TÁRSASÁG A SZABADSÁGJOGOKÉRT

TASZ

Belügyminisztérium
jogszabaly@bm.gov.hu

Tisztelt Belügyminisztérium!

A kormany.hu honlapon 2015. március 30-n megjelent, 2015. április 2-ig véleményezhető, Az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításának tervezete véleményezéseként az alábbi álláspontot küldjük meg Önöknek.

A tervezet szerint új elektronikus személyi igazolvány bevezetését tervezi jövő januártól a kormány, amely szükségtelenné tenné a TAJ-kártyát, az adóigazolványt, de akár közlekedési bérletként is szolgálhatna. Az új igazolvány biometrikus adatot is tartalmazó chipje a személyazonosításon kívül más funkcióra is alkalmassá tenné a kártyát, ide kerülhet például az elektronikus közigazgatási eljárások igénybevételéhez szükséges elektronikus aláírás is. A javaslat szól arról is, hogy az egy adott személyt érintő, különböző nyilvántartásokban (idegenrendészeti, lakcímnyilvántartó, adóhivatal, társadalombiztosítás, közlekedésrendészet, rendőrségi) szereplő adatokat a korábbinál egyszerűbben összekapcsolhatóvá kell tenni.

A Társaság a Szabadságjogokért (TASZ) elvileg is ellenez minden olyan intézkedést, amely a hatékonyság vagy a hivatali kényelem indokával az állam információs hatalmának kiterjesztését valósítja meg. A tervezett intézkedések álláspontunk szerint szembemennek az adatvédelem egyik legfontosabb alapelvével, a célhozkötöttséggel, relativizálják a személyes adatok továbbításának és a különböző célú adatkezelések összekapcsolásának főszabályszerű tilalmát, és áttörik az univerzális azonosító tilalmát, mindezzel pedig megkérdőjelezik az osztott információs rendszerek doktrínáját. Ez utóbbi pedig a polgárok információs autonómiájának fontos garanciája, amelyet jelenleg éppen erősíteni, mint megszüntetni lenne szükséges.

Az osztott információs rendszerek[1]

Az osztott információs rendszerek doktrínája jegyében a huszadik század hatvanas-hetvenes éveiben megszületett jogszabályok tekinthetők az első modern értelemben vett adatvédelmi szabályozásoknak. Ezek a szabályok a nagy állami adatkezelések

[1] Az osztott információs rendszerekről szóló szöveg a TASZ szakmai igazgatója, Szabó Máté Dániel: *Az információs hatalom alkotmányos korlátai* című könyve (Miskolci Egyetem, Miskolc, 2012.) információs hatalommegosztásról szóló fejezetének vonatkozó részlete.

1136 Budapest, Tátra u. 15/b I.em.1. tel: 209-0046 fax: 279-0755
e-mail: tasz@tasz.hu w homepage: http://www.tasz.hu

számítógépes összekapcsolása miatti aggodalmakra voltak válaszok,[2] így egyszerre reagáltak az államnak az egyre nagyobb információs hatalmi igényeire, vagyis arra, hogy bővülő funkciói gyakorlásához egyre több és összetettebb ismeretekkel kívánt az állam rendelkezni a polgárokról, valamint arra is, hogy a technológiai fejlődés következtében sok adatot könnyen lehetett összegyűjteni, rendszerezni, továbbítani és összekapcsolni.[3]

Az információs hatalommegosztás arra a kihívásra adott válasz, hogy az egyetlen kézben összpontosuló információ az információ birtokosa számára a funkciójához képest indokolatlan mértékű hatalmat jelent mások felett. Ugyanarra az adatalanyra vonatkozó több információ még nagyobb hatalmat jelenthet felette. Az adatalany feletti információs hatalom pedig nem csupán egyenesen arányos mértékben növekszik a hatalom birtokosa rendelkezésére álló, az érintettre vonatkozó adatok számával, hanem ennél nagyobb mértékben. Az ugyanazon személyhez kapcsolódó különböző adatok együtt minden egyes újabb adattal kiegészülve értékesebbek, mintha értéküket egyszerűen összeadnánk. Ezért az információs hatalom úgynevezett személyiségprofilt igyekszik kialakítani, az adatalanyra vonatkozó ismeretek összekapcsolásával próbál minél többet megtudni róla. Az osztott információs rendszerek követelménye erre úgy reagál, hogy igyekszik megakadályozni azt, hogy egyvalaki (egyetlen személy, egyetlen szervezet) túl sokat tudhasson ugyanarról az adatalanyról.

