamosan álláspontunk szerint a jogalkotónak felül kell vizsgálnia azt.

A hozzájárulás fogalma

Az Avtv. a hozzájárulás fogalmát nem tartalmazza. Az irányelv szerint a hozzájárulás

az adatany beleegyezéséra utaló jelzést tartalmaz.

(Megjegyezzük, hogy a magyar adatvédelmi biztos évek óta hasonló módon értelmezi a hozzájárulás fogalmát.) A brit törvény nem definiálja, csak használja a hozzájárulás (consent) fogalmát. A törvényi meghatározás hiánya tudatos döntés eredménye: a törvényalkotó szerint a fogalom jogi tartalma az egyéb jogágakban használt értelmezésekből meghatározható[39], s az irányelv rendelkezései alapján pontosítható.

Jay és Hamilton szerint az irányelv meghatározásának (d) pontja kizárja a hozzájárulás fogalmából a hallgatással történő beleegyezést. Hasonlóan foglal állást a brit adatvédelmi biztos az 1998-as törvény értelmezését segítendő útmutatóban: „a felek között valamiféle aktív kommunikációnak kell lezajlania. Az adatkezelők nem következtethetnek hozzájárulásra valamely közlésre adott válasz hiányából, pl. abból, hogy egy ügyfél nem küld vissza egy nyomtatványt, ill. nem válaszol arra”[40].

Az ilyen gyakorlatot a Data Protection Tribunal már a korábbi törvény hatálya alatt jogszerűtlennek minősítette a British Gas Trading Ltd. v. Data Protection Registrar ügyben hozott döntés során. A gázszolgáltató cég előfizetői adatbázisát kívánta értékesíteni, s a számlákhoz mellékelt szórólapokban hívta fel előfizetőinek figyelmét arra, hogy – díjmentesen feladható nyomtatvány segítségével –

37 Lásd az adatvédelmi biztos ajánlását a Citibank Rt. adatkezelésével kapcsolatos vizsgálat megállapításairól: az Adatvédelmi Biztos Beszámolója 1999, Adatvédelmi Biztos Irodája, 2000.

38 Jelen tanulmány szerzője a kérdésben állásfoglalásért fordult az adatvédelmi biztoshoz. Problémát okoz, hogy egyes korai adatvédelmi biztosi értelmezések szerint „egy adatkezelésnek csak egy adatkezelője lehet”. Álláspontunk szerint ez az értelmezés a hatályos jog vonatkozásában is téves.

39 Lásd errol Jay-Hamilton 2-23 és következo pontok

40 The Data Protection Act 1998 – An Introduction, Office of the Data Protection Registrar, 1998, 10.o.

tiltakozhatnak adataik tervezett továbbítása ellen. A Tribunal álláspontja szerint adott esetben a tiltakozás hiánya nem minősíthető a beleegyezés jelzésének. Ugyanakkor a beleegyezést jelzi, amennyiben valamely visszaküldött nyomtatványon az adatalany nem jelöli meg az erre a célra szolgáló mezőben (opt-out box), hogy valamely adatkezelési cselekmény ellen tiltakozik[41].

Figyelemre méltó a Jay és Hamilton által az (a) ponttal kapcsolatban tett azon megjegyzés, mely szerint „információhasználatra vonatkozó valamely szektor által követett olyan általános gyakorlat, amely hatásában megfosztja az egyént a választás lehetőségétől, megkérdőjelezhető olyan esetben, amikor a felhasználás adott módjai nem nélkülözhetetlenek (essential) a szerződés céljaihoz"[42].

A brit törvény az érzékeny adatok kezelésével kapcsolatban használja a kifejezett hozzájárulás (explicit consent) fogalmát, amelyet szintén nem határoz meg. Jay és Hamilton szerint nem világos, hogy a „kifejezett" jelző a hozzájárulás formájára vagy magára a hozzájárulásra vonatkozik - az előbbi esetben e rendelkezés alapján akár írásbeli hozzájárulás is megkívánható lenne[43]. Az adatvédelmi biztos állásfoglalása szerint ebben az esetben

az adatany hozzájárulásának teljesen egyértelműnek kell lennie. A megfelelő esetekben ki kell terjednie az adatkezelés részleteire, a kezelt adat (ill. akár a kezelt információ) típusára, az adatkezelés céljára és az adatkezelés bármely olyan sajátos jellemzőjére, amely hatással lehet az egyénre, pl. az adatok esetleges közzétételére"[44].

A brit jogalkotás további, tanulságokat hordozó fejleménye az ún. „enforced subject access" tilalma. A kierőszakolt betekintés fogalma azt a gyakorlatot jelenti, amelynek során valaki – a gyakorlatban általában valamely munkavállaló – egy másik személy – tipikusan a reménybeli munkavállaló – részére csak akkor biztosít valamely előnyt – pl. az állásra történő jelentkezés elbírálását -, ha az utóbbi személy az előbbi rendelkezésére bocsátja az adatvédelmi törvénynek az adatalany betekintési jogát biztosító rendelkezései alapján beszerzett információkat[45]. E gyakorlat oda vezet, hogy az adatvédelmi törvény által biztosított jogok visszaélésszerű gyakorlása (ill. gyakoroltatása) segítségével éppenséggel korlátozható az egyéb magánszférája, s áttörhető az egyes hagyományos jogintézmények által a magánszféra számára nyújtott védelem.

Nagy-Britanniában a fő problémát az a munkáltatói gyakorlat okozta, amelynek során a munkáltatók a leendő munkavállalóktól olyan a rendőrség ill. a társadalombiztosítás birtokában levő – és az adatalany által az adatvédelmi törvény alapján igényelhető - adatok rendelkezésre bocsátását kérték, amelyekből következtetéseket lehet levonni arra nézve, hogy a leendő munkavállalót elítélték valamely bűncselekmény miatt – olyan esetben is, ha az elítélt a jelentkezés időpontjában az adott bűncselekmény vonatkozásában mentesítésben részesült (she has spent the conviction)[46].

