Pécsi Tudományegyetem
Állam- és Jogtudományi Kar
Doktori Iskola

DR. SZŐKE GERGELY LÁSZLÓ

AZ EURÓPAI ADATVÉDELMI JOG MEGÚJÍTÁSA.
TENDENCIÁK ÉS LEHETŐSÉGEK AZ ÖNSZABÁLYOZÁS TERÜLETÉN

Doktori értekezés

Témavezetők

Dr. Balogh Zsolt György, PhD,
tudományos főmunkatárs

Dr. Majtényi László,
az MTA doktora,
egyetemi tanár

Pécs 2014

KÖSZÖNETNYILVÁNÍTÁS

Egy doktori disszertáció elkészítéséhez a szerző elszántsága mellett sok-sok ember segítségére, támogatására és türelmére van szükség. Csupán néhányukat nevesítve szeretném ezért köszönetemet kifejezni.

Mindenekelőtt köszönöm témavezetőimnek, Balogh Zsolt Györgynek és Majtényi Lászlónak észrevételeiket, támogatásukat. Több évtizedes tapasztalatuk néha egy-egy félmondatba sűrítve is újabb és újabb gondolatok felé indított.

A doktori disszertáció ugyan egyéni kutatás eredménye, de nem előzmények nélkülié. A pécsi műhely keretében az elmúlt években számos olyan adatvédelmi kutatás zajlott, amelyek alapvetően hatottak az adatvédelemmel kapcsolatos felfogásomra. Az adatvédelmi biztos hivatalában eltöltött két éves szakértői tevékenységem úgyszintén jelentős tapasztalatokkal gazdagított. Köszönöm az ezek keretében folytatott számos inspiráló szakmai beszélgetést Polyák Gábornak, Rátai Balázsnak, Kiss Attilának és Böröcz Istvánnak, illetve Jóri Andrásnak és Trócsányi Sárának.

A disszertáció szövegének gondozásában, az elütések és nyelvtani hibák elleni küzdelemben és az irodalomlista végleges összeállításában pedig elévülhetetlen érdemei vannak Kanyó Karolinának – ezúton is köszönöm munkáját.

A kutatás jelentős anyagi támogatása mellett a negyedéves határidők okozta teljesítménynövekedés okán is feltétlenül említést kell tennem arról, hogy „a kutatás a TÁMOP 4.2.4.A/2-11-1-2012-0001 Nemzeti Kiválóság Program című kiemelt projekt keretében zajlott. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.”

Végül, de nem utolsósorban köszönetet kell, hogy mondjak családomnak, különösen feleségemnek, Nórinak és kislányomnak, Emmának végtelen türelmükért. Az ő kitartó támogatásuk nélkül e dolgozat nem készült volna el.

TARTALOMJEGYZÉK

1. ALAPVETÉS

1.1 A témaválasztás indokolása és a dolgozat célkitűzései

A személyes adatok védelmét szabályozó jogi környezet az elmúlt évtizedekben izgalmas kutatási területté vált, amelynek egyik oka e jogterület folyamatos és gyors fejlődése. E változásokat elsősorban a technikai fejlődés és annak társadalmi hatásai, az információs társadalom kialakulása indukálja. Az adatvédelmi szabályozás megújítása jelenleg is éppen napirenden van: az Európai Unió 2009-ben kezdődött adatvédelmi reformjának célja új uniós adatvédelmi szabályozás kialakítása, az 1995-ben elfogadott adatvédelmi irányelv[1] új jogszabályokkal való felváltása.[2]

A témaválasztást két együttes tényező, egy objektív folyamat mellett személyes indíttatás is indokolja, amelyek meghatározzák a disszertáció szerkezetét is. Az adatvédelmi reform folyamatát és eddigi eredményeit a hazai jogirodalom legfeljebb egy-egy szűk területre koncentrálva, összességében alig dolgozta fel, így lényegesnek tartom e folyamat főbb eredményeinek bemutatását. Ezt azonban nem leíró és nem is minden részletre kiterjedő jelleggel, hanem – a 2. fejezetben foglalt történeti áttekintést követően – fejlődéstörténeti kontextusba helyezve teszem meg: a folyamat főbb lépéseinek bemutatása mellett a 3. fejezetben az új jogintézményeket és a Rendelettervezet[3] szövegét nem tételesen, hanem egy általam kidolgozott (elméleti) újgenerációs adatvédelmi szabályozási keretrendszerbe helyezve, kritikai szemlélettel elemzem. Ez azzal a praktikus indokkal is igazolható, miszerint a Rendelettervezet jelenlegi szövege korántsem végleges, az jelentősen módosulhat a jogalkotási folyamat során, így ennek átfogó és részletes elemzése csak a ténylegesen elfogadott jogszabályszöveg ismeretében célszerű.

A témaválasztás másik motivációja a Pécsi Tudományegyetem belső adatvédelmi felelőseként szerzett gyakorlati tapasztalat, miszerint egyrészt a személyes adatok tényleges védelmi szintjén az adatkezelők kellő tudatossággal igen sokat javíthatnak, másrészt az adatvédelmi szabályoknak való megfelelés korántsem triviális feladat, számos compliance kötelezettségnek kell megfelelni, amely tudatos tervezéssel jóval hatékonyabban megvalósítható. Az adatkezelők egy részénél ráadásul van valamilyen belső szabályozás az információbiztonság területén, amelynek eredményei és szemlélete az adatvédelem területén is jól hasznosíthatók. Ennek érdekében az 4. fejezetben először is áttekintem az adatvédelmi önszabályozással (és ennek részeként a belső szabályozással) kapcsolatos meglévő szabályokat és jogirodalmi nézeteket, ideértve az (ön)felügyeleti eszköznek tekinthető adatvédelmi audit és adatvédelmi tanúsítás jogintézményét is, majd

[1] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (a továbbiakban irányelv vagy adatvédelmi irányelv)

[2] E folyamat főbb elemeit ld. az 1.2.2 fejezetben

[3] Javaslat - Az Európai Parlament és a Tanács Rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet), COM(2012) 11 final (a továbbiakban bizottsági Rendelettervezet; a jelző nélküli „Rendelettervezet” a szövegtervezet legújabb, az Európai Parlament által jelentős módosításokkal elfogadott verziójára utal.)

iránymutatást adok az adatkezelők szintjén kialakítandó belső szabályozási rendszer kialakításához.

A fenti két tényező egymással szorosan összefügg. Az adatvédelmi reform egyik legfontosabb fejleménye éppen az adatkezelők szerepének előtérbe kerülése, a rájuk vonatkozó kötelezettségek növekedése és azok szigorúbb felügyelete. A korábbiakhoz képest jelentősen megnő a belső szabályozás és a „compliance-szemlélet" jelentősége, így nagyobb szükségük van az adatkezelőknek olyan útmutatásra, amely segítséget jelent a fokozódó compliance kötelezettségeknek való tervszerű megfelelésben.

A kutatás motivációi egyben megadják a dolgozat tárgyát és szerkezetét is. A disszertáció tárgya először is az európai adatvédelmi szabályozás történeti szempontú áttekintése, a jelenlegi szabályozási környezet kialakulásának bemutatása. Másodszor az európai adatvédelmi jog megújítását célzó adatvédelmi reform egyes eredményeinek összegzése, kritikai értékelése, és egy újgenerációs adatvédelmi szabályozási keretrendszerbe helyezése. Végül a dolgozat a szabályozás jól látható tendenciáiból, az adatkezelők növekvő compliance-kötelezettségeiből eredő kihívásokra is reagál: bemutatja, hogy az önszabályozásban és az adatkezelők belső szabályozásában rejlő lehetőségek miképpen alkalmasak e kihívások kezelésére.

A disszertációban alapvetően az adatvédelem európai szabályozásának fejlődését és tendenciáit elemzem. Egy rövid kitekintést leszámítva nem foglalkozom részletesen sem az Egyesült Államok, sem az egyes európai tagállamok belső szabályaival. Utóbbi kapcsán legfeljebb az egyes jogintézményekhez kapcsolódóan mutatok be jó vagy rossz gyakorlatokat, amennyiben ez a történeti fejlődés vagy egyes tendenciák megértése miatt indokolt. Úgyszintén nem elemzem tételesen az új magyar adatvédelmi szabályozást, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt,[4] de a jogszabály egyes intézményeit elemzem az elvi szabályozási keretrendszer valamint az adatvédelmi audit és tanúsítás témaköreinél. Ugyanakkor a dolgozat eredményei, meglátásai a hazai tudományos közönségnek szólnak, és nagyon is értelmezhetőek a hazai adatvédelmi jogi rezsimben.

Végül meg kell jegyezni, hogy a dolgozatnak nem tárgya az információs jogok körébe tartozó másik alapvető jog, a gyakran az adatvédelmi szabályozás „párjának" is tekintett információszabadság (közérdekű adatok nyilvánossága).

1.2 A személyes adatok védelmével kapcsolatos alapvetés

A bevezető fejezetnek nem célja, hogy teljes egészében, mintegy tankönyvszerűen bemutassa az adatvédelem alapintézményeit; felteszem, hogy a dolgozat célközönsége ezeket alapvetően ismeri. Célszerű ugyanakkor egyrészt néhány alapfogalomnak a tisztázása, másrészt az adatvédelem jelenlegi helyzetének, elsősorban az Európai Unió szintjén zajló adatvédelmi reformnak az áttekintése.

[4] A továbbiakban Infotv. vagy új adatvédelmi törvény

1.2.1 Fogalmi tisztázás

Az adatvédelmi terminológia alapjai a magyar jogirodalomban alapvetően jól kidolgozottak, így a disszertáció során ezekre támaszkodhatom.

Az adatvédelem Jóri András meghatározása szerint „olyan jogi védelem, amely az egyének magánszférájának védelmét célozza az egyénnel kapcsolatba hozható adatok (személyes adatok) kezelésére vonatkozó szabályok előírásával".[5] A fogalom logikáját követve az adatvédelmet a magánszféra védelmének egyik, de korántsem egyetlen eszközének tekintem. Az adatvédelem azonban ennél tágabban is meghatározható. Székely Iván szerint az adatvédelem „a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozását, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége."[6] E fogalom alapján tehát az adatvédelem nemcsak a jogi, de a más szabályozási eszközökkel nyújtott védelmet is felöleli. Tekintettel arra, hogy a disszertáció hangsúlyozottan kitér a személyes adatok jogszabályoktól különböző szabályozási eszközökkel történő védelmére is, a dolgozat során alapvetően e tágabb meghatározást követem.

A magánszféra (privacy) meghatározására számtalan kísérlet történt az elmúlt bő évszázadban, Warren és Brandeis híres tanulmányától kezdődően Westin korszakalkotó művén és Schoeman antológiáján keresztül Solove könyvéig.[7] Meg kell jegyezni ugyanakkor, hogy az angol „privacy" kifejezésnek eleve tágabb a tartalma, mint amit magyarul „magánszférának" lehet fordítani, az Egyesült Államokban ebbe a kérdéskörbe a szélesebb értelemben vett önrendelkezés, például az abortusszal kapcsolatos döntés is beletartozik. Solove és Rotenberg épp ezért különbséget tesz az „információs" és a „rendelkezési" privacy között: míg az információs privacy (information privacy)[8] a személyes adatok gyűjtésével, felhasználásával és hozzáférhetővé tételével kapcsolatos fogalom, a rendelkezési privacy az embernek a saját testére és a családjára vonatkozó döntéshozatali szabadságára (pl. fogamzásgátlással, gyermeknemzéssel, abortusszal kapcsolatos kérdésekre) vonatkozik.[9] A legújabb jogirodalom e felosztáson túlmegy, és – a teljes védelem új technológiai és társadalmi környezetben való biztosítása érdekében – a privacy hét különböző típusát (aspektusát) különbözteti meg.[10] A magyar jogirodalomban a privacy, magánszféra és adatvédelem kapcsolata szintén megjelenik, egyrészt az adatvédelmi tárgyú könyvek bevezetőiben,[11] másrészt önálló tanulmányként is: Szabó

[5] Jóri, 2005, 20.
[6] Székely, 2002, 131.
[7] Warren – Brandeis, 1890, valamint Westin, Alan F.: Privacy and freedom, 1967, Atheneum, New York, Schoeman, Ferdinand, D (szerk.): Philosophical Dimensions of Privacy: An Anthology, 1984, Cambridge University Press, Cambridge, Solove, Daniel, J.: Understanding Privacy, 2008, Harvard University Press, Cambridge, London. A sort természetesen hosszasan lehetne folytatni.
[8] Bevett kifejezés továbbá a "data privacy" is.
[9] Solove és Rotenberg gondolatait idézi Szabó, 2012, 35.
[10] A privacy hét típusa: 1. privacy of the person, 2. privacy of behaviour and action, 3. privacy of data and image, 4. privacy of communication, 5. privacy of thoughts and feelings, 6. privacy of location and space, és 7. privacy of association. A szerzők hangsúlyozzák, hogy a "privacy" dinamikusan változó fogalom, amelynek tartalma a technológiai és társadalmi fejlődéssel összhangban folyamatosan változik. Finn – Wright – Friedewald, 2013, 28.
[11] Jóri, 2005, 11-16., Majtényi, 2006, 63-73.

Máté Dániel privacy-meghatározása igen tágan azonosítja azt az önrendelkezéssel, amely „az egyén joga ahhoz, hogy magáról döntsön”, és végső soron az a tartalma, hogy „mindenki maga döntheti el, mi lesz a saját sorsa, mit tesz magával, a testével és a rá vonatkozó ismeretekkel.”[12] A magánszféra kifejezetést ennél jellemzően szűkebben szokás érteni, de általánosan elfogadott definíció nem található.[13]

E rövid terminológiai áttekintést követően rögzíthető, hogy a dolgozat alapvetően és szándékoltan az adatvédelem (személyes adatok védelmének) szabályozásával foglalkozik, amelyet tehát – követve a jogirodalomban is kialakult álláspontot – a magánszféra-védelem egyik eszközének tekintek. A fogalmi bizonytalanságok mellett ugyanakkor természetesen többször is használom a dolgozat során a magánszféra-védelem kifejezést is, egyrészt olyankor, amikor a (történeti) kontextus ezt megköveteli, másrészt olyankor, amikor az adatvédelemnél tágabb jelenségre utalok.

Felmerül egy további – az eddigiekhez képest technikai részletkérdésnek tekinthető, mégis fontos – tisztázandó kérdés, amely az európai és a magyar adatvédelmi jog terminológiai különbségéből fakad. Az európai adatvédelmi jogban a „data processing” kifejezés magyar fordítása „adatfeldolgozás”, amely azonban tartalmilag a magyar jog „adatkezelés” fogalmának felel meg, és az „adatfeldolgozás” kifejezés egy másik definíciót takar. A dolgozat során főszabály szerint a magyar terminológiát követjük, amikor azonban az Európai Unió valamely vonatkozó dokumentumát idézzük vagy elemezzük, az adatfeldolgozás kifejezés alatt az európai terminológiához igazodva adatkezelést értünk. Ennek kapcsán meg kell jegyeznem, hogy egyetértek Jóri Andrással aki szerint az adatkezelés – adatfeldolgozás tartalma az adatokon végzett művelet alapján nem, csak az azt végző alanyok alapján határolható el egymástól.[14] Utóbbit mind az európai, mind a magyar jogalkotó meg is teszi (adatkezelő-adatfeldolgozó), így a magyar adatkezelés-adatfeldolgozás fogalmak elkülönítése egyébként sem indokolt.[15]

A fogalmi alapvetés körében ki kell térni az adatvédelem – adatbiztonság – informatikai biztonság – információbiztonság kifejezésekre is. Az adatvédelem nem az adat, hanem a mögötte álló adatalany védelmét hivatott jogi eszközökkel biztosítani. A személyes adatok tényleges, informatikai és fizikai védelmére az adatvédelmi szabályozásban az adatbiztonság kifejezés használatos,[16] amelynek célja a személyes adatok „véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése” elleni védelem.[17] Az adatbiztonsági szabályok által garantált védelem mind az informatikai eszközökkel végzett, mind a manuális adatkezelésekre kiterjed.

[12] Szabó, 2005, 46. Ez a megközelítés egészen közel áll az amerikai felfogáshoz.
[13] Majtényi szerint a személyiség meghatározása nem is nagyon lehetséges: „A (személyes) privacy védelme beismerést és elismerést jelent. Annak elismerését, hogy tudjuk, az emberi lényeknek van személyiségük, de beismerjük, hogy nem tudjuk azt a jogban meghatározni” Majtényi, 2006, 67-68.
[14] Jóri, 2005, 154.
[15] Az adatvédelem további alapfogalmainak ismertetésétől eltekintek, mivel a 4.5 fejezetben a belső szabályozás kiépítése kapcsán az alapfogalmak bemutatásra kerülnek.
[16] Megjegyezzük, hogy az adatbiztonságot ennél tágabban, az informatikai biztonság szinonimájaként is lehet definiálni, mi azonban egyértelműen a szűkebb, személyes adatokra vonatkozó megközelítést követjük.
[17] 95/46/EK irányelv 17. cikk (1) bekezdés

Ehhez képest az informatikai biztonság „az informatikai rendszer olyan – az érintett[18] számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos."[19] Az informatikai biztonság tehát nem csak a személyes adatok, hanem bármilyen elektronikus adat technikai védelmét magában foglalja, ugyanakkor a védelem eszközei nem korlátozódnak kizárólag informatikai eszközökre (kriptográfiai megoldások, tűzfal stb.), hanem kiterjednek az informatikai infrastruktúra fizikai védelmére is.[20] Az informatikai biztonsági követelményeknek való megfelelés így az ezen eszközökkel kezelt személyes adatok biztonságát is szolgálja.[21]

Végül a legtágabb kifejezés az információbiztonság, amely bármilyen típusú adat bármely formában történő megjelenésének védelmét hivatott biztosítani,[22] azaz e fogalom kiterjed a manuálisan, papír alapon kezelt adatok védelmére is.[23]

1.2.2 Az adatvédelmi reform

A disszertáció témájának egyik aktualitását – egyben nehézségét is – az adja, hogy napirenden van az európai adatvédelmi szabályozás jelentős átalakítása. Amint azt a későbbiekben részletesen kifejtem, az elmúlt 10-15 év technológiai-társadalmi változásai az adatvédelem újragondolását tették szükségessé, amely folyamat az előző évtized végén meg is indult először az Európai Unió, majd 2011-ben, az 1981-es adatvédelmi egyezmény[24] 30. évfordulóján az Európa Tanács keretein belül is. Utóbbi eredményeként 2012. novemberére elkészült egy átfogó új javaslat, amely számos újítást tartalmaz az Egyezmény jelenleg hatályos szövegéhez képest.[25] Tekintettel azonban arra, hogy az Európai Unió adatvédelmi joga várhatóan továbbra is jóval magasabb követelményeket támaszt majd az adatkezelőkkel szemben, így a disszertáció során az Európai Unióban zajló folyamatokra koncentrálok.

Az EU adatvédelmi reformjának első jelentősebb állomásai a Bizottság által 2009-ben összehívott konferencia majd a nyilvános konzultáció megkezdése voltak. A konzultáció keretében számos üzleti és szakmai szervezettől, magánszemélytől érkezett módosítási javaslat. 2010-ben az Európai Tanács elfogadta az ún. Stockholmi Programot, amelynek hangsúlyos eleme a személyes adatok védelmének biztosítása az információs

[18] Itt az „érintett" kifejezés köznapi értelemben használatos
[19] Muha Lajos definícióját idézi Szádeczky, 2011, 7.
[20] Szádeczky, 2011, 7.
[21] Az informatikai biztonság tárgya azonban minden esetben az informatikai rendszer védelme, így a manuálisan kezelt adatok adatbiztonsági kérdései kívül esnek a hatókörén.
[22] Ld. részletesen Szádeczky összefoglalóját: Szádeczky, 2011, 9.
[23] Az adatbiztonság így az információbiztonság azon részeként is értelmezhető, amelynek célja a személyes adatok védelme, függetlenül az adathordozó jellegétől.
[24] Európa Tanács, 1981
[25] Az egyezmény jelentőségét az adja, hogy számos Európai Unión kívüli állam is részese, és a modernizáció kifejezett célja a területi hatály további bővítése, az adatvédelmi (minimum)szabályozás globalizációja. Az egyezmény tervezett új szövege – többek között – bevezeti az egyezménybe is az adatkezelési jogalapokat, bővíti az érintettek jogait, új adatkezelési elveket vezet be, vagy pontosítja a korábbiakat. Az új szövegtervezet természetesen támaszkodik az európai jogfejlődés elmúlt 30 éves eredményeire és az Európai Unió párhuzamosan zajló adatvédelmi reformja kapcsán kialakult álláspontokra, és ezeken nem is megy túl. Az egyezmény modernizációjáról ld. részletesen: Terwangne, 2014.

társadalomban. Az Európai Tanács ebben kifejezetten felkéri a Bizottságot arra, hogy „értékelje a különböző adatvédelmi eszközök működését, és szükség szerint nyújtson be további jogalkotási és nem jogalkotási kezdeményezéseket a fenti [személyes adatok védelmét biztosító] elvek hatékony alkalmazásának fenntartása érdekében”.[26] A Bizottság a felkérésnek eleget téve 2010. április 20-án elfogadta a Stockholmi Program végrehajtásáról szóló cselekvési tervet,[27] melyben hangsúlyozta, hogy az Uniónak gondoskodnia kell az adatvédelemre vonatkozó alapvető jog következetes alkalmazásáról.

A Bizottság ezt követően 2010-ben közleményt[28] bocsátott ki az adatvédelem átfogó megközelítéséről, az esetleges adatvédelmi reform főbb kérdésköreiről. Ezt újabb konzultációs időszak követte,[29] miközben folyt a műhelymunka az Európai Alapjogi Ügynökség és az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) és a 29-es adatvédelmi munkacsoport[30] műhelyeiben is – utóbbi számos nagyjelentőségű, az új szabályozási tervekre érdemi hatást gyakorló állásfoglalást vagy véleményt adott ki a 2009-2012 között.[31]

A Bizottság végül 2012. január 25-én hozta nyilvánosságra az új adatvédelmi szabályozás általa javasolt kereteit. A reformcsomag két jogszabály-tervezetet tartalmaz:

- Javaslat - Az Európai Parlament és a Tanács rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet),
- Javaslat - Az Európai Parlament és a Tanács irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.[32]

Az új irányelvre vonatkozó javaslatnak ugyan a maga területén igen jelentős szerepe lehet, jelen dolgozatban azonban az adatvédelem általános tendenciáira és általános szabályaira koncentrálunk, így az Európai Unió vagy valamely tagállam szektorális adatvédelmi szabályozására csak akkor térünk ki, ha ez valamely jogintézmény bemutatása során indokolt.

---

[26] Stockholmi Program, 2010, 11.
[27] Európai Bizottság, 2010a
[28] Európai Bizottság, 2010c
[29] A konzultáció részleteiről ld. bővebben Könyves-Tóth, 2013, 12-13. A két konzultáció válaszainak összefoglalása megtalálható a Bizottság weboldalain: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm [2014.01.05.], és http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm [2014.01.05.]
[30] Az adatvédelmi irányelv 29. cikke alapján létrejött, adatvédelemmel foglalkozó munkacsoport (a továbbiakban 29-es munkacsoport vagy adatvédelmi munkacsoport)
[31] Ezek közül a legfontosabb az adatvédelem jövőjéről szóló 2009-ben kiadott vélemény (WP29, 2009), de a Bizottság később láthatóan támaszkodott a 29-es munkacsoport elszámoltathatóságról szóló, 2010-ben kiadott 3/2010 számú véleményére (WP29, 2010b) is.
[32] Javaslat - Az Európai Parlament és a Tanács irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, COM/2012/010 final (a továbbiakban irányelv-tervezet)

Az általános adatvédelmi rendelet tervezetével kapcsolatos egyik legjelentősebb észrevétel a jogforrás formájával kapcsolatos: a Bizottság a jelenlegi irányelvet egy, a tagállamokban további jogalkotási aktus nélkül is közvetlenül alkalmazandó és közvetlenül hatályos jogforrással, rendelettel kívánja felváltani, ezáltal az irányelvvel elért harmonizációhoz képest egységesebb európai adatvédelmi szabályozást biztosítva (legalábbis ígérve).[33] A Bizottság szerint a hatályos irányelv „célkitűzéseit és alapelveit tekintve továbbra is érvényes, de nem akadályozza meg az Unión belüli személyesadat-védelem széttagolt megvalósítását, a jogbizonytalanságot és azt a széles körben elterjedt közvélekedést, miszerint az online tevékenység jelentős kockázatokat rejt magában", így egy szilárdabb, átfogóbb és következetesebb adatvédelmi politikára van szükség.[34]

További fontos tényező, hogy az adatvédelmi jog helye az Európai Unión belül is megváltozott, a Lisszaboni Szerződés elfogadása két jelentős változást is hozott e téren. Először is, az Európai Unió Alapjogi Chartájának[35] kötelező jogszabályként való elismerésével[36] a személyes adatok védelme önállóan nevesítve, a magán- és családi élet védelmétől elkülönülten is megjelent az alapvető jogok között, azaz Európai szinten is közvetlen alapjogvédelemben részesül. Másodszor, a Lisszaboni Szerződéssel módosított Európai Unió Működéséről szóló Szerződés 16. cikk (2) bekezdése 2008-ban új, önálló jogalapot teremtett az adatvédelmi szabályok elfogadására: az EUMSZ felhatalmazza az Európai Parlamentet és Tanácsot, hogy rendes jogalkotási eljárás keretében megalkossa a személyes adatok feldolgozása tekintetében történő védelmére, valamint az ilyen adatok szabad áramlására vonatkozó szabályokat.[37] E felhatalmazás az állami és a magánszektorra egyaránt kiterjed.[38]

A Bizottság Rendelettervezete hatalmas visszhangot kapott. Amint azt később bemutatom, a tervezet igen jelentős módosításokat javasol az adatvédelem területén, korántsem a jelenleg hatályos szabályozás finomhangolásáról van szó, hanem egy új, az adatkezelőket középpontba állító megközelítésről. A Rendelettervezettel kapcsolatban tucatnyi publikáció jelent meg, és a jogalkotási folyamat során több mint 3000 (!) módosító indítvány érkezett. A hatalmas érdeklődésnek is köszönhetően az Európai Parlament illetékes Állampolgári Jogi, Bel- és Igazságügyi Bizottságának[39] majd két évébe telt, míg kidolgozott egy kompromisszumos szövegtervezetet[40] az Európai Parlament számára. A

[33] A tagállami végrehajtás – már csak a személyes adatok védelmével kapcsolatos kisebb nagyobb kulturális különbségek miatt is – a rendeleti forma esetén is fenntarthat különbözőségeket, amelyek azonban vélhetően a jelenlegiekhez képest kisebbek lesznek.
[34] Bizottsági Rendelettervezet, Indokolás, 2.
[35] Az Európai Unió Alapjogi Chartája 2012/C 326/02 (Továbbiakban Alapjogi Charta), 8. cikk.
[36] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata 2012/C 326/01 (Továbbiakban EUSZ), 6. cikk
[37] Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata 2012/C 326/01 (Továbbiakban EUMSZ), 16. cikk (2) bekezdés
[38] WP29, 2009, 5.
[39] A továbbiakban: LIBE Bizottság
[40] Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012, Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht, (kifejezetten e dokumentum a továbbiakban: LIBE Javaslat. Az Európai Parlament által elfogadott verziója tartalmában megegyezik a LIBE Javaslattal)

LIBE javaslat az eredeti bizottsági szövegtervezetet nagymértékben megváltoztatta, és – némi meglepetésre – alapvetően tovább szigorított a szabályokon.[41]

A LIBE szövegtervezete mögött valódi támogatás állt: az Európai Parlament 2014. március 12-i plenáris ülésén óriási szótöbbséggel (621 igen, 10 nem, és 22 tartózkodás mellett), változtatás nélkül elfogadta a LIBE Bizottság javaslatát, amely így a jogalkotási folyamatban a Parlament szövegtervezete[42] lett, és amelyet ezt követően az Európai Unió Tanácsa tárgyal.

Az adatvédelmi reform további folytatását az eddigi pozitív folyamatok ellenére számos, elsősorban üzleti[43] és politikai okokból eredő bizonytalanság övezi. A szövegtervezet Tanácson belüli támogatása néhány vitás pont miatt erősen kérdéses, 2014 folyamán pedig új Európai Parlament és új Bizottság alakul(t). E testületeknek a korábbiaktól eltérő szakmai és/vagy politikai álláspontja és különösen elkötelezettsége lehet.[44] A disszertáció során a kézirat lezárásának napján nyilvános legújabb szövegtervezetet vesszük figyelembe, amely jelenleg az Európai Parlament szövegtervezete.

1.3 Önszabályozás és szervezeti szabályozás

A disszertáció bevezető fejezetében indokolt röviden áttekinteni az önszabályozás és a szervezeti szintű szabályozás egymáshoz való viszonyát is. Itt csupán az önszabályozással kapcsolatos alapfogalmakat szeretném bemutatni, különös tekintettel arra is, hogy a vonatkozó szakirodalom elsősorban valamely terület iparági szintű önszabályozására fókuszál (sok esetben elismerve egyébként a fogalom ennél tágabb jelentését), és ebből a nézőpontból elemzi az abban rejlő lehetőségeket, azok előnyeit, hátrányait. A dolgozat egy olyan önszabályozási eszközre: a szervezeti szintű (belső) szabályozásra koncentrál, amellyel az önszabályozással foglalkozó irodalom ritkábban foglalkozik. Ezzel együtt is érdemes azonban áttekinteni az önszabályozás funkcióit, és főbb jellemzőit (előnyeit-hátrányait), már csak azért is, hogy a szervezeti szintű szabályozás formáit megfelelően elhelyezhessem az önszabályozás rendszerében.

Az önszabályozás és társszabályozás számos ágazat területén megtalálható, rendszerint egyedi sajátosságokkal. Ismert példák a domain-szabályozás, a médiajog (ideértve az online tartalomszabályozást is), a reklámjog, az energiajog, a fogyasztóvédelem, a pénzügyi szektor és végül a személyes adatok védelmének szabályozása is. Utóbbi területtel részletesen is foglalkozom: az adatvédelem önszabályozási formáit, ideértve a szervezeti szintű szabályozást is, a 4. fejezet ismerteti részletesen.

---

[41] Igaz, számos rendelkezésnél gyengítette is a védelem szintjét.

[42] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 (a továbbiakban Rendelettervezet)

[43] A szigorúbb adatvédelmi szabályok számos nagyvállalat számára jelentős többletköltséget okozhatnak, így az adatvédelmi reform során sokan erőteljes lobbitevékenységet folytatnak. A http://lobbyplag.eu weboldalon jól végigkövethetők a módosító javaslatok mögötti iparági érdekek.

[44] A márciusi parlamenti támogatás mértéke ugyanakkor azt sugallja, hogy egy más politikai összetétel önmagában nem befolyásolja a Parlament álláspontját.

1.3.1 Önszabályozás, társszabályozás, szervezeti szabályozás

Az önszabályozás egy gyakran hivatkozott Európai Uniós dokumentum, a jogalkotás minőségének javításáról szóló, az Európai Parlament, az Európai Unió Tanácsa és az Európai Bizottság között 2003-ban létrejött intézményközi megállapodás szerint „a gazdasági vállalkozások, társadalmi partnerek, nem-kormányzati szervezetek, egyesületek azon lehetőségét foglalja magában, hogy egymás között és saját maguk számára (európai szinten) közös iránymutatásokat (így különösen magatartási kódexeket vagy iparági megállapodásokat) fogadjanak el."[45]

A jogirodalomban található felosztás szerint „a »tiszta önszabályozás« (pure self-regulation) kizár bármiféle állami vagy más külső beavatkozást, az ellenőrzés lefolytatására kizárólag a szabályozott szervezetek jogosultak."[46] Előfordul ugyanakkor, hogy az állam kifejezetten utal az önszabályozásra, és ehhez valamilyen jogi relevanciát is kapcsol.[47]

Társszabályozásnak tekinthető az a helyzet, amelyben az állami szerepvállalás ennél továbbmegy: az állam kijelöli a szabályozási kereteket, például meghatározza az elérendő célokat, vagy egyes általános szabályokat; illetve a normatív szabályok (kódexek) létrejötte és/vagy azok érvényesítése a szakmai és állami szervek együttműködésének köszönhető, például egy adott magatartási kódexet az állam (valamely szerve) hagy jóvá.[48]

A fenti jelenségek között a gyakorlatban nincs éles határvonal,[49] így az állami szerepvállalás mértéke sokkal inkább skálaként írható le a teljes (hagyományos) jogi szabályozástól a „tiszta önszabályozásig." Erre tekintettel az önszabályozás kifejezést az ön- és társszabályozásra egyaránt használjuk, mivel végső soron apró részletkérdéseken múlik, hogy pontosan milyen mechanizmusról is van szó, így a társszabályozás tekinthető az önszabályozás egyik formájának is.

A fenti fogalmak azonban elsősorban iparági önszabályozási szintet feltételezve értelmezhetőek. Az önszabályozás azonban ennél tágabban is érthető, eszerint nem jelent mást, mint „a nem állami" szabályozást, és átfogja a szervezetek általi magán-szabályalkotás legkülönbözőbb formáit is.[50] A dolgozat során az önszabályozást tágan értelmezve beleértem az iparági szintnél alacsonyabb, szervezeti szintű, azaz egy-egy szervezetre vagy szervezetcsoportra (pl. vállalatcsoportra) vonatkozó belső szabályozást is. Egy adott szervezet kizárólag saját magára vonatkozó szabályai a média területén is az önszabályozás rendszerének részét képezi: „a magas szintű szakmai önszabályozás […] eleme a médiaszolgáltatók által elfogadott, szerkesztői politikát meghatározó szakmai irányelvek lefektetése", mint például a BBC iránymutatásai.[51] Az adatvédelem területén

[45] European Parliament – European Commission, 2003, 3. (22. pont). A magyar fordítást ld. Nagy, 2012, 143.
[46] Bartle és Vass gondolatait idézi Csink – Mayer, 2012, 35.
[47] Csink – Mayer, 2012, 35.
[48] Csink – Mayer, 2012, 38-39.
[49] Nagy, 2012, 142.
[50] Nagy, 2012, 142.
[51] Csink – Mayer, 2012, 44. Ennek elsősorban a „belső" szerkesztői függetlenség biztosításában van szerepe. Emellett pl. az RTL Klub Való Világ 4 című műsorával kapcsolatos szerkesztési kódexét a szerzők – igaz, különösebb elméleti okfejtés nélkül – szintén az önszabályozás részének tekintik. Ld. Bakos-Krausz, 2011

szintén találhatók erre vonatkozó utalások: Bennet és Raab az adatvédelmi önszabályozás eszközeinek tekinti az (1) adatvédelmi nyilatkozatokat (privacy commitment), (2) a magatartási kódexeket (privacy codes of practice), akár egy szervezetre, akár egy szektorra vonatkozóan, (3) a szabványokat (privacy standards) és végül (4) a tanúsítványokat (privacy seals).[52] Megjegyezzük, hogy az adatvédelem területén ezen szabályrendszerek érintettre gyakorolt hatása akár jóval nagyobb is lehet, mint az iparági önszabályozásé.[53]

Az önszabályozás fogalmát tehát a szervezetek belső szabályozására is kiterjesztem, amely tulajdonképpen szerződéses (különösen általános szerződési feltételekkel szabályozott) viszonyokat is jelenthet, ez azonban önmagában szintén nem ismeretlen más önszabályozási formáknál sem: a Domainregisztrációs Szabályzat a domainigénylők számára ÁSZF-ként jelenik meg, míg a pénzügyi területen elfogadott hitelezési Magatartási Kódex[54] – önkéntes csatlakozás alapján – az üzletszabályzat részévé válik.[55] A szervezeti szabályozás ön- és társszabályozás is lehet: általában az államnak alapvetően nincs szerepe a normák megalkotásban, de egyes területeken jogszabályok meghatározhatnak bizonyos szempontokat (például az egészségügyi szolgáltatók adatkezelési szabályzata tekintetében),[56] emellett pedig az állam részt vehet a belső normák közvetett kikényszerítésében (különösen, ha azok a törvényi szabályokhoz képest nem tartalmaznak új szabályokat, hanem azok értelmezését, végrehajtását szolgálják).

1.3.2 Az önszabályozás funkciói

Az önszabályozás egyes esetekben teljes egészében helyettesítheti az állami szabályozást egy adott területen, akár azért, mert az adott terület szabályozására még nem került sor, akár azért, mert az állam tudatosan nem szabályoz egy adott területet.[57] Ide tartozik az az eset is, amikor állami szabályozás mellett az érintett szereplők további normatív szabályokat állapítanak meg, olyanokat, amelyek tehát az önszabályozás nélkül nem léteznének.

A különböző önszabályozó normáknak lehet az állami szabályozást pontosító, magyarázó, értelmező, mintegy „végrehajtási szabály" jellegű szerepe is: ilyen esetekben nem új normatív kötelezettségről van szó, hanem valamely állam által előírt szabály tartalommal történő kitöltéséről, konkretizálásáról.[58] Ennek azért lehet különös jelentősége, mert ilyen esetekben e szabályok megsértése a jogszabályok megsértését is jelentheti, már csak azért is, mert e szabályok sokszor az adott terület bírósági-hatósági esetjogán, értelmezésén alapulnak.