Az osztott információs rendszereket megvalósító jogi eszközök természetesen nem abszolút érvényűek. Az osztott információs rendszerek doktrínája nem zárja ki a szituatív, magyar terminológiával élve célhozkötött, mérlegelésen alapuló összekapcsolást, a célhozkötött vagy az anoním profilalkotást. Nem zárja ki az úgynevezett interoperábilis rendszerek kiépítését sem, amelyek képesek egymással kommunikálni, de amelyek egyúttal kizárják a korlátlan összekapcsolás lehetőségét. Ezekben a rendszerekben az összekapcsolás lehetőségének a megteremése ellensúlyként az adatok összekapcsolása kérdésében való döntési kompetenciák megosztását igényli.

Kompetenciák szerinti elválasztás: a célhozkötöttség

Az osztott információs rendszerek doktrínája tulajdonképpen *az adatkezeléseknek a kompetenciák szerinti elválasztását* jelenti, azt, hogy mindenki csak azokat a személyes adatokat kezelje, amelyek a jog által elismert saját funkciói betöltéséhez, feladatai ellátásához, az adatvédelmi nyelven megfogalmazva az adatkezelés céljának eléréséhez szükségesek. Az információs hatalommegosztás fogalmát bevezető német alkotmánybírósági határozat szerint az információs hatalommegosztás lényegi követelménye, hogy az államot nem lehet egyetlen adatkezelőként felfogni, hanem ellenkezőleg, az állam egymástól különböző entitásokból áll, amelyek önálló adatkezelőkként járnak el. A célhozkötöttség és a – magyar jogi nyelvben ennek részeként értelmezett, ám meg nem fogalmazott – célmeghatározás[4] elve szerint a személyes adatok kezelésének célját már az adatok gyűjtésekor meg kell határozni, és ez a cél az, amely meghatározza az adatkezelés egészét, többek között a gyűjtendő

[2] Jóri András: *Adatvédelmi kézikönyv. Elmélet, történet, kommentár*. Budapest, Osiris Kiadó, 2005., 24. oldal.

[3] Majtényi László: Az információs jogok. In: Halmai Gábor – Tóth Gábor Attila (szerk.): *Emberi Jogok*. Budapest, Osiris Kiadó, 2003., 582. oldal.

[4] Zweckbindung, angol nyelven purpose specification, a kifejezésnek a magyar jogi szabályozásban megfelelője nincs.

adatok körét, mert csak olyan adatot szabad gyűjteni és majdan kezelni, amely a kitűzött cél eléréséhez szükséges, elengedhetetlen. Az adatkezelés célját az állami szervek esetében a szervek hatásköre határozza meg. Szervezeti megoldásokkal kell biztosítani az egymással az adatkezelés célja szerint nem összefüggő eljárások szeparációját.

Az osztott információs rendszerek követelménye tehát részben az adatelkerülési és a célmeghatározási elveken keresztül érvényesül. A magyar terminológiában mindkettő a célhozkötöttség részét képezi. Az *adatelkerülés* (más szóval adatminimalizálás vagy adattakarékosság) elve szerint korlátozni szükséges a kezelt személyes adatok körét, mégpedig arra való tekintettel, hogy mi szükséges a személyes adat kezelése céljának eléréséhez. Az elv nevezhető szükségességi elvnek is, sok adatvédelmi dokumentum a célhozkötöttség fogalma részeként tárgyalja.[5] Az elv számos adatvédelmi szabály megalkotásának indoka. Ez magyarázza azokat a szabályokat, amelyek szerint a kezelt személyes adatoknak gyűjtésük és kezelésük célja szempontjából megfelelőnek, relevánsnak és nem túlzott mértékűnek kell lenniük.[6] Megjelenik abban a szabályban is, amely szerint a személyes adatok kezelését meg kell szüntetni (azokat törölni vagy anonimizálni kell), amint az adatkezelési cél már nem indokolja a kezelésüket.[7] Ugyanez az elv érvényesül azokban az általános szabályokban is, amelyek alapvetően megtiltják a személyes adatok kezelését, ha az nem valamilyen előre meghatározott célt szolgál.[8] A *célmeghatározás elve* az előzőekben tárgyalt elvhez hasonló, ám mégis eltérő, további követelményeket támaszt. Eszerint az adatokat csak legitim célra szabad kezelni, és tilos olyan célra használni, amely nem következik ebből az előre meghatározott célból.[9] A célmeghatározást gyakran nevezik célkorlátozásnak is (*purpose finality* vagy *purpose limitation*). Az elv több részre bontható, részei önálló elvekként is funkcionálhatnak: (1) az adatkezelési céloknak (előre) meghatározottaknak kell lenniük, (2) amelyek legitimek, és (3) amelyek mindenkor összefüggésben állnak az eredeti adatgyűjtési céllal, vagyis az adatkezelésnek minden fázisában az eredeti céljának kell megfelelnie. (Ez utóbbi elvet nevezhetnénk szűkebb értelemben vett célhozkötöttségnek is: az adatkezelést köti annak célja.) A célmeghatározás majdnem minden nemzetközi adatvédelmi dokumentumban szerepel.[10]