---

41 Az ügyet ismerteti James Mullock – Piers Leigh-Pollitt: The Data Protection Act Explained, The Stationery Office, London, 1999, 121. o., The Fourteenth Annual Report of The Data Protection Registrar, The Stationery Office, London, 1998, 16-19.o., a döntés szövegét lásd uo. 89. és köv. o.

42 Jay-Hamilton, i.m. 2-25 pont.

43 Jay-Hamilton, i.m. 2-30 pont.

44 The Data Protection Act 1998 – An Introduction, Office of the Data Protection Registrar, Wilmslow, 1998, 10. o.

45 George Howarth definíciója, idézi Jay-Hamilton i.m. 19-03

46 A „mentesítést" (a gördülékenyebb fogalmazás kedvéért használjuk ezt a magyar jogi szakszót) az 1974-es Rehabilitation of Offenders Act szabályozza, a törvény értelmében a „kitöltött" (spent) buncselekmények tekintetében az elkövetot úgy kell tekinteni, mint aki nem követte el a buncselekményt, ill. mint akit annak elkövetésével nem is vádolták, ill. annak elkövetése miatt nem ítélték el. A Secretary of State rendeletben határozza meg azon eseteket, amelyekben a mentesítés nem érvényesül (The Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975). Ilyenek pl. egyes kinevezések a büntető-igazságszolgáltatás posztjaira, egyes gyermekek ill. fiatalkorúak gondozásával kapcsolatos pozíciók, stb. Az ilyen pozíciókat meghirdeto munkáltatók jogszeruen hozzáférhetnek a bunügyi nyilvántartás adataihoz, s lehetoség van erre nemzetbiztonsági ellenorzés esetében is (a jogszeru hozzáférést szintén a Secretary of State által kibocsátott rendelet szabályozza. Lásd errol: Jay-Hamilton, i.m. 19-05

A törvényhozó az 1997-es rendőrségi törvénnyel a bűnügyi nyilvántartás új rendszerét alakította ki, és az 1998-as adatvédelmi törvényben kriminalizálta a "kierőszakolt betekintés" gyakorlatát.

Az 1997-es Police Act háromféle igazolás kibocsátását teszi lehetővé: ezek a Criminal Convictions Certificate, amely csak azon bűncselekményekre vonatkozó adatokat tartalmazza, amelyek vonatkozásában az elítélt nem mentesült, ám ezek közül sem tartalmazza a kisebb veszélyességű („not recordable") cselekményeket. Az igazolások második típusa a Criminal Record Certificate, amely a központi bűnügyi nyilvántartásban szereplő valamennyi ítéletre vonatkozó adatot tartalmazza (azon cselekményekkel kapcsolatban is, amelyekre nézve az elkövető mentesült), ill. tartalmaz figyelmeztetésekre vonatkozó adatokat is. A harmadik típus igazolás az Enhanced Criminal Records Certificate, amely a központi bűnügyi nyilvántartás teljes adattartalma mellett a rendőrség helyi nyilvántartásaiban őrzött adatokat is tartalmaz.

Az első típusú igazolás szolgálja általában a büntetlen előélet igazolását. A második típusú igazolás kibocsátását az adatalany csak közösen kérheti a Secretary of State által nyilvántartásba vett szervvel. Ezen igazolás kibocsátása akkor történhet, ha a pályázó gyermekekkel ill. idősekkel való kapcsolat fenntartását kívánó állásra pályázik, nemzetbiztonsági szempontból releváns pozíciót tölt be; ilyen igazolás szükséges egyes az egészségügyben ill. a gyógyszeriparban munkát vállalók ill. hiteintézetek és pénzügyi szolgáltatók felsőbb vezetői részére. A harmadik típusú igazolás kibocsátása abban az esetben kérhető, ha valamely személy olyan állásra pályázik, amelyben 18 éven aluli személyekkel kell rendszeresen érintkeznie, ill. ezt az igazolást követelik meg a szerencsejáték-engedélyekre (gaming, betting and lottery licenses) pályázóktól is.

Az 1998-as adatvédelmi törvény vonatkozó szakasza a következőképpen rendelkezik:

Tilos valamely számára más személy által nyújtandó szolgáltatásra vonatkozó szerződéssel kapcsolatban azt követelni, hogy e más személy vagy harmadik fél „releváns rekordot" (relevant record) bocsásson rendelkezésre vagy mutasson be.

A törvény további rendelkezése szerint a köz számára (ingyenesen vagy visszterhesen) valamely árut vagy szolgáltatást nyújtó személy sem teheti függővé az áru/szolgáltatás nyújtását a „releváns rekord" rendelkezésre bocsátásától vagy bemutatásától.

A „releváns rekordokat" a törvény táblázatban sorolja fel, amely táblázathoz a Secretary of State rendelettel – az adatkezelők és az adatok meghatározásával - újabb adatköröket csatolhat. A táblázatban jelenleg meghatározott adatkezelők által kezelt, az adatalany által elkövetett bűncselekményekre és büntetésekre vonatkozó adatok ill. az adatalanynak a társadalombiztosítás szervei által kezelt adatai találhatók.

A törvényben meghatározott adatkör megkövetelése – egyes, itt nem részletezendő kivételektől eltekintve – bűncselekményt valósít meg, és pénzbüntetéssel büntetendő.

A „hozzájárulás" fogalmát a tervezet az Avtv-től eltérően meghatározta az EU-irányelvnek megfelelően. A meghatározás szerint „az adatalany hozzájárulása az adatalany kívánságának önkéntes, határozott és tájékozott kinyilvánítása, amellyel félreérthetetlen beleegyezését fejezi ki az őt érintő személyes adatok feldolgozásába"[47].

47 A meghatározásban „adatfeldolgozás" helyett az „adatkezelés" fogalmat kellett volna használni.

Az adatkezelés feltételei

Az Avtv. kapcsán már korábban kiemeltük, hogy annak szabályozásában igen következetesen érvényesül az információs önrendelkezési jog, adatkezelés jogalapját csak az érintett hozzájárulása, vagy törvény adhatja. Szóltunk a célhozkötöttség elvéről és az Avtv. legfontosabb rendelkezéseiről. Az alábbiakban előbb a brit törvénynek az adatkezelés feltételeire vonatkozó szabályozását ismertetjük, majd kitérünk a Tervezetben foglalt változásokra.