---

[52] A szerzők külön nevesítik a Safe Harbour Egyezményt is az önszabályozás eszközei között. Bennet és Raab önszabályozással kapcsolatos felosztását ld. Bennet-Raab, 2006, 151-175.

[53] És akár szélesebb kört is elérhet. Valamely globális adatkezelő, pl. a Facebook közösségi oldal privacy policy-je összességében jelentősebb hatással van az adatvédelem tényleges szintjére, mint például egy államon belüli, néhány vállalatot érintő iparági szabályozás.

[54] A lakosság részére hitelt nyújtó pénzügyi szervezetek ügyfelekkel szembeni tisztességes magatartásáról szóló Magatartási Kódex

[55] Kovács – Polyák, 2012, 125.

[56] Ld. 62/1997. (XII. 21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről

[57] Az önszabályozást gyakran tekintik az iparág állami szabályozás előli menekülésének is. Ld. például az Egyesült Államok iparági adatvédelmi önszabályozását, Jóri, 2005, 53.

[58] Kissé más megközelítésben, de ilyen funkcióra való utalást ld. még Nagy, 2012, 144.

1.3.3 Normaalkotás és normaérvényesítés

A vonatkozó szakirodalomban ugyan néha összemosódik, de fontosnak tartom elméleti szinten is megkülönböztetni az önszabályozás során a szabályalkotásra illetve a szabályok betartásának ellenőrzésére (compliance-check) és kikényszerítésére szolgáló mechanizmusokat. Az első a követendő magatartási forma előírására (norma megalkotására), míg a második e normák különböző szervezetek általi felügyeletére, kikényszeríthetőségére utal.[59] E két jelenség kétségkívül sokszor összekapcsolódik egymással, de ez korántsem szükségszerű. Az egyértelműen (ön)felügyeleti eszköznek tekinthető adatvédelmi audit például jellemzően a jogszabályok érvényesülését is vizsgálja, míg egyes önszabályozás keretében elfogadott normák megsértése – ilyen-olyan jogtechnikai megoldással – állami szervek által is szankcionálható.[60]

1.3.4 Az önszabályozás előnyei, hátrányai

Az önszabályozással kapcsolatos egyik fontos jellemző a hatékonyság, a szabályozás magasabb hatásfoka, mely abból eredhet, hogy a szabályozásban alapvetően iparági szereplők vesznek részt, akik megfelelő szakértelemmel rendelkeznek az adott területen,[61] így lehetővé válik a „speciális iparági tudás" hasznosítása.[62] Ugyanakkor kételyek merülhetnek fel a tekintetben, hogy az iparág szereplői ezt a tudást valóban a közjó érdekében, és nem saját érdekeiknek megfelelően hasznosítják. Fennáll a kockázata annak, hogy a szabályozás egyoldalú iparági befolyás alá kerül.[63]

Gyakran hangoztatott érv az önszabályozás rugalmassága. Egy kevésbé formalizált működésű szakmai szervezet elvileg könnyebben tudja a szabályait módosítani, mint a kormányzat.[64] Ezért különösen kedvelt eszköz azokon a területeken, ahol a gyors technológiai fejlődés az életviszonyok gyors változását eredményezi: a jog sokkal inkább alkalmas az alapvetően stabil, mintsem a gyorsan változó életviszonyok szabályozására. A „jogszabály […] a szabályozott viszonyok tartós jövőbeli rendezésére törekszik. A jog tartósság-igénye élesen szemben áll a technológiai – és az azzal párhuzamos társadalmi – fejlődés gyorsaságával."[65] Meg kell azonban jegyezni, hogy az ismert és működő önszabályozási területeken e gyorsaságnak a gyakorlatban nem nagyon kellett érvényesülnie. Jó példa erre a domainigénylés nemzetközi, európai szintű[66] és magyarországi szabályozása, amely kifejezetten „stabil" területnek mondható: a vonatkozó szabályok változása egyáltalán nem gyakoribb, mint általában a jogszabályok módosítása.

Az önszabályozás a szabályok érvényesülését is hatékonyabbá teheti, mivel az érintettek maguk is részt vesznek a szabályok elfogadásában, így nagyobb lehet az önkéntes

[59] Nagy, 2012, 143-144.
[60] E megkülönböztetést a 4.1 fejezetben az adatvédelmi önszabályozással kapcsolatban részletezem.
[61] Csink – Mayer, 2012, 40.
[62] Nagy, 2012, 150.
[63] Nagy, 2012, 151., Csink – Mayer, 2012, 41.
[64] Csink – Mayer, 2012, 40.
[65] Polyák, 2002, 3.
[66] A .eu domain nevekkel kapcsolatos szabályozás nem is önszabályozás keretében, hanem rendelet, azaz jogszabály formájában jelenik meg [a Bizottság 874/2004/EK rendelete (2004. április 28.) a.eu felső szintű domain bevezetésére és funkcióira vonatkozó általános szabályok, valamint a bejegyzésre irányadó elvek megállapításáról]

jogkövetési hajlandóság.[67] Ez a tényező felértékelődik azokon a határokon átnyúló területeken (pl. az Internetes szolgáltatásokkal kapcsolatos kérdéseknél), ahol az állami jogérvényesítést eleve alacsony hatékonyságú.[68] Az önszabályozás megemelheti a szervezetek szakmai színvonalát, és arra ösztönözheti a szereplőket, hogy igyekezzenek a „felmerülő problémákat »házon belül« megoldani, ahelyett, hogy indokolatlanul sokszor forduljanak a szabályozóhoz". Ugyanakkor ellenérvek is felhozhatók: a piaci érdekek a jogérvényesítés során is kiszoríthatják az állampolgárok, fogyasztók érdekeit, az önszabályozás „önkiszolgálássá" válhat, a végrehajtás elnehezülhet.[69] Ráadásul egyes szereplők ki is maradhatnak az önszabályozás hatálya alól, így az ő esetükben egyáltalán nem érvényesülnek a (vélt) előnyök.

További előny lehet(ne), hogy a normaalkotás és vitarendezés önszabályozás keretében való megoldása az állam számára költségcsökkenésként jelentkezik. A rendszer összességében azonban nem feltétlenül olcsóbb, csupán az állam helyett az iparági szereplők viselik a költségeket.[70]

Egyes területeken az önszabályozás létjogosultságát más tényezők is indokolhatják: a média területén például az a tény, hogy a média egyik funkciója az állam ellenőrzése, azaz az állami működés a médiatartalmak tárgya, így indokolt, ha nem kizárólag állami szervek vesznek részt e tartalom felügyeletében.[71]

Az önszabályozás kapcsán egy további fontos negatív jellemzőt, a verseny potenciális korlátozását is érdemes megemlíteni. A magas szintű, minőségi szolgáltatást célzó iparági intézkedések egyben belépési korlátként jelentkezhetnek a potenciális új piacra lépők számára, különösen, ha más korlátozások pl. reklámkorlátozások is érvényesülnek.[72] Más esetekben ugyanakkor éppen az önszabályozásban részt vevő szervezetek kerülnek hátrányba azáltal, hogy betartanak olyan szabályokat, amelyeket a versenytársaik nem, és ez többletköltséget okoz számukra. Az agresszív üzletpolitikájú vállalkozások ráadásul kihasználhatják az ágazati önszabályozás miatt fennálló fogyasztói bizalmat, hosszabb távon éppen ezzel rontva a teljes szektor megítélését.[73]

Az önszabályozással kapcsolatos előnyök és hátrányok áttekintésekor ismét rá kell mutatnom arra, hogy e jellemzők alapvetően az iparági szintű önszabályozásra, és nem a szervezeti szintű (belső) szabályozásra irányadók. Amennyiben az önszabályozás nem a hiányzó szabályok pótlását, hanem a meglévő, akár egészen részletes szabályok értelmezését, tartalommal való megtöltését, helyi (szervezeti) viszonyokra való adaptálását szolgálja, és ha az állam nem vonul ki teljesen a jogérvényesítésből, hanem mintegy mögöttes szervezetként – különböző jogtechnikai megoldásokkal – részt vesz a szabályok érvényesítésében, akkor kialakítható egy olyan társszabályozási keret, amelyben a fenti hátrányok jó része kiküszöbölhető – igaz, egyes előnyök is csak korlátozottan

[67] Nagy, 2012, 150.
[68] Polyák, 2002, 3, és Bayer, 2002, 252.
[69] Csink – Mayer, 2012, 41.
[70] Nagy, 2012, 150, Csink – Mayer, 2012, 41.
[71] Tófalvy, 2013, 87.
[72] Nagy, 2012, 151.
[73] Ez jellemző például az Egyesült Államok egyes szektorainak adatvédelmi önszabályozására, Banisar, 2001, 26.

érvényesülnek. Álláspontom szerint a 4. fejezetben bemutatott, az adatkezelők szintjén elfogadott belső szabályozási rendszer éppen megfelel e kritériumoknak.

1.4 A kutatás tézisei és módszertana

A fentiek alapján a disszertáció egymással szorosan összefüggő tézisei a következők.

1) Az elmúlt évtized technológiai fejlődése az adatvédelmi szabályozást (újra) olyan kihívások elé állította, amelyre jelen formájában nem tud hatékony választ adni. A disszertáció során igazolom, hogy ennek következtében az adatvédelem alapjait érintő új megközelítésre és szabályozási koncepcióra van szükség.
2) Az új megközelítés központi eleme, hogy az „érintett-központú" szabályozás felől nagymértékben el kell tolódni az „adatkezelő-központú" szabályozás felé.
3) A dolgozat során kimutatom, hogy e hangsúlyeltolódás következtében a korábbiakhoz képest jóval nagyobb szerepet kap az adatkezelők belső szabályozása, amely az önszabályozás egyik eszközének tekinthető.
4) A belső szabályozással történő adatvédelmi megfelelés (compliance) korántsem triviális feladat, de kialakítható egy belső szabályozásra vonatkozó útmutató, amely az adatkezelők számára mintaként szolgálhat. A disszertációban bemutatom ennek kiindulópontjait.

A tézisek nagymértékben meghatározzák a dolgozat szerkezetét és a kutatás módszertanát is. A 2. fejezetben részletesen áttekintem az adatvédelem eddigi fejlődését, hogy választ kapjak arra a kérdésre, miként alakult ki az adatvédelem jelenlegi, „érintett-központú" rendszere. Ennek érdekében áttekintem az elmúlt negyven-ötven év technológiai fejlődését, annak az egyén magánszférájára gyakorolt hatását, valamint az adott kor adatvédelmi szabályozásának főbb jellemzőit. A fejezet elsősorban történeti-leíró módszert követ, és interdiszciplináris megközelítést alkalmaz. A technológia és társadalmi fejlődés kapcsán, ahol csak lehetett, törekedtem az adott témakör eredeti – tehát adatvédelmi jogi szempontokkal még át nem itatott – forrásait is használni.

A 3. fejezetben – az első tézis igazolása érdekében – az adatvédelmi szabályozást érő, a technológia fejlődéséből, illetve a már működő technológiák egészen újfajta alkalmazásából, valamint a felhasználói attitűdváltozásokból eredő kihívásokat és a jelenlegi adatvédelmi rezsim kritikáját tekintem át. Ezt követően felvázolom egy újgenerációs, „adatkezelő-központú" adatvédelmi szabályozás főbb elemeit, és ennek fényében elemzem az új adatvédelmi Rendelettervezet vonatkozó rendelkezéseit. Rámutatok arra is, hogy az adatkezelők növekvő szerepe milyen új kihívásokat jelent számukra, és az ezekre adott válaszokban milyen szerepe lehet egy tudatosan kialakított belső szabályozásnak. E fejezet során egyrészt rendszerező és leíró-kritikai, másrészt, az új szabályozási megközelítés kapcsán, kritikai-elemző módszert alkalmazok.

Tekintettel arra, hogy az adatkezelők belső szabályozása az önszabályozás egyik formájának tekinthető, a 4. fejezetben rendszerező módszert követve tekintem át az adatvédelmi önszabályozás fontosabb eszközeit, ideértve az adatkezelők belső szabályozását is. Kritikai szemléletű elemzésnek vetem alá a már működő önszabályozási

eszközöket, és következtetéseket vonok le azok létjogosultságával és funkcióival kapcsolatban. Végül a fejezet végén javaslatokat teszek egy belső szabályozási rendszer kialakításának első lépéseire, amelynek deklarált célja, hogy praktikus segítséget nyújtson az adatkezelők számára az adatvédelmi megfelelés (compliance) eléréséhez. E fejezet kifejezetten gyakorlatorientált megközelítést alkalmaz, és alapul szolgálhat a témakör további kutatásához.

2. AZ ADATVÉDELMI JOG EURÓPAI FEJLŐDÉSE

2.1 Bevezető gondolatok

Az adatvédelmi szabályozás jelenleg zajló paradigmaváltásának megértéséhez, valamint a technológia fejlődés adatvédelmi szabályozásra gyakorolt hatásának feltárásához elengedhetetlen az adatvédelem eddigi rövid, de intenzív szabályozás- és elmélettörténetének áttekintése.

2.1.1 A korszakolás jelentősége

Az adatvédelmi jog viszonylag rövid története ellenére a szakirodalom a szabályozás több generációját különbözteti meg, amelyek különböző – de mindannyiszor a technológia fejlődéséhez, és az ehhez szorosan kapcsolódó társadalmi változásokhoz köthető – kihívásokra reagálva hasonló szabályozási célokat eltérő megközelítéssel igyekeztek megvalósítani. Az adatvédelemmel foglalkozó szerzők álláspontja ugyanakkor nem egységes a tekintetben, hogy pontosan hány generációt érdemes megkülönböztetni, illetve hogy az egyes nemzetközi, európai és nemzeti jogforrások pontosan melyik generációhoz tartoznak.

Gyakran idézett forrás Mayer-Schönberger Viktor esszéje,[74] aki az összeurópai adatvédelmi szabályozást (1998-ig) vizsgálva négy generációt különböztet meg. A német jogirodalom – elsősorban a német adatvédelmi jog fejlődését elemezve – szintén gyakran használja a generációs felosztást és a fejlődés korszakolását.[75]

A magyar jogirodalomban először Majtényi László foglalja össze az adatvédelem korszakait, és három generációt különböztet meg: az első generációs szabályok a 70-es években fejlődtek ki, és az állami, számítógépes (legalább részben automatizált) nyilvántartásokkal szemben igyekeztek valamilyen védelmet biztosítani. A második generációs szabályok a 80-as, 90-es években jelentek meg, és a jogalkotó már nem csak az automatizált, de a papíralapú nyilvántartásokat is a szabályozás hatálya alá vonta. Végül Majtényi szerint a harmadik generációs szabályok főbb jellemzői az európai integráció sajátosságainak figyelembe vétele, és a szektorális szabályok megjelenése.[76]

A magyar jogirodalomban az eddigi legrészletesebb elemzés az adatvédelem történetéről Jóri András munkásságában található. Jóri szintén három korszakot különböztet meg, de a 80-as, 90-es évek fejleményeit egy szabályozási generációhoz sorolja, és a harmadik generációs szabályozás egyes elemeinek megjelenését a német Teledienstedatenschutzgesetz (TDDSG)[77] 1997-es megalkotásához köti.[78]

[74] Mayer-Schönberger, 1998.
[75] Bäumler és Bizer felosztásáról ld. Jóri, 2005, 22-23., Bodenschatz 2010-ből visszatekintve is négy korszakot különböztet meg, Bodenschatz, 2010, 31-39.
[76] Majtényi, 2003, 582-583.
[77] Gesetz über den Datenschutz bei Telediensten (TDDSG) 1997 I 1871.
[78] Jóri, 2005, 24-66.

Végül Majtényi felosztásához nyúl vissza később Hegedűs Bulcsú is. Ő a második generációs szabályozás fő jellemzőjeként azt emeli ki, hogy annak hatálya már az üzleti élet gyakran igen adatéhes szereplőire is kiterjed.[79] Emellett nála is megjelenik egy újabb – negyedik – generációs szabályozás gondolata, amelynek főbb jellemzői az önszabályozás, az Internettel kapcsolatban megjelenő adatvédelmi kérdések és a magánszférát erősítő technológiák megjelenése.[80]

E vázlatos áttekintésből látható, hogy több közös pont ellenére sem lehetséges a generációk közötti korszakváltások határát egyértelműen kijelölni, és ebből következően az egyes nemzetközi, európai vagy nemzeti szintű jogforrásokat egyértelműen egyik vagy másik generációhoz tartozónak tekinteni. A generációs felosztásnál valójában nagyobb jelentősége van az egyes szabályozások főbb jellemzőit és a fejlődés tendenciáit kutatni. Egy adott szabályozási modellre jellemző jelenség vagy jogintézmény rendszerint jóval korábban megjelenik a jogirodalomban. Emellett egy-egy időszakban elfogadásra kerülhetnek olyan jogszabályok is, amelyek már inkább egy későbbi generáció „előhírnökei".[81] Ezzel együtt is a megfelelő korszakolás átláthatóvá teszi a történeti áttekintést, így indokoltnak tartom az adatvédelem fejlődését mégiscsak e logikai séma mentén bemutatni.

A generációk vagy korszakok számának meghatározásakor azt gondolom, hogy csak a valóban jelentős, koncepcionális kérdésekben is újítást jelentő változások esetén érdemes új generációs szabályozásról beszélni. Így az adatvédelem története során alapvetően két különböző nagy szabályozási korszak (generáció) különböztethető meg, azzal, hogy az elmúlt évtizedben megjelentek olyan tendenciák, amelyek egy új, harmadik generációs adatvédelmi szabályozás kialakulása felé mutatnak. A disszertáció egyik kiindulópontja tehát az, hogy az elmúlt egy-másfél évtizedben bekövetkezett technológiai és társadalmi változások következtében az adatvédelmi szabályozás újra megérett az átfogó reformra, és olyan új szabályokra van szükség, amelyek az eddigiektől jelentősen eltérő hangsúlyokat állapítanak meg. Az Európai Bizottság adatvédelmi rendelettervezete nagyjából megfelel ezen kritériumnak, így az (pontosabban annak a kézirat lezárásakor fellelhető szövegverziója) a harmadik generációs szabályozás (korántsem tökéletes) „mintaszabályozásának" tekinthető.

2.1.2 Technológia-társadalom-jog – az áttekintés módszertana

Az alábbiakban részletesen áttekintem az adatvédelmi szabályozás három korszakát. Az első két szabályozási generációt történeti, leíró jelleggel e fejezet keretein belül, a legújabbat pedig a paradigmaváltásról szóló következő fejezetben. Az egyes szabályozási generációk elemzését az adott kor technológiai és társadalmi hátterének bemutatásával kezdem, mivel az adatvédelmi szabályozás fejlődésének megértéséhez szükséges ennek vizsgálata.

[79] Hegedűs, 2013, 137-138.
[80] Hegedűs, 2013, 139-145.
[81] Ilyennek tekinthető például az 1977-es BDSG, amely az elfogadás időpontja alapján az adatvédelmi jogalkotás első korszakához tartozik, de egyébként az állami szféra mellett már a magán adatkezelőkre is vonatkozott, és hangsúlyos szerepet kap az érintett hozzájárulása, mint adatkezelési jogalap. E tendenciák általánosan azonban csak később terjednek el, és inkább a második generációs szabályozásra jellemzőek.

A technológia és társadalom egymásra gyakorolt hatása önmagában is széles körben tárgyalt, gazdag jogirodalommal rendelkező témakör.[82] Az adatvédelem fejlődése szempontjából ezzel kapcsolatban három elméletre érdemes utalni: (1) A technológiai determinizmus a technológia fejlődésének autonómiáját hangsúlyozza, amely teljes egészében meghatározza a társadalmat – ez alapján a társadalmi változások elsődleges mozgatórugója a technológia fejlődése.[83] (2) A technológiai neutralizmus ezzel szemben azt mondja, hogy a technológia önmagában semleges, kizárólag a – társadalom által meghatározott – felhasználási mód lehet „jó" vagy „rossz", azaz a technológia társadalmi kontroll alatt marad.[84] (3) A technológiai realizmus igyekszik a kérdéskör komplexitását hangsúlyozni, és sokkal inkább kölcsönös egymásra hatásként értelmezni a technológia, társadalom és közpolitika viszonyát.[85] Egyetértek Castellsszel, aki e közvetítő nézetet kifejtve megállapítja, hogy a „technológia természetesen nem határozza meg a társadalmat. Ugyanakkor a társadalom sem írja elő a technológiai változás irányát, mivel a tudományos felfedezések és a technológiai újítások folyamatába, illetve ezek társadalmi alkalmazásába sok tényező beleszól – köztük az egyéni feltalálókészség és a vállalkozó szellem – úgyhogy a végső eredmény a kölcsönhatások bonyolult mintázatától függ".[86]

Az adatvédelem történetének elemzése során is látható, hogy a technológia jellege, költségei és elérhetősége nagymértékben meghatározza azok felhasználóit, és így az adatkezelések alanyait is – míg e tényezők együttesen befolyásolják az adatkezelésekkel járó, magánszférára gyakorolt potenciális hatásokat (elsősorban veszélyeket). Egy-egy új technológia használata gyakran lerombol bizonyos, a magánszférát korábban védő természetes korlátot azzal, hogy valamely potenciálisan vagy ténylegesen sértő magatartást (akár állami cselekvést, akár üzleti gyakorlatot) lehetővé vagy legalábbis a korábbiaknál jóval könnyebben vagy olcsóbban elérhetővé tesz.[87] A technológia okozta társadalmi változásokkal (amely, mint látható, inkább bonyolult kölcsönhatásként jellemezhető) kapcsolatos közgondolkodás – Európában elsősorban az információs társadalommal kapcsolatos diskurzus keretein belül – pedig jelentősen befolyásolta azt, hogy e

[82] Áttekintő jelleggel ld. például Regan, 1995, 10-15. és Ropolyi, 2006, 68-71.

[83] Langdon Winner gondolatait idézi Regan, 1995, 11. A technológiai determinizmus további ismert képviselője Marshall McLuhan, aki a társadalom összes változását lényegében egyetlen tényezőre, a kommunikációs eszközök és lehetőségek változására vezette vissza. A technológia és a kommunikációs szabályozás kölcsönhatását ld. részletesen Polyák, 2011. 31-34.

[84] Regan, 1995, 11., Az elmélet kritikáját ld. Zágoni, 2000, 24.

[85] Regan, 1995, 11.

[86] Castells, 2005, 38. Később Castells kiemeli, hogy a társadalmak jövőjét inkább az határozza meg, hogy képesek-e birtokba venni az adott technológiát. Példaként a könyvnyomtatás kínai feltalálását hozza, amely azonban a nagyfokú írástudatlanság miatt jóval kisebb hatású volt, mint Európában. Castells, 2005, 41, 67.

[87] Csak néhány, a dolgozatban később részletesen is elemzett példa: az automatizált állami nyilvántartásokban könnyebb és gyorsabb a keresés, egyszerűbb az adatbázisok összekapcsolhatósága; az elektronikus úton küldött direktmarketing üzenetek költsége töredéke a papír alapon küldött reklámok költségének; a kamerarendszerek fejlődésével egyre nagyobb terület egyre jobb minőségben figyelhető meg, az arcfelismerő rendszerek az azonnali azonosítást is lehetővé teszik; a hatalmas felbontású fényképezőgépekkel egyre nehezebb olyan tömegfelvételt készíteni, amelyen nem látszódnak felismerhetően az azon szereplők arcvonásai; egy új, mélyebb keresési és szűrési lehetősége bevezetése egy közösségi oldalon alapvetően befolyásolja, hogy milyen adat milyen kontextusban jelenhet meg mások számára (és így azt is, hogy ennek fényében mit kívánna az érintett nyilvánosságra hozni vagy megosztani); stb.

jelenségekre a társadalom, előbb-utóbb a jogalkotás eszközével (is) élve, illetve a jogszabályok végrehajtása során, miként reagál.[88]

Ezek alapján tehát egy adott kor technológiai és társadalmi hátterének bemutatását követően a korszak adatvédelmi szabályozásának főbb jellemzőit elemzem. Mielőtt azonban sor kerül az európai adatvédelmi szabályozás 1970-től tartó történetének bemutatására, érdemes vázlatosan áttekinteni a magánszféra-védelem korábbi előzményeit is.

2.1.3 Történeti előzmények

Az adatvédelmi jog kialakulása alapvetően az 1970-es évekre kibontakozó technológiai forradalomra adott válaszlépésként értékelhető. Ugyanakkor már az első magánszféra-védelemmel foglalkozó tanulmány, Samuel D. Warren és Louis D. Brandeis sokat hivatkozott,[89] 1890-ben a Harvard Law Review hasábjain megjelent, „The Right to Privacy" című tanulmánya[90] is alapvetően az adott kor technológiai és társadalmi változásaira reagált. A Kodak 1888-ban dobta piacra a fényképezés történetében mérföldkőnek számító Kodak 1 fényképezőgépét, amely egyrészt széles körnek tette elérhetővé a fényképezőgép használatát, másrészt lehetővé tette az azonnali – az alany hosszas egyhelyben maradását nem igénylő – fényképkészítést. Míg korábban egyértelmű volt az érintett személy beleegyezése a fénykép elkészítésébe, az új készülékkel lehetővé vált az azonnali, akár titokban történő fotózás is.[91] A szerzők emellett kiemelik a sajtó, különösen a bulvársajtó fokozódó szerepét: „a sajtó minden irányban átlépi a magántulajdon és tisztesség nyilvánvaló határait. A pletyka többé nem csak a restek és gonoszok kenyere, hanem üzletté vált, amit ipari méretekben, pimaszul űznek […] csupán azért, hogy az érzéketlen és lusta emberek elfoglalhassák magukat valamivel, [és] ezen a téren – mint az üzleti élet más ágazataiban is – a kínálat teremti meg a keresletet"[92] – írták több, mint 120 éve![93]

A szerzők e jelenségekre tekintettel arra jutnak, hogy válaszul szükséges lenne egy új jog, a magánszférához való jog elismerése.[94] Ezt a manapság használatos magánszféra-védelem fogalmához képest jóval szűkebben értelmezték, mintegy „egyedül hagyatáshoz való jogként" (right to be left alone). A magánszférához való jog a szerzők érvelése szerint – a korábbiaktól eltérően – a valós tények közlésével szembeni védelmet is biztosítani

[88] A technológia történetét és a társadalmi változásokat természetesen nem a teljesség igényével elemzem, hanem csak azokra a jelentségekre térek ki, amelyek az adatvédelmi szabályozásra hatással voltak.
[89] A tanulmány egyes elemeit és hatását elemzi például Jóri, 2005, 14-15, Majtényi, 2006, 28-30., Sólyom, 1983, 201-211. Az Információs Társadalom című folyóirat 2005/2. számában teljes tanulmányt szán a témának Simon Éva (Simon, 2005, 32-43). Ugyanitt megjelent az eredeti tanulmány magyar nyelvű fordítása is.
[90] Warren – Brandeis, 1890.
[91] A Kodak szlogenje szerint „ön megnyomja a gombot, a többi a mi dolgunk". A cég ugyanis vállalta a fényképek előhívását is, amelyet korábban csak megfelelő szakértelemmel rendelkező fényképészek tudtak megtenni. Kodak, 2013.
[92] Warren – Brandeis, 2005, 9.
[93] A jogirodalomban elterjedt anekdota szerint azonban Warrent személyesen is feldühítette egy róla szóló, a magánélete körébe tartozó, de egyébként ártalmatlan tartalmú híradás, miszerint feleségével egyik nap esküvői reggelit adtak (vélhetően az unokahúguk esküvőjének bejelentésére). Simon, 2005, 37-38.
[94] Warren – Brandeis, 1890, 195.

hivatott.[95] Igen előremutató volt az a gondolatuk is, miszerint a magánszféra megsértése minden további tényleges kár nélkül is kártérítési kötelezettséget kell, hogy megalapozzon.

A tanulmány nem azonnal váltott ki éles reakciókat, inkább később bizonyult „korszakos teljesítménynek", hatása csak lassan mutatkozott meg.[96] A magánszférához való jog végül a XX. század első felében a bírói gyakorlat alapján fokozatosan vált elfogadottá az Egyesült Államok jogában.[97] Az európai jogrendszerek aztán az Amerikai Egyesült Államok jogrendszerét követve kezdtek a háborítatlan magánélethez való joggal foglalkozni, ám a huszadik század végére az amerikainál hatékonyabb magánélet-védelmi rendszereket építettek ki.[98] Míg Warren és Brandeis a privacy védelmét egyértelműen magánjogi jogviszonyokra alkalmazta, addig Európában e témakör a XX. század során elsősorban (de legalábbis először) az állami információs túlhatalommal szembeni aggodalmak miatt került előtérbe.

E félelmek eleinte a szépirodalomban, később a társadalomtudományi és jogi szakirodalomban is megjelentek. Előbbi területen kétségtelenül George Orwell 1984 című regénye a legismertebb, amelyben a totalitárius állam a „telekép" technológiáját használja az emberek folyamatos megfigyelésére. Az orwelli „Nagy Testvér" kifejezés aztán széles körben vált a megfigyelő és elnyomó állam jelképévé (e fenyegetéshez aztán később az európai közgondolkodásban is csatlakoztak az üzleti élet „Kis Testvérnek" nevezett szereplői is).

Az információs jogok teljes hiányának állapotát igen nyomasztóan érezheti át az olvasó Franz Kafka: A per című művének végsőkig kiszolgáltatott főhősének (Josef K.) történetén keresztül is. A magyar költészetben ugyancsak megjelenik a „levegőtlenség érzése": József Attila Levegőt! című versének sorai világos és hatásos kifejezőereje miatt gyakran idézettek a magyar adatvédelmi szakirodalomban is:[99] „Számon tarthatják, mit telefonoztam/ s mikor, miért, kinek./ Aktába írják, miről álmodoztam,/ s azt is, ki érti meg./ És nem sejthetem, mikor lesz elég ok,/ előkotorni azt a kartotékot,/ mely jogom sérti meg."[100]

A II. világháború tapasztalatai is különös óvatosságra intettek. A háború borzalmai és a náci rémtettek nemcsak az emberi jogok elfogadásának és nemzetközivé válásának adott új

[95] Simon, 2005, 36.
[96] Sólyom, 1983, 211.
[97] A különböző, eleinte a magánszférához való jog el nem ismeréséről, majd mégis annak fokozatos elfogadásáról szóló bírósági döntéseket ld. Simon, 2005, 39-41.
[98] Szabó, 2012, 32.
[99] A szépirodalom és az adatvédelem kapcsolatát ld. pl. Balogh, 1998, 152-153., Jóri, 2005, 21-22. A kérdéssel legrészletesebben Majtényi László foglalkozik (Majtényi, 2006, 41-55.), aki nemcsak, hogy maga is keresi a „Nagy Privacy Metaforát" (és találja meg végül József Attila idézett versében), de a nemzetközi szakirodalomban is népszerű metaforakeresés okait is kutatja: „Olyasmiről beszélünk ugyanis, amiről nem tudjuk, hogy micsoda. Mindenki, aki a privacyvédelemmel foglalkozik, valamelyest szenved attól, hogy a védelem tárgya, alanya bár megnevezhető, meghatározhatatlan. Ezért menekülnek a képes beszédhez. A szerzők mindegyike valami sipolyt keres a jogi burkon, hogy azt megnyitva, meglesse az *én*t." Majtényi, 2006, 46.
[100] Részlet József Attila: Levegőt! című verséből. József Attila minden verse és versfordítása, Szépirodalmi Könyvkiadó, Budapest. 1980, 389.

lendületet,[101] de a (hatékony) állami nyilvántartásokkal és a modern technológiával való visszaélések lehetőségére is rámutattak.

A lyukkártya-technológia az 1935-ös és 1939-es német népszámlálások kiszolgálása mellett a háború logisztikáját, a zsidóüldözés különböző formáit és a holokauszt szervezését is igen hatékonnyá tette.[102] Az IBM és – a később állami kézbe vett – német leányvállalata, a Dehomag[103] által kínált technológia (és a hozzá tartozó komoly és folyamatos technikai támogatás) hozzájárult a zsidó népesség faji alapú megszámlálásához és azonosításához, javaik felméréséhez, és a zsidó kötődésű vállalkozások számbavételéhez is (amely e javak elkobzásához és a zsidó vállalkozások államosításához vezetett).[104] Ugyanez a technika szolgálta ki a holokauszt megszervezését is, a vasúti menetrendek optimalizálásától a koncentrációs táborok adminisztrációjáig bezárólag.[105] Emellett a náci Németország nagymértékben támaszkodott a lyukkártyarendszerre a háború és az utánpótlás szervezésében is.[106]

A hollandiai zsidóság nagyarányú elhurcolását ugyancsak a hatékony és átfogó népesség-nyilvántartás tette lehetővé, amelyet – lyukkártya-technológiával támogatva – az 1930-as években hoztak létre az állami feladatok hatékonyabb ellátása érdekében. A nyilvántartás megalkotásakor a holland állampolgárok még joggal bíztak a kormányzatukban – a náci megszállással járó veszélyekkel azonban nem számoltak. Míg Hollandiából a zsidóság 73%-át vitték el a németek, addig Franciaországból csak 25%-öt.[107] Franciaországban ugyanis egyrészt a korábbi népszámlálások során nem kérdeztek rá a vallási hovatartozásra, így kész nyilvántartás nem állt rendelkezésre.[108] Másrészt a lyukkártyarendszert a közigazgatásban csak jóval kisebb mértékben sikerült elterjeszteni, mint Hollandiában vagy Németországban, így a gyors népesség-összeírási kísérletek is döntően kudarcba fulladtak.[109]

Magyarországon az 1941-es népszámlálás adatait használták fel a német nemzetiségű állampolgárok világháborút követő kitelepítése során:[110] „Németországba áttelepülni köteles az a magyar állampolgár, aki a legutolsó népszámlálási összeírás alkalmával német nemzetiségűnek vagy anyanyelvűnek vallotta magát”.[111] A KSH végül az elfogadott jogszabályok alapján kénytelen volt együttműködni a kitelepítést lebonyolító szervekkel.[112]

---

[101] Kardos, 2003, 67.
[102] Galántai, 2003, 5.
[103] Deutsche Hollerith-Maschinen Gesellschaft mbH
[104] Black, 2002, 90-91.
[105] Black, 2002, 23-25., 200-201., 256.
[106] Black, 2002, 157-159.
[107] Mayer-Schönberger, 2009, 141.
[108] Black, 2002, 236.
[109] „Sem a franciák, sem a németek nem tudták pontosan kideríteni, hogy az elkövetkezendő hónapok, sőt a hátralévő háborús évek alatt ki, milyen módszerrel végzett népszámlálást az országban.” Black, 2002, 238. A holland és francia rendszer összehasonlítását ld. részletesen Black, 2002, 222-250.
[110] Hegedűs, 2013, 130.
[111] A 12330/1945. ME rendelet 1. §-át idézi Dobos, 2005.
[112] A példa jól megvilágítja azt is, hogy milyen jelentős különbség van a között, hogy egy szervezet nem jogosult (az éppen hatályos jogszabályok szerint) bizonyos adatok átadására, és a között, hogy a szerv nem is rendelkezik az adott személyes adatokkal (mert például az adatokat anonimizálták), és így nem is képes személyes adatok átadására. Az ezzel kapcsolatos dilemmák, pro és kontra érvek a mai napig megjelennek az adatvédelemről szóló diskurzusban. Ezt a problémakört Majtényi a ruandai polgárháború példájával

Megjegyzendő, hogy ez volt az első olyan népszámlálás, amely nem az anyanyelvre, hanem a nemzetiségre kérdezett rá – heves vitát kiváltva a statisztikusok körében arról, hogy ilyen szubjektív jellemzőt a statisztika tudománya egyáltalán használhat-e.[113]

Ezek az információk, legalábbis olyan alaposan feldolgozva, mint ahogyan jelenleg hozzáférhetőek, a 60-70-es években – az adatvédelmi diskurzus kezdetén – ugyan nem feltétlenül álltak rendelkezésre, de a történelmi tapasztalatokra való utalás gyakran megjelenik a szakirodalomban.[114]

2.2 Az első generációs adatvédelmi szabályozás kialakulása és jellemzői

Az adatvédelmi szabályozás első generációjának megjelenése az 1970-es évekre tehető, alapvetően – csakúgy, mint eredetileg Warren és Brandeis cikke, és mint azóta több, adatvédelmet érintő jelentős változás – a technológia fejlődéséből eredő veszélyekre adott jogi válaszlépésként.