Külön figyelmet érdemel az elv azon része, amely szerint csak legitim célra lehet személyes adatot kezelni, ebben ugyanis a jogi dokumentumokban nagyobb eltérések mutatkoznak. Vannak olyan források, amelyek szerint a célnak „jogszerűnek" kell

[5] Így használja például az Európa Tanács is a statisztikai adatok céljára gyűjtött és kezelt adatok védelméről szóló ajánlásában is, § 4.7 [Recommendation No R (97) 18 on the Protection of Personal Data Collected and Processed for Statistical Purposes, 30. 09. 1997.] Német nyelven adattakarékosság néven említik, Datensparsamkeit.

[6] Például: AZ EU adatvédelmi irányelvének 6. § (1) c) pontja.

[7] EU adatvédelmi irányelv 6. § (1) e). Ez következik az OECD adatvédelmi irányelvek preambulumának 54. pontjából is.

[8] Lásd az irányelv 7. és 8. cikkét. Tulajdonképpen ilyen szabályt találunk az USA 1974-es Federal Privacy Act-ben is. Az 5 U.S.C. 552a(e)(1) kimondja, hogy minden adatkezelési rendszert kezelő szövetségi ügynökség köteles az egyénekről csak azokat az információkat kezelni, amelyek relevánsak és szükségesek az ügynökségnek a törvényben vagy az elnök rendeletében meghatározott feladatai ellátásához. Hasonló tartalmú az (5) bekezdésben foglalt szabály is.

[9] Ilyen szabályokat találunk az OECD Irányelvek 9. cikkében, valamint az ENSZ adatvédelmi irányelvek 3. alapelvében.

[10] Az Európa Tanács adatvédelmi egyezményének 5(b) Cikke, az EU adatvédelmi irányelvének 6(1)(b) Cikke, ENSZ adatvédelmi irányelvek 3 alapelve, OECD adatvédelmi irányelvek 9 szakasza.

lennie.[11] Más források a célok társadalmilag igazolt voltára helyezik a hangsúlyt.[12] Sokak szerint tehát a legitimitás követelménye a társadalmilag elfogadható célokra korlátozza a lehetséges adatkezelési célokat, vagyis csak a társadalmi értékeknek megfelelő, társadalmilag igazolható célok elfogadhatóak legitim adatkezelési célként.[13] Annak meghatározása, hogy mely célok elfogadhatóak társadalmilag, természetesen mindig nyitott, és állandóan változó tartalommal megválaszolható kérdés marad, részben ezért is tartom elfogadhatóbbnak a formális megközelítést. A másodikként említett megközelítés az információs jogban könnyen oda vezethet, hogy összecsúszik a jogszerűség és a társadalmilag igazoltság követelménye, amely azzal jár, hogy a társadalmilag kívánatos cél önmagában legitimálja az adatkezelést, és jogszerűség helyett érdekek és nem az azokat szolgálni hivatott jogok konfliktusában kell döntést hozni. Az adatvédelmi szabályoknak és intézmények első látásra kizárólag jogszerűséggel összefüggő eljárási normáinak, csak nagyon kis hányada hozható közvetlen kapcsolatba a norma társadalmi igazolásával.[14] Az adatvédelmi hatóságok hatáskörében megmutatkozó szabadság, a mérlegelési jogkörök azonban alkalmassá tették őket, hogy jogalkalmazásukban az alkalmazott norma társadalmi igazoltságára is tekintettel legyenek. Különösen így van ez azon hatóságok esetében, amelyek előzetes engedélyezést is végeznek.[15] A hatóságok az adatkezelésnek a társadalmilag igazolt voltára vonatkozó elvárásukat pedig elsősorban a célhozkötöttség fogalmán keresztül érvényesíthették.[16]

Számos adatvédelmi rezsim helyezi a hangsúlyt elsődlegesen a célhozkötöttségre, úgy határozza meg annak szabályait, mintha szinte kizárólag a célhozkötöttség lenne az adatkezelés hatékony korlátja. E tekintetében nagy nyomás helyeződik a magyar jogrendszerre is, a hazai adatvédelmi rendszer ugyanis egészen a közelmúltig nem ezt az utat követte, ám az európai integráció következtében a magyar adatvédelmi szabályozás is elmozdult ebbe az irányba,[17] illetve időről időre megfogalmazódik annak igénye, hogy az adatkezelést jogalaphoz kötő szabályozás helyett a tisztán célhozkötöttségen alapuló adatkezelés rendszerére kellene áttérni.[18] Az EU

[11] Lásd például OECD Irányelveket és az Egyesült Királyság adatvédelmi törvényének 2. adatvédelmi alapelvét.