A brit adatvédelmi törvény lényegi rendelkezéseit az ún. adatvédelmi alapelvek (data protection principles) tartalmazzák, amelyek a törvény 1. mellékletében találhatók. A melléklet az alapelvek felsorolása mellett azok értelmezését segítő rendelkezéseket is tartalmaz.

Az első adatvédelmi alapelv szerint szenzitív adat esetén ezen felül legalább a törvény 3. mellékletében foglalt valamely feltétel nem teljesül.

Az adatkezelés jogszerűségének fogalma nem szorul különösebb magyarázatra[48], etekintetben az adatkezelés lehetséges jogalapjairól szóló 2. és 3. melléklet rendelkezéseit ismertetjük. A „tisztességesség" követelményének értelmezéséhez a törvény egyes rendelkezései nyújtanak segítséget (1. melléklet, II. rész, 1-4 szakaszok: az ún. „fair processing code"). A „tisztességesség" követelménye igen fontos: a brit adatvédelmi biztosok igen gyakran léptek fel adatkezelést érintő „tisztességtelen" gyakorlat ellen – lásd pl. a hitelinformációs szolgáltatók által kezelt, harmadik személyekre vonatkozó információ ügyében a Data Protection Tribunal által a 90-es évek elején hozott határozatokat. A „tisztességesség" jelen tanulmány központi témája szempontjából is igen fontos: olyan jogi követelményt állít, amelynek megvalósulását a gyakorlatban leginkább a „legjobb gyakorlat" maghatározása, magatartáskódexek megalkotása, a szervezet által követett adatvédelmi gyakorlat auditáltatása segíthet elő.

Jogszerű adatkezelésnek valamely cselekmény csak a törvény által (a 2. mellékletben) felsorolt feltételek valamelyikének teljesítése esetében minősülhet). Amennyiben szenzitív adatokról van szó, ezen felül további (a 3. mellékletben) felsorolt feltételek egyikének is teljesülnie kell.

Az adatkezelés a következő esetekben jogszerű:

1. Az adatalany hozzájárult az adatkezeléshez

2. Az adatkezelés szükséges

(a) valamely olyan szerződés teljesítéséhez, amelyben az adatalany szerződő fél, vagy

(b) a szerződés megkötéséhez az adatalany kezdeményezésére (request) teendő lépésekhez.

3. Az adatkezelés szükséges bármely olyan szerződésen kívüli jogi kötelezettség teljesítéséhez (compliance), amelynek az adatkezelő (data processor) az alanya.

4. Az adatkezelés az adatalany létfontosságú érdekeinek (vital interests) megóvásához szükséges.

5. Az adatkezelés szükséges

48 Lásd errol Jay-Hamilton: i.m. 3-04 – 3-13 pontok. Említést érdemelnek a Jay és Hamilton által a „tisztességes" és „jogszeru" fogalma közötti összefüggésrol írottak: az egyik általuk ismertetett álláspont szerint a „jogszeruség" követelménye valójában felesleges, hiszen nem képzelheto el olyan „tisztességes" adatfeldolgozás, amely jogszerutlen lenne. A másik álláspont szerint a „tisztességesség" fogalma két magánfél közötti viszonyra vonatkoztatható, míg a „jogszeruség" követelményének érvényesítése során az állam kényszerít ki bizonyos társadalmi normákat. Plasztikus példájukat lásd i.m. 3-13 p.

(a) az igazságszolgáltatás működéséhez (the administration of the justice)

(b) bármely személyre bármely törvény (enactment) által vagy alapján (by or under) ruházott jogkör (function) gyakorlásához

(c) bármely állami, miniszteri vagy központi közigazgatási szerv által gyakorolt jogkör (functions of the Crown, a Minister of the Crown or a government department) gyakorlásához

(d) bármely személy által közérdekből gyakorolt közfeladat (function of public nature) gyakorlásához.

6. (1) Az adatkezelés valamely adatkezelő vagy olyan harmadik fél jogos érdekeinek érvényrejuttatásához szükséges, akiknek az adatot továbbítják, kivéve, ha az adatkezelés az adott esetben nem igazolható (unwarranted), mert az sérti az adatany jogait (rights and freedoms) vagy jogos érdekeit.

(2) A Secretary of State rendelettel szabályozhatja azt, hogy meghatározott körülmények esetén ez (az előbbi bekezdésben meghatározott) feltétel teljesül-e vagy sem.

Látható, hogy a brit törvény alapján az EU-irányelvhez – és a Tervezethez – hasonlóan a hatályos magyar törvénynél jóval szélesebb körben – adott esetben az adatkezelő üzleti érdekéből is – végezhető adatkezelés.

A hozzájárulás fogalmáról lásd a definíciókról szóló részben írottakat. Ami a 2. pontot, vagyis a szerződés teljesítéséhez szükséges adatkezeléseket illeti, az első bekezdés nem igényel magyarázatot. A második bekezdés célja Jay és Hamilton szerint valószínűsíthetően az volt, hogy annak alapján elvégezhető legyen a hitelképesség előzetes vizsgálata (credit reference check) hitel- vagy hiteljellegű szerződés megkötése előtt, ám álláspontjuk szerint a fogalmazás különös, ugyanis az ilyen vizsgálat nem az adatalany (vagyis az adós), hanem a hitelező kívánságára történik. Így a hitelképesség vizsgálata inkább hozzájárulás alapján képzelhető el, hacsak nem osztjuk azt az értelmezést, amely szerint az ilyen vizsgálat lényegi része bármely hitelmegállapodásnak, s így a hitelért folyamodó személy kívánja a hitelképesség vizsgálatát[49].