2.2.1 Technológiai és társadalmi háttér

A számítástechnika fejlődésében az 1950-es és 60-as években jelentős áttörés történt: először az elektroncsövek tranzisztorokkal való felváltása, majd az integrált áramkör megjelenése és alkalmazása lehetővé tette a korábbi, szobányi méretű gépek leváltását jóval kisebb (de még mindig legalább egy mai italautomatának megfelelő méretű), megbízhatóbb és alacsonyabb energiafelhasználású eszközökre.[115] Az ún. harmadik generációs számítógépek megjelenése egyértelműen az IBM S-360-as, 1965-ben piacra dobott gépcsaládjához köthető, amelyet a felhasználók a saját igényeinek megfelelő tárkapacitással, sebességgel és egyéb képességekkel rendelhettek meg. Ebben az időszakban alakul ki a használatra kész (ready to use) rendszerek szállítása, amely a szoftverek installálása mellett magában foglalta a rendszerek karbantartását, a felhasználók képzését és a velük való későbbi konzultációt is. Ekkora már nem különültek el az üzleti illetve műszaki-tudományos funkciót támogató rendszerek, a számítógépek univerzálissá váltak.[116]

Már e korai időszakban megjelent – a később az adatvédelmi szabályozás egyik fontos tényezőjévé váló – informatikai biztonság, illetve adatbiztonság témaköre. Az informatikai rendszerek védelmét a gyártók a hardverek kialakítása és a szoftverfejlesztés során is figyelembe vették, és megjelentek az első informatikai biztonsággal foglalkozó kutatások is. Tekintettel arra, hogy a távoli hozzáférés problémája ekkor még marginális volt, az intézkedések nagy része a fizikai védelem megteremtését célozta.[117] Emellett megjelent az

illusztrálja, ahol az uszítók rádióban olvasták be a meggyilkolandók neveit – „mégsem mindegy az sem, hogy a még valamennyire konszolidált hatalom (mely mindig csak viszonylagosan normális) milyen adatbázisokat hagy tébolyult utódjára.” Majtényi, 2006, 80. A holland zsidók tragédiája ugyanezt támasztja alá.

[113] Heinz – Lakatos, 2004, 2-3. Hasonló vita felmerült a 2011-es magyarországi népszámlálás során is.

[114] Ld. pl. Burkert, 1999, 49-50.

[115] Raffai, 1997, 367-369., Hegedűs, 2013, 132.

[116] Raffai, 1997, 369-370.

[117] Belovich, 2010, 7., 10.

adatbiztonság kérdésköre is: egy, az IBM által finanszírozott, 1972 és 1974 között tartó kutatás eredményeként elkészült egy adatbiztonságról szóló átfogó tanulmány, amely az informatikai biztonság kérdését a magánszférára, ill. a személyes adatok védelmére vonatkoztatva is vizsgálja.[118]

A számítástechnika fejlődése tehát az 1960-as évek végére eljutott arra a szintre, hogy reális lehetőséggé váljon az állami nyilvántartások adatainak elektronikus tárolása, és a nyilvántartásokban való gyors keresés.[119] Az adatokkal való visszaélések – a papír alapú elkülönített adatbázisok fizikai jellemzőinél fogva fennálló – természetes korlátai ledőltek. A papír alapú adatbázisok korábban fizikai határt szabtak az adatkezelőnek a tekintetben, hogy mennyi adatot képes kezelni. A papír tömege, az átláthatóságot biztosító nyilvántartási rendszer költséges volt, és a sokszor különálló adatállományokban való keresés időigényes, megfelelő katalogizáltság nélkül pedig szinte lehetetlen volt.[120]

Az automatizált adatfeldolgozásra való igénnyel párhuzamosan Európa szerte megjelentek a különböző állami nyilvántartások egységesítésének vagy legalábbis összekapcsolásának tervei.[121] Később, az információs társadalomról szóló diskurzus során a centralizáció-decentralizáció kérdése egyébként is hangsúlyossá vált – mindkét irány mellett komoly érvek hozhatók.[122] A költségcsökkentés és az államok „természetes" központosító törekvései azonban ebben az időszakban alapvetően a centralizált rendszerek felé mutattak. A nyilvántartások egységesítése, illetve egy nagy, mindenre kiterjedő központi (népesség-) nyilvántartás létrehozása és működtetése a legegyszerűbben valamilyen egységes személyi azonosító használatával lehetséges,[123] így több államban is kísérletet tettek ezek bevezetésére. E törekvések alapvetően az egyre több feladatot magára vállaló jóléti állam információigényét voltak hivatottak kiszolgálni.[124]

A technológia magas költségei miatt annak használatát csak a nagy adatkezelők, elsősorban az állam különböző szervei és néhány nagyvállalat[125] engedhették meg maguknak. A technológia fejlettsége tehát közvetlenül meghatározta az azt felhasználók, és

[118] Schäfer, 2013, 29. Ld. még Charles Babbage Institute, 2013

[119] Bár az Egyesült Államok Népszámlálási Hivatala már 1951-ben alkalmazott elektroncsöves, egyenként több mint 1 millió dollárba kerülő számítógépeket. Hegedűs, 2013, 131-132.

[120] Hegedűs, 2013, 133.

[121] Burkert, 1999, 44-51.

[122] A „nagy rendszerek" hívei azok optimálisabb kihasználtságát és így a fajlagos költségek csökkentését, valamint a szabványosításban rejlő előnyöket hangsúlyozták. A decentralizált, de együttműködő rendszereket támogató szakértők a rossz értelemben vett uniformizálást és a szabadságjogok fenyegetését hozták fel ellenérvként, vitatva egyébként a költségcsökkentő hatást is (mivel a centralizált rendszerekhez lényegesen drágább hardver és szoftver, az üzemeltetéshez pedig felkészült szakembergárda szükséges). Balogh, 1998, 154-155.

[123] Ld. Jóri, 2005, 24. Sólyom így fogalmaz: „a rendszernek velejárója az emberek megszámozása", Sólyom, 1988, 25.

[124] A társadalom nagyfokú ellenőrzése és irányítása tehát nem csak a diktatúrákban megjelenő igény, hanem az egyre több területen aktív szerepet játszó szociális jóléti állam velejárója is. Részletesen ld. Mayer-Schönberger 1998, 222.

[125] A 60-as években a számítógépek „megkezdték a csendes bevonulást a nagyobb termelő vállalatok, a légiközlekedés, a pénzügyi szektor" világába is. Ld. Z. Karvalics, 2003, 146. Ebben az időszakban megkezdődik a pénzforgalom elektronikus alapokra helyezése is, Németországban például 1959-ben jelenik meg az elektronikus bankszámla. Schäfer, 2013, 28.

így a potenciális adatkezelők körét is: ez államonként néhány, elsősorban állami szervet jelentett, így a szabályozás is erre a körre koncentrált.[126]

Igen korán felmerült a nemzetközi adattovábbításokkal kapcsolatos problémakör is. Néhány nemzetközi adattovábbítási botrány felhívta a figyelmet a határokon átnyúló adatáramlás szabályozásának szükségességére,[127] így az adatvédelmi szabályozás történetében korán megszülettek az első nemzetközi adatvédelmi szabályok is.

A 60-as évek közepétől kezdve a számítástechnika fejlődésének társadalomra gyakorolt hatása a társadalomelmélet képviselőit is foglalkoztatni kezdte, így megjelentek az elektronikus adatfeldolgozás magánszférára gyakorolt hatásairól szóló első felvetések.[128] Az 1970-es években napvilágot láttak az első, kormányzatok számára készült jelentések,[129] és az információs társadalom kialakulásáról szóló diskurzus első művei is.[130] 1973-ban jelent meg Daniel Bell iskolateremtő esszéje a posztindusztriális társadalomról,[131] amelyben Bell – az információs társadalom kifejezést a posztindusztriális társadalom helyettesítőjeként használva – egy olyan szolgáltató társadalom eljövetelét vizionálja, amelyben a rendszerezett elméleti tudás és az ezzel együtt járó innovációs készség jelentik a társadalom meghatározó stratégiai erőforrását.[132]

2.2.2 Az első adatvédelmi szabályok elfogadása

2.2.2.1 Nemzeti szintű törvényhozás

A fenti technikai-társadalmi háttér ismeretében talán nem meglepő, hogy élénk vita alakult ki, amikor a németországi Hessen tartomány egységes népesség-nyilvántartó adatbázis kialakítását kezdte meg. A „Nagy Hesseni Terv" című előkészítő dokumentumot áthatja – Sólyom kifejezésével élve – a „technokrata aggálytalanság". A kormányzat a társadalom államosítását és funkcionálisan integrált igazgatási rendszert vizionál – ahol is a „statisztikai hivatal a rendőrséggel, iskolával, orvossal" kommunikál. Az egységes, az egyént személyi számmal azonosító adatbázisban mintegy 70 információt terveztek tárolni.[133] A terv végül egészen más formában valósult meg, és 1970-ben elfogadásra

[126] Jóri, 2005, 24.
[127] 1974-ben például a svéd adatvédelmi hatóság tiltott meg egy Egyesült Királyságba tervezett adattovábbítást az adatvédelmi szabályok hiánya miatt, egy későbbi hasonló esetben a francia hatóság tette ugyanezt egy Olaszországba tervezett adattovábbítással. Burkert, 1999, 51., 53.
[128] Ld. például Arthur Millernek a Michigan Law Review folyóiratban 1969-ben megjelent „Personal Privacy in the Computer Age" című írását (Miller, 1969, különösen 1107-1109), de a kérdéssel Westin híres műve, a „Privacy and Freedom" is foglalkozik. A „Computer and Privacy" irodalom feldolgozásáról ld. még Bennett, 1992, 53-55.
[129] A legismertebbek talán az Egyesült Királyságban készült Younger-jelentés (1973) és Lindop-jelentés (1978), amelyek e célból végzett közvélemény-kutatások eredményeit is felhasználva tettek javaslatokat a személyes adatok védelmével kapcsolatos szabályozás elveire (Jay – Hamilton, 1999, 2-4.)
[130] Ld. például Brian Murphy 60-as években végzett kutatásainak összefoglalását Balogh, 1998. 150. Említhetjük még James Martin és Adrian R. D. Norman „The computerized society. An appraisal of the impact of computers on society over the next fifteen years." című, 1970-ben megjelent munkáját.
[131] Daniel Bell: The coming of postindustrial society: a venture in social forecasting, Basic Books, New York, 1973.
[132] Balogh, 1998, 150., Hassan, 2008, 52-53.
[133] Sólyom, 1988, 25.

került Európa első adatvédelmi törvénye, amely döntően meghatározta az elkövetkezendő évek adatvédelmi vitáinak irányát Németországban és azon kívül is.[134]

Európa számos országában születtek a hessenihez hasonló tervek, több esetben hasonló vitát és megoldásokat generálva. Franciaországban szintén egységes azonosítószám alapján tervezték összevonni a meglévő nyilvántartásokat – ráadásul, igen szerencsétlen módon, titkos terv keretében, így itt egy 1974-es sajtócikk kényszerítette ki a társadalmi vitát. Egy másik, a gyermekeket születésüktől fogva nyilvántartó adatbázis a „problémás" gyermekek kiszűrését szolgálta volna. Találóan jegyzi meg Burkert, hogy „egy ilyen adatbank szimbolikus jelentősége – a nem túl távoli történelmi múlt fényében – drámai volt".[135]

Emellett 1973-ban Svédországban, 1974-ben az Amerikai Egyesült Államokban, 1977-ben a Német Szövetségi Köztársaságban (immár szövetségi szinten), 1978-ban Dániában, Norvégiában, Ausztriában és az imént bemutatott folyamatok lezárásaként Franciaországban fogadtak el adatvédelmi törvényeket.[136]

2.2.2.2 Nemzetközi dokumentumok

A nemzetközi adattovábbítás nehézségeire reagálva nemzetközi színtéren is elindult az adatvédelmi jogalkotás, egyrészt az OECD,[137] másrészt az Európa Tanács égisze alatt.[138] A jogalkotás folyamata során e két szervezet szorosan együttműködött, így végül a kiadott illetve elfogadott normaszövegek is alapvetően hasonlók.[139]

Az OECD irányelvek[140] elfogadására 1980-ban került sor, és bár nem kötelező szabályokat tartalmaz, jelentőségét az adja, hogy a szervezetnek az Egyesült Államok is tagja, így az ebben foglalt elvek az európai és amerikai szabályozás közös nevezőjének tekinthetők.[141] Az OECD ajánlás célkitűzése kettős: a magánélet védelme és a határokon átnyúló adatáramlás biztosítása. Ez a kettőség hosszú távon is kényes egyensúlyozást vetített előre, és később, az EU adatvédelmi irányelvében is jelentős hangsúlyt kapott.

Az OECD irányelvek mind az állami, mind a magánszféra adatkezelőire kiterjednek, és nem tesznek különbséget az automatizált és manuális adatkezelések között sem. Az egyes alapelvek, a korlátozott adatgyűjtés alapelve, az adatminőség alapelve, a cél meghatározásának alapelve, a (további) felhasználás korlátozásának alapelve, a biztonság alapelve, a nyíltság alapelve, a személyes részvétel alapelve, és az elszámoltathatóság alapelve igen előremutatóak voltak abban az időben, ugyanakkor a dokumentum „csak"

[134] Simitis, 1987, 5.
[135] Burkert, 1999, 49-50., saját fordítás
[136] Hegedűs, 2013, 137.
[137] Organisation for Economic Co-operation and Development, Gazdasági Együttműködési és Fejlesztési Szervezet
[138] A hazai jogirodalomban ellentétes álláspontok találhatók arra nézve, hogy az OECD alapelvek és az ET adatvédelmi egyezménye az első illetve második generációs adatvédelmi szabályázáshoz tartoznak-e. (Majtényi, 2003, 582., Jóri, 2005, 29-30., Hegedűs, 2013, 136., 138.). Mivel álláspontom szerint a generációk közötti különbségek szempontjából az érintett rendelkezési jogával kapcsolatos különbségeknek nagyobb súlya van, mint annak, hogy kiterjed-e a szabályozás hatálya a manuális adatkezelésre vagy sem, így e szempont mentén, és az elfogadásának dátuma alapján is az első generációs szabályok között tárgyaljuk.
[139] Rudgard, 2012, 7.
[140] OECD, 1980
[141] Jóri, 2005, 28. Ugyanez igaz Ausztráliára, Kanadára és Japánra is, Kosta, 2013, 27.

általános elveket határoz meg, amelyek kifejtése további nemzeti szintű jogalkotást feltételez.[142] Az érintett szerepe az első adatvédelmi törvényekéhez képest jelentősebb, az érintetti jogok hangsúlyosabbak, és korlátozottan ugyan, de az adatkezelés során szerepet kap az érintett hozzájárulása is.[143] Az OECD irányelvek azonban összességében nem garantálnak olyan mértékű rendelkezési jogot az adatalanyok számára, mint a későbbi európai adatvédelmi szabályok.

A másik jelentős, jogi kötőerővel is bíró nemzetközi dokumentum az Európa Tanács majd egy évtizedes előkészítő folyamatok eredményeként[144] 1981-ben elfogadott adatvédelmi egyezménye.[145] Az egyezmény hatálya mind az állami, mind a nem állami adatkezelők automatizált („gépi") adatkezeléseire kiterjed, de az aláíró államok dönthetnek úgy, hogy alkalmazzák a rendelkezéseit a manuális adatkezelésekre is.[146] Az egyezmény elsősorban az adatok minőségével, az érintetteknek biztosított jogokkal és az országhatárokat átlépő adatáramlással kapcsolatos szabályokat tartalmaz, de megjelenik benne a különleges adatokra vonatkozó fokozottabb védelem igénye, a megfelelő szankciórendszer követelménye, valamint az adatbiztonság szempontja is. Az egyezményben azonban érintőlegesen sincs szó az érintett hozzájárulásáról, mint az adatkezelés esetleges jogalapjáról.[147] Az egyezmény korához képest igen előremutató szabályozást tartalmaz, sok helyen az OECD irányelvekhez hasonló szabályokat ír elő, az aláíró tagállamok számára azonban immár kötelező jelleggel. Összességében mindkét dokumentum jelentős hatást gyakorolt később az Európai Unió adatvédelmi irányelvére is, amely azonban a legtöbb ponton jóval továbbmegy a személyes adatok védelme tekintetében, igaz, a területi hatálya a mai napig szűkebb az ET adatvédelmi egyezményénél.[148]

2.2.3 Az első generációs szabályozás főbb jellemzői

1. Az első generációs szabályozást áthatotta a „Nagy Testvér" információs túlhatalmától való félelem, így e jogszabályok elsődleges célja a nagy (döntően állami) adatbázisok átláthatóságának megteremtése volt.[149] Ugyanakkor kezdetektől fogva felmerült, hogy a szabályozás hatálya kiterjedjen-e a nem állami adatkezelőkre. A hesseni törvény, inkább a tartományi hatáskörből, mintsem szigorú elvi megfontolásokból fakadóan, még csak az állami szervekre vonatkozó szabályokat tartalmazott, a német szövetségi adatvédelmi

[142] Az egyes alapelvek részletezésétől eltekintek, mivel az a magyar jogirodalomban több helyen is megtalálható, ld. Jóri, 2005, 28-29, Majtényi, 2006, 95-96., Hegedűs, 2013, 146-148. A dokumentum az alapelveken felül részletesen rendelkezik a személyes adatok akadálytalan áramlásáról is.

[143] A korlátozott adatgyűjtés elve alapján a személyes adatok gyűjtését törvényes és tisztességes eszközökkel kell beszerezni, és, megfelelő esetben, az alany tudtával vagy beleegyezésével. A „megfelelő eset" és az adatalany „tudta vagy beleegyezése" kitétel igen tág teret enged a kifejezett hozzájárulás nélküli adatkezeléseknek is. Egy másik rendelkezés esetében nagyobb a hozzájárulás szerepe: a (további) felhasználás korlátozásának alapelve alapján az eredeti céltól eltérő célra történő adatkezelés csak törvény alapján vagy az érintett hozzájárulásával lehetséges. A hozzájárulás szerepéről ld. részletesen Kosta, 2013, 30-33.

[144] Az előzményekről ld. Balogh, 1998, 190.

[145] Európa Tanács, 1981

[146] Magyarország is ezzel a vállalással csatlakozott az egyezményhez, az erről szóló törvény 1998-ban lépett hatályba, Jóri, 2005, 29.

[147] A részletes szabályok a magyar jogirodalomban szintén több helyen fellelhetők, ld. Balogh, 1998, 190-198., Jóri, 2005, 29-30., Hegedűs, 2013, 148-150.

[148] Éppen e területi hatály adja az egyezmény jelenleg is folyó modernizációjának jelentőségét.

[149] Jóri, 2005, 24.

törvény azonban – épp e kérdés körül kialakult igen hosszas vita után – az állami- és magán adatkezelőkre egyaránt kiterjedt, csakúgy, mint az 1978-as francia és dán szabályozás.[150]

2. Az első generációs szabályok hatálya alapvetően csak az automatizált adatkezelésekre (a hagyományos, manuális adatkezelésekre nem) terjedt ki, tárgyuk elsősorban a nyilvántartást kiszolgáló technológia volt.[151] E jellemző a törvények szóhasználatában is tetten érhető: magánszféra és annak védelme helyett a szabályozás „adatbankokról", „adatbázisokról" és „rekordokról" szól. Ehhez szorosan kapcsolódva már a legelső adatvédelmi jogszabályokban hangsúlyos szerepet kapnak az adatbiztonságra, azaz az adatok jogosulatlan hozzáférése, megváltoztatása, nyilvánosságra hozatala vagy megsemmisítése, illetve véletlen megsemmisülése vagy sérülése elleni technikai és szervezési intézkedésekre vonatkozó szabályok.[152]

3. További fontos jellemző, hogy e törvények még nem biztosítottak általános rendelkezési jogot az adatalanyok számára a személyes adataik felett, de biztosítottak néhány részjogosítványt, például a betekintés és a helyesbítés jogát. Ezek később ugyan az információs önrendelkezési jog részjogosítványai,[153] illetve általában az érintetti kontroll gyakorlásának fontos eszközei lettek, ekkor azonban e jogoknak csupán szűk, funkcionális szerepük volt, amelyek az adatok pontosságát szolgálták.[154] Ezzel összhangban az érintett hozzájárulása és általában az adatkezelés jogalapjának kérdése vagy egyáltalán meg sem jelenik, vagy nem különösebben hangsúlyos.[155] Az első és második generációs szabályozás közötti legfontosabb elhatárolási szempont épp az érintettek rendelkezési jogának terjedelme.

4. Már e korai jogszabályok megalkotása során felismerte a jogalkotó azt, hogy az adatvédelem érvényesülése csak megfelelő felügyelőhatóságok felállítása mellett biztosítható. A jogszabályok rendezték az ombudsman jellegű vagy hatósági hatáskörökkel (is) rendelkező felügyelőszervek feladat- és hatásköreit. Így a hesseni törvény létrehozta a Hesseni Adatvédelmi Biztos[156] intézményét, a francia jogszabály a kezdetektől fogva részletesen szabályozta a francia adatvédelmi hatóság (CNIL)[157] jogállását, míg Svédországban a *Swedish Data Inspection Board* végezte és végzi az adatvédelem felügyeletét.[158]

---

[150] Burkert, 1999, 47-50.
[151] Jóri, 2005, 25.
[152] Mayer-Schönberger, 1998, 223-224.
[153] Jóri, 2005, 24.
[154] Mayer-Schönberger, 1998, 226.
[155] A svéd törvény például egyáltalán nem szól a hozzájárulásáról. Németországban a hesseni törvény ugyancsak nem említi az érintetti hozzájárulást – mivel azonban ennek hatálya csak az állami adatkezelésekre terjed ki, ennek túl sok értelme nem is lenne. Az ET egyezményben egyáltalán nem, az OECD irányelvekben pedig soft law szabályként jelenik meg a hozzájárulás. Ugyanakkor például a német szövetségi szinten elfogadott BDSG már az adatkezelés kizárólagos jogalapjainak jelöli a hozzájárulást és a jogszabályi felhatalmazást, aktív szereplővé változtatva az adatalanyt (Kosta, 2013, 43., 47., 49-50). A BDSG így tulajdonképpen kilóg az első generációs szabályok sorából.
[156] Der Hessische Datenschutzbeauftragte
[157] Commission nationale de l'informatique et des libertés
[158] Burkert, 1999, 46. 50-51. Csupán néhány példát emeltem ki, számos további nemzeti hatóság jött létre.

5. Az 1973-as svéd törvény vezette be azt a később általánossá váló kötelezettséget, miszerint az adatkezelők kötelesek egy nyilvánosan hozzáférhető hatósági nyilvántartásba bejelenteni az egyes adatkezeléseiket (adatbázisaikat). Ez egyrészt biztosította az állampolgárok és fogyasztók számára az adatkezelések átláthatóságát, másrészt segítette az adatvédelmi hatóságok jogalkalmazó tevékenységét.[159] Az adatbázisok bejelentési vagy engedélyeztetési kötelezettsége az első generációs szabályozások fontos jellemzői voltak,[160] Jóri ugyanakkor felhívja a figyelmet arra, hogy ez a jogintézmény egy olyan korban született, amikor ez csupán néhány, de jelentős mértékű adatbázist kezelő adatkezelőre vonatkozó kötelezettség volt, és az elektronikus környezetben végzett mindennapi adatkezelések korában anakronisztikussá válhat.[161]

2.3 A második generációs adatvédelmi szabályozás kialakulása és jellemzői

Az adatvédelmi szabályozás második nagy korszakának a 80-as és 90-es évek időszaka tekinthető. E két évtizedben az informatika és számítástechnika igen jelentős fejlődésen ment keresztül, és jó szívvel indokolható lenne ezen belül további korszakokat és adatvédelmi szabályozási generációkat megkülönböztetni – mint ahogy ezt sokan meg is teszik.[162] Ugyancsak jelentős területi eltérések fedezhetők fel az egyes európai államok adatvédelmi jogának fejlődése során.[163] Mindezzel együtt az adatvédelmi szabályozás alapkövei – több időbeli változást és térbeli különbséget elismerve – alapvetően azonosak ebben az időszakban, amelyben természetesen nagy szerepe van az Európai Unió jogharmonizációs törekvésének. Az 1995-ös adatvédelmi irányelv egyik bravúrja, hogy a különböző tagállami megközelítéseket – igaz, számos kompromisszum árán – sikerült többé-kevésbé közös gondolati-filozófiai platformra helyeznie.[164]

Meg kell azonban jegyezni, hogy e törekvés csak a 90-es évek végén ért be, és lényegében a 80-as évek végére kialakult elméleti-dogmatikai alapokon nyugszik. Az adatvédelmi szabályozás „fáziskésése” már ebben az időben megkezdődött, és jelenleg is tart. Ennek okai először is a jog hagyományos követő jellegében, másodszor az EU jogalkotási mechanizmusában keresendők. Harmadszor, és ez talán a leglényegesebb, pedig abból a tényből fakad, hogy a jogalkotás során valóban két, egymással ellentétesnek tűnő érdek között kell egyensúlyt teremteni. Elfogadni egyrészt azt, hogy a (személyes) adatok hatékony felhasználása és a személyes adatok szabad áramlása az információs társadalom kiépítésének és a közös gazdasági térség kialakításának egyik kulcsa, másrészt elismerni, hogy a személyes adatok védelme az egyének magánszféra-védelmének fontos eszköze, és

[159] Burkert, 1999, 48.
[160] Mayer-Schönberger, 1998, 223.
[161] Jóri, 2005, 41.
[162] Ld. Mayer-Schönberger Viktor, 1998, vagy Bäumler és Bizer felosztását (Jóri, 2005, 22-23.), illetve Majtényi László (Majtényi, 2003, 582-583.) és Hegedűs Bulcsú (Hegedűs, 2013, 137-145.) korszakolását
[163] Ld. erről részletesen Burkert, 1999, 44-57.
[164] Megjegyezve ugyanakkor, hogy így is számtalan tagállami eltérés tapasztalható. Erre tekintettel a jelenleg zajló adatvédelmi reform során a Bizottság közvetlenül alkalmazható és közvetlenül hatályos rendeletre tett javaslatot. A szabályozási forma önmagában is heves vita tárgya a jogalkotási folyamat során.

biztosítani ennek a (lehetőleg azonosan) magas szintű védelmét az Európa Unió tagállamaiban, illetve európai polgárok adatai esetén lehetőleg azon kívül is.

Mielőtt azonban rátérek a második generációs szabályozás kialakulására és jellemzőire, érdemes áttekinteni az XX. század utolsó két évtizedének – történelmi léptékkel nézve is igen jelentős – technológiai-társadalmi változásait.

2.3.1 Technológiai és társadalmi háttér

2.3.1.1 Az IKT fejlődése a 80-as, 90-es években

A számítástechnika területén tovább folytatódó miniatürizáció és az ún. magasan integrált áramkörök széleskörű elterjedése lehetővé tette a „mikroszámítógépek”[165] megjelenését. Az 1980-as évek legnagyobb újdonsága kétségkívül a személyi számítógép (PC) megjelenése volt. Több más – azóta nagyrészt eltűnt vagy átalakult – vállalkozás mellett mindenképpen megemlítendő az Apple, amely 1976-ban jelent meg első saját számítógépével, de igazi áttörést számára az 1984-ben bemutatott Macintosh hozott,[166] valamint az IBM, amely 1981-ben lépett piacra saját személyi számítógépével. A 80-as évek második felében (először épp a Macintoshsal) megjelenik a grafikus felhasználói felület, valamint az egér, mint navigációs eszköz is.

A személyi számítógépek megjelenése drasztikus változásokat hozott. A nagyteljesítményű számítógépes kapacitás a korábbinál lényegesen szélesebb kör számára vált elérhetővé. A gépek kezeléséhez – a korábbiakkal ellentétben – már nem kellett speciális szakértelem, az átlagember közvetlenül is képes volt a számítógépes műveletek elvégzésére, és azok eredményeit (adatok, grafikus munkák stb.) azonnal érzékelhette.[167] A számítógépek alkalmazása igen gyorsan elterjedt az üzleti életben, a nagyvállalatok mellett egyre inkább a kis- és középvállalkozások mindennapjainak részévé vált,[168] majd megjelent a felhasználók otthonaiban is. Az 1990-es évekre a PC kétségkívül meghódította a fejlett világ jelentős részét: 2000-ben több mint félmilliárd személyi számítógépet használtak világszerte.[169]

Az 1990-es évekre „beérett” egy másik forradalmi fejlesztés, az Internet is. Az 1969-ben katonai célú, ARPANET néven induló hálózat polgári használata a 90-es évek elejéig lényegében tudományos célokra szorítkozott, az egyébként folyamatosan bővülő hálózat tagjai egyetemek, könyvtárak voltak. A hálózat jelentőségét egyértelműen a szabványosított, TCP/IP protokoll segítségével történő kommunikáció adja, így a hálózat bármely tagja (számítógépe) képes bármely más taggal – akár közvetlenül is –

[165] A korabeli irodalomban található mikorszámítógép elnevezés lényegében a hagyományos méretű asztali gépek (desktop) méretére utal.
[166] Médiatörténeti érdekesség, hogy a Macintosh piacra dobását az Apple Orwell 1984 című művére utalva vezette be, amelyben az ekkor óriásvállalatként működő IBM jelképezte a Nagy Testvért, amelynek uralmát megtöri az Apple számítógépe. Az elmúlt években aztán többször épp az Apple (pl. az iPhone helymeghatározási adatok küldésével kapcsolatos) technikai megoldásai váltottak ki félelmeket a magánszféra-védelemmel foglalkozók körében.
[167] Raffai, 1997, 85-86.
[168] Az IBM pl. az AS 400-as sorozatát kifejezetten könnyen kezelhető, kis-és középvállalkozásoknak szánt számítógépcsaládként mutatta be 1988-ban. IBM, 2014
[169] ETForecast, 2014

kommunikálni. Az Internet nagyfokú elterjedése egyrészt a hírközlési hálózati infrastruktúra jelentős fejlődésének,[170] másrészt az 1991-re kifejlesztett, World Wide Web szolgáltatásnak köszönhető, amely grafikus felületével és linkeken alapuló, hypertext jellegű felépítésével az Internet legismertebb, bárki által könnyedén használható szolgáltatásává vált. Az 1990-es évek második fele egyértelműen az Internet „kommercializálódásának" időszaka, egyre több vállalkozás jelent meg a világhálón (eleinte statikus információkkal, majd fokozatosan elektronikus kereskedelmi szolgáltatásokkal is).[171] Sorra jöttek létre az ún. dotcom cégek, amelyek hagyományos üzlethelyiséggel egyáltalán nem rendelkeztek, és kizárólag online kereskedelemre rendezkedtek be. E vállalkozások tényleges pénzügyi sikereinél lényegesen nagyobb volt azonban a szektor fejlődésével kapcsolatos várakozás, ami végül az online szolgáltatásokat kínáló cégek túlértékeléséhez, az első dotcom-buborék kialakulásához vezetett, amely 2001-ben látványosan kipukkadt: a technológiai részvényeket tömörítő NASDAQ index 2000-2001-ben hatalmasat zuhant (dotcom válság).

A 90-es évek végére az adatfeldolgozás (számítástechnika) és az adattovábbítás (távközlés) technológiája tehát látványosan összekapcsolódott (konvergencia folyamat).[172] Az Internet kereskedelmi célú megjelenése és elterjedése a korábbi, önálló egységként funkcionáló számítógépeket egyetlen, azonos technikai paramétereket és elveket használó, világméretű hálózattá kötötte össze. Minden korábbinál könnyebbé és gyorsabbá vált az adatok (ideértve a személyes adatokat is) nyilvánosságra hozatala vagy továbbítása akár a világ valamely távoli pontjára is. Az Interneten közzétett adatok ráadásul – a technológia jellegénél fogva – főszabály szerint megőrződnek, az adatok törlése jelentős időt és figyelmet igényel, a „felejtés drága üzlet" lett.[173]

2.3.1.2 A technológiai alkalmazási területei

Az egyre szélesebb körben elterjedő számítógép-használat az állam (közigazgatás) működésére is jelentős hatást gyakorolt. Ugyanakkor a központosított vagy egységesített adatbázisok létrejötte helyett a hangsúly a közigazgatási folyamatok hatékonyabbá tételére és a közigazgatási szolgáltatások elektronikus úton történő igénybevétele felé tolódott el. A technológiai fejlődés tehát továbbra is jelentős hatással volt az államigazgatás működésére; a 90-es évektől kezdve a közigazgatás informatikai alapú – de fontos szemléletváltozással, a szolgáltató állam ideájával[174] is megtámogatott – megújítása folyamatosan napirenden van. E fejlemények azonban az adatvédelmi szabályozás fejlődése szempontjából kisebb jelentőséggel bírtak, a magánszféra sérelmével kapcsolatos aggodalmak fokozatosan egyre inkább az üzleti élet szereplőivel szemben kezdtek megfogalmazódni.

---

[170] Az Európai Unió a 90-es évek során jelentős erőfeszítéseket tett a hírközlési infrastruktúra és piac fejlesztése érdekében, amelyet alapvetően e piac liberalizációjával kívánt (most már látható: sikerrel) elérni.
[171] Leiner, 2009
[172] A konvergencia folyamat több szinten is értelmezhető. A hálózati konvergencia lényege, hogy a különböző típusú hálózati platformokon is lehetséges az alapvetően hasonló szolgáltatástípusok (hang, adat, kép) továbbítása. Ennek hatására kialakult a szolgáltatások konvergenciája, eszerint egy-egy szolgáltató egyaránt nyújt Internet-előfizetést, telefon és kábeltelevíziós szolgáltatást („triple-play" szolgáltatás), végül – a gyakorlatban jóval később – megfigyelhető a fogyasztói eszközök, például telefon, televízió, és személyi számítógép összefonódása (eszközök konvergenciája). Ld. részletesen EC, 1997, 1.
[173] Székely, 2012. 350.
[174] Erről ld. részletesen Budai, 2009, 15-60.

Az informatikai és kommunikációs technológiák fejlődése és széles körű elterjedése alaposan átalakította az üzleti szférát is. A 90-es években megjelentek a szervezeti szinten is integrált ún. vállalati erőforrás-tervező rendszerek (ERP),[175] amelyek igyekeztek integrálni és egységes vállalati adatbázis segítségével egységesíteni a korábban szigetszerűen működő alkalmazásokat. A 90-es évek végére pedig megjelentek – részben az ERP rendszer részeként, részben önállóan – az ügyfélkapcsolat-menedzsment rendszerek (CRM),[176] amelyek a vállalatok (gyakran természetes személy) ügyfeleinek kiszolgálását állították a vállalati működés középpontjává, komolyan felértékelve az ügyféladatok jelentőségét[177] – a 90-es években induló hűségprogramok és pontgyűjtési lehetőségek lényegében ügyféladatbázis-építési célt szolgáltak[178] (és szolgálnak azóta is). Végül megemlítendő, hogy ugyancsak ebben az évtizedben kezdtek elterjedni az adatbányászati technikák, amelyek célja új (előre akár nem is feltételezett) szabályok, összefüggések és tendenciák feltárása a meglévő (személyes) adatok különböző módszerekkel történő elemzése segítségével.[179]

Az állampolgárok és a jogalkotó számára e háttérben zajló folyamatoknál lényegesen látványosabb terület volt a marketingeszközök változása: az eleinte hagyományos (papír alapú), majd az új kommunikációs csatornákon (ekkor elsősorban e-mailen keresztül) megvalósuló direktmarketing térhódítása. A fogyasztók név- és lakcímadatai, valamint elektronikus levelezési címe a direktmarketing-vállalkozások adatgyűjtésének elsőszámú célpontjává váltak. Végül meg kell említeni az elektronikus kereskedelem és ezzel összhangban az online marketing (bannerek és szöveges linkek) megjelenését[180] az 90-es évek második felében. Az online szolgáltatásokból eredő adatvédelmi fenyegetések azonban ebben az időszakban inkább csak gyülekező felhőnek tűntek, amelyek aztán – a jóslatokat nagyrészt beteljesítve – a 2000-es években realizálódtak.

E tendenciák egyértelművé tették, hogy az üzleti szektor, (a „Kis Testvér") adatéhsége legalábbis vetekszik az államéval. Ezáltal a korábbi néhány, „jól látható" adatbázist (és azok kezelőit) adatkezelők milliói váltották fel. Ezek egy része – például pénzintézetek, hírközlési szolgáltatók stb. – ráadásul egy-egy érintettről is igen nagyszámú, az érintett magánszférája szempontjából érzékeny adatot kezeltek.[181] Olyan új szabályozásra volt tehát szükség, amely képes ezt a helyzetet kezelni.