[12] EU irányelv, ET Egyezmény.

[13] Lee A. Bygrave: Core principles of data protection. *Privacy Law and Policy Reporter*, February 2001 - Volume 7, No. 9. http://austlii.law.uts.edu.au/au/journals/PLPR/2001/9.html. Az adatkezelési cél társadalmi értékekkel való kapcsolatát hangsúlyozza NSW Privacy Committee *Guidelines for the Operation of Personal Data Systems* Background Paper 31 Sydney 1977., 3. oldal, és Michael D. Kirby: Transborder data flows and the "basic rules" of data privacy. *Stanford Journal of International Law* 1981, 27., 46. oldal.

[14] Ez alóli kivétel a személyek regisztrációjáról szóló, már hatályon kívül helyezett 1988. évi holland törvény 4(2) szakasza, amely szerint az adatkezelés célja nem lehet jogellenes, nem lehet ellentétes a közrenddel és a közerkölccsel. Bygrave i.m., 20. végjegyzet.

[15] Lásd az 1973. évi svéd adatvédelmi törvény 3(1) szakaszát, és az 1978. évi norvég adatvédelmi törvény 10. szakaszát. Ma mindkettő hatályon kívül helyezve.

[16] Ma már kevesebb adatvédelmi hatóság végez előzetes ellenőrzést, a jelenség azonban ma sem példa nélküli. Lásd például a 2000. évi norvég adatvédelmi törvény 33. szakaszát.

[17] Lásd például a ma már nem hatályos Avtv. célhozkötöttségi szabályát tartalmazó 5. §-ába az Európai Unióhoz való csatlakozás miatt történt módosításával bekerült új (4) bekezdést, amely szerint személyes adatot különösen akkor lehet kezelni, ha ez közérdekű feladat vagy az adatkezelő törvényi kötelezettségének teljesítéséhez, az adatkezelő hivatalos feladatának gyakorlásához, az érintett létfontosságú érdekeinek védelméhez, az érintett és az adatkezelő között létrejött szerződés teljesítéséhez, az adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez, társadalmi szervezetek jogszerű működéséhez szükséges.

[18] Ez tulajdonképpen mára megtörtént. Az Infotv.-ben a legitim cél – bizonyos feltételek mellett – már önálló adatkezelési jogalapként jelenik meg. A 6. § (1) bekezdés szerint személyes adat kezelhető

adatvédelmi irányelvének szabályai szerint különleges adatnak nem minősülő személyes adatok esetében önmagában egy legitim adatkezelési cél is jogszerűvé teheti az adatkezelést.[19] Ez a magyar rendszerben nem lenne elegendő az adatkezelés jogszerűségéhez, mivel nálunk a célhozkötöttségi feltételek megvalósulása mellett az adatkezelés jogszerűségéhez az is szükséges, hogy legyen annak jogalapja.

Adattovábbítási tilalmak

Az osztott információs rendszerek fogalmi eleme *a személyes adatok továbbításának főszabályszerű tiltása*: azokat az egyes adatkezelők egymásnak általában nem továbbíthatják. Adattovábbítás alatt az adatvédelmi szövegkörnyezetben valójában a mások személyes adatának a megosztását, pontosabban hozzáférhetővé tételét szokás érteni: egy személyes adatot az adatkezelő azzal továbbít, hogy hozzáférhetővé teszi azt egy meghatározott harmadik személynek, aki ennélfogva szintén adatkezelő lesz.[20] Az adattovábbítás megvalósulásához egyáltalán nem szükséges sem az, hogy a továbbított személyes adat kikerüljön az adatkezelő ellenőrzése alól (vagy végérvényesen átkerüljön egy másik adatkezelő ellenőrzése alá), sem pedig az, hogy az adatot az adattovábbítás címzettje megismerje, értelmezze, vagy akár csak birtokba vegye. Az adattovábbítás megtörténik a hozzáférhetővé tétel mozzanatával, azzal, hogy a címzett számára az adatkezelő megnyitja az adat megismerésének elvi és gyakorlati lehetőségét. E meghatározás szerint az adattovábbítás lényege, hogy annak következtében már csak a címzettől függ, hogy ténylegesen megismeri-e a továbbított adatot.[21]

---

akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll. A legitim adatkezelési cél egy másik szabály szerint meg is hosszabbíthatja a jogalap érvényességét. Az Infotv. 6. § (5) bekezdés szerint ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll, további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

[19] Az EU adatvédelmi irányelvének 7. cikkében az adatkezelés feltételei, mint többek között a hozzájárulás és a legitim cél vagylagos kapcsolatban kerülnek felsorolásra.