Szintén érdekes a szükségesség fogalma. Jay és Hamilton szerint valószínű, hogy az adatvédelmi biztos a szükséges fogalmat nem úgy fogja értelmezni, mint amely az adatkezelő szempontjából „kívánatos", hanem mint „amely nélkül a szándékolt cél lehetetlenné vagy a kivihetetlenné (impractical) válna"[50]. Éppen a hitelezési kockázat felmérésekor igen nehéz meghatározni azt, hogy mi a „szükséges" szó tartalma az adott esetben. A gyakorlatban valószínűtlen, hogy a brit adatvédelmi biztos pl. a hitelinformációs szolgáltatások által biztosított – nem harmadik személyekre vonatkozó – adatok bizonyos körét „szükségtelennek" minősítené – ráadásul az adatkezelők ebben az esetben a hozzájárulásra hagyatkozhatnának az adatkezelés során, s ez ellen már csak a hozzájárulás önkéntes voltát vizsgálva lehetne fellépni, amely a gyakorlatban szintén nem valószínű[51].

A szerződésen kívüli jogi kötelezettségek teljesítésének értelmezésével kapcsolatban különösebb probléma nem merül fel. Az adatalany létfontosságú érdekeivel kapcsolatban említést érdemel az adatvédelmi biztos értelmezése, amely szerint ezen az alapon csak akkor kezelhető személyes adat, ha az a szó legszorosabb értelmében létkérdés („matter of life and death"), pl. abban az esetben, ha a

49 Jay-Hamilton: i.m. 4-11, 4-12

50 Jay-Hamilton: i.m. 4-13

51 Carol Hufton, az ODPC hitelinformációs rendszerekkel kapcsolatos panaszok vizsgálatát végzo csoportának vezetoje (Senior Compliance Manager) személyes közlése szerint ezen adatok ismerete a hivatal álláspontja szerint is szükséges a hitelelbírálás folyamata során.

súlyos közlekedési balesetet szenvedett, öntudatlan személy egészségügyi adatainak ismeretére van szükség a kezelést végző korház intenzív osztályán[52]. Jay és Hamilton szerint ez a megszorító értelmezés vitatható: a „létfontosságú érdek" (vital interest) ugyanis jelenthet általában nagyon fontos, lényeges érdeket is. Ugyanakkor az adatvédelmi biztos értelmezését támasztja alá álláspontjuk szerint az, hogy bár az irányelv azon rendelkezése, amelyet e szakasz ültet át a brit jogba, nem egyértelműsíti a „létfontosságú érdek" fogalmát, annak megszorító értelmezését támasztja alá az irányelv preambuluma[53].

Az 5. pont alatt felsorolt esetekben a helyzet hasonló a 3. pontban felsoroltakhoz, ám az adatkezelésre nem csak valamely kötelezettség, hanem valamely jog gyakorlása is felhatalmazást adhat[54].

A 6. pont alatt említett rendelkezés, amely az adatkezelő jogos érdekeire hivatkozva tesz lehetővé adatkezelést, talán a legvitatottabb a 2. melléklet szakaszai közül. Az adatkezelőnek ugyanis magának kell mérlegelnie, vajon az adatkezelés igazolható-e ezen az alapon, ill. sérti-e az adatalany jogait.

Szenzitív adatok kezelése során a törvény 2. mellékletében valamely feltétel mellett a 3. mellékletben felsorolt valamely alapelvnek is teljesülnie kell ahhoz, hogy az adatkezelés jogszerűnek minősülhessen. A szenzitív adatok kezelésének a melléklet által felsorolt lehetséges jogalapjai a következők:

(2) E szakasz alkalmazásában "gyógykezelésnek" (medical purposes) a betegségmegelőzés, a diagnózis, az orvostudományi kutatás, a gondozás, ápolás és az egészségügyi szolgáltatások szervezése minősül.

(2) A Sectetary of State rendeletben határozhatja meg azokat a kürülményeket, amelyek mellett az (1)(a) és (1)(b) bekezdésben foglaltak szerinti adatkezelés az (1)(c) bekezdés alkalmazásában úgy minősül, mint amely az adatalanyok szabadságainak és jogainak megfelelelő védelme mellett történik.

10. Egyéb, a Secretary of State által rendeletben e szakasz alapján meghatározott körülmények szerinti adatkezelés.

A szenzitív adatok kezelését lehetővé feltételeinek részletes tárgyalását mellőzzük[55].

A "tisztességes" adatkezelés feltételeit a törvény 1. mellékletének egyes értelmező rendelkezései határozzák meg. Lényeges, hogy a törvény nem sorol fel minden olyan körülményt, amely valamely adatkezelést "tisztességtelenné" tehet.

Az értelmező rendelkezések szerint különös figyelmet kell fordítani arra, hogy az adatkezelő hogyan szerezte be az adatokat - nem alkalmazott-e megtévesztést, nem vezette-e félre az adatalanyt. Ezek a rendelkezések írják elő azt is, hogy bizonyos információkról (az adatkezelő kiléte, képviselőjének kiléte, az adatkezelés célja vagy céljai, ill. más egyéb olyan információk, amelyek adatalany általi ismerete az adatkezelés különös körülményeire tekintettel szükséges ahhoz, hogy az adatkezelés tisztességes legyen) már az adatfelvételkor, ill. amennyiben az adatot nem az adatanytól szerzik be, meghatározott határidő beálltával tájékoztassák az adatalanyt. Ez a tájékoztatási kötelezettség újdonság a brit adatvédelmi jogban, és az adatkezelők számára az új törvény egyik legfontosabb rendelkezése.

A második adatvédelmi alapelv szerint személyes adat csak egy vagy több meghatározott és jogszerű cél érdekében szerezhető be/gyűjthető, a továbbfeldolgozás bármely olyan módon, amely

52 The Data Protection Act 1998 – An Introduction, Office of the Data Protection Registrar, Wilmslow, 1998
53 Jay-Hamilton: i.m. 4-15, lásd az irányelv 7. cikkét
54 Az e rendelkezéssel – foképp a (d) ponttal – kapcsolatos értelmezési bizonytalanságokról lásd Jay-Hamilton: i.m. 4-17 és köv. pontok
55Lásd erre Jay-Hamilton: i.m. 5-01 - 5-28, Mullock - Leigh-Pollitt: i.m. 123-127. o.

összeegyeztethetetlen az eredeti céllal, tilos.