További jelentős fejlemény a 90-es években a globalizálódó üzleti világnak köszönhetően a határokon átnyúló adatáramlás volumenének dinamikus növekedése. Az információ és annak hatékony felhasználása kétségtelenül a gazdasági fejlődés egyik motorja lett, így a vállalkozások közötti, gyakran határokon átnyúló adatáramlás biztosítása, az üzleti kapcsolatok fenntartása fontos prioritássá vált. Emellett a globális multinacionális nagyvállalatokon belüli feladatmegosztás is gyakran azt eredményezi, hogy a vállalaton

[175] Enterprise Resources Planning
[176] Customer Relationship Management
[177] A CRM rendszerekről ld. részletesen pl. Mester, 2007
[178] Regan, 1995, 1.
[179] Benkőné – Bodnár – Gyurkó, 2008, 185., 189-190.
[180] Turow – Draper, 2012, 134-135. A „cookie" ugyan a 90-es évek közepén jelent meg, de a felhasználók viselkedésén alapuló marketing csak a 2000-es évek második felétől jellemző.
[181] A "Kis Testvér" előretöréséről ld. pl. Majtényi, 2006, 36., Hegedűs, 2013. 137.

vagy vállalatcsoporton belüli adatáramlás is külföldi adattovábbítással jár együtt. A hatékony adattovábbítás biztosítása és a személyes adatok magas szintű védelme közötti kényes egyensúly megtalálása az adatvédelmi szabályozás egyik kulcskérdése lett.[182]

2.3.1.3 Az informatikai biztonság problémaköre

A PC és az Internet megjelenése az informatikai biztonságra is jelentős (alapvetően negatív) hatást gyakorolt. A költséghatékonyság a személyi számítógépek biztonságossági kérdéseit háttérbe szorította, a gyártók a korábban a nagygépekre kialakított hardveres intézkedések egy részét is elhagyták, mivel e számítógépeket alapvetően otthoni (elszigetelt) felhasználásra tervezték.[183] A korai szoftverek hasonló hiányosságban szenvedtek, egyrészt szintén költségcsökkentési okokból, másrészt az alapvetően egyfelhasználós modellben a biztonsági aggályok elenyészőek voltak. A PC-k széles körű vállalati felhasználásával és az Internet megjelenésével azonban a korábbi kockázatok jelentősen megnőttek. Az Internet infrastruktúrájának kialakításakor a biztonsági szempontok pedig azért nem kerültek előtérbe, mert a hozzáférésre jogosultak eleinte szűk kört alkottak.[184] Az Internet széleskörű elterjedésével így – az utólagos, az infrastruktúrába nem a kezdetektől „kódolt" megoldások ellenére is – egy alapvetően sérülékeny rendszer jött létre, amelyet azonban vállalkozások tömegei használnak többek között kritikus fontosságú (és gyakran személyes) adatokat tartalmazó adatbázisok üzemeltetésére is.[185] Emellett az Internettel megjelenik a távoli hozzáférés lehetősége, és az átlagfelhasználók tömegei (akár otthoni, akár vállalati használat során) nincsenek felkészülve az informatikai rendszer sérülékenységéből adódó kockázatokra.

A 80-as, 90-es években egyre fokozottabb figyelmet kap a számítógépes bűnözés. A különböző számítógépes környezetben elkövetett bűncselekmények „fókuszában az elektronikus adat áll," amely egyszerre lehet ezen bűncselekmények eszköze (bankkártyával visszaélés) és célja (pl. hackertámadás személyes adatok vagy jogilag védett más titkok kifürkészésére).[186] A számítógépes bűncselekmények volumenét és az okozott kár mértékét e bűncselekmények magas látenciája miatt nehéz felbecsülni. Ennek oka egyrészt az, hogy a bűncselekmények sértettjei túl későn, vagy egyáltalán nem észlelik a sérelmükre elkövetett bűncselekményeket, másrészt az, hogy a sértetteknek sokszor nem áll érdekében eljárást indítani (a bankok, pénzintézetek például joggal tartanak az ügyfelek bizalomvesztésétől).[187] Ugyanakkor Nagy Zoltán szerint „[s]zubjektíve túlbecsüljük a számítógépes környezetben elkövetett bűncselekmények számát, veszélyességét", a média

[182] A probléma összetettsége legélesebb talán az Egyesült Államokkal folytatott, végül a "Safe Harbour" Egyezmény megkötésével záruló tárgyalássorozat során vált világossá.
[183] A 80-as évek elején a hálózatosodást alapvetően lebutított terminálok központi hálózatra kapcsolódásaként képzelték el, és nem PC-k többé-kevésbé egyenrangú hálózataként, mint ahogy később megvalósult (Belovich, 2010, 13.)
[184] Megjegyezzük, hogy a biztonsági aggályokat felvető, alapvetően anonim hozzáférést biztosító protokollok alkalmazása a másik oldalon nagyban hozzájárult az Internet szabadságához, az internetes tartalmak feletti kontroll megnehezítéséhez, amely alapján e médium a szólás- és sajtószabadság legjelentősebb eszköze lett.
[185] Belovich, 2010, 12-16.
[186] Nagy, 2009, 51-52.
[187] Balogh, 1998, 262-263. Épp ezt a látenciát hivatott csökkenteni az utóbbi néhány évben nagy figyelmet kapott, és a hírközlési szolgáltatóknál bevezetett, a személyes adatokat érintő incidensek bejelentési kötelezettsége (Data Breach Notification).

sokszor túlzó beszámolói, illetve a potenciálisan valóban nagy (pl. az energetikai, honvédelmi, államigazgatási rendszerekkel szembeni) fenyegetés miatt – ezek tényleges realizálódása ugyanakkor viszonylag ritka.[188]

A másik oldalról nézve azonban jelentősen fejlődtek az adatok biztonságát szolgáló technológiák, például a szimmetrikus és aszimmetrikus titkosítási technológiák is,[189] amelyek az internetes kommunikáció biztonságosabbá tétele mellett a személyes adatok technikai eszközökkel való védelmét, a privátszférát erősítő technológiák alkalmazását is lehetővé teszik. Általában is egyre hangsúlyosabb szerepet kap az informatikai biztonság témaköre: az első széles körben elerjedt informatikai biztonsági szabványt 1983-ban készítette az Amerikai Egyesült Államok Védelmi Minisztériuma,[190] majd a 90-es években egyre több informatikai biztonsági szabvány jelent meg.[191] A háttérben jelentős küzdelem indult az informatikai rendszerek támadói és a védelmükért felelős szakemberek között, és e küzdelem a nemzetbiztonsági szinttől az ipari kémkedésen át a személyes adatok és magánszféra védelmének szintjéig egyaránt értelmezhető.

2.3.1.4 Adatvédelem és információs társadalom

A 80-as, 90-es évekre kiteljesedett az információs társadalom kialakulásával kapcsolatos elméleti diskurzus. Az információs társadalom fogalmára számos elméleti meghatározás található, a legtalálóbban talán William J. Martin fogalmaz; eszerint az információs társadalom „egy olyan társadalom, amelyben az élet minősége, éppúgy, mint a társadalmi változások és a gazdasági fejlődés, egyre nagyobb mértékben az információtól és annak felhasználásától függ”.[192] Világossá vált tehát, hogy a gazdasági-társadalmi változások fő mozgatórugója az információ felértékelődése és az információ felhasználásának hatékonysága lett. Ugyancsak elfogadottá vált, hogy a változások olyan horderejűek, amelyek összemérhetőek a XVIII. századi ipari forradalomével: „valamennyi ilyen forradalmi átalakulás közös jellemző vonása a mindent átható jelleg, vagyis a változások behatolnak az emberi tevékenység minden területére […] szervesen beépülve e tevékenységek szövetébe. Más szóval ezek a forradalmak az új termékek létrehozása mellett elsősorban folyamatra orientáltak.”[193]

Az információs társadalomról szóló szakmai közbeszédben rendre megjelentek a magánszférát féltő gondolatok is.[194] Széles körben elfogadottá vált, hogy az egyenként

[188] Nagy, 2009, 33-34.
[189] Részletesen ld. Szádeczky, 2011, 20-22.
[190] Trusted Computer Systems Evaluation Criteria (TCSEC), Szádeczky, 2011, 131.
[191] 1991-ben Nagy-Britannia, Franciaország, Hollandia és Németország megalkotta az Information Technology Security Evaluation Criteria (ITSEC) elnevezésű de facto szabványt, 1996-ban elkészült a Common Criteria szabvány, amelynek a második verziója ISO/IEC 15408 számmal nemzetközi de iure szabvánnyá is vált. Részletesen ld. Szádeczky, 2011, 133-134.
[192] Martin gondolatait idézi Balogh, 1998, 151.
[193] Castells korábbi technológiatörténeti kutatások, Kranzberg és Pursell eredményeit idézi és magyarázza. Castells, 2005, 67.
[194] Az információs társadalommal foglalkozó irodalom közül – messze a teljesség igénye nélkül – ld. pl. Lussato, 1989, 152-157., Friedrichs – Schaff, 1984, 254-260., Masuda, 1988, 102-110., vagy David Lyon sokkal óvatosabb megközelítését (David Lyon: The Information Society: Issues and Illusions, Polity Press, 1988.). Emellett, folytatva a 70-es években kezdődő tendenciát, kiterjedt irodalma lett a kifejezetten magánszféra szűküléséről szóló gondolatoknak, ld. Flaherty, D.H. Protecting Privacy in Surveillance

jelentéktelennek tűnő, nem különösebben érzékeny, a hagyományos titokvédelmi szabályozással védett „intim adatnak" nem minősülő személyes adatok más adatokkal összekapcsolva, új környezetbe helyezve, az adatokból további következtetéseket levonva igenis veszélyeztetik az egyén magánszféráját, és az infokommunikációs technológiából eredően ez a korábbinál lényegesen könnyebbé válik. „Nagyszámú ártatlan információból kibontakozhat egy táj, egy kép – a legtöbbször persze pontatlanul" – írja Lussato 1981-ben.[195] Hasonlóan fogalmazza meg ugyanezt Szabó Máté Dániel: összeáll „az individuumról alkotott művi kép, a személyiségprofil, az egyén virtuális, egymással összekapcsolt információkból álló profilja [… és az] egyén sorsát egyre inkább az határozza meg, hogy mit árul el róla a személyiségprofilja".[196]

A 90-es évek elejétől kezdődően – a hasonló amerikai és távol-keleti fejleményekre reagálva – az információs társadalom tervszerű kiépítése az Európai Közösségek/Unió kiemelt politikai programjává vált.[197] Mérföldkőnek tekinthető e területen az 1994-es Bangemann-jelentés,[198] amely külön fejezetet szentel a magánszféra védelmének. A dokumentum kiemeli, hogy az új technológiák alkalmazása érintheti az olyan érzékeny területeket, mint a személyek képmása, kommunikációja, mozgása és viselkedése. A jelentésben megjelenik az a félelem is, hogy a tagállami szintű, egyedi szabályozás akadályozhatja az új szolgáltatások szabad áramlását. E dokumentumban tehát már megjelenik az a kettősség, miszerint egyik oldalról biztosítani kell az adatok szabad áramlását, mivel az az információs társadalom fejlődésének motorja, másrészről azonban biztosítani kell a magánszféra megfelelő védelmét is. A Bangemann-jelentés megjegyzi, hogy európai szintű szabályozás nélkül a fogyasztói bizalom hiánya vélhetően aláássa az információs társadalom gyors fejlődését.[199] A jelentést számos, az információs társadalom kialakítását célul tűző stratégiai dokumentum követte a 90-es és a 2000-es években. E dokumentumokban a megfelelő szintű adatvédelem rendre az online szolgáltatásokba vetett bizalom (trust)[200] megteremtésének egyik fontos eszközeként, és így az információs társadalom kialakításának egyik szabályozási kérdéseként jelenik meg.[201]

Societeies, Chapel Hill, London, 1989, David Lyon: The Electronic Eye: The Rise of Surveillance Society, University of Minnesota Press, 1994, stb.

[195] Lussato, 1989, 153.

[196] Szabó, 2012, 16.

[197] Az EU információs társadalommal kapcsolatos politikájával kapcsolatban ld. http://europa.eu/legislation_summaries/information_society/index_hu.htm [2014.04.20.] Nemzeti szintű dokumentumok ennél korábban is napvilágot láttak, a legismertebb ezek közül talán az 1978-as francia Nora-Minc jelentés.

[198] Bangemann-jelentés, 1994

[199] Bangemann-jelentés, 1994, 18.

[200] Érdekesség, hogy az adatkezelések átláthatósága miatti bizalom illetve annak hiánya már a német alkotmánybíróság híres, 1983-as ítéletében is megjelenik, itt természeténél fogva az állammal, és nem a piaci szereplőkkel szemben: „Az az állami gyakorlat, amely nem törekszik az ilyen bizalom kialakítására az adatfeldolgozási folyamat nyilvánosságra hozása és a szigorú leárnyékolása révén, hosszabb távon az együttműködési készség gyengüléséhez vezetne, mert bizalmatlanságot szülne." Könyves-Tóth – Székely, 1991, 6.22

[201] Ld. például az „Európa útja az információs társadalomba" című akciótervet (EC, 1994, 6.), a „Konvergencia" Zöld könyvet (EC, 1997, 17., 29.), vagy az eEurope 2002 Akciótervet (EC, 2000, 10., 20.). A EU e kihívásokra az adatvédelmi irányelv megalkotásán túl szektorális adatvédelmi szabályok megalkotásával is reagált. A fogyasztói bizalom megteremtésének másik fontos eszköze a fogyasztóvédelmi szabályok erősítése szintén jelentős hangsúlyt kap.

2.3.2 Második generációs jogalkotás

Az elemzett változások az adatvédelmi szabályozásra is jelentős hatást gyakoroltak. Egyre inkább világossá vált, hogy az adatvédelmi szabályozás célja az érintett magánszférájának védelme kell, hogy legyen. Ehhez már nem elegendő a Nagy Testvért szimbolizáló néhány nagy állami adatbázis átláthatóságának biztosítása, mivel az adatkezelések ezernyi kisebb-nagyobb entitás keretein belül folynak. E helyzetre adekvát válasznak tűnt az állampolgárok felfegyverzése erős (több helyen alkotmányos) védelmet biztosító egyéni jogokkal, hogy ők maguk érvényesíthessék a magánszférájuk védelmét.[202]

2.3.2.1 Az információs önrendelkezési jog koncepciója

Az 1980-as, 90-es években az adatvédelmi jogalkotás jelentős változáson ment keresztül. E változások egyik legfontosabb elméleti-filozófiai előzményét a Német Szövetségi Alkotmánybíróság nagyhatású ún. népszámlálás-ítéletében[203] megfogalmazott információs önrendelkezési jog jelentette. Eszerint a Német Alaptörvény „biztosítja az egyénnek azt a jogot, hogy alapvetően maga döntsön személyes adatainak kiszolgálásáról és felhasználásáról," azaz arról, hogy „alapvetően mikor és milyen mértékben fedi fel személyes életének tényállásait."[204] A bíróság ezt közvetlenül az Alaptörvényből, a mindenkit megillető emberi méltósághoz és a személyiség szabad kibontakoztatásához való jogából vezette le, azaz az információs önrendelkezési jogot az érintett személyiségének szabad kibontakozásához való jog részének tekintette.[205]

Az információs önrendelkezési jog koncepciójának fontos eleme, hogy az érintettnek alapvetően át kell látnia az adatkezelés teljes folyamatát, mivel így képes csak megalapozott döntést hozni a személyes adatai kiszolgáltatásáról. Az érintetti jogok folyamatos erősödése, mely Európa-szerte érezhető tendencia volt, jól beleillett az információs önrendelkezési jog koncepciójába is.

Az ítélet ugyanakkor elismeri, hogy az információs önrendelkezési jog sem korlátlan, az korlátozható kényszerítő közérdekből, a normaszabatosság követelményének megfelelve, a korlátozás feltételeinek és terjedelmének meghatározásával.[206]

A bíróság az indokolásban kifejtette, hogy az automatikus adatfeldolgozás segítségével az egyént érintő adatok „műszaki szempontból korlátlanul tárolhatók és bármikor, a távolságra való tekintet nélkül, másodpercnyi gyorsasággal előkereshetők." Azokat ezenfelül „más adatállományokkal egy részben vagy messzemenően teljes személyiségképpé lehet összekapcsolni, anélkül, hogy az érintett annak helyességét és felhasználását kielégítően ellenőrizhetné",[207] így „valamely önmagában véve jelentéktelen adat új értéket nyerhet, ennyiben az automatikus adatfeldolgozás körülményei között nincs

[202] Mayer-Schönberger, 1998, 226.
[203] Az ítélet magyar nyelvű, kivonatolt változata elérhető: Könyves-Tóth – Székely, 1991, 6.1-6.39
[204] Könyves-Tóth – Székely, 1991, 6.1
[205] Rouvroy – Poullet, 2010, 53-54.
[206] Jóri, 2005, 26.
[207] Könyves-Tóth – Székely, 1991. 6.15

többé »jelentéktelen« adat. Az információk érzékenységének mértéke ezután nem függhet csupán attól, hogy bizalmas eseményekre vonatkoznak-e".[208]

A bíróság döntését elemezve először is egyetértek Hegedűs Bulcsúval, miszerint a döntés indokolása „klasszikus, első generációs adatvédelmi szemlélettel bír,"[209] az időpontjából adódóan nem is nagyon bírhat mással. A fent elemzett folyamatokat, a piaci szereplők, mint potenciális veszélyforrás megjelenését, a személyi számítástechnika elterjedését és különösen az Internet megjelenését a német alkotmánybíróság még nem láthatta előre, így a második generációs adatvédelmi szabályozást nagyban meghatározó információs önrendelkezés elve valójában nem közvetlenül e technikai-társadalmi jelenségekre reagálásként született, de végül mégis egészen jól működött az új kihívások kezelésére is.

Másodszor, meg kell említeni, hogy az információs önrendelkezési jog koncepciójában hangsúlyosan megjelenik az a gondolat is, miszerint az információs önrendelkezési jog nem csak az érintett „magánügye", hanem társadalmi jelentősége is van. A bíróság okfejtése szerint, ha valaki bizonytalan abban, hogy a szokásostól eltérő magatartását feljegyzik-e, inkább kerüli ezeket, és esetleg nem él más alapvető jogával pl. a gyülekezési vagy a véleményszabadság jogával sem. „Ez nemcsak az egyén kibontakozási esélyeit befolyásolná, hanem a közjót is, mert az önrendelkezés a polgárai cselekvő- és együttműködő-készségén alapuló, szabad, demokratikus közösség elemi működési feltételeinek egyike."[210] Az adatvédelem biztosítása tehát a szabad és demokratikus társadalom megőrzésének is eszköze.[211]

Végül meg kell említeni, hogy már az eredeti szövegben is felmerült az a gondolat, miszerint az érintett az „automatikus adatfeldolgozás körülményei között az adatok tárolását és feldolgozását nem tudja áttekinteni, […] így] az információs önrendelkezési jog hatékony védelme szempontjából a független adatvédelmi biztosok közreműködésének rendkívüli jelentősége van".[212] Az érintetti kontroll tényleges gyakorlásának hiánya később az információs önrendelkezési jogon illetve az érintett hozzájárulásán alapuló adatvédelmi rezsimmel szembeni fő kritikaként fogalmazódik meg.

Az információ önrendelkezési jog elve – számos más ország mellett – a magyar adatvédelmi szabályozásra is jelentős hatást gyakorolt. A személyes adatok védelméhez való jog 1989-ben bekerült az Alkotmányba, és 90-es évek elején több alkotmánybírósági határozat is értelmezte azt[213] – ezek során az Alkotmánybíróság figyelembe vette, és kifejezetten hivatkozta is a német kollégák 1983-as döntését. Az információs önrendelkezési jog elvét a gyakran idézett 15/1995 AB határozat fejti ki részletesen. Eszerint az „Alkotmánybíróság – a 20/1990. AB határozat szerinti eddigi gyakorlatát folytatva – a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként", amelynek „az a tartalma, hogy mindenki maga rendelkezik személyes adatainak

[208] Könyves-Tóth – Székely, 1991. 6.17
[209] Hegedűs, 2013, 150.
[210] Könyves-Tóth – Székely, 1991. 6.16. Ld. még erről Szabó, 2012, 39.
[211] Rouvroy – Poullet, 2010, 57.
[212] Könyves-Tóth – Székely, 1991. 6.18-6.19.
[213] E határozatokról ld. részletesen Majtényi 2006, 168-175.

feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is. Az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát,"[214] és a korlátozás csak akkor alkotmányos, ha megfelel az alapjogok korlátozására vonatkozó általános szabályoknak.[215]

2.3.2.2 Az Európai Unió adatvédelmi szabályozása

Az Európai Unió – más nemzetközi szervezetekhez képest – meglehetősen későn szánta rá magát adatvédelmi jogalkotásra, így mintegy „kihagyva" az első szabályozási hullámot, egyben tanulva az addigra lassan évtizedes tapasztalatokból. A 1980-as évek nemzetközi szintű jogalkotási eredményeit, az OECD irányelvek és az ET-egyezmény elfogadását követően az Európai Bizottság alapvetően azt az álláspontot képviselte, hogy az Egyezményhez való csatlakozás megoldja a közösségi harmonizáció problémáját is, és nincs szükség közösségi szintű szabályozásra.[216] Az Európai Parlament ugyanakkor folyamatosan arra ösztönözte a Bizottságot, hogy kezdeményezzen közösségi jogalkotást is e területen. A nemzeti szabályozási eltérések különbözőségeire néhány látványos, nemzeti hatósági vétóval megakadályozott határon átnyúló adattovábbítási kísérletet kísérő botrány is rávilágított.[217]

A Bizottság végül 1990-ben kiadta az adatvédelmi irányelv első szövegtervezetét,[218] amelyet hosszas vitát követően,[219] az eredeti javaslatot többször érdemben átdolgozva az Európai Parlament és Tanács 1995. október 24-én fogadott el.[220] Ugyan a szövegezés nehézkességén érződik a számtalan kompromisszum hatása,[221] és több eltérést engedő szövegrész is csökkenti az egységes szabályozás szintjét, az irányelv elfogadása mégis hatalmas előrelépés volt a harmonizált európai adatvédelmi jog felé.

Az irányelv preambuluma, ami lényegében indokolásként funkcionál, közvetlenül utal a technológia fejlődéséből eredő kockázatokra. Az irányelv elfogadását az is motiválta, hogy „a Közösségben a gazdasági és társadalmi tevékenység számos területén egyre többször

[214] 15/1991. (IV. 13.) AB határozat. Az Alkotmánybíróság nevesíti az információs önrendelkezési jog garanciáit is. A határozat értelmezését ld. Balogh, 1998, 175-177.
[215] A magyar jogirodalomban ismert az információs önrendelkezési jog ennél tágabb megfogalmazása is. Szabó Máté Dániel e jog négy szelvényét különbözteti meg, amelynek elemei (1) az egyénre vonatkozó ismeretekkel kapcsolatos önkifejezés joga és (2) az eltitkolás és rejtőzködés joga, valamint (3) a külvilágra vonatkozó, de az egyént valamiképpen érintő ismeretek megismerésének illetve (4) az ismeretektől való elzárkózás joga. Ld. részletesen Szabó, 2012, 40-43. Jelen dolgozatban az információs önrendelkezési jogot ennél szűkebben értve, az 1991-es AB döntésnek megfelelően használom.
[216] Jóri, 2005, 30.
[217] Burkert, 1999, 52-53.
[218] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final
[219] Az Egyesült Királyság például kifejezetten ellenezte az irányelv megalkotását.
[220] Jay – Hamilton, 1999, 10.
[221] A végleges szövegben megjelennek egyes tagállamokra „jellemző" (és vélhetően bevált) jogintézmények is, így a belső adatvédelmi felelős a német, a magatartási kódexek a holland, az automatizált egyedi döntéssel kapcsolatos szabályok a francia nemzeti szabályozás mintájára kerültek be az irányelvbe (Burkert, 1999, 53.)

folyamodnak a személyes adatok feldolgozásához; [és] az informatika terén elért haladás az ilyen adatok feldolgozását és cseréjét lényegesen megkönnyíti;" és „a növekvő tudományos és műszaki együttműködés és az új telekommunikációs hálózatok összehangolt bevezetése a Közösségben szükségessé teszi, és megkönnyíti a személyes adatok határokon keresztül történő áramlását."[222]

Az irányelv (már a címében is) két, elviekben egyenrangú és elsőre ellentétesnek tűnő célt fogalmaz meg: az egyének védelmét és a személyes adatok szabad áramlását. Az irányelv logikája alapján a személyes adatok szabad áramlását épp az egységesen magas szintű védelemmel lehet biztosítani, amelyet az EU tagállamain belül a harmonizációból adódóan adottnak tekint, harmadik országba pedig a „megfelelő szintű védelem" elismerése mellett biztosítja ugyanezt. E koncepción keresztül az EU sikeresen „exportálta" adatvédelmi szabályozását,[223] az irányelv jelentős hatást gyakorolt számos EU-n kívüli állam adatvédelmi jogára, állami szintű szabályozást illetve egyes országokban (ágazati és adatkezelői szinten elfogadott) önszabályozási mechanizmusokat inspirálva. Burkert szerint az irányelvvel az adatvédelmi szabályozás az információs társadalom európai, társadalmi értékekre koncentráló megközelítésének szimbólumává vált az Egyesült Államok „információs-szupersztráda típusú", gazdasági folyamatokat szem előtt tartó értékválasztásával szemben.[224]

Az irányelv a második generációs szabályozás tipikus dokumentuma, és bár természetesen jelentősen merít a korábbi dokumentumok (elsősorban az ET-egyezmény) megoldásaiból, az irányelv szabályozási újításai vitathatatlanok.[225] Bennett kiemeli, hogy az adatvédelmi irányelv a rendelkezések alkalmazhatósága alapján nem tesz különbséget a közszféra, és a magánszektor adatkezelői között (szemben egyébként az eredeti, 1990-es tervezettel), és hogy a hatálya mind az automatizált, mind a manuális adatkezelésekre kiterjed. A felügyelő hatóság jogállására vonatkozó rendelkezések pedig alapvetően erősebb jogköröket írnak elő, mint ami a tagállamok jogában akkoriban általában jellemző.[226] Jay és Hamilton is úgy értékeli, hogy az adatvédelmi irányelv jelentős előrelépést tesz a korábbi adatvédelmi gondolkodáshoz és szabályokhoz képest. Ennek főbb elemei, hogy (1) a hatálya a manuális adatkezelésekre is kiterjed, (2) megállapítja az adatkezelés jogszerűségének minimumfeltételeit (jogalapjait), (3) speciális szabályokat állapít meg egyes érzékeny adatok kezelésére, (4) kiterjedt érintetti jogokat biztosít az adatalanyok számára, (5) részletesen szabályozza a határon átnyúló adattovábbítások kérdéskörét, és (6) megerősíti az adatkezelés adatbiztonsági követelményeit.[227] Mayer-Schönberger a német

[222] 95/46/EK, (4), (6) preambulum-bekezdés
[223] Az irányelv jelentősen befolyásolta Új-Zéland, Hongkong, Kanada és több dél-amerikai állam adatvédelmi szabályozását. Jóri, 2005, 33.
[224] Burkert 1999, 56. Jóri az EU-USA hatások elemzésekor felhívja a figyelmet két ellentétes tendenciára: a Safe-Harbour Egyezménnyel úgy tűnt, hogy Európa képes valamelyest az USA-ba is exportálni adatvédelmi politikáját, ugyanakkor a 2001. szeptember 11. utáni fejlemények (pl. a légi utasok személyes adatainak átadásáról szóló megállapodás) az Egyesült Államok erősödő befolyását jelzik (Jóri, 2005, 35.) Többen a jelenleg zajló adatvédelmi reform politikai tétjének tartják, hogy az EU képes-e visszavenni a kezdeményezést az adatvédelmi politika területén.
[225] Magyar összefoglalást ld. pl. Jóri, 2005, 32-33.
[226] Bennett, 1998, 106-108.
[227] Jay – Hamilton, 1999, 10.

jogfejlődés eredményeinek (ideértve természetesen az információs önrendelkezési jog elvét is) hatásait vizsgálva megállapítja, hogy azok jelentős hatással voltak az irányelvre:[228] az adatvédelmi irányelv az érintett hozzájárulását a jogalapok között elsőként említi,[229] és széles körben biztosítja az érintett jogait az adatkezelés folyamata során.[230]

A technológia fejlődésére az Európai Unió az adatvédelmi irányelv elfogadását követően hamarosan szektorális adatvédelmi szabály megalkotásával is reagált. A 97/66/EK irányelv[231] a távközlési szektor adatvédelmi szabályait tisztázta, kitérve a kommunikáció bizalmasságára, a forgalmi és számlázási adatokra, és a kéretlen telefonhívásokra és faxüzenetekre vonatkozó szabályokra is.

2.3.2.3 Nemzeti jogalkotás

A német alkotmánybíróság által 1983-ban megfogalmazott információs önrendelkezési jog elvének jelentős hatása volt számos európai állam jogrendszerére. Mindenekelőtt a jogalkotó ennek megfelelően módosította a német adatvédelmi jog tartományi és szövetségi szintű szabályait, de az elv érezhetően hatott a 1986-os osztrák törvénymódosításra, valamint a norvég, finn és holland szabályozásra is.[232]

A legjelentősebb változásokat persze maga az adatvédelmi irányelv ösztönözte, amely az információs önrendelkezési jog elvét ugyan nem vette át, de az első generációs szabályozáshoz képest jelentős előrelépést tett számos területen (és különösen az érintetti kontroll megteremtésében), és összességében a második generációs adatvédelmi jogalkotás legfontosabb példájának tekinthető. Az irányelvet a tagállamoknak 1998-ig kellett implementálniuk,[233] így az irányelv jogi megoldásai – kisebb-nagyobb, de jelentéktelennek semmiképp sem mondható különbségekkel – az évtized végére az EU tagállamok belső jogának részévé vált.

Az 1990-es években, a szocialista rendszerek összeomlását követően Kelet-Közép-Európa országai is sorra fogadták el adatvédelmi törvényeiket. A személyes adatok védelme rendszerint emberi jogként bekerült ezen országok alkotmányaiba is, leginkább a kommunizmussal való szakítás szimbólumaként. Egyes államok adatvédelmi joga nemcsak időben előzte meg például az olasz és görög adatvédelmi jog megalkotását, de némelyik – ideértve például a magyar szabályozást is – szigorában, szabályozási filozófiájában az akkori nyugat-európai átlagot is meghaladta.[234] 1992-ben Csehszlovákiában[235] és Magyarországon, később – immár az adatvédelmi irányelv figyelembevételével – 1997-ben

[228] Amely egyébként erősen kompromisszumokat igénylő jogszabály révén az információs önrendelkezési jog talaján álló szabályozásnál alacsonyabb védelmi szintet garantál.
[229] A hozzájárulás az általános jogalapok, a különleges adatokra vonatkozó jogalapok és a megfelelő védelmi szintet nem biztosító harmadik országba történő adattovábbítás jogalapjai között egyaránt szerepel.
[230] Mayer-Schönberger, 1998, 234.
[231] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (a továbbiakban: távközlési adatvédelmi irányelv). A jogszabályt 2002-ben új irányelv váltotta fel (Az Európai Parlament és a Tanács 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (a továbbiakban: hírközlési adatvédelmi irányelv)
[232] Mayer-Schönberger munkája alapján összefoglalja Jóri, 2005, 27.
[233] Több tagállam jelentős késéssel ültette át az irányelvet, de végül ez minden tagállamban megtörtént.
[234] Majtényi, 2006, 97.
[235] A szétválást követően a cseh és szlovák adatvédelmi jog része is lett.

Lengyelországban, majd 1998-ban, felváltva a 92-es szabályozást, Szlovákiában fogadtak el adatvédelmi törvényeket. Ezek hatálya mind az állami szféra, mind a magánszféra szereplőinek manuális és számítógépes adatkezeléseire kiterjedtek.[236] Az 1990-es évek végére tehát Európa szerte megjelentek az adatvédelmi jogszabályok, függetlenül attól, hogy az adott állam az Európai Unió tagja volt-e vagy sem.

2.3.2.4 Az adatvédelmi szabályozás kialakulása Magyarországon

Magyarországon – igaz, nem a nyugat-európai, első generációs szabályozási modellt követve, de – egészen korán, már 1977-ben megjelent a jogrendszerben a személyes adatok védelmére való utalás: a Ptk. a személyhez fűződő jogok között úgy rendelkezett, hogy a számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat, és hogy a nyilvántartott adatokról tájékoztatást – az érintett személyen kívül – csak az arra jogosult szervnek vagy személynek lehet adni. Emellett rögzítette az érintett helyesbítéshez való jogát is.[237] Később az 1992-es adatvédelmi törvény módosította e rendelkezést, kiterjesztve annak hatályát a manuális adatkezelésekre is.[238]

1981-ben Vámos Tibor akadémikus tett javaslatot egy immár önálló informatikai törvény megalkotására, ez azonban a politika részéről ekkor visszhang nélkül maradt. A 80-as évek második felében azonban a KSH szellemi műhelyében (többek között Könyves-Tóth Pál aktív közreműködése mellett) elindult egy előkészítő munka, amelynek keretében 1987-ben Sólyom László (a KSH megbízásából) készített szabályozási koncepciót és szövegtervezetet.[239]

1989-ben a személyes adatok védelme és a közérdekű adatok nyilvánossága alapvető jogként bekerült az Alkotmányba. A kodifikációs előkészítő munkák tehát a jogállami forradalom idején is zajlottak, és az adatvédelem és információszabadság kérdése e folyamatok egyik jelképe lett. A 90-es évek elejére elfogadottá vált, hogy nemcsak a demokratikus intézményrendszer díszeként szükséges a kérdés törvényi szabályozása, hanem konkrét szerepe is van az állami információpolitika alakításában.[240]

Egészen korán, szintén 1989-ben lezajlott az első adatvédelemmel kapcsolatos közvélemény-kutatás,[241] amely azt mutatta, hogy a magyarok viszonylag komoly jelentőséget tulajdonítanak a magánszféra védelmének,[242] nagyjából-egészében ismerik a főbb állami adatkezeléseket, és egyben igen bizalmatlanok is e szervezetekkel szemben.[243]

---

[236] Majtényi, 2006, 98-104.
[237] Régi Ptk. 83. § (1978. március 1-től hatályos szöveg). E rendelkezéseknek azonban szocializmus alatt érdemi joggyakorlata nem volt.
[238] E rendelkezések a régi Ptk. hatályon kívül helyezéséig megmaradtak. Az új Ptk. nevesített személyiségi jogként nevesíti a személyes adatok védelméhez való jogot, de további szabályokat egyáltalán nem tartalmaz.
[239] Könyves-Tóth, 1992, 807.
[240] Balogh, 1998, 201.
[241] Székely Iván, Tölgyesi János és Várnai Gábor közreműködésével. Az eredmények összefoglalását ld. Székely, 1991
[242] Megelőzve például a munkanélküliség, a női egyenjogúság, a bevándorlás, és a munkáshatalom kérdését (Székely, 1991, 17.). Majtényi a vizsgálat elemzésekor megjegyzi: „Nagyon is figyelemre méltó, hogy a privacy fontosságát éppen a szólásszabadság és az információszabadság közé lőtték be a hazai válaszadók”. (Majtényi, 2006, 58.)
[243] Székely, 1991, 43.

Az Országgyűlés aztán 1992-ben elfogadta a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. LXIII. törvényt, amely egyértelműen a második generációs adatvédelmi jogalkotás terméke. A törvény hatálya mind az állami szféra, mind a magánszféra szereplőinek manuális és számítógépes adatkezeléseire kiterjedt.[244] A törvény kifejezetten az Alkotmányban nevesített személyes adatok védelméhez, valamint a közérdekű adatok nyilvánosságához fűződő jogok[245] érvényesülését kívánta szolgálni. Az Alkotmánybíróság által 1991-ben részletesen kifejtett információs önrendelkezési jog koncepciója (bár maga a kifejezés ebben a formában nem szerepelt a jogszabályban) áthatja a törvény rendelkezéseit. Mindenekelőtt megjelent a törvény céljában, ti. hogy személyes adataival mindenki maga rendelkezzen. Az adatkezelés jogalapja kizárólag az érintett hozzájárulása vagy törvény, illetve annak felhatalmazása alapján önkormányzati rendelet lehet. A törvény széles körben garantálta az érintettek tájékoztatáshoz, helyesbítéshez és – a törvényen alapuló adatkezelések kivételével – törléshez való jogát; utóbbival tulajdonképpen lehetővé téve az adatkezeléshez adott hozzájárulás visszavonását. A célhoz kötöttség követelménye és a készletező adatkezelés tilalma úgyszintén az adatvédelmi törvény hangsúlyos eleme volt. E rendelkezések elvben igen széles rendelkezési jogot és kontrollt biztosítottak az érintettek számára, ugyanakkor az adatkezelési jogalapok ilyen szűkre szabása a gyakorlatban később jelentős nehézségeket, majd az adatvédelmi irányelvvel való inkonformitást okozott.

2.3.3 A második generációs szabályozás főbb jellemzői

1. Mint azt korábban bemutattam, a személyi számítástechnika és később az Internet elterjedése alapjaiban változtatta meg az üzleti szféra adatkezelési gyakorlatát és potenciálját, és a világosság vált, hogy a Kis Testvérek adatéhsége az államével vetekszik, és adatkezeléseik ugyancsak veszélyt jelenthetnek az érintettek magánszférájára.[246] A második generációs szabályozás jellemzője, hogy, felismerve ezt a veszélyt, hatálya immár minden esetben kiterjed az üzleti szféra adatkezeléseire is.[247]

2. Ugyancsak széles körben elfogadottá vált, hogy az adatvédelmi szabályozás hatályát nem csak a számítógéppel, de a manuálisan végzett adatkezelésekre is ki kell terjeszteni. A magánszféra veszélyeztetését ugyan az adatkezelések automatizálása hozta felszínre, de a gyakorlatban nincs értelme az adatkezelés módja alapján különböző szabályokat felállítani, már csak azért sem, mert az adatkezelések nagyon gyakran „vegyesek”: az adott személyes

[244] Az adatvédelmi törvény, szokatlan módon, egészen 2004-ig egyáltalán nem tartalmazta a hatályáról szóló rendelkezéseket, de épp ezen (esetleges) korlátozó szabályok hiánya miatt azt minden adatkezelésre alkalmazni kellett. Ugyanakkor az Avtv. olyan módon módosította a Ptk. személyes adatok kezelésére vonatkozó szabályait, hogy azok a számítógéppel végzett adatkezelés mellett a „más módon történő”, azaz manuális adatkezelésre is kiterjedjenek.