[20] Ennek felel meg az Infotv. 3. § 11. pontjában olvasható definíció: „adattovábbítás: ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik." Lásd továbbá az adattovábbítás, a hozzáférhetővé tétel és az adatszolgáltatás adatvédelmi biztosi értelmezéséről: Jóri i.m. 151. oldal.

[21] Továbbítottnak minősül az adat akkor is, ha a címzett egyébként soha nem ismeri azt meg, például azért, mert nem érdekli. Adattovábbítás tehát nemcsak akkor történik, amikor az adatok hordozóját a címzett birtokába adják, hanem akkor is, ha az adatokhoz hozzáférést engedő elérési utat biztosítanak, például egy adatbázisba való belépéshez szükséges jelszót. Nem számít ugyanakkor adattovábbításnak az, ha az adathordozót a címzett birtokába adják, de annak tartalmához ő azért nem fér hozzá, mert azt titkosították, a dekódoláshoz szükséges kulcsot viszont nem hozzák a tudomására. Ebben az esetben a titkosítás megszüntetéséhez szükséges kulcs átadásával teszik magukat az adatokat hozzáférhetővé a címzett számára, ezzel történik csak meg az adattovábbítás, annak ellenére, hogy az adatok hordozója már ezt megelőzően is a címzett birtokában volt. Meg kell jegyezni, hogy a titkosítással kapcsolatos megállapítás mindig csak átmenetileg állja meg a helyét: a megbízható titkosítás is csak átmenetileg tudja kizárni az illetéktelen hozzáférést, hiszen a technika fejlődése a titkosító megoldásokat folyamatosan egyre elavultabbá teszi. Egy backdoor nélküli, tehát tökéletes titkosító algoritmusok által generált kódot egyéb támpontok híján csak az összes lehetséges kulcs felhasználásával lehet visszafejteni, ez rengeteg időbe (egyetlen számítógép esetén száz–százmilliárd évbe, több számítógép összekapcsolása esetén ennél kevesebbe) telik, a számítógépek teljesítményének rohamos

Az adattovábbításnak ez a fogalma korszerű, bár 1992-es megalkotásakor még nem látszhatott, hogy az információs rendszerek egyre inkább a megosztás felé mozdulnak el, az internet tartalma ma igen jelentős részben a tartalmak (részben személyes adatok) megosztásának (hozzáférhetővé tételének) a különböző igényeknek megfelelő igazítása szerint ismerhető meg, az interneten végezhető egyik legfontosabb művelet a megosztás (share) lett.[22] A valóság így különösen alkalmazhatóvá tette az adattovábbítás fenti meghatározásnak megfelelő fogalmát.

Így határozható meg tehát az az adattovábbítás, amit az osztott információs rendszerek elve szerint főszabály szerint tiltani kell: az információs hatalom egy kézben való összpontosulása azzal akadályozandó meg, a hatalmat úgy kell megosztani, hogy senki sem férhet hozzá korlátlanul a mások által kezelt adatokhoz, nem válhat tehát mindentudóvá. (Érdekes nyelvi jelenség az, hogy a *megosztás tiltása* kell ahhoz, hogy az információs hatalom *megosztott* legyen.) Az adattovábbítások tiltása egyrészt azt akadályozza meg, hogy a hatalmi helyzetben lévő adatkezelő a neki kiszolgáltatott adatalanyt újabb adatkezelőknek szolgáltassa ki, ennyiben közvetlenül korlátozza a hatalmát. Másrészt pedig közvetve is korlátozza, úgy, hogy az adattovábbítások tilalma a személyiségprofilok kialakítása elé állít gátat. Az adatok összekapcsolásának tilalma ugyanis ennek is előfeltétele.

Az adattovábbítást az adatvédelmi szabályok különböző szabályozási megoldásokkal tiltják, olyan feltételhez kötik, amely be nem következése esetén tilalmazott az adatot továbbítása. E feltétel legjellemzőbben az adattovábbítás jogalapja, vagy valamilyen előre meghatározott cél. A jogalapra koncentráló adatvédelmi szabályozás ezt úgy oldja meg, hogy az adattovábbítás mint a lehetséges adatkezelési műveletek egyike ugyanúgy tilalmazott megfelelő jogalap hiányában, mint bármely más adatkezelési művelet. A magyar adatvédelmi szabályozás korábban külön foglalkozott az adattovábbítás jogalapjával, így tilalmával is,[23] ma már ilyen nincs, de ma is tilos főszabály szerint (megfelelő jogalap hiányában) az adattovábbítás, mégpedig a minden adatkezelésre vonatkozó lehetséges jogalapokat meghatározó „általános adatkezelési tilalom" alapján.