A harmadik alapelv a szükségesség elve, amely szerint a kezelt adatoknak az adatkezelés célja tekintetében adekvátnak, relevánsnak kell lennie, a kezelt adatok köre a célhoz viszonyítva nem lehet túl széles (excessive). A negyedik alapev szerint a kezelt személyes adatoknak pontosaknak, és amennyiben szükséges, aktuálisnak kell lenniük; az ötödik alapelv szerint pedig az adott célból kezelt személyes adatok csak addig tárolhatók, ameddig ez a szóbanforgó célhoz képest szükséges. A hatodik alapelv szól az érintett jogairól: a személyes adatok az adatalanynak a törvény által biztosított jogaival összhangban kezelhetők. (A törvény által ismert jogok: a betekintés joga (subject access); az adatkezelés megakadályozásának joga (right to prevent processing) direktmarketing célú adatkezelés esetén általában ill. egyéb esetekben, amelyekben ez az adatalanynak vagy másnak számottevő kárt vagy sérelmet okozna, számos kivétellel; az automatikus úton történő döntéssel kapcsolatos jogok (értesítés, felülvizsgálat kérsének a joga); kártérítés és egyéb igények érvényesítésének joga.)

A nyolcadik alapelv szerint nem lehet az Európai Gazdasági Térség (European Economic Area) területén kívülre személyes adatot továbbítani, kivéve, ha az adott ország vagy terület az adatalanyoknak a védelem "adekvát" szintjét biztosítja az adatkezelés során.

A brit adatvédelmi törvénynek az adatkezelés jogalapját szabályozó igen részletes rendelkezéseivel szemben már korábban kiemeltük a magyar törvény leegyszerűsített, az információs önrendelkezési jogot a maga tisztaságában kifejező megoldását (adatkezelés hozzájárulás vagy törvényi/törvényen alapján kibocsátott) felhatalmazás alapján).

Az Irányelv sok, a magyar adatvédelmi törvény által nem ismert esetben is lehetővé teszi az adatok kezelését; összességében jóval kevésbé korlátozza az adatkezelő lehetőségeit, mint amennyire azt a tájékozatlan megfigyelő számos – főképp az Egyesült Államokból eredő – bírálat nyomán feltételezné[56]. Az adatkezelés – a brit törvényhez hasonlóan – az Irányelv rendelkezései szerint is jogszerű olyan esetben, ha az az adatalany létfontosságú érdekének védelmében szükséges; ha az adatkezelés valamely olyan szerződés teljesítéséhez szükséges, amelyben az adatalany szerződő fél; vagy ha „az adatkezelés az adatkezelő vagy azon harmadik személy jogszerű érdekeit szolgálja, amely részére az adatokat hozzáférhetővé teszik, kivéve, ha az adatalany magánszférájának védelméhez fűződő érdek erősebb, mint az adatkezeléshez fűződő érdek[57]. Ez utóbbi rendelkezés különösen nagy eltérést jelent a hatályos hazai szabályokhoz képest, hiszen kifejezetten megfogalmazza (és konkrét esetben a – természetesen szankcióknak kitett – adatkezelőre hagyja) azt az érdekmérlegelési lehetőséget, amelyet a hatályos Avtv. a törvényhozónak tart fenn.

A Tervezet gyökeresen megváltoztatta volna ezt a helyzetet. Személyes adat kezelését abban az esetben is lehetővé tette volna, „ha az az adatkezelő munkajogi, társadalombiztosítási kötelezettségei teljesítéséhez szükséges”, ill. „ha az adatalany létfontosságú érdeke védelme indokolja az adatkezelést”. A Tervezet átvett az Irányelvből azt a szabályozást is, amely szerint jogszerű az adatkezelés abban az esetben, ha az „olyan szerződés teljesítéséhez szükséges, amelyben az adatalany fél vagy az adatalany szerződéskötésre irányuló szándékát kifejező kérelmének teljesítését célozza”, ill. ha – az állami vagy önkormányzati szerv kivételével – „az adatkezelő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha ez nyilvánvalóan ellentétes az adatalany személyes adatai védelméhez fűződő jogával”. A „szerződéskötésre irányuló szándékot kifejező kérelem” teljesítéséhez szükséges adatkezelés lehetőségével kapcsolatban utalunk a brit törvény hasonló rendelkezéseihez kapcsolódóan írtakra: ez a szabály megteremtheti a hitelinformációs rendszerek működésének feltételeit – ám nem szabad

56 Az európai adatvédelmi jog kritikusainak tipikus álláspontját fogalmazza meg pl: Lucas Bergkamp: The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-driven Economy Computer Law and Security Report Vol. 18. no. 1. 2002 31-47 o.

57 Lásd az Irányelv 7. cikkét.

elfelejteni, hogy kellően határozatlan ahhoz is, hogy az adatvédelmi biztos vagy a bíróságok más jogértelmezésre jussanak.Az adatkezelő jogos érdeke által igazolt adatkezelés pedig a legnyilvánvalóbb példája annak, hogy az információs önrendelkezési jog érvényesülése magából az új adatvédelmi törvényből következően korlátozottabb lesz, mint korábban.

A külföldre irányuló adattovábbítással kapcsolatban a hatályos Avtv. kifejezetten szigorú – következetes érvényesítésük esetén a nemzetközi kereskedelmi forgalmat is hátráltató – szabályt tartalmaz. Ennek értelmében személyes adat Magyarországról - az adathordozótól vagy az adatátvitel módjától függetlenül - külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy azt törvény lehetővé teszi, feltéve, ha az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatra nézve teljesülnek. E kérdés tárgyalásakor kiemelendő, hogy az Európai Unió adatvédelmi irányelvének kettős célja van. Az egyik értelemszerűen a természetes személyek védelem adataik kezelése során – a másik azonban a személyes adatok szabad áramlásának biztosítása. Az EU-irányelv elfogadásának egyik fő ösztönző ereje ugyanis éppen az volt, hogy az elfogadott tagállami törvények különböző szinten biztosítottak védelmet a személyek számára, s a törvényekben megjelentek olyan rendelkezések is, amelyek a „megengedőbb" adatvédelmi jogokkal rendelkező országok irányába korlátozták az adott államból történő adatexportot. Az ilyen szabályozás természetesen ellene hatott az egységes belső piac kialakításának, hiszen a nemzetközi nagyvállalatok rendszereiben, ill. több, különböző országban elhelyezkedő, együttműködő szolgáltató által nyújtott szolgáltatások esetén (pl. a nemzetközi kártyatársaságok által kibocsátott kártyák használata során) elkerülhetetlen személyes adatoknak országhatárokon túli továbbítása.