[245] A magyar jogalkotó igen előremutató megoldást választott, amikor e két alapvető jogot közös törvényben, egymásra tekintettel szabályozta, és a felügyeletükre is közös intézményt hozott létre. Később több más állam is hasonlóan járt el. A magyar jogszabályi környezet jelentős hatással volt Brandenburg tartomány – és közvetetten az annak mintájára készült berlini és schleswig-holsteini jogalkotásra is. Dix, 2001, 69-74.

[246] Később kiderül, hogy a kis testvérek adatgyűjtése a Nagy Testvér tevékenységét is nagyban segítheti (ld. 3.1.2.2 fejezetet)

[247] E ponton azonban az Egyesült Államok adatvédelmi jogának fejlődése látványosan eltér az európai útról; az amerikai adatvédelmi szabályozás hatálya általános jelleggel nem terjed ki az üzleti szféra adatkezelőire.

adat az adatkezelőnél papír alapon és számítógéppel kezelt digitális adatként egyaránt megjelenhet.

3. A személyes adatok védelme több államban alkotmányos alapjogként védett. Ez tipikus állomása a kelet-közép-európai adatvédelmi jogfejlődésnek, de több nyugat-európai országban, így Spanyolországban, Portugáliában, Görögországban, Németországban, Ausztriában, Hollandiában is alkotmányos szintű a személyes adatok védelméhez fűződő jog. Amíg tehát az adatvédelem fejlődésének második korszakára egyértelműen a kis testvér előretörése jellemző, számos államban a jogalkotó jelentősen megerősítette az egyén állammal szembeni pozícióját is. Az alapjogi védelem – bár ez a vonatkozó szakirodalomban sokat tárgyalt és vitatott témakör – magánjogi jogviszonyokra való kiterjesztése[248] alapvetően elfogadottá vált.[249] Egyértelműen az alapjogi védelem megerősödését mutatja, hogy 2000-ben a nizzai csúcstalálkozón aláírt Alapjogi Charta – igaz, ekkor még kötelező erő nélkül[250] – már a magán- és családi élet védelmétől elkülönült fejezetben, önállóan nevesített alapjogként tárgyalja a személyes adatok védelméhez fűződő jogot. A Charta az „adatvédelem hatékonyságára komoly befolyást gyakorol az Európai Unión belül és azon kívül is." […] Ez idáig a magánélet, a magántitok védelmét garantáló rendelkezések adták az adatvédelem nemzetközi jogi hivatkozási alapját. Ettől kezdve a személyes adatok védelme nevesített alapjoggá vált a nemzetközi jogban."[251]

4. A második generációs szabályozás legfontosabb jellemzője az adatalany szerepének megerősödése. Az érintett szerepe jelentősen megnő, egyes esetekben az adatkezeléshez a hozzájárulására van szükség, más esetekben joga van tiltakozni bizonyos adatkezelések ellen,[252] míg az információs önrendelkezési jogon alapuló adatvédelmi rezsimekben az érintettek általános és igen széles rendelkezési jogot kaptak személyes adataik kezelésével kapcsolatban. Az érintetti részvételi jogok kiszélesedése lehetővé teszi a folyamatos kontroll megvalósítását. Az adatkezeléssel kapcsolatos döntések meghozatala (legalábbis elvileg) tehát nagyrészt az érintetthez került át, elvárva egyben egyfajta aktív részvételt is a részéről.[253]

Ebben a szabályozási logikában kiemelt szerepet kap az érintett hozzájárulása: a hozzájárulás az irányelv alapján az egyik legfontosabb adatkezelési jogalap, amely szerepet kap a különleges adatok kezelése és az adatok harmadik országba történő továbbítása kapcsán is –utóbbi esetben a hozzájárulás legalizálja a megfelelő védelemmel nem rendelkező országokba történő adattovábbítást is.[254] Bár az irányelv az egyes jogalapok között elvileg nem teremt hierarchiát, a gyakorlatban a hozzájárulás tényleges

[248] Azaz a horizontális hatály elismerése
[249] Gárdos-Orosz, 2011, 72., 146-147.
[250] A Parlament és a Bizottság már 2001-ben nyilatkozattal ismerte el, hogy tevékenységét a Charta keretei között végzi, és egyre többször jelent meg hivatkozási alapként az Európai Bíróság előtt is (az Elsőfokú Bíróság és a főügyészek több esetben hivatkoztak rá, maga az Európai Bíróság ugyanakkor tartózkodott ettől), ld. Gárdos-Orosz, 2011, 178. A Charta végül a Lisszaboni Szerződéssel 2009-ben kötelező jogi normává vált.
[251] Majtényi, 2003, 581.
[252] Mayer-Schönberger, 1998, 227.
[253] Mayer-Schönberger, 1998, 231.
[254] A hozzájárulás szerepéről ld. még Kosta, 2013, 105., 108., valamint WP29, 2011b, 5-6.

szerepe az egyes országok adatvédelmi kultúrájában eltérő szerepet kapott: látunk példát arra, hogy a törvényi felhatalmazáson kívül a hozzájárulás szinte az egyetlen széles körben alkalmazható jogalap (pl. eleinte Németországban, vagy egészen 2012-ig Magyarországon), továbbá arra is, hogy a hozzájárulás a többi jogalaphoz képest valamilyen módon kiemelt szerepet kap,[255] míg más államok adatvédelmi jogában és kultúrájában az érintett hozzájárulásának szerepe jóval kisebb (pl. Egyesült Királyság).

A második generációs szabályozás fő jellemzője tehát, hogy a technológia-specifikus megközelítés helyett (amelyet a technológia gyors fejlődése reménytelenné tett) a jogalkotó absztrakt szabályokat alkotott, és – bízva abban, hogy azzal élni is fog – az érintettet széleskörű rendelkezési joggal ruházta fel az adatkezelés egész folyamatára nézve,[256] számítva egyben aktív közreműködésére is.[257]

5. Ugyanakkor ebben az időszakban is megjelentek már egyes, az érintett alkupozícióját erősíteni kívánó, de néhol az információs önrendelkezési jogot tulajdonképpen szűkítő (paternalista) imperatív szabályok az adatvédelem területén.[258] Ilyen például a felróhatóságtól független vagy fokozott felelősséget elváró adatvédelmi szankciók megjelenése, a különleges adatok kezelésének – kivételekkel megtört, de – főszabály szerinti tiltása,[259] a célhoz kötöttség követelményének abszolút, az érintett hozzájárulásától független követelménye,[260] vagy a magyar szabályozásban a további adatfeldolgozó igénybevételének tilalma.

6. Néha ugyan újabb generációs szabályozás jellemzőjeként tekintenek a szektorális szabályozás megjelenésére és elterjedésére,[261] álláspontom szerint azonban az egyes ágazati adatvédelmi szabályok megjelenése jól illeszkedik a második generációs szabályozás paradigmájába, sőt – legalábbis egyes területeken – szükségszerűen következik az információs önrendelkezési jog elvéből és a jogalapokon nyugvó adatvédelmi szabályozás logikájából. Amennyiben ugyanis az információs önrendelkezési jog, mint alkotmányos jog csak jogszabályi szinten korlátozható, szükségszerűen megjelennek az adatkezelést elrendelő szektorális szabályok azokon a területeken (pl. az államigazgatás során történő adatkezelés kapcsán), ahol az érintett hozzájárulása nem jöhet

[255] Erre példa lehet Észtország, Belgium (a különleges adatok tekintetében), Görögország, Norvégia (ld. Bygrave-Schartum, 2010, 165.), vagy az Európai Bíróság jogalapok közvetlen hatályát kimondó döntésének alapjául szolgáló spanyol szabályozás, illetve 2012-től a hatályos magyar szabályozás.
[256] Mayer-Schönberger, 1998, 230-231., ill. e gondolatokat idézi és magyarázza Jóri, 2005, 27.
[257] Solove ezt a megközelítést nagyon találóan privacy self-management-nek nevezi. Solove, 2013, 1880.
[258] Az információs önrendelkezési joggal szemben megfogalmazott kritikákra egy lehetséges válasz lehet annak paternalista, imperatív szabályokkal megvalósuló korlátozása. Ez esetben az állam igyekszik megvédeni az érintettet saját akaratától függetlenül, illetve akár azzal szemben is. E megközelítésnek egyes elemei már a 80-as, 90-es években megjelentek.
[259] Mayer-Schönberger, 1998, 233. A szerző felosztása szerint ezek már a negyedik generációs szabályozás jellemzői.
[260] Azaz az érintett hozzájárulásával sem lehet cél nélkül vagy a meghatározott célhoz nem szükséges adatok kezelése. Ez az irányelv és a magyar szabályozás vonatkozásában is fennáll. Ld. Bygrave-Schartum, 2010, 164., illetve Jóri-Bártfai, 2005, 161. Az irányelvben található még néhány, az érintett rendelkezésétől függetlenül alkalmazandó szabály, így például az adatbiztonsági intézkedések, vagy az adatkezelés bejelentési kötelezettsége.
[261] Mayer-Schönberger, 1998, 233., Majtényi, 2003, 583.

szóba jogalapként.[262] Emellett az adatkezelések számának drasztikus növekedése, az egyes államigazgatási vagy piaci szektorokban megjelenő adatkezelések speciális problémái és a technológiai fejlődésre adott válaszok is szektorális adatvédelmi szabályok megalkotásához vezettek.[263]

A szektorális szabályozás nemcsak az állami vagy egyéb kötelezően elrendelt adatkezelések esetén jelenti az információs önrendelkezési jog korlátozását. A szektorális adatvédelmi szabályok gyakran piaci viszonyokra is vonatkoznak, és egy adott jogviszony kapcsán meghatározzák az adatkezelési cél(oka)t, a kezelhető adatok körét, az adatkezelés időtartamát, az adatok továbbításának szabályait, így e tényezőket tulajdonképpen kiveszi a jogalkotó a szolgáltató és az érintett alkufolyamatából.

7. Fontos, rendszerszintű következményekkel járó változás a második generációs szabályozás keretében az adatkezelési jogalapok megjelenése és elterjedése. Az adatvédelmi irányelvben – és így a tagállami adatvédelmi szabályozásban is – hangsúlyos szerepet kapnak az adatkezelés jogalapjai, amelyek a korábbi nemzetközi dokumentumokban nem jelentek meg.[264] Az irányelv alapján az adatkezelőnek mindenképpen kell valamilyen jogalapot igazolnia, szemben például az Egyesült Államok rendszerével, ahol az adatkezelés mindaddig jogszerű, míg a jog valamilyen tiltást vagy korlátozást nem ír elő. Igaz, az irányelv 7. cikk f) pontjában foglalt érdekmérlegelésen alapuló jogalap igen tág mérlegelési lehetőséget ad az adatkezelőnek, egy esetleges jogvita során azonban mégiscsak neki kell igazolnia az adatkezelés jogalapjának fennállást, és ennek sikertelensége az adatkezelés jogellenességét eredményezi.

8. További fontos tendencia az adatvédelmi felügyelőhatóságok szerepének erősödése. Az érintetti kontroll erősödésével párhuzamosan megjelent az a jogosítvány is, hogy az adatalanyok e szervekhez fordulhatnak bejelentéseikkel. Egyes országokban inkább ombudsman-jellegű intézmények, máshol érdemi döntési jogosultsággal is rendelkező hatóságok jöttek létre.[265] Az évezred végére az irányelv harmonizációs törekvései ellenére is összességében elég változó, de az első generációs szabályozási környezethez képest jóval erősebb és főként szélesebb feladat- és hatáskörökkel rendelkező adatvédelmi felügyelőszervek találhatók Európa országaiban.

9. Az adatkezelések számának növekedésével párhuzamosan egyszerűsödnek a nyilvántartásba-vételi kötelezettségre vonatkozó szabályok is. Több helyen az adatkezelések (adatbázisok) engedélyezését bejelentési kötelezettség váltotta fel.[266] A

[262] A népszámlálás ítélet például Németországban jogalkotási dömpinget eredményezett, amely az igazgatáson belül megteremtette a jogalapot a status quo fenntartására (Jóri, 2005, 36.)
[263] Például a direktmarketing szabályozása, a pénzügyi szektor vagy egészségügyi szektor szabályozása, vagy az EU szintén is megjelenő hírközlési adatvédelmi szabályrendszer.
[264] Ld. WP29, 2014, 6-7. Ugyanakkor egyes nemzeti jogokban már korábban is megjelentek adatkezelési jogalapok, így a német BDSG már 1977 óta zárt felsorolásként listázza az adatkezelés jogalapjait. (Kosta, 2013, 50.)
[265] A felügyelőhatóságok szerepének változásáról ld. részletesen Mayer-Schönberger, 1998, 227-228., 234.
[266] Jóri, 2005, 27-28.

bejelentésre vonatkozó keretszabályok azonban bekerültek az irányelvbe is,[267] amely így harmonizálta, de egyben „be is betonozta" a bejelentési kötelezettség intézményét.[268]

10. Végül az adatvédelmi irányelv alapján e korszakban alakult ki a harmadik országba történő adattovábbítások harmonizált feltételrendszere, amelynek kulcsfogalma a „megfelelő védelmi szint" biztosítása. E koncepción keresztül az Európai Unió számos államba sikerrel exportálta az európai típusú adatvédelmi megközelítést,[269] és a nemzetközi adattovábbítások részletes feltételrendszerének kidolgozása jelentős hatást gyakorolt a különböző önszabályozási mechanizmusokra is.

2.3.4 Egy alternatív megoldás: kitekintés az Egyesült Államok adatvédelmi szabályozására

Az Egyesült Államok adatvédelmi joga a második generációs szabályozás időszakában elvált az európai fejlődés útjától, azaz a felmerülő technikai és társadalmi fejlődés által kiváltott kihívásokra egészen másként reagált, mint Európa államai. A második generációs (európai) szabályozás értékelése és az önszabályozási eszközök részletes elemzéséhez egyaránt érdekes lehet egy rövid kitekintést adni az Egyesült Államok adatvédelmi szabályozására.

Az állami (hatósági) adatkezelésekre az Egyesült Államokban is létezik átfogó, szövetségi szintű szabályozás (Privacy Act, 1974), de az az Európában megszokottnál enyhébb szabályokat ír elő (például számos esetben az adatokat az eredetitől eltérő célra is fel lehet használni, az 1936 óta használatos társadalombiztosítási szám egyre inkább általános azonosító szerepét tölti be az egyes hatósági adatkezelések során, az adatkezelés minőségi követelményei alól sok a törvényi kivétel, stb.).[270] E törvény azonban a piaci szereplők adatkezelésére nem alkalmazható, és rájuk nézve nincs is átfogó adatvédelmi szabályozás, azaz az adatvédelem hatályának ilyen irányú kiterjesztésére az Egyesült Államokban nem került sor.

Számos jól körülhatárolt területre vonatkozóan azonban született privacy-védő szektorális szabályozás: találhatók például adatvédelmi szabályok a banktitok és a hírközlési szabályozás kapcsán, a gyermekek online tevékenységére, az elektronikus úton küldött direktmarketing-üzenetekre vonatkozóan, vagy olyan speciális területeken, mint a munkavállalók poligráfos vizsgálata,[271] vagy a kikölcsönzött videofilmek listájának nyilvánossága.[272] Az e jogszabályok által biztosított védelmi szint igen különböző, és

[267] 95/46/EK, 18-19. cikk

[268] Az irányelv jelentős eltérést enged ugyan a bejelentési kötelezettség tagállami szabályozásában, az adatkezelések számának további drasztikus növekedése kapcsán felmerülhet a bejelentési kötelezettség teljes eltörlése is (ld. erről pl. Jóri, 2005, 41.), amely azonban tagállami hatáskörben jelenleg nem oldható meg. Az EU új adatvédelmi rendeletének tervezete – igaz számos más, adatkezelőt érintő kötelezettség bevezetése mellett – már nem tartalmazza a bejelentési kötelezettséget.

[269] Jóri, 2005, 33-35.

[270] Sziklay, 2011 41.

[271] A korábbi és jelenlegi szektorális szabályozásokról ld. Regan, 1995, 6-7., Sziklay, 2011, 41., valamint az alábbi weblapot: http://www.informationshield.com/usprivacylaws.html [2014.05.10.]

[272] A Video Privacy Act (1988) arról szól, hogy az érintett beleegyezése szükséges a rá vonatkozó kölcsönzési és kapcsolódó adatok harmadik személynek történő átadásához. A törvény egy videofilm-kölcsönzési lista nyilvánosságával kapcsolatos botrányt követően került megalkotásra. Szigeti, 2009, 161-

összességében elmarad az európai védelmi szinttől,[273] különös tekintettel arra, hogy az Egyesült Államokban egységes adatvédelmi felügyelőhatóság sem működik, hanem az egyes ágazatokat egyébként felügyelő hatóságok, illetve a gazdasági szférában – a fogyasztóvédelmi jogok megsértésének szankciórendszerén keresztül – a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission) lát el felügyeleti feladatokat.

A különbségek alapját Whitman az eltérő alkotmányos értékválasztásban látja: az európai alkotmányosság központi eleme az emberi méltóság, míg az amerikaié az emberi szabadság. Whitman amellett érvel, hogy az amerikai privacy-felfogás nem gyengébb, mint az európai, csak más alapjogi felfogásra épül.[274] Meg kell említeni azt is, hogy egyes, a legújabb európai adatvédelmi jogban kifejezetten újnak számító és az adatvédelmi szabályozást erősítő jogintézmények az Egyesült Államokban már korábban megjelentek: az egyes szektorokban kötelező adatvédelmi hatásvizsgálat (Privacy Impact Assessment) vagy az adatvédelmi incidensek bejelentési kötelezettsége (Data Breach Notification) az új európai Rendelettervezetnek is fontos újításai. Ugyancsak említésre érdemes, hogy az Egyesült Államokban is zajlik annak vizsgálata, hogy a Safe Harbour elvek alapján mégiscsak elfogadjanak széles körben kötelező szabályokat a piaci szereplők számára.[275]

Az esetleges jelentős változásokig az Egyesült Államok megközelítése azonban összességében inkább a laisser faire elvet követi, és a jogalkotó kiindulópontként az adatvédelmi kérdéseket is a piaci erőviszonyokra és az iparági önszabályozásra hagyja, és csak akkor kíván e folyamatokba beavatkozni, ha az önszabályozás sikertelen.[276] Ez a modell nem szükségszerűen jelenti, hogy a piaci szereplők semmilyen adatvédelmi szabályrendszert ne követnének. Egyrészt számos területen létezik önszabályozás, másrészt önkéntesen is elfogadhatnak bizonyos adatvédelmi elveket, amelyekről adatvédelmi nyilatkozatok segítségével tájékoztatják a potenciális érintetteket. Utóbbi esetben a vállalkozások jellemzően az FTC által is ajánlott ún. Fair Information Practices Principles[277] vagy az OECD által kidolgozott adatvédelmi elveket fogadják el magukra nézve kötelezőnek. Ezek az európai szintű szabályozásnál alacsonyabb védelmi szintet garantálnak, elvileg azonban nincs akadálya ezeknél akár jóval szigorúbb adatvédelmi szabályok önkéntes elfogadásának sem.

Felmerül persze a kérdés, hogy kötelező állami szabályozás hiányában miért fogadna el egy szervezet magára nézve korlátozó jellegű szabályokat. A „tisztán" piaci alapú privacy-szabályozásnak az (lenne) a lényege, amint azt Swire összefoglalja, hogy a fogyasztók kényszerítik ki a megfelelő védelmet azáltal, hogy a vállalkozás adatkezelési gyakorlata

---

162. Szigeti épp emiatt az Egyesült Államok szabályozását a partikuláris jelzővel illeti, amely szerinte nem azonos a szektorálissal. „Az utóbbi egy funkcionálisan összefüggő terület szabályait (lásd: pénzügyi szektor, egészségügyi adatkezelés), míg az előbbi a szabályozás hatályának és mélységének részlegességét, széttöredezettséget hivatott kifejezni." Szigeti, 2009, 165.

[273] Az a tény, hogy egy-egy területen létezik szabályozás, csak annyit jelent, hogy a törvényhozó foglalkozik az adott területtel. Jó példa erre az ún. CAN-SPAM Act opt-out rendszert biztosító, az európainál tehát lényegesen megengedőbb szabályozása.

[274] Whitman gondolatait idézi Sziklay, 2011, 39. Whitman tanulmányát ld. Whitman, 2004

[275] Ld. Hirsch, 2013, 92-95.

[276] Movius – Krup, 2009. 174.

[277] A Fair Information Practices elveit eredetileg 1973-ban dolgozták ki az Egyesült Államokban, azóta számtalan verzióban és területen jelent meg adatvédelmi ajánlásként. Bővebben ld. (Kosta, 2013, 77.)

(akár jó, akár rossz) hírneve részévé válik, és a fogyasztók az általuk preferált adatkezelési gyakorlatot folytató szolgáltatót választják majd. Így a vállalkozások számára alapvetően a fogyasztók (privacy) igényeinek kiszolgálása jelenti a kényszerítő erőt. E modell jogi érvekkel is alátámasztható. A piaci viszonyok alapvető szabályozó eszköze a (mellérendelt alanyok) szerződése, így az adatvédelem kérdését is e keretek között kell megoldani, és az állami szabályozás e viszonyokba való beavatkozást jelent. Az alapjogi alapú megközelítés elsősorban az állampolgár–állam viszonylatában alakult ki, ahol az állampolgárok az állam kényszerítő erejével állhatnak szembe.[278]

A tisztán üzleti modellt azonban Swire is kritizálja.[279] A piaci kudarcok okai elsősorban az információs aszimmetriában keresendők: a vállalkozás a fogyasztóhoz képest jóval pontosabban tudja, hogy mit szeretne tenni az adatokkal, és az érintetteknek jelentős költségbe (időbe és erőfeszítésbe) kerül ezen információk megismerése, a vonatkozó adatvédelmi nyilatkozat tanulmányozása. Még ennél is sokkal több erőfeszítésbe telik, ha egyáltalán lehetséges, az arról való meggyőződés, hogy a vállalkozás valóban betartja a nyilatkozatában vállaltakat. A felhasználók a teljes informáltság (elvi lehetősége) mellett sincsenek egyenlő alkupozícióban, a fogyasztó részéről szakértelmet és jelentős erőfeszítés igényelne, hogy „tárgyaljon” például egy online szolgáltatóval vagy egy nagy távközlési vagy pénzügyi szolgáltatóval az adatvédelem kívánatos szintjéről, és ezen erőfeszítések szinte bizonyosan nem térülnek meg.[280]

A piaci szabályozás kritikájával egyébként egyetértve fel kell hívni a figyelmet néhány tényezőre. A fogyasztók ideje/figyelme és alkupozíciója az idézett tanulmány (1997) óta jelentősen romlott, mivel az Internet és mobiltechnológia elterjedése miatt megsokszorozódtak azok az esetek, amikor az egyén adatkezeléssel együtt járó szerződéses kapcsolatba lép.[281] Emellett, és ez lényegesen nagyobb gond, ezek a problémák a legszigorúbb, az információs önrendelkezési jogot következetesen elismerő adatvédelmi jogi rezsimben[282] is maradéktalanul fennállnak. A praktikus különbség például az online szolgáltatások igénybevétele során mindössze egy apró checkbox-pipa egy weblapon vagy egy jóváhagyó érintés a mobiltelefonon. Míg a tisztán piaci modellben az érintett a fenti okok miatt végső soron nem fog az adatvédelmi szempontok miatt más partnerrel szerződni, addig utóbbi rezsimben végső soron nem fog az egyébként őt megillető széleskörű (alapvető) jogaival élni, és így összességében az érintett erős jogi pozíciója a gyakorlatban alig realizálódik. Ez alól azok az esetek jelenthetnek fontos kivételt, ahol a tisztességtelen/jogellenes adatkezelés kellően mélyen behatol az érintettek intimszférájába

[278] Swire, 1997, 3-4. Európában széles körben elfogadottá vált az alapvető jogok horizontális hatálya, azaz azok nem csak az állam-állampolgár viszonylatban nyújtanak védelmet, hanem magánjogi jogviszonyokban, például a piaci szereplők jogellenes adatkezelésével szemben is.

[279] Alapvetően az önszabályozás modelljét tartja helyesnek, amely végülis nem terjeszkedik túl a szerződéses jogviszonyon.

[280] Swire, 1997. 4. Ez az egyensúlytalanság Swire szerint ráadásul mindenképp az adatok lehető legszélesebb körű felhasználásához vezet, mivel a vállalkozás az adatok hasznosításából eredő előnyöket teljes egészében élvezik, míg az ebből eredő hátrányokat korlátozottan szenvedik el.

[281] Érdemes a számos online profilra, közösségi hálózatokra, mobiltelefonra letölthető, helymeghatározási adatokat is igénylő applikációkra gondolni.

[282] Mint amilyen például az 1992-es Avtv-n alapuló magyar adatvédelmi szabályozás.

(például tolakodó direktmarketing üzenetek vagy telefonhívások), és annak valóban zavaró volta miatt az érintett mégiscsak fellép, és igénybe veszi a jogvédelmi eszközöket.[283]

2.4 Következtetések

A dolgozat jelen fejezetében részletesen áttekintettem az adatvédelmi szabályozás európai történetét – rövid kitekintéssel az Egyesült Államok szabályozására. A jogterület fejlődését – elsősorban a könnyebb áttekinthetőség kedvéért – generációs felosztásban tárgyaltam, többször hangsúlyozva, hogy éles cezúra az egyes korszakok között nem húzható, valamelyik szabályozási generáció jellemzője rendszerint már korábban megtalálható volt egyes nemzeti jogszabályokban vagy a jogirodalomban. A részletes történeti elemzés során feltártam a technológiai fejlődésnek, és a technológia alkalmazásából eredő társadalmi változásoknak az adatvédelmi szabályozásra gyakorolt hatását.

A második fejezet kutatásai eredményei alapján az alábbi következtetések vonhatók le. A technológia fejlődésével egyre több olyan eszköz jött létre, amely a megfigyelés, az adatfeldolgozás, vagy az adatközlés hatékonyságát fokozták, összességében – potenciálisan vagy ténylegesen – folyamatosan szűkítve az egyének magánszféráját. Ahogy Székely Iván fogalmaz: „Az információs magánélet határainak történeti változását »omlások« sorozatával" írhatjuk le, a technológiai fejlődés következtében a magánélet hagyományos határai folyamatosan erodálódtak.[284]

Az adatvédelemmel kapcsolatos gondolkodás és jogalkotás közvetlenül reflektált a technológia fejlődésére. Az első generációs adatvédelmi szabályozás a nagy állami adatbázisok összekapcsolása kapcsán felmerülő, az állami információs túlhatalomtól (a Nagy Testvértől) való félelemre adott közvetlen és első reakciónak tekinthető. Az érintettek magánszférájának védelmét a jogalkotó az adatkezelők korlátozásával kívánta biztosítani, és a szabályozás szintjén még nem merült fel a személyes adatok feletti érintetti kontroll megteremtésének igénye. A szabályozás tehát egyértelműen „adatkezelő-központú" volt, igaz ez akkoriban néhány nagy, elsősorban állami adatkezelőt jelentett.

A technológia fejlődése, a PC majd az Internet megjelenése egyértelműen növelte az információs túlhatalom lehetőségét, de elsősorban nem az állam, hanem milliónyi potenciális új adatkezelő, az üzleti szféra szereplőinek oldalán. Az új szereplők megjelenésével egyrészt felmerült az igény a szabályozás hatályának kiterjesztésére, másrészt reménytelennek tűnt az adatkezelőkre és a konkrét adatkezelési technológiára koncentráló szabályozás fenntartása. A jogalkotó alapvetően absztrakt szabályokat és elveket tartalmazó, a magánélet védelmét új – immár nemcsak az „intim" adatokra, hanem minden, egyénre vonatkozó adatra alkalmazandó – szabályokkal kívánta biztosítani, és az érintetti kontrollt előtérbe helyező szabályozást alakított ki. Ennek kapcsán visszanyúlt a magánszférát személyes adatok feletti érintetti kontrollként értelmező jogirodalmi koncepcióhoz: Westin híres könyvében például a privacy-t úgy határozza meg, mint az „egyének, csoportok vagy intézmények igénye annak meghatározására, hogy mikor,

[283] E problémakörről ld. még a második generációs szabályozás kritikáját a 3.2.1 fejezetben.
[284] Székely, 2004, 47-48.

hogyan, és milyen mértékben közölnek másokkal magukról információt".[285] Jelentős hatással volt a második generációs szabályozásra a német alkotmánybíróság 1983-as ítéletében megfogalmazott, az érintetti kontrollt talán a legteljesebben elismerő információs önrendelkezési jog elve is.

Az érintett tényleges szerepe ugyan tagállamonként kisebb-nagyobb eltéréseket[286] mutatott, (az irányelv kompromisszumos szövegezése sem kényszerítette ki az érintett azonos pozícióba helyezését), összességében azonban megállapítható, hogy az európai adatvédelmi szabályozás központi elemévé vált az érintetti kontroll gondolata, az adatvédelmi szabályozás logikája alapvetően „érintett-központúvá" vált. „A jogalkotó abban reménykedett – anélkül, hogy a lelkesedését elméleti vagy empirikus okokkal alátámasztotta volna – hogy a [jogokkal felvértezett] egyén lesz a sikeres adatvédelem legmegfelelőbb garanciája."[287]

A fentiek alapján az látható, hogy a szabályozás közvetlenül reagált,[288] méghozzá Európában alapvetően a „több adatvédelem" útját járva, a 80-as években kialakult technológiai változásokra, elsősorban a személyi számítástechnika és a kis testvérek, mint adatkezelők megjelenésére.

* * *

Megállapítható emellett, hogy az állami adatkezelésekkel szemben az adatvédelem szabályozása nagyjából-egészében jól működött (és működik ma is): az egyes adatkezeléseket egymástól a legtöbb államban elválasztották, ahol az adatvédelem alapjogi szintű védelmet is kapott, az alkotmánybíróságok eredményesen éltek annak előnyeivel, a Nagy Testvér negatív víziója alapvetően – nyilván az adatvédelmi szabályozáson kívül több más tényezőnek is köszönhetően – nem valósult meg.[289] Látni kell azonban azt is, hogy az állami adatkezelések terén a részletes szektorális szabályoknak köszönhetően lényegében továbbra is „adatkezelő-központú" a szabályozás, az érintetti kontroll jóval kisebb szerepet játszik (az adatkezelés tényét, célját, idejét, a kezelt adatok körét stb. alapvetően jogszabály, és nem az érintett határozza meg).[290]

---

[285] Saját fordítás. Az eredeti definíció így hangzik: „the claims of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." Westin, 1967, 7.

[286] Azon országokban, ahol az adatvédelmi szabályozás az információs önrendelkezési jog elvén alapul, illetve ahol – akár ennek következtében, akár ettől függetlenül – az érintett hozzájárulásának kiemelt jelentőséget tulajdonítottak, ez a kontroll nagyobb szerepet kapott, míg más államokban kisebb a jelentősége.

[287] Mayer-Schönberger, 1998, 227.

[288] Ld. például az adatvédelmi irányelv (4) és (6) preambulum-bekezdését.

[289] Az Echelon és nemrég a PRISM rendszer működésével kapcsolatos botrányok azt mutatják, hogy vannak nagy volumenű, átláthatatlan állami megfigyelések, amelyekben egyáltalán nem tisztázott az állam és a piaci szereplők (elsősorban a nagy internetes vállalkozások) viszonya. Az új technológiák és szolgáltatások azonban általánosságban nem vezettek új diktatúrák kialakulásához vagy meglévők megerősödéséhez, sőt pl. az arab tavasz eseményei során kifejezetten a hatalommal való szembeszegülést és nem az állampolgárok elnyomását segítették. A kínai internetcenzúra sikere egyszerre példázhatja egyrészt azt, hogy a diktatórikus hatalom kifejezetten tart e technológiák széleskörű szabad használatától, másrészt azt, hogy technikailag lehetséges e decentralizáltnak tűnő hálózatot is érdemben korlátozni. Kérdéses, hogy a korlátozás mellett mennyiben tudja hatékonyan a saját (pl. propaganda, totális megfigyelés) céljaira fordítani.

[290] Ugyanez igaz néhány piaci szektor adatkezelésére is.

A piaci szféra adatkezeléseivel kapcsolatban azonban azt látom, hogy a korszakot meghatározó jelentős tényező, az Internet megjelenése, és a 90-es évek derekától kezdődő elterjedése a szabályozás alapvető logikája szempontjából reflektálatlan maradt: szektorális szabályozás született ugyan, de ez az adatvédelmi szabályozás fundamentumait nem érintette. Az érintetti kontrollon alapuló szabályozás – annak ellenére, hogy a potenciális problémáival a szakirodalom már igen korán elkezdett foglalkozni – ugyanakkor egy ideig egészen jól bevált egy új technológiai környezetben is. A web 1.0 online szolgáltatásainak „látható részei" alapvetően jól idomultak e rendszerhez: mind a tájékoztatás, mind az érintetti hozzájárulás könnyedén megadható online környezetben, így a szolgáltatók nagy része – legalábbis a regisztrációt igénylő szolgáltatások esetén – hozzájárulás-jogalappal kezelte a személyes adatokat.

Egyes problémák első jelei az ezredforduló környékén már látszódtak. Egyre terjedtek egyes „kevésbé látványos" adatkezelések, így például az online világban már a weblap megtekintésével együttjáró cookie-elhelyezés, háttérben futó webanalitikák készítése, IP-cím alapján történő földrajzihely-meghatározás, később a targetált hirdetések megjelenése; az „offline világban" a pontgyűjtő akciókkal történő vásárlói követés, az ügyféladatbázis (CRM) és vállalatirányítási rendszerek működése, adatbányászati módszerek és félig-meddig automatizált üzleti döntések előtérbe kerülése, a ritkán vagy sosem törlődő biztonsági mentések készítése, stb. E háttérfolyamatok fő jellemzője, hogy átláthatatlanok nemcsak az érintettek,[291] de jellemzően a felügyelőhatóságok és az adatvédelemmel foglalkozó szakemberek és szakpolitikusok számára is. Az adatkezelőkön kívül egyre kevésbé tudta bárki is feltárni, hogy pontosan mi történik a vállalkozások informatikai rendszerének mélyén.

[291] Függetlenül attól, hogy valamely adatkezelési tájékoztató homályos pontja alapján megadott hozzájárulással vagy más, pl. érdekmérlegelésen alapuló jogalappal történt az adatkezelés.

3. PARADIGMAVÁLTÁS AZ ADATVÉDELEM EURÓPAI SZABÁLYOZÁSÁBAN

A 90-es évek végére Európában kialakult egy – egyes (részlet)kérdésekben jelentős eltéréseket is mutató – összességében mégis viszonylag egységes megközelítésű és jól harmonizált adatvédelmi szabályrendszer. Ennek az elméleti-filozófiai alapjai egészen a 80-as évekig nyúlnak vissza, és a szabályozás lényegi elemeit az Internet elterjedése tulajdonképpen nem érintette. Az elmúlt évek technológiai-társadalmi változásai és az érintettek adatvédelmi attitűdjének vizsgálati eredményei azonban felerősítették az adatvédelmi szabályozás kritikusainak hangját, és egyre szélesebb körben elfogadottá vált a szabályozás felülvizsgálatának igénye. Az Európai Unió szintjén e folyamat el is indult 2009-ben, és végül egy, az Európai Parlament által elfogadott, de véglegesnek korántsem tekinthető, és jövőjét tekintve is igen bizonytalan új Rendelettervezetben realizálódott.

Az alábbiakban mindenekelőtt összegzem az adatvédelmet ért legújabb technológiai kihívásokat, azok társadalmi hatásait, valamint a felhasználók adatvédelemhez való hozzáállását kutató felmérések eredményeit. Kritikai-elemző módszerrel áttekintem a jelenlegi adatvédelmi rezsimet ért főbb bírálatokat, és az adatvédelmi szabályozás változtatásaira tett szakirodalmi javaslatokat, majd felvázolom egy újgenerációs adatvédelmi szabályozás legfontosabb elemeit, és vizsgálom, hogy az európai adatvédelmi Rendelettervezet mennyire illik e rendszerbe. Végül összegzem és kiemelem e fejezet következtetéseit, és igazolom a disszertáció egyes téziseit.

3.1 Technológiai és társadalmi háttér

Az elmúlt 10-15 évben számos olyan technológiai változás történt, amely továbbra is jelentős kihívás elé állítja az adatvédelem szabályozását. Az újabb jelenségek mögött – legalábbis a 60-as, 70-es évekkel összehasonlítva – kevésbé forradalmi technikai újítások, sokkal inkább a korábbi technológiákban rejlő lehetőségek továbbgondolása, tömeges elterjedése és/vagy új típusú (üzleti) hasznosítása áll. Ez azonban nem jelenti azt, hogy e fejlemények ne gyakorolnának igen jelentős hatást az egyének magánszférájára, sőt, az alábbi összefoglaló alapján joggal mondhatjuk, hogy a magánszférát ért kihívások a korábbi évekhez képest jelentősen megnőttek. Az alábbiakban – egymásra tekintettel is – bemutatom e jelenségeket és azok adatvédelmi szabályozásra gyakorolt potenciális hatásait.