Az adatkezelések összekapcsolásának tilalma

Az adattovábbítások főszabályszerű tiltása mellett szintén az osztott információs rendszerek fogalmi eleme *a különböző adatkezelések összekapcsolásának tilalma*. A különböző adatkezelések – jellemzően ugyanazon adatalanyokra vonatkozó, ám eltérő céllal kezelt és eltérő adatkört érintő adatok – összekapcsolásának minősül különböző adatkezelők által végzett adatkezelések összekötésével, ebben az esetben az

növekedésével azonban ez az idő is rohamosan csökken. A ma feltörhetetlennek mondott titkosítás pár év múlva a nagyobb teljesítményű számítógépekkel könnyen és gyorsan feltörhetővé válhat. Dave Forrest: *Barát vagy ellenség? – A totális kontroll forgatókönyve*. Budapest, Focus Kiadó, 2005. ,191-193. oldal. Az adattovábbítás fogalmának elemzése szempontjából ez azt a kérdést veti fel, hogy mikor továbbított az az adat, amelyhez a címzett csak egy távoli és bizonytalan, jövőben bekövetkező feltétel teljesülése esetén férhet hozzá. Álláspontom szerint az adatkezelő akkor továbbítja az adatot, amikor már látható, hogy a címzettnek előreláthatóan meglesz a technikai lehetősége a hozzáférésre, ennek ellenére nem „veszi vissza" a hordozó birtokát.

[22] Ez leginkább az úgynevezett webkettes (web 2.0) alkalmazások elterjedése miatt van így. Mivel azok elsősorban a felhasználói tartalmaknak, a felhasználó saját adatainak a másokkal (meghatározott körrel vagy a teljes nyilvánossággal) való megosztását teszik lehetővé, elsősorban információs önrendelkezési kérdésnek tartom, ezért ott tárgyalom részletesen.

[23] A már nem hatályos Avtv. 8. § (1) bekezdése. Az Avtv. helyébe lépő Infotv. ilyen szabályt nem tartalmaz.

összekapcsolás adattovábbítást is megvalósít; és ugyancsak ennek tekintendő egyazon adatkezelő különböző adatkezeléseinek összekapcsolásával is. Az előbbi típusú összekapcsolás megakadályozható lenne az előzőekben tárgyalt továbbítás-tilalommal is, az utóbbira azonban ez nem nyújt megoldást, ezért léteznek olyan szabályok, amelyek tiltják az ugyanazon adatkezelőnél kezelt eltérő célú és adattartalmú adatkezelések összekapcsolását.[24] A tilalom azt juttatja kifejezésre, hogy a célhozkötöttség elve azt is magában foglalja, hogy egyazon szervezeten belül – az egész államon, és a közhatalmi szervezeteken belül is, de minden más adatkezelői szervezet is ideérthető – csak akkor kapcsolhatók össze az adatok, ha az összekapcsolás jogalapja és célja tisztázott. Az összekapcsolás tilalma a személyiségprofil kialakításának korlátját jelenti. Arról szól, hogy még az sem, aki egy adott adatalanyról egyszerre ismeri A és B adatot, ha A adatot egy bizonyos cél érdekében kezeli, B adatot pedig egy ettől eltérő célra, akkor egyik vagy másik, esetleg egy ezektől független célra nem kapcsolhatja össze azokat az érintettel, mert az már többet árulna el róla, mint amit az egyes célok önmagukban indokolnak. A személyiségprofilról korábban írtak szerint A és B adat összekapcsolása nem csupán az ismeretek összeadását, hanem egy új minőségű tudást jelent, amely – hacsak nem jogszerű célja az adatkezelésnek – kerülendő. Itt is releváns az *adatelkerülés* elve, amely a célhozkötöttség elvéből származtatható alapelv: eszerint az adatkezelő köteles az adatfelvétel, -tárolás, -továbbítás stb. során a személyes adatok kezelését minimalizálni, lehetőség szerint elkerülni. Ha tehát egy adatkezelési cél személyes adatok kezelése nélkül, akkor ezt a megoldást kell választani. Amennyiben ez nem lehetséges, akkor az adatkezelést a lehető legkevesebb adat használatával kell megoldani. Vonatkozik ez az előző példában említett, az A és B adat összekapcsolásával létrejött új minőségű ismeret kezelésére is.

Az univerzális azonosítók használatának tilalma

Az osztott információs rendszerek elvének érvényesülését szolgálja végül az univerzális személyazonosítók használatának tilalma. Az univerzális személyazonosítók olyan személyes adatok, amelyeket kifejezetten abból a célból hoznak létre és használnak, hogy egymástól különböző (akár egyazon adatkezelő által, akár különböző szervezeteknél kezelt) személyes adatokat könnyen össze lehessen kapcsolni. Ám az univerzális azonosító ezen kívül (1) korlátozás nélkül használható, tehát nincs tekintettel a használata semmilyen specifikus, előre meghatározott célra, (2) általános, vagyis mindenkinek van ilyen (jellemzően minden országlakosnak kiosztják), és (3) egységes, tehát egyazon elv szerint képzett mindenki esetében.