Az Avtv. tehát – az EU irányelvtől eltérően – az érintett hozzájárulásának megléte esetén is ahhoz köti a személyes adatok külföldre történő továbbítását, hogy a magyar adatvédelmi jogszabályoknak megfelelő feltételek külföldön is fennálljanak. Míg az EU irányelve kijelöli azt a szervet – a Bizottságot - amely a magyar törvénynél egyébként etekintetben enyhébb követelményeket megfogalmazó irányelvhez képest méri fel egyes, EU-n kívüli országok jogrendjét, a magyar törvény nem szól arról, ki méri fel, hogy a külföldi adatkezelőnél teljesülnek-e az adatvédelem feltételei. Az EU irányelv alapján ráadásul a Bizottság az eset összes körülményei alapján, a célország jogszabályai, azok érvényesülése figyelembevételével, de az önszabályozásra, az iparági magatartáskódexekre és egyéb szabályozó eszközökre tekintettel határoz abban a kérdésben, vajon „megfelelő" (adekvát) egy célország által a továbbított személyes adatok számára nyújtott védelmi szint, vagy sem[58]. A magyar törvény által támasztott feltételek elvileg megteremthetők akár államközi[59], akár az adatexportőr és –importőr társaság közötti szerződéssel. Arra nézve, hogy mely államban biztosítottak szerződés nélkül, vagyis az adott ország adatvédelmi joga által a magyarországival azonos feltételek, a magyar törvény indokolása, valamint egy közös, az adatvédelmi biztos és az igazságügyi miniszter által kiadott tájékoztató (8001/1999. (IK.6.) IM) adhat iránymutatást. Ezek alapján – bár hangsúlyozni kell, hogy a tájékoztató kifejezetten a levéltári kutatások vonatkozásában sorolja fel az azonos védelmet nyújtó államokat – az Európa Tanács adatvédelmi egyezményét aláíró államok minősülnek ilyen államnak[60]. Egy ajánlásában

58 A magyar adatvédelmi jog által nyújtott védelmet egyébként az EU Bizottság 2000. júliusi döntésével az EU adatvédelmi irányelve szerint „megfelelőnek" minősítette.

59 Lásd a 13/2002. (I. 31.) Korm. sz. rendeletet a Magyar Köztársaság Kormánya és Izrael Állam Kormánya között a magyarországi levéltárakban őrzött, védett személyes adatot tartalmazó Holocaust-dokumentumok másolatának a jeruzsálemi Yad Vashem, a Holocaust Mártírjai és Hősei Megemlékezési Hivatala részére történő átadása és felhasználása tárgyában készült adatvédelmi szerződés kihirdetéséről.

60 A hivatkozott tájékoztató szövegét lásd : Az adatvédelmi biztos beszámolója 2000, OBH 2001, 358. o. Az ET egyezmény tagállamai 2002. augusztus 2-i állapot szerint: Ausztria, Belgium, Ciprus, Cseh Köztársaság, Dánia, Egyesült Királyság, Észtország, Finnország, Franciaország, Görögország, Hollandia, Írország, Izland, Lengyelország, Lettország, Litvánia, Luxemburg, Magyarország, Németország, Norvégia, Olaszország, Portugália, Románia, Spanyolország, Svájc, Svédország , Szlovákia és Szlovénia ; a mindenkori állapont megtekinthető a http://www.coe.fr honlapon.

az adatvédelmi biztos úgy fogalmazott, hogy a magyar adatvédelmi követelményeknek „az EU tagországokon kívül az Európa Tanács adatvédelmi egyezményét kihirdető országok" minősülnek[61].

A külföldre történő adattovábbítással kapcsolatos kérdés az a fent már említett probléma is„ hogy az adatkezelő és az adatfeldolgozó közötti adatforgalom törvényen (magán az Avtv. rendelkezésén) alapuló adattovábbítás-e, ill. ahhoz szükséges-e az érintett hozzájárulása. Összességében az Avtv. külföldre irányuló adattovábbítással kapcsolatos rendelkezései az EU csatlakozás küszöbén indokolatlanul szigorúnak, végiggondolatlannak és – az Avtv. számos más rendelkezéséhez hasonlóan – szerencsétlenül megfogalmazottnak minősíthetők. A Tervezet átvette volna az „adekvát védelem" Irányelvből származó koncepcióját.

Az Avtv-vel kapcsolatban számos további kritika is megfogalmazható. Az Irányelv előírja független, az adatvédelmi jog rendelkezéseinek érvényesülését felügyelő szerv létesítését[62]. A magyar jogalkotó annak idején az adatvédelmi biztost hatósági jogkörökkel nem rendelkező országgyűlési biztosként (ombudsmanként)[63] hozta létre. Az ombudsman nem az államigazgatási eljárás szabályai szerint jár el, s nem kötelezhet határozatban[64]. Az ombudsman hagyományosan a közigazgatás külső kontrolljának egy intézménye – az adatvédelmi biztos azonban minden adatkezelőt, így a magánszféra szereplőit is ellenőrizni hivatott. A legtöbb EU-tagállamban a biztost nem nevezik „ombudsman"-nak, s hatásköre is jóval bővebb, mint a magyar adatvédelmi biztosé. A brit adatvédelmi biztos „enforcement notice" kibocsátásával kötelezhet, és bírságolhat is; a határozat megtámadható a Data Protection Tribunal elnevezésű különbíróság előtt. A 2000-ben született cseh törvény szerint annak megsértőjére a cseh adatvédelmi hivatal bírságot szabhat ki. A 2002. szeptember 1-én hatályba lépett szlovák törvény szerint az adatvédelmi hatóság által kiszabható bírság legfelső összege 1 millió szlovák korona[65]. Az irodalomban azért bírálják az EU-tagállamok szabályozását, mert azok a versenyhatóság által kiszabható bírságokhoz képest kisebb összegű bírságok kiszabását teszik lehetővé: ezzel szemben Magyarországon ilyen lehetőség egyáltalán nincs[66].