3.1.1 Technológiai háttér

3.1.1.1 Web 2.0-es szolgáltatások megjelenése

A leggyakrabban említett kihívást kétségtelenül az internetes szolgáltatások terén bekövetkezett változások jelentik. A 2001-es dotcom válságot követő időszakban az Internetes szolgáltatások és a felhasználás jellege megváltozott. Míg a 90-es évekre inkább

a statikus tartalmak, és a felhasználók felé irányuló információáramlás volt jellemző,[292] addig az új évezredben megjelenő szolgáltatások egyik lényegi jellemzője, hogy drasztikusan megváltozik a tartalomszolgáltatás jellege, és előtérbe kerülnek a felhasználók által generált tartalmak (User Generated Content), legyen az akár egy személyes profiloldal egy közösségi oldalon, egy blogbejegyzés, egy kép vagy egy video feltöltése. A felhasználóknak nemcsak a tartalmak előállításában lett nagyobb szerepe, de egyre inkább ők a tartalomtovábbítás (megosztás) és a tartalom-kiválasztás[293] főszereplői is. Az Internet ezen korszakát gyakran „web 2.0" elnevezéssel szokás jelölni.[294]

Ezek a lehetőségek átalakítják a felhasználók viselkedését is. A tendencia egyrészt az érintettek saját magukról történő, korábban hihetetlen mértékű adatközlést hozta magával, amely elsősorban a közösségi oldalakon szembetűnő:[295] „úgy tűnik, az emberek szeretnek online posztolni és másokról személyes, gyakran intim információkat keresni".[296] Ez önmagában még összhangban is lehetne az adatvédelem „érintetti kontrollt" középpontba helyező megközelítésével, de a többi technikai és társadalmi változásra tekintettel az érintettre nézve mégis jelentős kockázattal jár.[297] Amennyiben ezek a tartalmak más érintettek személyes adatainak nyilvánosságra hozatalával és/vagy továbbításával járnak (mint ahogy a gyakorlatban gyakran ez történik), ez azt is eredményezheti, hogy felhasználók tömege kerülhet adatkezelői pozícióba, és válhat így az adatvédelmi szabályozás kötelezettjévé.[298]

A közösségi oldalak megjelenésével azonban jóval többről van szó, mint hogy a felhasználók – átgondolva vagy átgondolatlanul – magukról vagy másokról információkat osztanak meg. A közösségi oldalakon rendszerint valós adatokkal történő regisztráció ugyanis egyértelműen összekapcsolhatóvá teszi a felhasználók tényleges személyét az „online profiljukkal". Utóbbiba a felhasználók által megadott adatokon kívül sokminden más is beletartozik: a viselkedésalapú reklámozás miatt követéssel (tracking) nyert

[292] "A web 1.0 nem szól másról, mint az online jelenlétről, a megmutatkozásról, cégek esetében a prospektus jellegű (ritkán frissülő) weboldalakról […] a különböző híroldalakról, vagyis a papírvilág egyfajta online leképezéséről, ahol a visszajelzés magától értetődő formája az e-mail vagy a telefon." Herendy, 2010

[293] A népszerűség alapján történő hírfolyam-megjelenések a közösségi oldalakon, a felhasználók által jónak értékelt szolgáltatások előtérbe helyezése például egy szállásfoglaló oldalon, a sokat olvasott blogok megjelenítése a hírportálok főoldalán, az "akik ezt a könyvet/zenét megvették, megnézték ezt is" típusú ajánlók, stb. mind azt mutatják, hogy a tartalom-kiválasztási mechanizmus (akár médiatartalom szerkesztéséről, akár szolgáltatásról van szó) részben átkerül a felhasználókhoz.

[294] A web 2.0 kifejezés Tim O'Reilly-nek köszönhetően vált ismertté és divatossá. Ld. részletesen O'Reilly, 2005. Az Internetes szolgáltatások korszakolása széles körben elfogadott módon nem kidolgozott, éles korszakhatárt, vagy a jelenleg elérhető szolgáltatásokat egyértelműen kategorizálni, a „web 2.0" fogalmát egyértelműen definiálni nehézkes, a kifejezés azonban – többé-kevésbé azonos jelentéstartalommal – széles körben elterjedt.

[295] Az Internetes szolgáltatásokban rejlő különbségeket szellemes feldolgozó, és az adatvédelem szempontjából nagyon is lényegre törő megfogalmazás szerint: „Web 1.0: Bring the web into our lives; Web 2.0: Bring our lives into the web" Ld. http://www.zeldman.com/2006/10/17/web-20-thinking-game [2014.05.20.]

[296] Tene, 2011, 15, 21.

[297] Különösen azért, mert az érintett egy-egy, általa esetleg ártatlannak vélt, vagy adott szituációban éppen az érdekeinek megfelelő adatközlés felett gyakorlatilag elveszti a kontrollt, és nem tudhatja, hogy az esetleg más kontextusban, más adatokkal összevetve milyen következtetések levonására alkalmas (ld. erről 3.2.1 fejezetet).

[298] Polefkó, 2011, 32., Alsenoy – Ballet – Kuczerawy – Dumortier, 2009, 70.

böngészési szokások,[299] a számítógépének paraméterei, a neki címzett (adott szolgáltatón keresztül küldött) levelek és üzenetek tartalma, és az ezekből egyre fejlődő adatbányászati eszközökkel levont további következtetések mind-mind könnyedén és közvetlenül összerendelhetők a felhasználó tényleges személyével.[300]

3.1.1.2 Felhőszolgáltatások megjelenése

Az elmúlt években egyre nagyobb mértékben terjednek a különböző felhőszolgáltatások. Ennek kapcsán megkülönböztethető az infrastruktúra, mint szolgáltatás (infrastructure as a serice, IaaS), a platform, mint szolgáltatás (platform as a service, PaaS) és szoftver, mint szolgáltatás (software as a service, SaaS) igénybevétele,[301] és e szolgáltatások természetesen kombinálhatóak, egymásra tekintettel is igénybe vehetőek.[302] A felhőszolgáltatások elterjedésének[303] köszönhetően nagymértékben változik a személyes adatok tárolásának módja is. Mind a vállalkozások, mind a magánszemélyek egyre több adatot és dokumentumot (e-maileket, képeket, bejegyzéseket, szöveges fájlokat, üzleti kalkulációkat stb.) tárolnak a „felhőben", azaz online tárhelyeken (ténylegesen távoli szerverparkok adathordozóin). Emellett egyre többször (online) szolgáltatásként veszik igénybe a különböző alkalmazásokat, szoftvereket – legyen az egy online szövegszerkesztő vagy prezentációkészítő program, játék, vagy éppen egy vállalkozás CRM vagy ERP rendszere.[304]

A felhőszolgáltatások jól látható előnyöket kínálnak: a felhasználó bárhonnan, többféle eszközzel hozzáférhet a dokumentumaihoz, szolgáltatások hatalmas választékából válogathat, a számítási kapacitást alapvetően nem neki kell biztosítania,[305] a dokumentumait könnyen megoszthatja másokkal, és nem kell aggódnia amiatt, hogy elveszíti az adatait (a biztonsági mentéseket és más informatikai biztonsági intézkedések a szolgáltató megteszi).[306]

Ugyanakkor számos jogi és biztonsági kockázat és bizonytalanság is felmerül. Először is bizonytalan a felhőszolgáltatást nyújtó szolgáltatókra (vagy a szolgáltató-lánc, jogi értelemben tulajdonképpen alvállalkozói lánc tagjaira) vonatkozó joghatóság. Könnyen előfordulhat, hogy a szolgáltatóknak a felhasználóétól teljesen idegen, akár jóval alacsonyabb védelmi szintet garantáló adatvédelmi szabályoknak kell csak megfelelniük,

[299] A Facebook "Like" gombjának működéséről, és az ezzel történő követésről ld. részletesen Roosendaal, 2012. A tanulmány nemcsak részletesen bemutatja a követés mechanizmusát, de egyértelművé teszi, hogy a követés a Facebook regisztrációval nem rendelkezőket is érinti (Roosendaal, 2012, 16-18.).

[300] Korábban ezek az információk „csak" egy IP címhez voltak rendelhetők. Több lépésben, más adatkezelőket bevonva ugyan az IP cím is összekapcsolható a felhasználóval, így az szintén személyes adatnak tekinthető, jelenleg azonban egyetlen adatkezelő képes ezeket az adatokat összekapcsolni.

[301] Ennek jellemzőit ld. Szádeczky, 2011, 49-51.

[302] Ruiter – Warnier, 2011, 362.

[303] Valójában sem a felhőszolgáltatás sem a mögötte meghúzódó koncepció nem új. A számítási kapacitás szolgáltatásként való igénybevétele a számítástechnika hajnalán megjelent (Dhillon – Kolkowska, 2011, 345.), és, mint azt korábban említettem, a 80-as évek elején a hálózatosodást is alapvetően lebutított terminálok központi hálózatra kapcsolódásaként képzelték el (ld. 2.3.1.3 fejezetet). A web alapú e-mail vagy bármilyen online tárhely igénybevétele (például egy honlap céljára) pedig lényegében majd' két évtizede „felhőszolgáltatás".

[304] Tene, 2011, 16.

[305] A költséghatékonyság a vállalatok számára is vonzóvá teszik e szolgáltatásokat (Szádeczky, 2011, 54.)

[306] Cavoukian, 2008, 92-93.

de még az elvileg azonos védelmi szintű szabályok kikényszerítése is igen nehézkes, a gyakorlatban szinte lehetetlen lehet.[307] Másodszor biztonsági aggályok is felmerülnek. A cloud szolgáltató ugyan vélhetően magasabb szintű védelmet alkalmaz egy átlagos felhasználóhoz képest, de az adatok koncentráltságából kifolyóan a támadás valószínűsége és az elszenvedett kár is lényegesen nagyobb. Számos adatvesztéssel, adatszivárgással járó botrány mutatja e rendszerek sérülékenységét, aminek egyik oka lehet, hogy a profitmaximalizálásra törekvő szolgáltatók a biztonsági intézkedésekre nem fordítanak elég erőforrást. Mások úgy érvelnek, hogy adatbiztonsági incidensek a felhőszolgáltatásoktól függetlenül is bekövetkezhetnek.[308]

Az alkalmazott információbiztonság tényleges védelmi szintjétől függetlenül azonban egyvalami egészen biztos: a felhőszolgáltatást igénybe vevők dokumentumaik és adataik feletti kontrollja, azaz az adatok feletti „fizikai ráhatás" lehetősége, a biztonsági intézkedések megválasztásának szabadsága és a jogérvényesítés lehetőségei lényegesen csökkennek. Fokozza a kiszolgáltatottságot, hogy a felhőben jelenleg alkalmazott rendszerek és szolgáltatások nem szabványosak, az átjárhatóság az egyes szolgáltatók között nehézkes.[309] Az adatok esetleges elvesztésétől való félelem így a nagy és tőkeerős – gyakran monopol- vagy oligopolhelyzetben lévő, de bizalmat sugalló – vállalkozások felé tereli a felhasználókat.

3.1.1.3 Piaci koncentráció

Az online szolgáltatások – a közösségi oldalaknál elsősorban az ún. hálózati hatásnak,[310] más oldalaknál alapvetően az informatikai biztonság iránti bizalomnak köszönhetően – néhány piaci szereplő kezében koncentrálódnak. A globális online szolgáltatók[311] olyan pozícióban vannak a felhasználókkal szemben, ami nemcsak a személyes adatok kezelésével kapcsolatos alkufolyamatot teszi reménytelenné, de azt is eredményezi, hogy a felhasználók nem is akarnak más szolgáltatást igénybe venni, mert annak értékét éppen az adja, hogy sokan mások is azt használják. E szolgáltatók az érintetti hozzájárulással legalizált adatkezelésekre vonatkozó feltételeket egyoldalúan, előre meghatározzák („take it or leave it"), lényegében az ÁSZF részévé teszik. Ez akkor is igaz, ha a közösségi oldalak jellemzően viszonylag széleskörű beállítási lehetőségeket kínálnak: mind az alapbeállításokat, mind a mozgásteret egyoldalúan határozzák meg, ráadásul ezek jellemzően csak a másokkal megosztott, és nem a szolgáltató által az érintettre vonatkozó adatokkal kapcsolatos beállítási lehetőségeket jelent.[312] Az adatkezelési feltételek (és

[307] A felhőszolgáltatások által felvetett jogi problémákról ld. részletesen: Ruiter – Warnier, 2011, 372-374.
[308] Dhillon – Kolkowska, 2011, 346-347.
[309] Szádeczky, 2011, 53.
[310] Ennek lényege, hogy egy szolgáltatás annál értékesebb, minél többen veszik mások is igénybe. Így – mintegy pozitív spirálként – robbanásszerűen nőhet egy-egy szolgáltatás felhasználóinak száma.
[311] Microsoft, Google, Facebook, Twitter, hogy csak a leginkább közismerteket említsem.
[312] Igen tanulságos az a kutatás, amely részletesen kidolgozott módszertan segítségével vetette össze néhány közösségi oldal adatvédelmi nyilatkozatának és szabályzatainak az adatvédelmi beállításokkal való összhangját. A vizsgált közösségi oldalaknál (Google+, a Meet Me és a Zorpia) az összhang mértéke viszonylag alacsony volt: számos beállítás kapcsán nem volt egyértelmű, hogy az a privacy policy mely pontjára utal, míg néhány, a dokumentációban szereplő lehetőség nem jelent meg valós választási lehetőségként a felhasználók számára. A Google+ esetén mind a beállítások, mind a dokumentáció nehezen átlátható és töredezett volt, azaz a felhasználók több különböző helyen találhatták meg azokat (Anthonysamy

általában a szerződési feltételek) diktálása során tehát egyértelmű az erőfölényük a felhasználókkal szemben.

3.1.1.4 Mobileszközök és mindent átható számítástechnika

A fenti, tartalmi jellegű változtatások mellett ki kell térni az eszközök terén bekövetkezett változásokra is. A mobiltelefonok megjelenésével és elterjedésével egy új, adott esetben igen sokatmondó személyes adat vált potenciálisan megismerhetővé: az érintett meghatározott időpontban való tartózkodási helye.[313] Ehhez az információhoz eleinte csak szűk, jól szabályozott adatkezelői kör férhetett hozzá, mindenekelőtt a hírközlési szolgáltatók, illetve azok a szervezetek, amelyek a törvényben meghatározott célokból a hírközlési szolgáltatóktól adatot igényelhetnek.[314] Az okostelefonok térnyerésének köszönhetően azonban egyre több olyan kényelmi szolgáltatás jelenik meg, amelynek keretében valamely adatkezelő hozzá kíván, és az adott szolgáltatás nyújtásához valóban hozzá is kell férnie a helymeghatározási adatokhoz.[315] A „Bring Your Own Device" (BYOD) tendenciának[316] köszönhetően ráadásul a munkahelyi és magánjellegű adatok szétválasztása nehézkes, a munkáltató az eszközön tárolt adatokhoz könnyen hozzáférhet. Összességében tehát az mobilizáció új adatkörök létrejöttét eredményezi, amelyek egy potenciálisan széles kör számára válhatnak – akár az adatalany egyetlen koppintással megadott hozzájárulása, akár más jogalap alapján – elérhetővé és kezelhetővé.

A mobileszközök nem merülnek ki a(z okos)telefonokban, tabletekben és más hasonló eszközökben. A közeljövő egyik igen ígéretes területe a viselhető technológia (okosszemüveg, okosóra, egészségügyi alapadatokat mérő szenzorokkal ellátott készülékek, stb.), így a mobileszközök további terjedése várható. Lehetővé válik emellett az eddigi „hagyományos" eszközök – az autótól a mosógépen, kávéfőzőn és sütőn át a termosztátig, a fogyasztásmérőktől[317] kezdve az utcán felszerelt arcfelismerő és forgalomszámláló kamerákig és időjárás-érzékelő szenzorokig – intelligenssé tétele és online kapcsolattal való ellátása is.[318] A „mindent átható számítástechnika",[319] illetve a

– Greenwood – Awais, 2012, 197-200.) Összességében tehát az adatvédelmi beállítások lehetősége is csak korlátozott kontrollt jelent a felhasználók számára.

[313] A tartózkodási hely már a cellainformációk alapján is viszonylag pontosan, az újabb készülékekben található GPS vevő segítségével pedig egészen pontosan meghatározható.

[314] A hírközlési szolgáltatók adatmegőrzési és adatszolgáltatási kötelezettségeinek terjedelme az elmúlt években is élénk viták tárgya volt.

[315] Gyakori megnevezése e szolgáltatásoknak a "Location Based Services" (LBS), amelyek egy része a felhasználó tartózkodási helyének (folyamatos) követésével is járhat.

[316] A tendencia emellett információbiztonsági problémákat is felvet, az eszközök megfelelő szintű védelméről a munkáltatók nehezen vagy alig tudnak gondoskodni. A BYOD adatvédelmi szempontú elemzéséről ld. például a brit információs biztos (továbbiakban: ICO) vonatkozó útmutatóját (ICO, 2013)

[317] Az energetika egyik aktuális kérdése az okosmérők alkalmazása (smart metering), amelynek lényege, hogy a gyakran (pl. 15 percenként) mért aktuális fogyasztási adatok azonnali feldolgozásával az infrastruktúra kihasználtsága hatékonyabbá válik, és jelentősen nőhet az energiamegtakarítás (Cuijpers – Koops, 2013, 269-271.)

[318] A legegyszerűbb megoldás, ha a tárgyakat RFID chippel látják el, és így azokat nyomon lehet követni (mérni lehet például, hogy pontosan hány termék van egy polcon, melyik ruhát vitték be a próbafülkébe, kinél van a papír alapú akta az ügyintézés során, stb.). Számos eszközt azonban valódi számítási kapacitással (processzor), és közvetlen internetes kapcsolattal, egyeseket pedig (például az autók fedélzeti számítógépét) szabványos operációs rendszerrel is felszerelnek.

[319] Angolul „ubiquitous computing" vagy „pervasive computing". Magyarul használatos a „mindenütt jelenlévő számítástechnika" is. A számítástechnika fejlődésének korszakolása: 1) nagygépek időszaka, 2)

hálózatba kapcsolódásra tekintettel a „dolgok internete”[320] kifejezésekkel leírt tendenciák során tehát összekapcsolódnak a fizikai világ tárgyai a virtuális világgal.[321] A jelenség fontos velejárója, hogy láthatatlanul segíti a mindennapokat, és – épp a mindent átható jelleg miatt – az egyénnek nincs érdemi lehetősége kimaradni belőle. E két jellemző jelentősen rontja az adatgyűjtés és adatkezelés átláthatóságát, az adatalany érdemi kontrollját, és az információs aszimmetria növekedéséhez vezet.[322]

3.1.1.5 Profilozás és viselkedésalapú marketing

A személyiségprofilok létrehozásának potenciális veszélye már az adatvédelem korai szakaszában, az első generációs szabályozás kialakulásakor felmerült; például a német népszámlálás-ítélet[323] és az Alkotmánybíróság 15/1991 (IV. 13.) AB határozata is utal rá. Később a profilalkotással kapcsolatos kérdések a jogirodalomban is többször megjelentek. „Az egyén sorsát egyre inkább az határozza meg, hogy mit árul el róla a személyiségprofilja, mit tartanak róla nyilván, és nem a fizikai valóság, amellyel a személyiségprofil sok esetben nem egyezik.” – írja Szabó Máté.[324] Egyetértve egyébként e megállapítással látni kell, hogy a virtuális profil és a fizikai valóság szükségszerűen nem egyezik, (vagy megfordítva: szükségszerűen kisebb-nagyobb mértékben torz, illetve hiányos). Egy konkrét személynek ugyanis számos virtuális profilja van, attól függően, hogy pontosan milyen adatok állnak az adott adatkezelő rendelkezésére. A „fizikai valóság” (az adatalany egy-egy tulajdonsága, pl. érdeklődési köre) ráadásul időben is dinamikusan változik.[325]

Az utóbbi időben jelentősen megnőtt az üzleti szférában a profilalkotás jelentősége, egyrészt mivel az online szolgáltatások és különösen a felhasználók által generált tartalmak elterjedésével újfajta adatok gyűjtése is lehetővé vált, másrészt egyre fejlettebb adatbányászati eszközök állnak rendelkezésre.[326] A személyiségprofilok egyenlőtlen kommunikációs helyzetet eredményeznek, és azok alapján következtetni lehet az érintett „terveire, jövőjére, megsértve szabad akaratát, méltóságát, s komoly visszaélések lehetőségét teremtve meg”.[327]

A személyiségprofil alkotásához szükséges adatok több forrásból gyűjthetők:

---

személyi számítástechnika (PC) időszaka, 3) mindent átható számítástechnika időszaka (Hassan, 2008, 3-4.) nagyjából egybecseng az adatvédelmi szabályozás általam javasolt korszakolásával is.

[320] Internet of Things

[321] Sundmaeker – Guillemin – Friess Woelfflé, 2010, 11. Az Európai Bizottság megbízásából készült szakértői anyag igen részletesen tárgyalja az “Internet of Things” koncepció elérésének útját.

[322] Čas, 2011, 140, 146-147. Az a gondolat, miszerint a magánszféra védelme nem eredményezheti a társadalmi életből való kimaradást, már a 80-as években felmerült, és a privacyvédelem aktivista megközelítéséhez, az információs önrendelkezési jog elismeréséhez vezetett (erről ld. részletesen Mayer-Schönberger, 1998, 228-229.

[323] Könyves-Tóth – Székely, 1991. 6.15

[324] Szabó, 2012, 16.

[325] Ráadásul még azt sem lehet mondani, hogy a teljes és valós képet az egyén maga láthatja: nemcsak az önismeret és önértékelés pszichológiai értelemben vett korlátai miatt, de azért sem, mert a legújabb adatbányászati technikákkal olyan információk is feltárhatók az érintettről, amellyel esetleg ő maga sincs tisztában, sőt, az esetleges jövőbeli viselkedése is – meghatározott valószínűséggel persze – előre jelezhető.

[326] A profilozás fogalmáról, csoportosításáról ld. Hildebrandt, 2010

[327] Balogh, 2004, 56.

1) Az adatalany által megadott adatok. Ezek származhatnak például egy regisztrációs űrlap kitöltéséből, vagy online vásárlás kapcsán megadott adatokból.
2) Az adatalany megfigyelésével létrejövő adatok. Tipikusan a felhasználók követéséből eredő, pl. böngészési szokásokból (ideértve elvi szinten a meglátogatott weblapokat, a rajtuk eltöltött időt, az oldalon történő egérmozgásokat, az esetlegesen megvásárolt termékeket), a közösségi oldalon folytatott aktivitásból, levél és üzenetváltásból származó, a felhasználó által létrehozott tartalmakból (posztok, blogok, videók), a fizikai helyzetéből (location tracking), vagy az egyre sokasodó szenzorokból származó adatok.[328]
3) Az előbbi adatokból az érintettre vonatkozó következtetések. Ezek kinyerésére egyre fejlettebb adatbányászati technológiák állnak rendelkezésre.[329]
4) Más forrásból származó adatokból (pl. hasonló mintázatú személyek adataiból) az érintettre vonatkoztatott következtetések.[330]

A profilozásnak számtalan technikája és alkalmazási területe van.[331] A jelenséget az egyik leginkább elterjedt, és adatvédelmi szempontból is gyakran elemzett megjelenési forma, a viselkedésalapú reklámozás működésének bemutatásával illusztráljuk.

A viselkedésalapú reklámozás folyamatában alapvetően három szereplő vesz részt: a hirdetők (reklámozók), akik terméket vagy szolgáltatást szeretnének népszerűsíteni; a közzétevők, akik potenciálisan látogatott internetes felülettel rendelkeznek (pl. online hírportálok);[332] és a reklámhálózat-szolgáltatók,[333] akik összekapcsolják a hirdetőket a közzétevőkkel.[334]

A rendszer lényege, hogy a reklámhálózat-szolgáltatók felépítik a felhasználók – nagyjából a fenti adatkörökből származó, elsősorban az online aktivitás alapján képzett – profilját. A felhasználók követése jellemzően valamilyen kliensoldali technológia, tartós cookie-k,[335] ún. flash-cookiek vagy Javascript fájlok segítségével, illetve a Facebook vagy más közösségi oldal „Like" vagy „Megosztás" gombjával történik. Ugyanakkor a cookie illetve más, a felhasználó eszközén tárolt adat segítségével történő követés helyett – éppen a hírközlési irányelv nemrég szigorított rendelkezései miatt[336] – egyre inkább terjed a böngésző-lenyomat alapján történő követés: a böngésző-beállítások ártatlannak tűnő adatai, például a böngésző típusa, verziószáma, a használt fontkészlet, a képernyőfelbontás

[328] A megfigyelés (más forrásokban: követés) komplexitásáról, a megfigyelés technológiáiról és különösen a megfigyelés gazdasági és politikai ösztönző-mechanizmusairól ld. részletesen Langheinrich – Finn – Coroama – Wright, 2014
[329] Ez az a pont, amely nemcsak az érintettek, de minden potenciális kontrollt gyakorló szervezet (felügyelőhatóságok, érdekvédelmi szervezetek) számára is teljesen átláthatatlan.
[330] Utóbbi két lehetőségre tekintettel a szakirodalom megkülönböztet direkt és indirekt profilozást (Jaquet-Chiffelle, 2010, 41-43.)
[331] A profilozásról ld. bővebben Hildebrandt – Gutwirth, 2010a
[332] Ilyen felület lehet akár egy mobiltelefonos applikáció valamelyik sávja is.
[333] Számos ilyen szolgáltató tevékenykedik a piacon, de a legismertebb ilyen szolgáltatás kétségkívül a Google Adwords. A reklámhálózat szolgáltató maga is kínálhat tartalmat, és így egyszerre lehet közzétevő is.
[334] WP29, 2010a, 5.
[335] Szokás „third party cookie"-nak is nevezni, ami arra utal, hogy nem a meglátogatott weboldal tartalomszolgáltatója, hanem harmadik fél (a reklámhálózat-szolgáltató) helyezi el. Erről és a Google Adwords működéséről ld. részletesen Böröcz, 2014, 154-158.
[336] A szigorú cookie-szabályozás elkésett, hatástalan, és ezért nagyrészt felesleges.

stb. elég nagy pontossággal alkalmas a felhasználó azonosítására.[337] A szolgáltatók dolgoznak az eszközökön átívelő követés lehetőségén is. Ha a felhasználó hajlandó a különböző eszközein belépni valamely szolgáltató fiókjába (pl. Facebook, Google, Microsoft),[338] akkor mindez könnyedén megoldható, de ennek hiányában is igyekeznek ezt megvalósítani.[339] Fontos tehát látni, hogy e technológiák működése részben[340] független attól, hogy a felhasználó regisztrált-e valamilyen szolgáltatásra, és annak során milyen adatokat adott meg.

A felépült (de persze folyamatosan változó) személyiségprofil alapján aztán a reklámhálózat-szolgáltató igyekszik az adott közzétevő (tartalomszolgáltató) weblapját látogató felhasználó számára leginkább releváns hirdetést közzétenni, mivel azokra jóval nagyobb arányban kattint. Egy adott weboldalon tehát a különböző felhasználóknak más-más hirdetések jelennek meg. A viselkedésalapú marketing másik megvalósulási formájában egy adott elektronikus kereskedelmi szolgáltató igyekszik – ugyancsak egy korábban felépített profil alapján – releváns ajánlatokat mutatni a felhasználónak.

Hangsúlyozni kell, hogy a viselkedésalapú marketing az tartalomszolgáltatók egyik fő bevételi forrása, és az online gazdaság egésze szempontjából is jelentős tényező. Az ingyenes tartalmakért és szolgáltatásokért cserébe tehát a felhasználók közvetlenül az adataikkal „fizetnek".[341]

A profilalkotásnak a reklámok targetálása mellett további – tényleges vagy potenciális – felhasználási területei is lehetnek. A profilok befolyásolják az internetes keresés találati eredményeit is, annak érdekében, hogy a felhasználó a számára leginkább releváns találatokat kapja. Pontosabban azt, ami a keresőszolgáltató szerint a számára leginkább releváns. A túlzott perszonalizáció oda vezethet, hogy – különösen a célzott reklámoknak, szűrt Facebook hírfolyamoknak, sőt, a hírportálok hasonló technikájának köszönhetően – a felhasználó számára elsősorban olyan tartalmak jelennek meg, ami az érdeklődési körének, ízlésének, világnézeti vagy politikai beállítottságának leginkább megfelelő, és elzáródhatnak az adott témakörrel kapcsolatos kritikus, más nézőpontból közelítő tartalmak, azaz a felhasználó ún. szűrőbuborékba kerül, amelyből csak igen nehezen léphet ki.[342] A legnagyobb probléma, hogy a felhasználók alapvetően e jelenséggel nincsenek tisztában: "A számítógép- és internethasználók százmilliói abban a naiv hitben használják az egyre újabb és divatosabb alkalmazásokat, hogy urai az általuk közölt

[337] Castelluccia, 2012, 23-25., és Tene – Polotensky, 2011, 6-13. (a tanulmányok több további, tracking technológiát is elemeznek, a dolgozatban csak a legelterjedtebbeket említem).
[338] Az okostelefonok operációs rendszerei által nyújtott előnyöket épp a felhasználói fiókba való belépéssel lehet igazán kihasználni.
[339] Ld. például egy erről szóló blogbejegyzést: McDermott, 2014
[340] Természetesen pontosabb profil alkotható a fiókkal rendelkező felhasználókról, mivel akkor a fiókhoz kapcsolódó adatai is profil részévé válhatnak, de a nem regisztrált felhasználók viselkedése is követhetők.
[341] Rauhofer, 2013, 1-2. A reklám és egyéb tartalom/szolgáltatás árukapcsolásként való megjelenése természetesen nem új jelenség. A hirdetéseknek a „hagyományos" média rendszerében is igen fontos finanszírozó szerepük van, csak a targetáltság hiánya miatt a közönség tagjai ez esetben csak a „figyelmükkel", és nem a személyes adataikkal fizetnek.
[342] A szűrőbuborék jelenségéről szóló rövid összefoglalót ld. az alábbi cikkekben: Varga, 2011, Kádár, 2012, míg a témakör részletes kifejtését ld. Pariser könyvében (Pariser, 2011), illetve weboldalán: http://www.thefilterbubble.com [2014.06.18.]

vagy róluk szóló információknak; […] a valóságban egy buborékból, a „filter bubble”-ból látják a külvilágot”[343]

A profilozás emellett elvileg alkalmas lehet differenciált árazás (árdiszkrimináció) alkalmazására,[344] kifinomult bűnözői profilok megalkotására, esetlegesen bűnözői magatartás illetve visszaesés előrejelzésére, valamint jövedelmező fogyasztói magatartás megerősítésére vagy kezdeményezésére (végső soron a fogyasztó manipulálására is).[345]

3.1.1.6 Big Data

A felhasználók által készített és közzétett tartalmaknak és az egyre növekvő számú adatgyűjtő szenzoroknak[346] köszönhetően az online adatmennyiség korábban elképzelhetetlen mértékben bővül. Ezen adatok egy része ugyan strukturáltan, adatbázisokba rendezve, nagyobb része azonban strukturálatlan formában létezik, – ilyenek lehetnek például a fényképek, ábrák, videók, audiofájlok weboldalak, pdf állományok, prezentációk, e-mailek, blogok, közösségi oldalakon történő bejegyzések, egyéb szöveges dokumentumok stb.[347] Természetesen a különböző adatbázisok és adatok a legkülönbözőbb hozzáférési jogosultságokkal érhetőek el. Ezt az adattömeget hagyományos adatbányászati módszerekkel már nem lehet kezelni, így az ún. „Big Data” jelenség központi kérdése, hogy miként oldható meg a hatalmas mennyiségű, igen sokféle, és gyorsuló ütemben bővülő adatmennyiség gyors (valósidejű) és megbízható elemzése.[348] Középpontba került tehát az adatbányászati technológiák fejlesztése, amelynek terén jelentős eredmények mutatkoznak.

A Big Data-ban rejlő lehetőségek kiaknázása rendkívüli üzleti lehetőségeket és jelentős össztársadalmi előnyöket rejt magában, így hasznosítható a profilozás kapcsán említett területeken, valamint az egészségügyi kutatásokban, az energetikai hálózatok hatékonyabbá tételében, a közlekedésfejlesztésben,[349] a közigazgatásban és a városfejlesztés (ún. Smart City kialakítása) területén.

---

[343] Székely, 2013, 11. A buborék fő problémái a láthatatlanság mellett az, hogy a felhasználó egyedül van benne, és hogy nincs igazi választási lehetősége, hogy benne akar-e lenni, vagy sem. Ez jelentősen különbözik az offline világban is (pl. tematikus tévécsatornák, vagy nyíltan vállalt politikai irányultságú napilapok formájában) megjelenő szűrésektől – ezekben az esetekben ugyanis az olvasó számít rá, hogy eleve egyféle megközelítés vagy nézőpont jelenik meg. Pariser, 2011, 9-10.

[344] A differenciált árazás lényege megpróbálni magasabb áron értékesíteni azoknak, akik hajlandóak az adott termékért többet fizetni, illetve kedvezményesen értékesíteni azoknak, akik magasabb áron vélhetően nem vennék meg. A differenciált árazás az offline világban is létezik, alapvetően csoportokra, és nem személyekre bontva (pl. diákkedvezmények). Igen izgalmas jogi kérdéseket vetne fel a differenciált árazás személyre szabott online alkalmazása: technikailag nincs akadálya annak, hogy a kialakított profil alapján gazdagabbnak vélt felhasználó magasabb árat lásson egy webshopban az adott termékre vonatkozóan, mint a szegényebbnek vélt felhasználó.

[345] Hildebrandt – Gutwirth, 2010b, 366.

[346] A szenzorok alatt a mindent átható számítástechnika legkülönfélébb eszközeire utalok.

[347] Az adatok lehetnek félig strukturáltak is; ekkor az adott adat rendelkezik bizonyos címkékkel (metaadatokkal), egy pdf fájl gyakran tartalmazza a szerző nevét, a létrehozás idejét stb. A strukturált és strukturálatlan adatokról részletesen ld. Racskó, 2014, 261-262.

[348] E jellemzőket “4V-ként” is említik, mint volume (mennyiség), variety (sokféleség), velocity (gyorsaság), veracity (megbízhatóság)

[349] Tene – Polotensky, 2012, 8-11.

Az új adatbányászati technológiák azért is különösen figyelemre méltóak, mert a felhalmozódó hatalmas információmennyiség, illetve az abból való értékes információk kinyerésének nehézségei és költségei (a „jel elválasztása a zajtól") tulajdonképpen egyfajta természetes védelmet is jelenthetnének az érintettek számára – korántsem olyan mértékűt persze, mint annak idején a papír alapú adatkezelések. A fenti, üzleti és kétségkívül jelentős társadalmi hasznot is hozó lehetőségek kiaknázása ugyanakkor az elmúlt negyven évben kialakult adatvédelmi szabályozás sarokköveit érintik: az anonimnak hitt adatok újra összekapcsolhatók lesznek az érintettel (de-anonimizálás), a célhoz kötöttség követelménye alig-alig tud érvényesülni, az adatminimalizálás elve pedig gyakorlatilag az új adatbányászati technológiák logikájával épp ellentétes.[350]

3.1.1.7 Néhány további tendencia

Az eddigi részletesen kifejtett tendenciák mellett – mintegy kulcsszószerűen – érdemes még továbbiakra is utalni.

Továbbra is jelentős a globalizáció hatása, tovább nőtt a vállalatok közötti, és a multinacionális vállalatokon belüli globális adatforgalom, amely természetesen az Internetes szolgáltatásokat nyújtó vállalkozásokra is igaz. Ez az offline és online szolgáltatások esetén jelenleg is komoly kihívás elé állítja az adatvédelmi szabályozást.

Néhány technológiai újítás, például a kereskedelmi forgalomban is kapható kamerákkal felszerelt drónokkal történő egyének közötti megfigyelés (peer-to-peer surveillance),[351] vagy a személyre szabott gyógyászathoz szükséges, családtagokat is érintő genetikai vizsgálatok és kutatások[352] ugyancsak újabb kihívások elé állíthatják magánszféra védelmének szabályozását.

Végül meg kell említeni a ma még ritkán használt, de folyamatos fejlesztés alatt álló új technológiák (Future and Emerging Technologies, FET) potenciális hatásait.[353] A mesterséges intelligencia és a robotika fejlődése eredményeként az emberi és gépi viselkedés és döntéshozatal egyre nehezebben megkülönböztethető, az emberi képességeket (látás, memória, fizikai teljesítőképesség) feljavító neuro- és bioelektronikai eszközök alkalmazása pedig elmossák az ember-gép közötti eddigi éles határvonalat. E fejlődés a jogrendszer számos területét érintik, és egyértelműen hatással lesznek a magánszféra-védelem és az adatvédelem területére is. Míg egyes kérdések akár a jelenlegi szabályozási környezet alapján, vagy annak kismértékű továbbfejlesztésével is megválaszolhatók,[354] az új technológiák elterjedése várhatóan egészen újfajta kérdéseket és aggályokat is felvetnek majd.[355]

[350] E problémakörről ld. részletesen: Tene – Polotensky, 2012, 19-25.
[351] Langheinrich – Finn – Coroama – Wright, 2014, 175.
[352] Tene, 2011, 20.
[353] A technológiák jogi szabályozásra gyakorolt hatását ld. részletesen: Székely – Szabó – Vissy, 2011
[354] Ld. például az automatizált adatfeldolgozással hozott döntésekre vonatkozó szabályokat.
[355] Székely – Szabó – Vissy, 2011, 6-9.