Az e tulajdonságokkal rendelkező személyi szám használatát előíró szabályokat semmisítette meg az Alkotmánybíróság a 15/1991. (IV. 13.) AB határozatában. Az Alkotmánybíróság úgy találta, hogy a személyi szám szabályozása anélkül tette az állami szerveknél kötelezővé, másutt lehetővé a személyi szám korlátlan használatát,

[24] Lásd például a magyar törvényt, amely a személyes adatok összekapcsolását is adatkezelési műveletnek tartja (Infotv. 3. § 10. pont), így ennek jogszerűsége is megfelelő jogalapot igényel. A törvény továbbá úgy rendelkezik, hogy a különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók. [Infotv. 7. § (4) bekezdés] A korábbi adatvédelmi törvény szerint a személyes adatok továbbítását és a különböző adatkezelések összekapcsolását korlátozó feltételek voltak alkalmazandók „az ugyanazon adatkezelő, valamint az állami és az önkormányzati szervek által kezelt adatok összekapcsolására is." [Avtv. 8. § (2) bekezdés]

hogy az abban rejlő veszélyeknek megfelelő biztosítékokat határozott volna meg. Ezért az Alkotmánybíróság alkotmányba ütközőnek, a személyes adatok védelméhez való joggal ellentétesnek, azt szükségtelenül és aránytalanul korlátozónak értékelte e szabályokat. Az Alkotmánybíróság a személyi szám alkotmányellenességét azért mondta ki, mert a népesség-nyilvántartásról szóló, 1991-ig hatályos törvényerejű rendelet a személyi számra vonatkozóan semmiféle korlátozást nem tartalmazott. Később az adatvédelmi törvénybe is bekerült egy olyan kifejezett rendelkezés, amely szerint a korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos,[25] (a ma hatályos törvény ilyet már nem tartalmaz).

A jogrendszerek egy része tiltja, vagy – ami ezzel eredményét tekintve egyenértékű – korlátozza az univerzális azonosítók használatát. A korlátozás azért egyenértékű ebben az esetben a tiltással, mert azzal, hogy a jog nem engedi meg egy azonosító használatát bármilyen célra végzett adatkezelésben, megfosztja az azonosítót az univerzalitásától és egységességétől, ennélfogva azok már nem számítanak univerzális azonosítóknak. Flaherty szerint ahogy az univerzális személyazonosító jel a valódi megfigyelő társadalom kulcsa volt, úgy az adatkezelési célok szerint különböző személyazonosító adatok használata a magánszféra-védelem megvalósulásához elengedhetetlen. Szerinte az univerzális azonosítót használó országokban – ő Svédországot, Kanadát és az Amerikai Egyesült Államokat hozza fel ezen állítása illusztrálására – lehetetlen a megfigyelés elkerülése.[26] Sok országban nem kifejezetten tilos tehát ezeknek az alkalmazása, mégis korlátozott a használatuk, és ezzel az univerzalitásuktól fosztják meg őket, vagyis tulajdonképpen mégis kizárják az univerzális azonosítók alkalmazásának lehetőségét. Az Amerikai Egyesült Államokban például a törvény a kormányzati szerveknek megtiltja, hogy pusztán azon az alapon tagadják meg valamely jog gyakorlását, kedvezmény igénybevételét, hogy az érintett nem adja meg a társadalombiztosítási azonosító számát. Az USA jogrendszere ugyanakkor egyáltalán nem korlátozza ezen azonosító használatát a magánszektorban.[27] Az univerzális személyazonosító használatával együtt járó veszélyek csökkentése értekében tehát korlátozni kell annak használatát. A korlátozás egy minimális formája a magánszektorban való korlátozás: olyan szabályok megalkotásával kell csökkenteni a nevezett veszélyeket, amelyek megtiltják az azonosító használatát a vállalkozások számára ügyfeleik és fogyasztóik, az iskolákban a tanulók és a kórházakban a páciensek azonosítására. A szabályoknak kikényszeríthetőnek kell lenniük, a jogellenes azonosító-használatot szankcionálniuk kell.

Az univerzális azonosítók előnyeik mellett ugyanis az információs önrendelkezés szempontjából súlyos kockázatot jelentenek, erre mutatott rá érzékletesen az Alkotmánybíróság.[28] A legtávolabb eső, különböző célú nyilvántartásokból összeszedett adatokból személyiségprofil előállítását teszik lehetővé, amely az érintett

[25] Avtv. 7. § (2) bekezdés.