A hatályos jog az adatvédelmi jog megsértőjét büntetőjogi szankcióval fenyegeti: a legtöbb magánszférabeli szereplőt ez veszi rá a jogkövetésre, s kevéssé az adatvédelmi biztos ajánlásai. További jogkövetésre ösztönző elem lehetne a kártérítési felelősség: a hatályos Avtv. a Ptk. szerinti veszélyes üzemi felelősséghez hasonlóan szabályozza az adatkezelő felelősségét[67]. Az Alkotmánybíróság egy határozata szerint a nemvagyoni kártérítésre vonatkozó igény jogalapja önmagában a személyiségi jog megsértése[68], azonban a bírói gyakorlat a kár bekövetkeztének bizonyítását is megkívánja, amely a személyes adatokhoz fűződő jog megsértése esetén igen ritkán sikeres[69]. A hatályos jog szerint tehát

---

61 A Citibank Rt. adatkezelésével kapcsolatos vizsgálat megállapításait összegző adatvédelmi biztosi ajánlás, 1999. december 22. Az ajánlás szövegét lásd a Függelékben.

62 Lásd Irányelv 28. cikk.

63 A foszabály alóli kivétel az az eset, amikor a biztos az államtitok vagy szolgálati titok minosítését indokolatlannak találja. A biztos ilyen esetben a minosítot a minosítés megváltoztatására vagy törlésére szólítja fel, a minosíto pedig – amennyiben a felszólítást megalapozatlannak találja – bírósághoz fordulhat. Lásd Avtv. 26. § (4) bek.

64 Kivéve egy titokminosítéssel kapcsolatos jogkört, lásd Avtv. 26. § (4) bek.

65 Lásd BNA World Data Protection Report, 2002. november, 9. o.

66 Lásd Steve Kenny-John Borking: The Value of Privacy Engineering, The Journal of Information Law and Technology, 2002 (1) <http://elj.warwick.ac.uk/jilt/02-1/kenny.html>

67 Lásd Avtv. 18. §

68 Lásd a 34/1992. (VI. 1.) AB határozat indokolását.

69 Lásd erre a BH 2001/12. sz. jogesetet. Egy másik, nem publikált esetben, amelyben a tényállás szerint két bank fúziója során az egyik bank összes ügyfelének adatai az alperes által sem vitatottan jogosulatlanul kerültek továbbításra, a Legfelsobb Bíróság nem fogadta el a felperesek azon érvelését, amely szerint nem vagyoni kártérítés érvényesítése esetén a kár fogalmába a személyiségi jogot ért – vagyoni mércével nem mérheto – hátrány, mint immateriális kárelem is beletartozna, s az Avtv. megsértésének bizonyítása után további bizonyításra a kár tekintetében nincs szükség (annak bekövetkezte is becslésen alapul, s megállapítása a bíróság feladata).

valamely cég által jogszerűtlenül végzett adatkezelés esetén (az adatvédelmi biztos ajánlása szerint is túlzott[70]) büntetőjogi szankció fenyegeti az adatkezelésért felelős vezetőt, magát a céget azonban legfeljebb az adatvédelmi biztos nyilvánosságra hozott ajánlásával járó PR-hátrány. Ez a szankciórendszer nyilvánvalóan elhibázott.

A Tervezet sajnálatos módon nem hozott volna érdemi változást. Az adatvédelmi biztosra változatlanul az országgyűlési biztosra vonatkozó rendelkezéseket kellett volna alkalmazni. A változás annyiban állt volna, hogy a biztos a Tervezet szerint elrendelhetné a jogosulatlanul kezelt adatok zárolását, törlését, megsemmisítését, ideiglenesen vagy véglegesen megtilthatná a jogosulatlan adatfeldolgozást. Ezen „intézkedések" ellen az adatkezelő bírósághoz fordulhatna, s a perben a tervezet szerint az „államigazgatási perekre" (sic) vonatkozó szabályok szerint kellett volna eljárni. Felmerül a kérdés, hogy amennyiben a jogszabályelőkészítő a Polgári Perrendtartásnak a közigazgatási határozatok felülvizsgálatáról szóló XX. fejezetét rendeli alkalmazni, akkor miért nem következetes, s rendeli az államigazgatási eljárás szabályairól szóló törvény hatálya alá a biztosi hivatal eljárását. A szöveg szerint nem megállapítható, hogy mely „intézkedés" bírósági felülvizsgálatáról van szó, mi a viszony egy „intézkedés" és egy „határozat" között? Segíti-e a jogbiztonságot az eljárási határidők hiánya abban a kvázi-közigazgatási eljárásban, amely végén a biztos „intézkedésével" elrendeli az adatok törlését. A biztos helyzetét erősített volna az a rendelkezés, amely szerint egyes jelentős adatkezelések (amelyek a lakosság széles körét érintik, ill. amelyek kapcsán az adatalany kiszolgáltatott helyzetben lehet – közüzemi, banki, biztosítási szolgáltatások) csak a biztos előzetes ellenőrzése és jóváhagyása mellett lennének végezhetők.