3.1.2 Társadalmi hatások

3.1.2.1 A technológia magánszférára gyakorolt hatása

A technológia – valójában inkább az arra épülő szolgáltatások – fejlődésének egyes elemeit az áttekinthetőség kedvéért külön alcímek alá rendeztem, de valójában egymással ezer szálon összefüggő, szövetszerűen összekapcsolódó, és egymásra kölcsönösen ható (jellemzően egymást erősítő) jelenségekről van szó. A Big Data problémakörnél tárgyalt új adatbányászati technikák a felhasználói tartalmak és a mindent átható technológia által létrejövő határtalan mennyiségű adatot elemzik, amelyek a profilozás hatékonyabb megvalósulását hozhatják; a globalizáció és a felhőszolgáltatások együtt lényegében ellehetetlenítik a (személyes) adatok feletti fizikai kontroll gyakorlását; a profilozás, a mindent átható számítástechnika és a közösségi oldalak rendszerint valós adatokon alapuló fiókjai pedig végképp összemossák a felhasználók „online" és „offline" világát. Drasztikusan nő az adatkezelések, valamint az érintettel kapcsolatban álló – mind a joghatóság, mind az adatbiztonság szempontjából – legkülönfélébb adatkezelők és adatfeldolgozók száma, egyes szolgáltatók ráadásul jelentős erőfölényből érvényesítik érdekeiket.

Az adatkezelések összetetté válása nem csak az érintett számára nehezíti meg a folyamatok áttekintését, de sokszor magát az adatkezelőt is komoly kihívás elé állítja. Az adatkezelő maga is bizonytalanná válhat egy-egy adat kezelésének feltételeire vonatkozóan: az adattovábbítások valamint az időben változó (a hozzájárulás alapját képező) adatvédelmi nyilatkozatok miatt nehézséget okozhat egy adatkezelőnek követni, hogy az adott adatnak pontosan mi volt a forrása, és hogy a kezelésükhöz pontosan milyen adatkezelési feltételek tartoznak.[356] Erre egy lehetséges megoldás lehet, ha az adatkezelő az adatokhoz metaadatként hozzáadja a kezelés feltételeit, és így összeköti a rá vonatkozó adatvédelmi nyilatkozattal,[357] ennek gyakorlati megvalósulása azonban korántsem egyszerű.

Összességében tehát a technológiai fejlődés és az abból eredő társadalmi változások adatvédelmi szempontból egy irányba hatnak: az adatkezelések átláthatatlansága és az információs hatalom aszimmetriája tovább fokozódik, az érintetti kontroll tényleges lehetősége pedig drasztikusan csökken.

3.1.2.2 Az állami adatkezelésekkel kapcsolatos tendenciák

Első ránézésre a technológia fejlődéséből eredő problémák inkább a piaci szereplők kapcsán merülnek fel, ugyanakkor látni kell, hogy a kis testvérek és a Nagy Testvér igen könnyen egymásra találnak. Az Edward Snowden nevével fémjelzett botrány, az amerikai titkosszolgálatok PRISM rendszere és adatgyűjtési gyakorlata egyes elemeinek nyilvánosságra kerülése egyértelműen azt mutatja, hogy a piaci viszonyok során felmerülő

[356] Adattovábbítás esetén például nehezen követhető, hogy az adatot begyűjtő adatkezelő milyen adatvédelmi nyilatkozat mellett kért hozzájárulást. A saját adatkezelések területén pedig a változásmenedzsment okoz nehézséget, azaz követni kellene, hogy az adott adat kezeléséhez az adatvédelmi nyilatkozatnak mely szövegverziója tartozott.

[357] Jøsang – Fritsch – Mahler, 2010, p. 133. Ráadásul e nehézségek csak a hozzájáruláson alapuló adatkezeléseket érintik, de az adatkezelésnek más jogalapja is lehet, amikor sokszor még annyi dokumentáció sincs, mint az adatvédelmi nyilatkozat – ilyen eset lehet tipikusan az érdekmérlegelésen alapuló adatkezelés.

adatvédelmi anomáliák az állampolgár–állam viszonylatában is meghatározó jelentőségűek.[358] A két szféra közötti kapcsolat – úgy tűnik – jogállamokban elfogadhatatlan módon szinte teljesen átláthatatlan. Nem világos, hogy a szolgáltatók által monitorozott adatok köre, célcsoportja, valamint az, hogy az összegyűjtött adatokhoz pontosan melyik állam mely szervei férnek hozzá, legálisan vagy illegálisan, a nagy online szolgáltatókkal együttműködve, vagy a védelmi rendszereiket megkerülve.

A biztonságpolitikai célok előtérbe kerülése elsősorban az Egyesült Államokat ért, 2001. szeptember 11-i terrortámadás következménye. Ezt követően a magánszféra-védelem szempontjai – egyébként a széles közvélemény támogatása mellett – egyértelműen háttérbe szorultak a nemzetbiztonsági célokkal szemben.[359] Az Egyesült Államok e tendenciát igyekszik Európa (és a világ más) adatkezelőivel szemben is érvényesíteni, nem is teljesen sikertelenül. A terrortámadás után „felerősödött az USA-ban különösen a harmadik országok polgárait érintően a személyes adatok minél szélesebb köre begyűjtésének, szinte korlátlan idejű tárolásának és különböző szempontok szerinti elemzésének, valamint azokhoz a bűnüldöző és nemzetbiztonsági szervek részéről történő korlátlan hozzáférésének igénye."[360] Európa igyekezett a bűnüldözési célú együttműködés erősítésében közreműködni, miközben egyes döntéseket – például a légiutasok adatainak átadásáról – éles adatvédelmi kritikák érték.[361]

A dolgozatban nem foglalkozom részletesen a biztonság és adatvédelem konfliktusával. Azt a tendenciát azonban mindenképp érdemes rögzíteni, hogy az adatvédelmi szabályozás válságával kapcsolatban előtérbe kerültek ugyan az (online) üzleti szférával kapcsolatos kérdések, a Nagy Testvér adatéhsége és az állami adatkezelésekkel kapcsolatos adatvédelmi kihívások korántsem szűntek meg, sőt, épp az említett üzleti tendenciákra tekintettel egészen újfajta adatgyűjtési lehetőségek nyíltak meg. Az adatkezelők részletes belső szabályozási rendszerének kialakítása e folyamatok átláthatóságát is növelheti, így a 4.5 fejezet megállapításai az állami szervek és a piaci szereplők számára egyaránt hasznosíthatók.

3.1.2.3 Az érintettek és az adatkezelők adatvédelmi attitűdje

Az adatvédelem fejlődési tendenciáit kutatva érdemes figyelembe venni azt is, hogy az új technológiák és szolgáltatások új felhasználói viselkedésmintákkal párosulhatnak. A felhasználók új generációjának a magánszférával kapcsolatos attitűdje eltérhet a korábbi generációétól;[362] az elmúlt években számos felmérés igyekezett ezt pontosan feltárni. Tekintettel arra, hogy a mintavétel, a feltett kérdések, a vizsgálat időszaka, a közvélemény-kutatás módszertana stb. az egyes kutatásoknál jelentősen különbözött, nincs mód az adatok statisztikai értelemben pontos összehasonlítására. Az egyes kutatások

[358] A Nagy Testvér és a kis testvérek együttműködése nem újkeletű, a 90-es években a PRISM botrányhoz igencsak hasonló Echelon-ügy foglalkoztatta sokáig a közvéleményt. Ennél kisebb súlyú összefonódások is előfordultak, Csehország például direktmarketing célokra adott el állami adatbázis a Procter&Gamble cégnek. (Majtényi, 2002, 96-97.) Az információs köz- és magánhatalom kapcsolatáról ld. még Szabó, 2012, 24-27.
[359] E folyamatról ld. részletesen Sziklay, 2009, 105-110.
[360] Szurday, 2009, 118.
[361] Szurday, 2009, 115-118.
[362] Tene, 2011, 15, 21, 23.

eredményeinek, következtetéseinek áttekintéséből azonban jól körülrajzolhatók olyan általános tendenciák, amelyek terén ugyan országonként,[363] korosztályonként vagy szempontok alapján lehetnek akár jelentősnek mondható eltérések is, de amelyek összességükben mégis alkalmasak arra, hogy összképet adjanak a felhasználók és adatkezelők adatvédelmi attitűdjéről.

Az eredmények áttekintéséhez és a következtetések levonásához az alábbi kutatások eredményeit használom fel:

- az Eurobarometer 2008-ban publikált, érintettek és adatkezelők hozzáállását egyaránt vizsgáló, sok esetben a 2003-as adatokkal, vagy 1990-ig visszamenő összehasonlítást is tartalmazó jelentéseit;[364]
- az Eurobarometer 2011-ben publikált, az adatvédelem és az elektronikus identitás témakörében végzett attitűdvizsgálatot;[365]
- a CONSENT projekt keretében végzett felmérés 2013-ban bemutatott eredményeit;[366]
- több, kifejezetten a fiatal generáció adatvédelemhez való hozzáállását vizsgáló tanulmányt,[367]
- végül néhány további, különböző privacy-kutatások eredményeit összegző szakirodalmi forrás megállapításait.

A felmérések jellemzően az online szolgáltatásokra és a piaci szereplő adatkezelőkre koncentráltak, így a Nagy Testvér adatkezeléseivel szembeni érintetti hozzáállásról releváns következtetéseket ezekből levonni csak egy-egy meghatározott területen lehet.

3.1.2.3.1 A magánszférával kapcsolatos aggodalmak és az adatkezelők iránti bizalom

A magánszférával kapcsolatos aggodalmakkal, félelmekkel és várakozásokkal kapcsolatban számos releváns eredmény született az elmúlt években.

A holland, belga és brit diákokon végzett felmérés azt mutatta, hogy az adatvédelmi aggodalmak más kérdésekkel, (pl. oktatás vagy egészségügyi ellátás színvonala, bűnözés,

[363] Az elemezett kutatásokat európai államokban végezték, az európaitól eltérő privacy-felfogásból és szabályozási rendszerből adódóan az Egyesült Államokat érintő közvélemény-kutatási eredményekre nem támaszkodom.

[364] Eurobarometer, 2008a, Eurobarometer, 2008b. A felmérés 27 tagállam összesen kb. 27.000, 15 évesnél idősebb polgárának személyes vagy telefonos megkérdezésén alapult. Az adatkezelőket érintő felmérést szintén 27 tagállamban, összesen 4835, tagállamonként a népességtől függően minimum 100, 200 vagy 300 adatkezelő (ill. az adott adatkezelőnél a személyes adatok védelméért felelős személy) megkérdezésével végezték. A kutatás az adatkezelők méretére nézve reprezentatív.

[365] Eurobarometer, 2011. A felmérés 27 tagállam összesen 26.574, 15 évesnél idősebb polgárának személyes megkérdezésén alapult, a minta a lakosságra nézve reprezentatív. Az eredmények több különböző csoportosításban is elemzésre kerültek.

[366] Brockdorff – Appleby-Arnold, 2013, Custers et. al., 2013

[367] Andrade és Monteleone tanulmánya a „digitális generáció” (digital natives) adatvédelmi hozzáállását vizsgálja (Andrade – Monteleone, 2013). Walrave és Heirman kutatása belga tinédzserek részvételével készült, 1318, 12-18 év közötti belga középiskolás papír alapú anonim megkérdezésével (Walrave és Heirman, 2011). Leenes és Oomen összesen 7635 brit, holland és belga egyetemista vagy főiskolás diákon végzett felmérés eredményeit rögzítette (Leenes – Omen, 2010).

bevándorlás, környezetszennyezés stb.) összevetve nem túl magas prioritásúak.[368] Ugyanakkor konkrétan rákérdezve igen nagy arányban fontosnak tartották az adatvédelem kérdését, ami azonban túl sokat nem árul el, mivel egyrészt ez volt a politikailag korrekt válasz, másrészt a kitöltők eleve felülreprezentáltak e téren: aki rászán kb. 30 percet a kérdőív kitöltésére, eleve fontosabbnak tartja az adatvédelem kérdését másoknál.[369] Az Eurobarometer 2008-as felmérése szerint az európaiak 64%-a aggódik személyes adatai megfelelő kezelése miatt,[370] míg a 2011-es felmérés – szűkebb, de érzékenyebb kérdés alapján – az európaiak csak mintegy 35-54%-a,[371] tehát szűk fele aggódik amiatt, hogy a viselkedését rögzítik.[372] Ennél jelentősebb arányban, a megkérdezettek több mint felét érinti kényelmetlenül a különböző adatgyűjtésen alapuló internetes profilozás (igaz, kb. 40%-ot ez nem zavar).[373]

Az aggodalmak inkább más esetekkel kapcsolatos ismereteken, mintsem közvetlen tapasztalatokon alapulnak. Adatvesztésről vagy identitáslopásról a megkérdezettek 55%-a hallott már, döntően a médiából, kisebb részt szóbeszéd alapján, ugyanakkor csak 2% volt közvetlenül érintett, és további 3% válaszolta, hogy a családja érintett.[374]

A felhasználók többsége tisztában van a különböző, személyes adatokat érintő műveletekkel (személyre szabott tartalmak és reklámok, adatok megosztása/eladása harmadik személyek számára), de e gyakorlatok elfogadottsága – még akkor, ha az érintett hozzájárult (!) –viszonylag alacsony.[375] A tudatossággal kapcsolatban hasonló eredményt mutatnak a belga tinédzserek válaszai is: nagy részüknél (72%) felmerül, hogy az adott weboldalnak miért is kellenek a gyűjteni kívánt adatok, 69% aggódik az adataik felhasználásával kapcsolatban, sőt, 73% keres valamilyen információt az adatkezelésről, mielőtt megadja az adatait.[376] Összességében tehát nagy többségük viszonylag szkeptikus.

Érdekes eredményeket mutatnak a bizalommal kapcsolatos kérdések. Az Eurobarometer 2008-as felmérései egyértelműen jóval nagyobb bizalmat mértek az állami szervek (egészségügyi intézmények: 82%, rendőrség: 80%, szociális ellátórendszer intézményei: 74%, adóhatóság: 69%), mint egyes piaci szereplők esetén (utazási irodák: 32%, piackutató cégek: 33%, bankkártya kibocsátók: 43%).[377] Az 1990-ig történő visszatekintés ráadásul jelentős bizalomnövekedést mutatott az állami szféra adatkezelőivel szemben, míg a piaci

[368] Leenes – Oomen, 2010, 144-145.
[369] Leenes – Oomen, 2010, 146.
[370] Érdekesség, hogy a jelentés tartalmaz egy 1990-ig történő visszatekintést is. Eszerint az aggodalom mértéke a vizsgált 18 évben szinte változatlan. A 15-24 éves korosztály valamivel kevésbé aggódik (53%), Eurobarometer, 2008, 7-9.
[371] A felhasználói aggodalom mértéke attól függ, hogy pontosan milyen körülmények között történik a megfigyelés. A legkevésbé a nyilvános helyen (34%), és az internetes szörfözés kapcsán (40%) történő megfigyelés, a leginkább a bankkártyás tranzakciók követése (54%) aggasztja az állampolgárokat.
[372] Eurobarometer, 2011, 64.
[373] Eurobarometer, 2011, 74.
[374] Eurobarometer, 2011, 132.
[375] Az adatok eladását például 7% feltétel nélkül elfogadja, 28% csak akkor, ha az adatkezelő rendelkezik hozzájárulással, a nagy többség viszont még ezzel a feltétellel sem fogadja azt el. Azaz a válaszadók bizonyos cselekményeket a hozzájárulás ellenére is szívesen tiltanának.
[376] Walrave – Heirman, 2011, 298.
[377] Eurobarometer, 2008, 10.

szereplők esetén inkább stagnálás vagy csökkenés figyelhető meg.[378] Az állami szervekkel szembeni nagyobb bizalmat és a piaci viszonyok kapcsán felmerülő bizalomhiányt az Eurobarometer 2011-es kutatása is megerősíti.[379] A CONSENT projekt eredményei alapján a fogyasztók sincsenek túl jó véleménnyel az adatkezelőkről: országonként eltérő mértékben, de a nagy többség (65-92%) úgy véli, hogy személyes adataikat tudtuk nélkül is felhasználják, és engedélyük nélkül harmadik személynek átadják, vagy kéretlen kereskedelmi üzenet küldésére használják.[380] Az Eurobarometer 2011-es felmérése hasonló értéket mutatott, a megkérdezettek átlagosan 70%-a aggódik a személyes adatok tudtuk nélküli további (eredeti céltól eltérő) kezelése miatt.[381] Végül ugyanezt a következtetést megerősíti egy harmadik forrás is, eszerint az felhasználók tartanak attól, hogy – akár az adatkezelő etikátlan eljárása, akár a figyelmetlenül megadott hozzájárulás miatt – az adatkezelők külön értesítés nélkül továbbadják a személyes adatokat.[382]

3.1.2.3.2 Az adatok megadásának szükségessége

Az Eurobarometer 2011-es felmérése alapján a megkérdezettek 75%-a szerint a személyes adatok növekvő feltárása a modern élet része, és 58% szerint nincs alternatívája a személyes adatok megadásának, ha termékeket vagy szolgáltatásokat kívánnak vásárolni illetve igénybe venni. A 15-24 éves korosztálynál érezhetően magasabbak ezek az értékek (83% és 69%).[383] Érdekes, hogy a holland, brit és belga egyetemistákat vizsgáló felmérésben ugyanerre a kérdésre összességében inkább semleges (50% közeli) válaszokat adtak,[384] pedig az Eurobarometer felmérése alapján mind a korcsoport, mind e nemzetek válaszadói az átlagnál magasabb arányban fogadták el az állítást.

Ugyanakkor, és ez mindenképp figyelemre méltó, a megkérdezettek csupán egyharmada válaszolta, hogy az adatok megosztása „nem nagy ügy", míg 63% ezzel nem értett egyet. A 15-24 éves korosztálynál ez az arány 43% illetve 55%, tehát a többség számára még ebben a korcsoportban is „nagy ügy" az adatok megosztása.[385]

3.1.2.3.3 Érintett jogai, érintetti kontroll

Az Eurobarometer 2008-as kutatása alapján – konkrétan rákérdezve, igaz/hamis válaszként megjelölve – a válaszadók döntő többsége tisztában volt az egyes érinteti jogokkal (betekintés: 59%, jogorvoslat: 71%, helyesbítés: 78%, tiltakozás: 88%).[386]

Az érintetti kontrollal kapcsolatban – vélhetően épp az érintetti jogok alapos ismerete miatt – a válaszadók alapvetően magabiztosak. A közösségi oldalakon megosztott tartalmak tekintetében 26% úgy érzi, hogy teljes, 52% pedig úgy, hogy részleges kontrollt gyakorol

[378] Eurobarometer, 2008, 18. Ez alátámasztani látszik azt a feltevést, miszerint az adatvédelmi szabályozás az állami adatkezelőkkel szemben nagyobb hatékonysággal működik (vagy legalábbis úgy látszik), mint a piaci szereplőkkel szemben.
[379] Az állami szervekben (mint átfogó kategória) a megkérdezettek 70%-a bízik, mint az internetes vállalkozásokban mindössze 22%-a! Eurobarometer, 2011, 138.
[380] Brockdorff – Appleby-Arnold, 2013, 9.
[381] Eurobarometer, 2011, 146.
[382] Morton, 2014, 276-277.
[383] Eurobarometer, 2011, 23-24., 27-28.
[384] Leenes – Oomen, 2010, 147-148.
[385] Eurobarometer, 2011, 30-31.
[386] Eurobarometer, 2008, 26.

(pl. törlés vagy javítás kapcsán), míg csupán 20% válaszolta azt, hogy egyáltalán nem érez ellenőrzést a megosztott adatai felett.[387] Az online vásárlás során megadott adatok kapcsán valamivel nagyobb kontrollvesztést éreznek a felhasználók.[388] A holland, belga és brit diákok többsége (70% felett) egyetértett vagy teljesen egyetértett azzal, hogy eldöntheti, kinek és mikor fedi fel személyes adatait, és nagyrészük úgy érezte, hogy érdemben képes a magánszférájának megvédésére. Ugyanakkor a már nyilvánosságra hozott adatok tekintetében (60-70%-ban) elismerték, hogy elvesztik az ellenőrzés lehetőségét[389] – ez tehát ellentmond az Eurobarometer eredményeinek, amely kifejezetten a megosztott tartalmakra kérdezett rá.

Fontos azonban hangsúlyozni, hogy az ellenőrzési-cselekvési potenciálra vonatkozó kérdések az érintett által megadott adatokra vonatkoztak. Látható azonban, hogy az érintettek követése, profilozása jelentős mértékben nem az általa megadott, hanem a megfigyelésével rögzített adatok segítségével történik, az ezekkel kapcsolatos kontroll-érzésre a felmérések nem terjedtek ki.

3.1.2.3.4 Tényleges érintetti magatartás

A fentieket követően érdemes megvizsgálni, hogy miként viselkednek ténylegesen az érintettek, és mennyiben igaz az a „privacy-paradoxonnak" is nevezett jelenség, miszerint a felhasználók tényleges magatartása nincs összhangban a magánszférával kapcsolatos félelmeivel.

Az egyik legérdekesebb kérdés az adatvédelmi nyilatkozatok (privacy policy) ismerete. Az Eurobarometer 2011-ben meglepő eredményt közölt, eszerint a válaszadók 58%-a rendszeresen elolvassa az adatvédelmi nyilatkozatokat. Ugyanakkor azok közül, akik elolvassák, kb. 40% nem érti meg teljes egészében a szöveget.[390] Más felmérések ezen optimizmusra okot adó eredményt nem erősítették meg, a CONSENT projekt keretében mindössze 24% válaszolta, hogy elolvassa, és 72%-uk azt, hogy soha, ritkán vagy néha olvassa csak el az adatvédelmi nyilatkozatokat.[391] Más, főleg amerikai kutatásokat összefoglaló források szintén inkább az alacsony olvasási hajlandóságot emelik ki, sőt bizonyos elemzések rámutatnak, hogy e dokumentumok alapos megismerése – egyszerűen az időigényessége miatt – jelentős gazdasági károkat okozna. Az Eurobarometer 2011-es felmérése szerint az adatvédelmi nyilatkozatot elolvasók 70%-a legalább egyszer nem vett igénybe egy szolgáltatást az adatvédelemmel kapcsolatos aggodalma miatt, tehát nem teljesen hatástalanok e dokumentumok.[392] Nagyon tanulságos ugyanakkor az is, hogy miért nem olvassák el a felhasználók a nyilatkozatokat. A CONSENT projektben a válaszadók 55%-a egyszerűen azért, mert túl hosszú. Emellett sokan úgy vélik, hogy az állam

[387] Eurobarometer, 2011, 127.
[388] Eurobarometer, 2011, 129.
[389] Leenes – Oomen, 2010, 147-148.
[390] Eurobarometer, 2011, 112-114. Országbontás alapján Magyarország az élen végzett, 76% (!) válaszolta azt, hogy rendszeresen elolvassa a weblapok adatvédelmi nyilatkozatát – személyes tapasztalatok alapján kissé szkeptikus vagyok az adat valóságtartalmát illetően. A legalacsonyabb arány is 45%-os, ami szintén magasnak mondható.
[391] Brockdorff – Appleby-Arnold, 2013, 17, Custers et. al., 2013, 443.
[392] Eurobarometer, 2011, 115. A jelentés inkább azt hangsúlyozza, hogy a válaszadók 70% hozzáigazítja viselkedését az olvasottakhoz, ami a pontos kérdés ismeretében némi csúsztatás.

megfelelő szabályai úgyis megvédik, és az offline világban működő „jogi védelem és rend" az online világban is megfelelő védelmet nyújt.[393] Az Eurobarometer 2011-es felmérése szerint azért nem olvassák el e dokumentumokat a felhasználók, mert elegendőnek tartják, ha látják, hogy van adatvédelmi nyilatkozat (41%), vagy azt gondolják, hogy a jogszabályok mindenképpen megvédik őket (27%), vagy pedig azért, mert a weboldal úgysem tartja be a nyilatkozatban leírtakat (24%).

A személyes adatok online megosztásával kapcsolatban a közvélemény-kutatások azt mutatják, hogy a felhasználók szívesen, sokszor nem kellő körültekintéssel, de nem is minden mérlegelést nélkülözve osztják meg személyes adataikat. Az Eurobarometer 2011-es kutatása szerint a közösségi oldalakat használók 80%-a megosztja a nevét, 51% fotókat, 39-39% pedig a lakcímét és a hobbijaival kapcsolatos információkat. A megosztás indokai között elsősorban a szolgáltatás elérése (61%), a másokkal való kapcsolattartás (52%) és a szórakozás (22%) szerepel, a megkérdezettek 43%-a szerint viszont sokszor a szükségesnél több adat megadását kérik a szolgáltatók, és ez a nagy többség számára zavaró.[394] A belga középiskolásokról szóló kutatás hasonló eredményeket mutatott, eszerint a privacy-paradoxon nagyrészt fennáll: az aggodalmak ellenére a megkérdezettek többsége közzétesz magáról vagy leíró, vagy azonosító adatokat (utóbbit jóval kisebb mértékben, lakcímet, otthoni vagy mobiltelefonszámot, pl. csak 10-20%-uk). Ugyanakkor az aggodalom mértéke és a megadott adatok között van kapcsolat, alapvetően igaz az, hogy minél jobban aggódik valaki a személyes adatai jogellenes kezelése miatt, annál kevésbé hajlandó megadni azokat – az összefüggés azonban egyáltalán nem egyenesen arányos.[395]

A CONSENT projekt eredményei alapján a válaszadók 75%-a (mindig, gyakran, vagy legalább néha) keresi az adatközlés kontrollálásának lehetőségét, pl. checkboxokat vagy az opt-out opciót biztosító funkciókat.[396] Egy, a „digitális generáció" (digital natives) privacy-tudatosságát vizsgáló, jelentős generációs különbségeket igazoló kutatás összefoglalója szintén e generáció viszonylagos tudatosságát emeli ki. Eszerint többségük a közösségi oldalakat inkább magánszférája részének tekinti, igyekszik kontrollálni, hogy kivel mit oszt meg, és az adatai, véleménye közlésére sokkal inkább az önkifejezés eszközeként, mintsem a magánszférájuk csökkenéseként tekintenek. Tudatosan hajlandóak lemondani a magánszférájuk egy részéről meghatározott előnyökért (kedvezményekért, kényelmi szolgáltatásokért, hírnévért stb.) cserébe.[397] Ezekhez hasonló megállapítást tesz az angol, belga és holland egyetemistákat vizsgáló kutatás is.[398]

Végül az adatalanyok aktivitása kapcsán érdemes megnézni az érintetti jogok tényleges gyakorlásáról szóló eredményeket az Eurobarometer 2008-as, adatkezelőket érintő

[393] Custers et. al., 2013, 442-443.
[394] Eurobarometer, 2011, 40., 46., 50., 54.
[395] A tanulmány egyik fontos tanulsága rossz hír a tinédzserek szüleinek: az adatok közzétételi hajlandósága nem függ attól, hogy a szülő milyen módon viszonyul a gyermeke internetezési szokásaihoz: együtt böngészve tanítja a veszélyre, korlátoz bizonyos oldalakat, vagy csak monitorozza a gyermek online aktivitását. (Walrave – Heirman, 2011, 302.)
[396] Custers et. al., 2013, 440.
[397] Andrade – Monteleone, 2013, 124. A tanulmány több más felmérés adatait felhasználva von le következtetéseket.
[398] Leenes – Oomen, 2010, 151.

felmérésére támaszkodva, amely azonban csak a betekintésre és a panaszra kérdezett rá. A válaszadók szerint az adatkezelők 46%-hoz érkezett a megelőző évben legalább egy betekintés iránti kérelem, de a kérelmek száma csak 18%-nál haladta meg a 10-et.[399] A panasszal élők aránya mindössze 3% volt, ami elsőre alacsony aránynak tűnik, de egy többezres vagy többtízezres adatbázis esetén valójában jelentékeny szám,[400] és nagyjából egybecseng a 2011-es kutatás eredményével, miszerint a válaszadók csupán 2%-a szenvedett el közvetlenül személyes adatokkal kapcsolatos visszaélést.

3.1.2.3.5 Szerepek – ki legyen a személyes adatok őre?

A dolgozat következtetései szempontjából is igen érdekes kérdés, hogy a polgárok szerint kinek a feladata a személyes adatok hatékony védelmének biztosítása. A kutatások általában nem, vagy csak közvetve térnek ki e kérdésre, néhány megállapítás azonban így is tehető.

Az állampolgárok mindenekelőtt egyértelműen igénylik a kontroll megtartását (legalábbis annak illúzióját). A megkérdezettek háromnegyede (74%-a) szerint kívánatos lenne, hogy bármilyen adatkezelést csak a hozzájárulásával lehessen végezni, 87%-uk szívesen kapna értesítést az adatai ellopása vagy elvesztése esetén, 75%-a szeretné, ha akkor töröltethetné a róla szóló adatot, amikor csak akarja, és 71% fontosnak tartja az adathordozhatósághoz való jogot.[401] Ha ezeket az igényeket összevetjük azzal, hogy ténylegesen mennyiben élnek e jogokkal, azt látjuk, hogy az érintettek szeretnék, ha e jogok és általában a kontroll lehetősége megilletné őket, de ténylegesen nemigen élnek vele. Az Eurobarometer 2011-es felmérésében résztvevő válaszadók alapján – a kérdést a közösségi oldalakkal kapcsolatban feltéve – a személyes adatokkal kapcsolatos felelősség elsősorban a felhasználóé (azaz az érintett vigyázzon a személyes adataira), másodsorban a közösségi oldalé (mint adatkezelő), végül harmadsorban a hatóságoké.[402] A kontroll vágyával párhuzamosan tehát a megkérdezettek hajlandóak az ezzel járó felelősséget is vállalni.

A belga, holland és brit diákok az érintett szerepének erősítésével kapcsolatos kérdésre kiegyenlített választ adtak, ugyanakkor az állam szerepét a szűk többség erősítené (nemzetiségtől függően 50-65% egyetért vagy teljesen egyetért).[403] Ugyancsak az állami védelem igényére mutatnak azok a válaszok, amelyeket az adatvédelmi nyilatkozatot nem olvasók adtak arra vonatkozóan, hogy ezt miért nem teszik meg.

A védelem megteremtésében az európaiak az adatvédelmi felelősre is számítanának. Nagy többségük (64%) úgy gondolja, hogy adataik nagyobb biztonságban vannak, ha a nagyobb cégeknél adatvédelmi felelős is gondoskodik a személyes adatok védelméről.[404]

3.1.2.3.6 Az adatkezelők adatvédelmi hozzáállása

[399] Az eredmények igen nagy különbségeket mutatnak az egyes tagállamokban. Az egyik szélsőség Franciaország, ahol az adatkezelők 75%-hoz egyáltalán nem érkezett betekintési kérelem. Magyarország az EU átlaghoz közelít.
[400] Eurobarometer, 2008b, 35-36.
[401] Eurobarometer, 2011, 148., 152., 158., 160.
[402] Eurobarometer, 2011, 178.
[403] Leenes – Oomen, 2010, 149-150.
[404] Eurobarometer, 2011, 187.

A fentiek mellett érdemes röviden bemutatni az adatkezelések másik szereplőjének, az adatkezelőknek az adatvédelmi tudatosságát és hozzáállását. E témakör ugyanakkor méltatlanul elhanyagolt, jóval kevesebb felmérés készült e témakörben, mint az érintettek attitűdjével kapcsolatban, így alapvetően az Eurobarometer 2008-as felmérésére támaszkodhatom.

Az első fontos kérdés az adatvédelmi szabályok ismertsége. Az adatvédelemért felelős munkatársak válaszai alapján az adatkezelők 69%-a legalább valamennyire ismeri a rá vonatkozó szabályokat (igaz, csak 13% ismeri igazán alaposan), ugyanakkor a szűk többség nem tartja alkalmasnak a hatályos szabályozást az új kihívások kezelésére. A szabályok elfogadottsága ugyanakkor elég magas: a megkérdezettek 91% inkább egyetértett abban, hogy kellenek az adatvédelmi előírások a polgárok magas szintű védelme érdekében, és csak 35% tartotta egyes esetekben túlzottan szigorúnak a szabályokat.[405]

Az adatkezelők szűk többsége (52%) saját bevallása szerint használ valamilyen privátszférát erősítő technológiát,[406] és csak 14% válaszolta azt, hogy nem is hallott ezekről. Adatvédelmi nyilatkozata viszont a többségnek nincs, csak 41% jelezte, hogy közzétesz rendszeresen felülvizsgált adatvédelmi nyilatkozatot, és csupán 17% vizsgálja valahogy, hogy a felhasználók elolvassák-e ezeket.[407]

3.1.2.3.7 Értékelő gondolatok

A felületes értékelések során gyakran előkerülő mítoszt, miszerint „a felhasználók a magánszférájukkal nem törődve, felelőtlenül megosztanak az Interneten mindenféle információt," a kutatások nem támasztják alá. Ugyanakkor az eredmények csak e szélsőséges nézet cáfolatát adják, és nem jelentik sem azt, hogy a szabályozás jelenlegi logikája és a felhasználók (különösen a fiatalabb korosztály) igényei találkoznának, sem azt, hogy nincs generációs különbség az adatvédelem megítélésében, és végül azt sem, hogy az érintetti kontroll megnyugtató megoldás a személyes adatok védelmére.

A közvélemény-kutatások egyik fontos tanulsága, hogy az érintettek adatvédelmi attitűdje alapvetően összetett, országonként is váratlanul jelentős eltérésekkel, sok esetben kifejezetten ellentmondásos eredményekkel. Néhány tendencia ugyanakkor egyértelműen kirajzolódik.

1. Más társadalmi problémákkal összehasonlítva a magánszféra védelme nem foglal el kiemelkedő helyet, de konkrétan rákérdezve a többség fontosnak érzi a személyes adatai védelmét. Ez önmagában azonban kissé félrevezető eredmény, mert egyértelműen ez tűnik a „politikailag korrekt" válasznak. A személyes adatok kezelésével kapcsolatos aggodalmak a kérdés konkrétságával nőnek, az adatok harmadik személyek számára történő továbbítása kapcsán például jóval többen aggódnak, mint általában a személyes adatok kezelésének jogszerűségén. Összességében alacsony az adatkezelőkbe vetett bizalom, a felhasználók nemigen bíznak abban, hogy az adatokat szakszerűen és

[405] Eurobarometer, 2008b, 9., 12., 16.
[406] Lényegében az összes adatnál igen jelentős a tagállamok közötti különbség, ez esetben 74%-os csúcsérték, és 28%-os minimumérték között oszlottak meg az egyes országok értékei.
[407] Eurobarometer, 2008b, 24., 37-38.

jogszerűen fogják kezelni. A bizalom mértéke nagyobb az állami szervekkel, mint a piaci szereplőkkel szemben.

A felméréseknek fontos, nagyjából egybehangzó tanulsága azonban az is, hogy a társadalom egy viszonylag széles rétege (30-40%) lényegében nem foglalkozik az adatvédelem kérdésével, azaz nem különösebben aggódik az esetleges visszaélések miatt, nem nagyon ismeri az online adatkezelési technikákat (például a cookie jelentőségét), és nem is mérlegeli tudatosan a személyes adatai megosztását.

2. Széles körben elfogadottá vált, hogy az adatok megadása a modern élet része, és a termékek megvételéhez, szolgáltatások igénybevételéhez elengedhetetlen. Ettől függetlenül az adatok megosztása a többségnek okoz némi kényelmetlen érzést, különösen, ha szükségtelennek tűnő adatokról van szó.

3. Az adatokkal kapcsolatos új jelenségek (viselkedésalapú reklámozás, adatok harmadik felek számára történő továbbítása stb.) viszonylag ismertek, noha ez az ismertség egyáltalán nem legitimálja a vállalkozások adatkezelési gyakorlatát. Sőt, a polgárok csak egy kisebb hányada fogadja el ezeket (még megadott hozzájárulás esetén is).

4. Az előző két pontból logikusnak tűnne egyfajta „kilátástalanság érzés": a felhasználó úgy érezheti, hiába aggódik a személyes adatai miatt, és hiába nem nagyon bízik abban, hogy megfelelő védelemben részesülnek, kénytelen megadni azokat akkor is, ha ettől kényelmetlenül érzi magát.

5. Ennek látszólag ellentmondanak az érintetti kontrollal kapcsolatos válaszok, amelyek meglepő magabiztosságot mutatnak. Ennek oka az lehet, hogy egyrészt a kontroll-érzés a felhasználók által megadott (és nem az egyébként róluk gyűjtött) adatok tekintetében áll fenn, másrészt a kutatások során jellemzően az érintetti jogokkal összekapcsolva (törlés, helyesbítés) vizsgálták, és e jogok széles körben ismertek. Más eredményekkel (például egyes adatkezelési gyakorlat elutasítása még hozzájárulás esetén is) összevetve ugyanakkor ezek az eredmények sokkal inkább a kontroll illúzióját, mint tényleges ellenőrzési lehetőséget támasztják alá.