[26] David H. Flaherty: *Protecting Privacy in Surveillande Societies. The federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill and London, The University of North Carolina Press, 1989., 406. oldal. Itt említésre érdemes az az eset, amely arról szól, hogy egy svéd nő a személyi száma miatt nem tudott elrejtőzni az erőszakoskodó férje elől, mert az azonosító születésétől a haláláig megváltoztathatatlan volt, és egész életében azonosította őt.

[27] Daniel J. Solove: *The Digital Person. Tecnology and Privacy in the Information Age*. New York, London, New York University Press, 2004., 116. oldal. Solove szerint a korlátozás nélkül használható azonosító megalkotásával az állam valamennyi polgárát olyan súlyos sérelmek lehetőségének teszi ki, mint például az identitáslopás.

[28] 15/1991. (IV. 13.) AB határozat.

tetszőlegesen széles tevékenységi körére kiterjedő és intimszférájába is behatoló művi kép, ami ugyanakkor az adatok kontextusból kiragadott volta miatt nagy valószínűséggel torz is. Az adatkezelő mégis ennek alapján hozza meg döntéseit, állít elő és ad tovább újabb, az érintett személyre vonatkozó információkat. A nagy mennyiségű összekapcsolt adat, amelyről az érintett legtöbbször nem is tud, kiszolgáltatottá teszi őt, egyenlőtlen kommunikációs helyzeteket hoz létre, amelyben az egyik fél nem tudhatja, hogy partnere milyen információkkal rendelkezik róla, illetve azt hiheti, hogy a másik fél adat-hozzáférése korlátlan. Akár tényleges a korlátlan adat-hozzáférés, akár csak az adatalany értékelése szerint áll fenn, e helyzet megvalósítja a Panopticon-helyzetet, és autonómia-vesztéshez vezet. A személyi számmal dolgozó állami adatkezelők hatalma így mértéktelenül megnő. Ha pedig a személyi számot a nem állami szférában is használhatják, ez nemcsak az ottani adatkezelőknek ad az érintett felett hatalmat, hanem az állam további hatalomnövekedéséhez vezet: még messzebbre terjeszti ki az adatokon keresztüli ellenőrzés lehetőségét, megteremti az információs köz- és magánhatalom szoros együttműködésének technikai lehetőségét. A korlátozás nélkül használható személyi szám így a totális ellenőrzés eszközévé válhat. Az államnak polgárai védelme érdekében pedig ezt a kockázatot a legkisebbre kell csökkentenie: a személyi szám használatát garanciális szabályokhoz kell kötnie.

Az univerzális személyi szám tehát lényegénél fogva ellentétes az információs hatalommegosztás elvével, azzal csakis a meghatározott célú adatkezelésre korlátozott használatú azonosító egyeztethető össze. Az ilyen korlátozott használatú személyi számot bevezető törvénynek szabályozási és ellenőrzési garanciákat kell tartalmaznia arra, hogy ezt a számot más összefüggésben ne használhassák. Sem az állam, sem az államigazgatás egésze nem tekinthető olyan egységnek, amelyen belül egyetlen egységes személyazonosító kódot lehetne bevezetni vagy használni. Az univerzális azonosító ellenében megalkotott szabályozásnak ezért az állam részére is adatkezelési szektoronként eltérő azonosítókat kell létrehoznia, és meg kell tiltania azok használatát az eredetitől eltérő célra.[29]

Budapest, 2015. április 1.

Dr. Szabó Máté Dániel
szakmai igazgató

[29] Ennek megfelelően hozta létre Magyarországon a jogalkotó az államigazgatás számára a három egymástól eltérő célú és eltérő körben alkalmazott azonosító jelet: a személyazonosító jelet, amelyet a népesség-nyilvántartás szervei használnak, az adóazonosító jelet, amelyet az adózással összefüggésben lehet használni, és a társadalombiztosítási azonosító jelet, amelyet a társadalombiztosítási ellátásokkal összefüggő adatkezelésekben használnak. Lásd a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvényt, valamint az ezeket az azonosítókat (is) kezelő állami szervek adatkezelését szabályozó szektorális törvényeket. Hasonló megoldást találunk Ausztrália jogrendszerében, ahol 1987-ben és 2007-ben is elbukott az univerzális azonosító bevezetésének ötlete, helyette három szakazonosítót használnak, egyet az egészségügyben, egyet az adózáshoz és egy harmadikat, a gépjárművezetői engedélyek számát általános államigazgatási ügyekhez. Más országokban, például Ausztriában a társadalombiztosítási szám mellett szektorspecifikus azonosítókat használnak.