Nem csak az adatvédelmi biztos intézményének a kellőnél kisebb mértékű reformja róható a Tervezet terhére. Abban – az Irányelv puszta implementálásán túl – nem jelennek meg az adatvédelmi jog legfrissebb fejleményeit jelentő intézmények. Üdvözlendő, hogy meghatározott adatkezelések ill. adatkezelők esetén a Tervezet kötelezővé tette volna belső adatvédelmi felelős kinevezését és belső adatvédelmi szabályzat megalkotását, amelyet véleményezésre az adatvédelmi biztosnak is be kellene mutatni. Ugyanakkor a Tervezet semmit nem tartalmaz az utóbbi évek más államokban történt jogalkotásának hozadékából. A brit törvény szerint az adatvédelmi biztos a „helyes gyakorlatot" rögzítő magatartáskódexeket alkothat meghatározott szektorok számára[71]. A biztosnak lehetősége van arra is, hogy az „adatkezelő hozzájárulásával megvizsgálja annak bármely adatkezelését a helyes gyakorlat vizsgálata céljából" (audit). Jay és Hamilton szerint az intézménynek így nincs értelme, hiszen az adatkezelőnek nem érdeke, hogy a biztos felfedje az általa követett, esetleg jogsértő gyakorlatot. A brit adatvédelmi biztos a törvénymódosítás során azt szerette volna elérni, hogy az adatkezelő hozzájárulásától függetlenül legyen jogosítványa az auditra[72]. Németországban 1997-ben fogadták el az információs- és kommunikációs szolgáltatásokról szóló törvényt (IuKDG), az Internettel s az ahhoz hasonló ún. „távszolgáltatásokkal" kapcsolatos jogviszonyokat szabályozó törvénykönyvet[73]. Ennek egyik cikke a „távszolgáltatási adatvédelmi törvény"[74]. Ez a törvény már tartalmazta azt az alapelvet, amely szerint a távszolgáltatást nyújtónak olyan technikai eszközöket kell használnia, amelyek működtetése nem jár személyes adatok kezelésével, ill. a lehető legkevesebb személyes adat kezelésével jár, sőt, e szempontokat már az eszközök tervezésekor is figyelembe kell venni[75] - ez a rendelkezés a szövetségi adatvédelmi törvénybe is bekerült ez év májusában hatályba lépett módosításakor[76] (az ún. „adattakarékosság elve"). Szintén új a szövetségi adatvédelmi törvényben az adatvédelmi audit intézménye: ennek lényege, hogy az adatkezelést végző eszközök előállítói és használói adatvédelmi- és

70 Lásd errol a Bünteto Törvénykönyv személyes adatok kezelésével kapcsolatos rendelkezéseinek módosítását kezdeményezo adatvédelmi biztosi ajánlás, 2001. április 25, http://www.obh.hu/adatved/magyar/btkajanl/btkaj.htm
71 Brit törvény 51. (7), Jay-Hamilton: i.m.: 21-09, 21-10.
72 Jay-Hamilton: i.m.: 21-10
73 Informations- und Kommunikationsdienste-Gesetz. Információk az IuKDG-rol: http://www.iukdg.de
74 Teledienstedatenschutzgesetz, TDDSG.
75 TDDSG 3. § (4)
76 BDSG 3. §

adatbiztonsági szempontból független szervezetekkel auditáltathatják eljárásrendjüket ill. eszközeiket[77]. Az intézmény a környezetvédelmi audit már az Uniós joganyagban is megjelenő példáját követi[78].

Összefoglalva: bemutattuk, hogy a hatályos Avtv. szabályozása számos ponton homályos, értelmezési bizonytalanságokra vezető rendelkezéseket tartalmaz. A fogalomrendszer teljes, a személyes adat, az adatkezelő, adatkezelés, adatfeldolgozó és adatfeldolgozós meghatározására kiterjedő átdolgozása mellett szükséges a szankciórendszer átdolgozása és az adatvédelmi biztos intézményének újraszabályozása is. Mivel a jogharmonizáció ahhoz vezet, hogy az Alkotmánybíróság 1991-es határozata nyomán született Avtv-hez képest az új szabályozás várhatóan az egyén információs önrendelkezési jogának szélesebb körű korlátozására ad majd lehetőséget az adatkezelők számára, óriási jelentősége annak, vajon meghonosodnak-e Magyarországon azok az intézmények, amelyek a jogkövetést segítik az adatkezelő számára: az önkéntes magatartáskódexek, a legjobb gyakorlatok, az adatvédelmi audit. Ezek nélkül félő, hogy az adatvédelmi jog csupán „írott jog" marad, vagy annak követését – a jelenlegi szankciórendszer mellett kifejezetten durva büntetőjogi – szankciók alkalmazásával lehet kikényszeríteni. A jogkövető magatartás azonban általában önkéntes, szankciók alkalmazására csak szélsőséges esetekben van szükség. Az általunk részletezett módosítások és új intézmények álláspontunk szerint alkalmasak arra, hogy az adatvédelmi jogot élő, általánosan követett joganyaggá változtassák.

77 Lásd BDSG 9. §. Az intézmény 1997-ben jelent meg a Tartományközi Médiaegyezményben (Mediendienste Staatsvertrag 17. §)

78 Lásd errol Flemming Moos: Datenschutz im Internet, in: Detlef Kröger-Marc A. Gimmy: Handbuch zum Internetrecht, Springer, 2000. 440. o.

Első Magyar Jogi Portál
és online Ügyvédi Szaknévsor

JOGI FÓRUM

jogi hírek

interjúk

publikációk

vitafórum

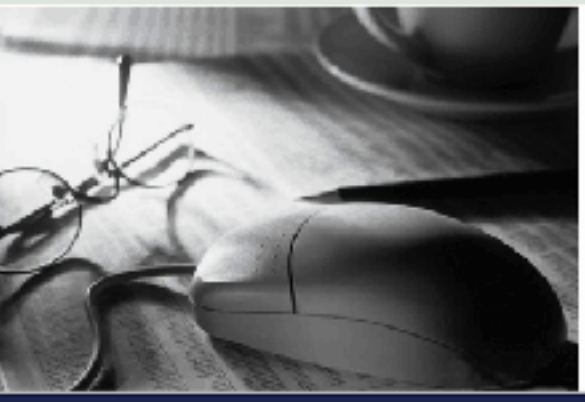
szaknévsor

jogi szakkönyv-katalógus

jogi állásbörze

szakmai rendezvények

heti hírlevél



országos ügyvédi szaknévsor

magyar, angol és német nyelven

ügyfél keres ügyvédet szolgáltatás

www.jogiforum.hu