6. Végső soron azonban – akár kilátástalanságból, akár az aggodalom hiányából, akár a kontroll érzéséből adódóan – a felhasználók elég könnyen megadják és megosztják a személyes adataikat, de – különösen a fiatalabb generáció – nem minden körültekintést nélkülözve, hanem az elérhető (gazdasági, reputációs) előnyöket is (jól-rosszul) mérlegelve. Mindent egybevetve ugyanakkor a felhasználók viselkedése nincs teljesen összhangban a félelmeikkel és a bizalmatlanságukkal, azaz a privacy-paradoxon jelensége – ha nem is annyira leegyszerűsítve, mint ahogy sokszor megjelenik – fennáll.[408]

7. A felhasználók jelentős része erősebb kontrollt igényelne magának, amellyel aztán – mint látható – csak mérsékelten él. Sokakban ugyanakkor megvan egy hamis biztonságérzet is, miszerint az állami szabályozás és állami fellépés kellő védelmet nyújt számára.

[408] A privacy-paradoxon az adatbiztonság kérdésére is igaz. Az Eurobarometer 2008-as felmérése alapján az internethasználók nagy többsége (82%) aggódik az adatbiztonság miatt, ugyanakkor csak kevesen (22%) tesznek ez ellen valamit biztonsági eszközök (tűzfal, szűrők stb.) használatával (Eurobarometer, 2008, 5.).

8. Az adatvédelemhez való hozzáállásban valóban létezik némi generációs különbség. Ezt az Eurobarometer 2008-as és 2011-es korcsoport szerint bontott adatai is alátámasztják, ugyanakkor a digitális generációról szóló tanulmány megállapításai néhol túlzottan optimistának tűnnek. Az azonban bizonyos, hogy a 15-24 éves korosztály valamivel kevésbé aggódik, több ismerettel rendelkezik az adatkezelési technikákról, valamivel könnyebben adja meg személyes adatait, és nagyobb kontrollt képes gyakorolni és tudatosabban előnyökre váltani a személyes adatai megosztását, mint az idősebb korcsoportok tagjai. Drasztikus különbség, netán éles ellentét azonban nem tapasztalható az egyes generációk között az adatvédelmi kérdésekhez való hozzáállásban.

3.1.2.4 Az informatikai biztonság helyzete

A fenti technikai folyamatoknak – illetve általában az információs társadalom kiteljesedésének – fontos következménye az informatikai biztonság és adatbiztonság kérdéskörének felértékelődése. A kérdéssel ugyan a szakemberek már a 70-es évektől foglalkoznak, de az informatikai rendszereknek való kiszolgáltatottság folyamatosan nő. A számítógépes bűnözés széleskörű szervezett bűnöző csoportok kezébe került, a korábban gyakoribbnak tekintett elkövetői motivációk (elbocsátott munkavállaló bosszúja, szellemi kihívás, unalom)[409] háttérbe szorultak, és előtérbe került a professzionális szervezett bűnözés keretében megvalósuló haszonszerzési cél. Egyre komolyabb fenyegetést jelent emellett a cyberterrorizmus, amely ellen nem elegendő az egyes szereplők informatikai biztonsági, egyedi, alulról építkező védelme, hanem állami szintű védekezés is szükséges.[410]

Mindezen folyamatok mellett – meglepő módon – az informatikai biztonságra vonatkozó szabályozás erős hiányosságokat mutat. A jogszabályi szintű szabályozásban „rendkívül heterogén az informatikai biztonságra vonatkozó előírások tartalma és hatálya. Nincsen olyan jogszabály, amely az információbiztonság vagy az informatikai biztonság területén keretszabályozás jelleggel minden területre kiterjedően határozna meg előírásokat. Ezzel szemben a különböző nemzetgazdasági ágakra, adatkezelésekre, egyes szakmák gyakorlására vonatkozó szabályok között gyakran található eltérő mélységű biztonsági szabályozás.”[411] Részben ezért, részben a műszaki vonalon hagyományosan erős szabványosításnak köszönhetően az informatikai biztonság területén jelentős a különböző szabványok szerepe, amelyek nem csak műszaki követelményeket, hanem a legalább ekkora jelentőséggel bíró szervezési intézkedések megtételét is szabályozzák. Az ISO/IEC

[409] Balogh, 1998, 280.
[410] Szádeczky, 2008, 203.
[411] Szádeczky, 2011, 85. A szabályozás jellegét tekintve megkülönböztet indirekt szabályozást, felületesen szabályozott és részletesen szabályozott területeket, valamint önkéntes önszabályozást. Szádeczky ugyan a magyar szabályozást vizsgálta részletesen, de más országokban is hasonló tendenciák figyelhetők meg. E területen az elmúlt évben ugyanakkor jelentős előrelépést tett a magyar jogalkotó: ugyan szintén nem átfogó jelleggel, csak a közigazgatási infrastruktúrára nézve, de – részben a közelmúltban tapasztalt kiberháborúk miatt – elkészült egy korszerű magyar információbiztonsági törvény. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban Ibtv.) jelentős mérföldkő a közigazgatási informatika szabályozásban. Szádeczky, 2013, 154.

27000-es szabványsorozat komplex információbiztonsági[412] irányítási rendszer bevezetését és tanúsítását teszi lehetővé.[413] Az információbiztonság belső szabályozásának az adatvédelem szempontjából az (is) a jelentősége, hogy az adatvédelmi motivációktól függetlenül segíti az adatbiztonság érvényesülését.

A személyes adatokkal kapcsolatos jogsértések egyre növekvő részét informatikai biztonsági incidens okozta. Az erre született jogi válaszok – az adatbiztonsági szabályozás erősítése, az adatvédelmi incidensek bejelentésének kötelezettsége – az adatvédelmi szabályozás új tendenciáinak fontos elemei.

3.1.2.5 Az adatvédelem helye az információs társadalomban

Az ezredfordulót követően megjelent, információs társadalommal kapcsolatos dokumentumok a fent részletezett technológiai változásokra csak részben reflektálnak, amely e dokumentumok időzítésének köszönhető: a technológiai-társadalmi változások sokkal inkább az évtized második felére jellemzőek. Ugyanakkor a legfrissebb dokumentumok is csak a tendenciák egy-egy részét említik, némelyik a mindent átható számítástechnikára, mások az okoshálózatokra (smart grid), az adatvédelemmel közvetlenül foglalkozó dokumentumok pedig inkább a web 2.0-es és a felhőalapú szolgáltatásokra hivatkozásnak – átfogó képet azonban lényegében egyik sem ad.

A 2002-ben kiadott eEurope 2005 akcióterv[414] elsősorban az hálózati infrastruktúra biztonságával foglalkozik, az adatvédelmi problémák és szabályozás aktualitásai kapcsán csak röviden utal a készülő hírközlési adatvédelmi irányelvre. Az i2010 program[415] ugyan megjegyzi, hogy a bizalmat keltő, biztonságos és megbízható hálózat működése érdekében az adatvédelmi szabályozás felülvizsgálata is megfontolandó, de összességében nem túl hangsúlyos e kérdéskör. A dokumentum azonban hivatkozik az egy évvel később, 2006-ban végül valóban elfogadott „Biztonságos Információs Társadalom" stratégiára, amely fontos, a magánszférát is jelentősen érintő tendenciaként azonosítja a mindent átható számítástechnika terjedését.[416] Összességében a 2000-es évek első felében az adatvédelem kérdése kissé háttérbe szorult az információs társadalomról szóló stratégiai dokumentumokban.

Az információs társadalommal kapcsolatos soron következő, jelenleg is „hatályos" stratégiát 2010-ben adta ki a Bizottság, „Az európai digitális menetrend" címmel, amely a 2010-2020 közötti időszakra állapít meg prioritásokat. E dokumentumban a Bizottság megerősíti az adatvédelem és az online szolgáltatásokba vetett bizalom közötti összefüggést. Egy 2009-ben végzett kutatás arra kereste a választ, hogy a felhasználók miért kerülik az internetes vásárlásokat, és a válaszadók majd' 30%-a a személyes adatok védelmével kapcsolatos aggodalmakat, 26%-a pedig általában a bizalomhiányt nevezte

[412] A szabványcsalád tehát már nem csak az informatikai eszközökkel tárolt adatok biztonságára (azaz az informatikai biztonságra) koncentrál. Az informatikai biztonság és információbiztonság elhatárolását ld. az 1.2.1 fejezetben.
[413] Szádeczky, 2011, 140-142.
[414] European Commission, 2002
[415] European Commission, 2005
[416] European Commission, 2006, 5.

meg ennek okaként.[417] A Bizottság ebből azt a következtetést vonta le, hogy az elektronikus kereskedelem elterjedésének egyik kulcsát továbbra is az online környezetbe vetett, a személyes adatok védelmével is megtámogatott[418] bizalom kiépítése és fenntartása jelenti. „Az európaiak nem fognak olyan technológiát felkarolni, amelyben nem bíznak – a digitális kor nem lehet egyenlő sem a Nagy Testvérrel, sem az „internetes vadnyugattal".[419] E kissé optimista nyilatkozatot az érintettek adatvédelmi attitűdjét vizsgáló felmérések részletes elemzése csak részben támasztja alá, mint láttuk a társadalom egy jelentős részét nem különösebben foglalkoztatják az adatvédelemmel kapcsolatos kérdések.

2009-2010-ben emellett több jelentős fejlemény is történt az EU adatvédelmi stratégiáját illetően. A 2009. decemberi csúcson az Európai Tanács által elfogadott, a szabadság, a biztonság, és a jog európai érvényesülését előmozdítani hivatott Stockholmi Programnak igen hangsúlyos eleme a személyes adatok védelmének információs társadalomban való biztosítása. Az Európai Tanács ebben felkérte a Bizottságot arra, hogy „értékelje a különböző adatvédelmi eszközök működését, és szükség szerint nyújtson be további jogalkotási és nem jogalkotási kezdeményezéseket". A dokumentumban megjelenik emellett az Európai Unió adatvédelem területén történő globális szerepvállalás igénye is: „globális szinten az Uniónak vezető szerepet kell vállalnia a személyes adatok védelmére vonatkozó nemzetközi normáknak" az előmozdításában.[420] A Bizottság a felkérésnek eleget téve 2010. április 20-án elfogadta a Stockholmi Program végrehajtásáról szóló cselekvési tervet.[421] Ebben kifejtette, hogy az Uniónak gondoskodnia kell az adatvédelemre vonatkozó alapvető jog következetes alkalmazásáról, és ugyanebben az évben kiadta az adatvédelem átfogó megközelítéséről szóló, az adatvédelmi reform főbb kérdésköreit áttekintő közleményét is.[422]

E dokumentumokban a korábbiakhoz képest hangsúlyeltolódás figyelhető meg az adatvédelem szerepét illetően: az Alapjogi Charta kötelező jogi normává válásával összhangban az adatvédelmi szabályozás e dokumentumokban már egyértelműen alapjogi megközelítésben jelenik meg: „az Uniónak gondoskodnia kell az adatvédelemre vonatkozó alapvető jog következetes alkalmazásáról. Meg kell szilárdítanunk az Unió helyzetét az egyének személyes adatainak védelme tekintetében, az összes uniós szakpolitika – így a bűnüldözés és a bűnmegelőzés, valamint nemzetközi kapcsolataink – terén."[423] A technikai-társadalmi tendenciákra tehát, csakúgy, mint az 1990-es években, az Európai Unió egyértelműen az adatvédelem jelentőségének növelésével, a „több adatvédelem" koncepciójával válaszolt.

[417] Európai Bizottság, 2010c, 13-14.
[418] A Bizottság foglalkozik a bizalom növelésének más eszközeivel, elsősorban a fogyasztóvédelmi szabályok erősítésével is.
[419] Európai Bizottság, 2010c, 18.
[420] Stockholmi Program, 2010, 11.
[421] Európai Bizottság, 2010a
[422] Európai Bizottság, 2010c
[423] Európai Bizottság, 2010a, 3.

3.2 Újgenerációs szabályrendszer szükségessége

Az elmúlt 10-15 évben a technológiai fejlődés és annak társadalmi hatásai által az adatvédelmet ért kihívásokra a hatályos szabályozás nem képes releváns választ adni, így sokan – ideértve az jogirodalmi források szerzői mellett az Európai Unió jogalkotó szerveit is – a hatályos adatvédelmi rezsim újragondolását sürgetik. A szakirodalmi források legtöbbször inkább csak egy-egy konkrét problémára kínáltak megoldási javaslatot, az Európai Unió adatvédelmi reformja azonban átfogó változásokat ígér.

Véleményem szerint az előző fejezetben bemutatott tendenciák hatására valóban szükségessé vált az adatvédelmi szabályozás alapos újragondolása, amelynek nem csupán egy-egy elemet, hanem a szabályozás alapjait kell érintenie. Olyan újgenerációs adatvédelmi szabályozás szükséges, amely alapvető jellemzőiben tér el a hatályos jogi környezettől – legalább annyiban, mint amennyiben a második generációs szabályok a korai adatvédelmi jogtól.

A következőkben először bemutatom az érintetti kontrollt középpontba helyező adatvédelmi szabályozással szembeni kritikákat, majd a változtatások irányára tett javaslatokat. Végül összefoglalom az általam helyesnek vélt szabályozási modell főbb elemeit, és megvizsgálom, hogy az adatvédelmi reform legfontosabb dokumentuma, az adatvédelmi rendelet tervezete mennyiben felel meg e modellnek.

3.2.1 A második generációs adatvédelmi szabályozás kritikája

Az érintetti kontrollt középpontba helyező és/vagy információs önrendelkezési jogon alapuló adatvédelmi szabályozással kapcsolatos aggályok már a 90-es években megjelentek a jogirodalomban.[424] Az adatvédelmi generációkat összefoglaló Mayer-Schönberger arra hívta fel a figyelmet, hogy az információs önrendelkezési jogon alapuló adatvédelem „fogatlan papírtigrisnek” bizonyulhat, mivel az érintettek többsége rutinszerűen megadja a jobb gazdasági és alkupozícióban lévő gazdálkodó szervezetnek az adatkezeléshez való hozzájárulást.[425] Az érintett pozícióját rontja az is, hogy nincs tisztában az adatok lehetséges felhasználási módjaival, annak értékével, emellett a tényleges adatkezelésről sem rendelkezik elegendő információval.[426] Az információs önrendelkezési jog alkalmazásával az adatvédelem tartalmi kérdéseit háttérbe szorították a

[424] Sőt, az információs önrendelkezési jogot megállapító ítéletben a német alkotmánybíróság maga is utalt arra, hogy érintettek az automatikus adatfeldolgozás körülményei között az adatok tárolását és feldolgozását nem tudják áttekinteni, így a védelem szempontjából a független adatvédelmi felügyeletnek rendkívüli jelentősége van. Ld. erről az 3.4.2 fejezetet.

[425] Mayer-Schönberger, 1998, 232.

[426] A hozzájárulás tényleges alkalmazása így legfeljebb a „felső-középosztály játékszere” lehet (Jóri, 2005, 37.), amelynek tagjai kellő kulturális és anyagi háttérrel rendelkeznek ahhoz, hogy valamelyest érvényesíthessék jogaikat. Más szerző úgy véli, csak az idősebb korosztály képes élni e jogokkal, vállalva, hogy hátralévő napjaira lemond a társadalmi, politikai, gazdasági értelemben vett aktív életről (Dan Geer gondolatait idézi Rauhofer, 2014, 11.). Ez utóbbi „kimaradás-taktika” nyilvánvalóan nem alkalmazható széles körben, és a közvélemény-kutatások is kifejezetten azt mutatták, hogy – korosztálytól függetlenül – az egyének nem kívánnak így reagálni az adatvédelem kapcsán felmerülő veszélyekre.

formális, jogalapra vonatkozó kérdések – az adatvédelmi ügyek vizsgálata gyakran a jogalapok formális vizsgálatában merül ki.[427]

Az utóbbi években megsokasodtak a hozzájárulással és érintetti kontrollal kapcsolatos kritikai észrevételek, amelyekhez immár számos empirikus kutatás is rendelkezésre áll.

Solove 2013-ban megjelent esszéjében úgyszintén kiemeli: a hozzájáruláson alapuló adatvédelem „semleges igyekszik lenni a tartalmat illetően – nem mond semmit arról, hogy a személyes adatok gyűjtése, felhasználása, vagy nyilvánosságra hozatala jó-e vagy rossz – inkább arra [az eljárási kérdésre] koncentrál, hogy az érintett beleegyezett-e a kérdéses adatkezelésbe." Így a hozzájárulás csaknem bármilyen adatkezelést legitimizál.[428] Ezután részletesen és tűpontosan elemzi az érintetti kontroll – ahogy nagyon találóan nevezi: „privacy self-management" – rendszerén alapuló adatvédelmi szabályozás főbb problémáit, két nagy csoportra: kognitív problémákra és strukturális problémákra osztva azokat.

A kognitív problémák közül elsőként az adatkezelés feltételeinek meg nem ismerését említi. Az adatkezelésről szóló tájékoztatásnak mind az Egyesült Államok „notice&choice" rendszerében, mind az európai, tájékozott belegyezésen alapuló adatvédelmi szabályozásban központi szerepe van. Számos felmérés szerint azonban a felhasználók – több hasonló dokumentumhoz, így végfelhasználói szerződéshez, ÁSZF-hez hasonlóan – ritkán olvassák el az adatkezelés feltételiről szóló dokumentumokat. Ráadásul ez szükségszerű, mert ugyan ez adatvédelmi szempontból nem jó, de gazdasági szempontból igen: az összes meglátogatott weboldal adatvédelmi nyilatkozatának elolvasása komoly nemzetgazdasági károkat okozna.[429] E tájékoztatók gyakran túlságosan hosszúak, összetettek, és egyes kérdésekben – az adatkezelő számára kényes kérdésekben, például az adatok további felhasználása vagy harmadik személyeknek történő továbbítása kapcsán – kellően ködösek, ráadásul időközönként változik is a tartalmuk. Ebből, valamint az adatkezelésre vonatkozó szakértelem általános hiányából adódóan az érintett akkor sem érti meg pontosan a tájékoztató tartalmát, ha egyébként elolvassa. A kognitív problémák közül a második a döntéshozatal torzulása. A viselkedéstudományok eredményei az adatvédelem területén is látszanak: az érintett igen csekély, de közvetlen és konkrét előnyért (pl. ingyenes e-mail tárhelyért vagy egy online szolgáltatásra történő regisztráció lehetőségéért) hajlandó vállalni egy esetlegesen nagyobb, de pontosan nem felmérhető absztrakt veszélyt, és az ebből eredő esetleges negatív következményeket.[430]

A strukturális problémák Solove szerint először is az adatkezelések mennyiségéből adódnak. Egy érintett olyan mennyiségű adatkezelővel kerül kapcsolatba (az államigazgatás és a „hagyományos" szerződéses viszonyok mellett tucatjával látogatott weboldalak és online regisztrációk, mobilalkalmazások stb. kapcsán), hogy még akkor is képtelen a róla szóló adatkezelések menedzselésére, ha egyébként e téren kifejezetten

[427] Bäumler, Mayer-Schönberger és Schwartz gondolatatit idézi és elemzi Jóri, 2005, 37-38. A második generációs szabályozás válságáról ld. Jóri, 2005, 36-42. Nagyon hasonló problémákról írt 1997-ben Swire is a piaci alapú adatvédelem kritikája kapcsán.
[428] Solove, 2013, 1880.
[429] Egy kutatás az Egyesült Államokra vetítve évente 781 milliárd dollárra becsülte ezt a veszteséget.
[430] Solove, 2013, 1883-1888.

magas érzékenységgel rendelkezik és sikeresen túljutott a kognitív problémákon. A második strukturális probléma, hogy a hatalmas adatmennyiségnek és az adatbányászati technikák folyamatos fejlődésének[431] köszönhetően az sem egyértelmű, hogy egyrészt pontosan mi minősül személyes adatnak és mi anonim adatnak, másrészt hogy egy újabb adat megadása egy-egy szolgáltatás során milyen potenciális veszélyeket rejt magában, ha valamely adatkezelő más adatokkal összekapcsolja illetve az adatokból további következtetéseket von le.[432] Az adatkezeléssel kapcsolatos döntések meghozatala során az érintettnek esélye sincs az előnyök és veszélyek helyes mérlegelésére.[433]

Végül Solove is felhívja a figyelmet arra, hogy az adatkezelések potenciálisan veszélyei nem csak az érintettet magát, hanem a társadalom egy jelentős részét érinthetik. Ezeket a tényezőket pedig egyénileg nem lehet figyelembe venni: elképzelhető, hogy az adott adatkezelés az érintett szempontjából kifejezetten előnyös, de össztársadalmi szinten veszélyeket hordoz magában.[434] Az a gondolat, miszerint a személyes adatok védelme messze nem az érintett magánügye, hanem a társadalom egészét érintő közügy egyáltalán nem új, de az utóbbi évtizedekben mintha háttérbe szorult volna. E megközelítés megjelent már az információs önrendelkezési jogról szóló német döntésben is,[435] Sólyom László pedig a híres 1988-as tanulmányában – az adatvédelem és a környezetvédelem párhuzamba állításával[436] – így ír erről: „Az adatvédelem és információszabadság lényege éppúgy nem az egyéni védelem, mint a környezetszennyezési ügyeké, hanem elsősorban rendszer kérdése. A konfliktusokat és igényeket azonban mindkét esetben a személyes érintettség, legtöbbször az egyéni kár tudatosítja. Az információs és kommunikációs technikák hosszú távú társadalmi hatásai éppoly bizonytalanul becsülhetők, mint a környezeti hatások."[437]

Kevésbé strukturáltan, de a hozzájárulással kapcsolatos kritikát számos más szerző is megfogalmaz. Az információs egyensúlytalanság (ti. hogy az adatkezelőnek jóval több ismerete van az adatkezelésről, mint az érintetteknek), az adatvédelmi nyilatkozatok hossza és nehézkessége (szakzsargon használata), az adatkezelők különböző okokból eredő erőfölénye és az érintettnek nem tetsző adatvédelmi szabályzatokkal, mint ÁSZF-lel való fellépés lehetetlensége, a saját adatok menedzselésével szembeni érintetti közöny és rövidlátás több szerzőnél is felmerül.[438] Az érintett néha egyértelműen a „gyengébb fél" pozíciójába kerül, és információ, termék, szolgáltatás vagy éppen munkalehetőség

[431] Vö. a Big Data problémakörrel.
[432] A modern adatbányászati eszközökkel az érintetti jövőbeli viselkedése is (hol pontosan, hol kevésbé) modellezhető. Így az adatkezelő olyan adatot is tudhat az érintettről (meghatározott valószínűséggel persze), amelyet az maga sem ismer. Solove, 2013, 1890.
[433] E tényezőkre tekintettel a közvélemény-kutatások eredménye, miszerint az érintetti úgy érzi, kontrollálja az általa megadott adatok sorsát, egészen más megvilágításba kerül, és a válaszok sokkal inkább az ellenőrzés-illúzióját, mintsem a valós kontroll meglétét támasztják alá.
[434] Solove, 2013, 1888-1893.
[435] Ld. az ítélet elemzését a 2.3.2.1 fejezetben.
[436] Nem véletlen, hogy néhány mostanában „felfedezett" jogintézmény (például az adatvédelmi hatásvizsgálat) a környezetvédelem területén is működik.
[437] Sólyom, 1988, 31.
[438] Bygrave-Schartum, 2010, 160-161., Jøsang – Fritsch – Mahler, 2010, 133.

megszerzése (megtartása) érdekében, függő helyzetéből adódóan kénytelen-kelletlen feladja a személyes adatai feletti kontrollt.[439]

A magyar adatvédelmi felfogás és a jogi szabályozás nagymértékben érintett-központú,[440] de a hozzájárulással kapcsolatos problémák a magyar jogirodalomban is felvetődnek. Jóri szerint „érdemes kiemelni azt, milyen kritikátlan lelkesedés övezi máig az információs önrendelkezési jogot a hazai adatvédelmi közgondolkodásban, miközben a külföldi irodalom már a 90-es évek közepétől felhívja a figyelmet arra, hogy [az] kiszolgáltatottá teszi az egyént a nagy gazdasági hatalommal bíró adatkezelők számára."[441] A „hozzájárulás a gyakorlatban nem jelent korlátot az adatkezelők számára" és az információs önrendelkezési jog érvényesülésével a „jog »magára hagyja« az adatkezelővel szemben" az érintettet.[442]

Természetesen számos érv szól az érintetti kontroll fontossága mellett is. Az információs önrendelkezési jog elvi megalapozottságát – az általános rendelkezési jog egyik szeletének értelmezve – szemléletesen mutatja be Szabó Máté Dániel. Az adatgyűjtés és profilalkotás eredményeként – mint írja – „az egyént és a személyiséget egyre inkább adatok, ismeretek fejezik ki."[443] Az információs társadalomban ráadásul az egyén egyre több olyan kapcsolatot tart fenn, amelynek a másik oldalán nem jelenik meg testi valójában, csupán információk valamilyen halmazaként – azaz a „külvilág számára virtualizálódik."[444] A fizikai lét mellett tehát egyre hangsúlyosabbá válik az egyén ismeretekben való létezése is. Ebből az okfejtésből következően az önrendelkezési jognak ki kell terjednie erre a szférára is: „Ha az önrendelkezési jog jelentése az, hogy önmagáról mindenki maga dönthet, és az önrendelkezés tárgya igen nagy részben valamilyen adatokkal leírható ismereteknek az összessége is, akkor az önrendelkezési jog ebben az esetben a jog alanyára és egyben tárgyára vonatkozó ismeretek feletti döntés szabadságát is jelenti. Az egyén a saját sorsáról igen jelentős mértékben úgy dönt, hogy a rá vonatkozó ismeretek sorsáról határoz."[445]

A hozzájárulásnak jelentős szerepe van a különböző a személyiségi jogok rendszerében is: a személyhez fűződő jogokat nem sérti az a magatartás, amelybe az érintett beleegyezett, mivel „az emberi egyéniség érvényesülése, illetőleg kibontakozása elé [...] nem volna helyes a hozzájárulás általános megtiltásával gátat emelni."[446]

Emellett – ha a hozzájárulás létjogosultságát gyakorlati oldalról közelítjük – a közvélemény-kutatások eredményei is összetett képet mutatnak: teljesen világos, hogy az érintettek egy részének nincs szándékában különösebben foglalkozni a magánszféra-védelmének menedzselésével. Úgyszintén az is, hogy egy másik része hiába szeretné, számos esetben – ilyen-olyan okokból – érdemben nem képes kontrollt gyakorolni a

[439] Rauhofer, 2013, 62.
[440] 2012-ig a törvényi felhatalmazáson és néhány szűk esetre alkalmazható különleges jogalapon kívül lényegében az érintetti hozzájárulás volt az egyetlen jogalap.
[441] Jóri – Bártfai, 2005, 161.
[442] Jóri, 2005, 72.
[443] Szabó, 2012, 30.
[444] Szabó, 2012, 31.
[445] Szabó, 2012, 31-32.
[446] Zoltán Ödön érveit idézi Jóri – Bártfai, 2005, 161.

személyes adatai kezelése felett.[447] Végül vannak, akik a szándék és képesség birtokában többé-kevésbé tudatosan cselekszenek, és vagy igyekeznek a lehető legkevesebbet feladni a magánszférájukból, vagy legalábbis bizonyos előnyökért cserébe, tudatosan mondanak le annak egy részéről.[448] Összességében azonban ez nem túl széles réteg.[449] Ugyanakkor néhányak aktivitása is igen jelentős szerepet játszhat az adatvédelem „ügyének" előmozdításában: alkotmánybírósági ügyeket kezdeményeznek (amelyik államban megtehetik), hatósági bejelentéseket tesznek, civil szervezetekhez fordulnak a magánszférájuk védelme érdekében.

Számos olyan esetkör van továbbá, amelyben az érintettek információs önrendelkezési jogukat széles körben is érvényesíteni tudják (vagy legalábbis szeretnék): leginkább azokban az esetekben, amikor az adatkezelés érezhetően behatol az érintett (szűk értelemben vett) privátszférájába, például a különféle direktmarketing üzenetek, közvetlen telefonos megkeresések során, hivatali packázás kapcsán, a sajtó által nyilvánosságra hozott (intim) személyes adatok vagy különösen érzékeny (pl. különleges adatok) kapcsán, vagy – hogy egy szélsőséges esetet is említsek – olyan esetben, amikor az érintett éppen arról dönt, hogy beköltözik e valamely valóságshow keretében egy minden percét kamerával megörökítő és élő adásban közvetítő villába. Ezeknél az eseteknél a magánszférába való behatolás közvetlenül érzékelhető. Egy távoli szerveren történő, cookie-k és böngészési jellemzők alapján történő követés és profilozás, de még egy egyébként tényleges következményekkel járó „távoli" döntés, például egy hitelkérelem szoftveres elutasítása is alig érzékelhető magánszférát érintő kérdésként. Az adatvédelmi szabályozás egyik fontos új kiindulópontja azonban a 60-as, 70-es évektől kezdődően éppen volt, hogy az egyébként „ártatlan" adatok kezelése is potenciális veszélyt jelenthet, és lehetőség szerint csökkenteni kell az információs egyensúlytalanságot. Az érintett önrendelkezési joga ezt – anélkül, hogy érzékelné a magánszférája közvetlen csorbulását – csak nagyon korlátozottan tudja csökkenteni.[450]

A fenti eredményeket – a technológiai fejlődés tendenciáit, a közvélemény-kutatások eredményeit a kritikai észrevételeket, és az érintetti kontroll elvi és gyakorlati megalapozása mellett szóló érveket egyaránt figyelembe véve az a következtetés vonható le, hogy az adatvédelmi szabályozás középpontjába nem az érintettet kell állítani. Ugyanakkor sem a kritikát megfogalmazó szerzőknél,[451] sem az általam javasolt rendszerben nincs arról szó, hogy az érintetti kontrollal, vagy egyes országokban az információs önrendelkezési joggal kapcsolatban visszalépésre lenne szükség. Nem az érintett pozíciójával van baj, hanem annak jelentős túlértékelésével, azzal hogy a második

[447] Még akkor sem, ha esetleg úgy érzi, hogy igen.
[448] A közvélemény-kutatások adatai mellett erre Solove is felhívja a figyelmet (Solove, 2013, 1900.)
[449] És bizonyosan szűkebb annál, mint aki egy kérdésre ilyen tartalmú választ ad. Leginkább a válaszadók azon szűk metszete tartozhat ide, aki 1) kellően aggódik a magánszférájáért, és 2) valóban kellő ismerettel rendelkezik az adatkezelési technikákat illetően (ez kulcskérdés!), 3) nem törődik bele, hogy az adatok megadása a modern élet velejárja, 4) az adatok megosztása számára „nagy ügy", és végül 5) a magatartását a hozzáállásához igazítja.
[450] Nem véletlen, hogy az információs hatalom megosztásának eszközei kapcsán Szabó Máté Dániel (elismerve az információs hatalom magánjellegét) alapvetően az állam információs hatalmának korlátozására koncentrál, ld. Szabó, 2012, 137-182.
[451] Solove például óva int a túlzottan paternalista szabályok alkalmazásától is (Solove, 2013, 1894-1898.)

generációs szabályozás elsősorban (de nem kizárólagosan) az érintetti kontrollra építve kívánta a magánszféra védelmét és az információs egyensúlytalanságot megoldani.[452] Összességében tehát az érintett jelenlegi jogi pozícióját nagyjából-egészében meg kell tartani, tudomásul véve, hogy tényleges korlátként csak ritkán funkcionál.[453] Különösebben megerősíteni e pozíciót nem érdemes, az esetleges erősítésétől hatékonyabb adatvédelmi szabályozást várni pedig kifejezetten tévút.[454]

3.2.2 Az adatvédelmi jog fejlesztésének irányai

Az adatvédelemmel foglalkozó szerzők és az Európai Unió, mint jogalkotó szerv egyaránt számos lehetséges – sokszor persze egymásnak ellentmondó – fejlődési irányt fogalmaztak meg, új elvi megközelítést, vagy egy-egy meghatározott problémára reagáló konkrét módosítást javasolva, ritkábban – és az adatvédelmi rendelettervezet nyilvánvalóan ide tartozik – teljes szabályozási modellt felvázolva. Az alábbiakban e javaslatokból mutatok be néhányat, messze a teljesség igénye nélkül.

3.2.2.1 Elvi megközelítéssel kapcsolatos javaslatok

Többen az alapjogi szemlélet erősítését javasolják a felmerülő problémák kezelésére. A személyes adatok védelméhez való jog alapjogi pozíciójának megerősítése mellett, az alapjog korlátozás szigorú szabályainak maximális betartása, és az adatkezelést korlátozó elvek (célhoz kötöttség, arányosság, adatminimalizálás) következetesebb alkalmazása mellett foglal állást például Rodotà.[455]

Ezen a területen igen érdekes fejlemény a Német Szövetségi Köztársaság Alkotmánybíróságának 2008-ban hozott döntése, amely új alapvető jogként nevesíti az információtechnológiai rendszerek biztonságához és sérthetetlenségéhez való jogot. A védelem közvetlen tárgya a rendszer bizalmassága és sérthetetlensége, azaz a magánszféra védelmét egy további közvetítőn, a rendszer védelmén keresztül valósítja meg, függetlenül attól, hogy abban előfordul-e személyes adat, ha az egyébként képes a személyes adatok olyan körét és fajtáit kezelni, hogy a „rendszerhez való hozzáféréssel lehetővé válik bepillantani egy személy életvitelének lényeges részébe, vagy akár megbízható képet alkotni személyiségéről.”[456]

Több szerző hangsúlyozza, hogy a privacy-szabályozásnak a formális kérdések felől el kell tolódnia a tartalmi, garanciális kérdések,[457] például az érintetti jogok és a célhoz kötöttség követelményének következetesebb érvényesítése felé.[458]

---

[452] Többször hangsúlyoztam az előző fejezet során, hogy az érintetti kontroll szerepe államonként jelentősen eltér, egyes államokban, például Magyarországon, különösen erős.
[453] A hozzájárulás csökkenő szerepéről ld. még Zanfir, 2014, 253-254., Kosta, 2011, 318., Ezzel ellenkező érvelést ld. Brownsword, 2010, 108-109.
[454] Jó példa erre a hírközlési adatvédelmi irányelv cookie-szabályozása. A weblapok – a lehető legdiszkrétebb – felugró ablakokkal igyekeznek hozzájárulást kérni és/vagy tájékoztatást, az érintettek ezért többszázszor kattintanak mindenfelé, miközben a cookie-technológián alapuló adatgyűjtés egyértelműen leáldozóban van (az újabb technikákról ld. a 3.1.1.5 fejezetet).
[455] Rodotà, 2010, 80-82.
[456] Szabó, 2012, 76-77.
[457] Solove, 2013, 1902-1903. E kijelentését elsősorban az amerikai jogrendszerre érti, de felvetése az európai szabályozási keretek között is értelmezhető.

Végül az egyik legjelentősebb új elvi megközelítés az adatvédelem területén az elszámoltathatóság (accountability) elvének alkalmazása. Az elv – jogterületektől függetlenül megfogalmazott – lényege, hogy a szervezet felelősségét komolyan véve, a jogalkotó különböző mechanizmusokat alkalmaz arra, hogy a szervezeteket rászorítsa arra, hogy belső irányítási struktúra, eljárásrendek és szervezeti kultúra kialakításával, érjék el a jogszabályi megfelelést. Azaz a jogalkotó igyekszik rászorítani e szervezeteket, hogy valóban „meg akarják tenni, amit meg kell tenni".[459] Az elv angolszász eredetű, és az adatvédelmen kívül más jogterületeken, például a pénzügyi jog vagy – inkább ajánlásként – a versenyjog területén is használatos.[460] A szakirodalmi források és az adatvédelmi reform előkészítő dokumentumai is nagy jelentőséget tulajdonítanak az elv adatvédelem területén történő alkalmazásának, és az adatvédelmi elvek korábbinál jelentősen jobb végrehajtását várják tőle.

3.2.2.2 Egyes jogintézményeket érintő javaslatok

A fenti, inkább az adatvédelmi szabályozás általános megközelítését érintő javaslatok mellett számos, egy-egy jogintézményt érintő javaslat is született.

Többen a személyes adatok fogalmának újragondolását szorgalmazzák, mivel az új technológiáknak köszönhetően elmosódik a személyes és az anonim adatok közötti határvonal.[461] A profilozás technikájára tekintettel megjelent az a gondolat is, miszerint a „profilt" önállóan definiálva, speciális szabályokkal kellene védeni, illetve erősíteni az érintettek jogait a profilalkotás részleteinek megismerése érdekében.[462]

Eleni Kosta a hozzájárulás elemzéséről írt könyvének konklúziójában a svéd megoldásra hívja fel a figyelmet, amely számos kötelezettség alól mentesíti a nem strukturált adatkezeléseket végző adatkezelőket, ezáltal kivéve például a Lindqvist-ügyhöz hasonló esetekben a természetes személy adatkezelőket".[463]

Úgyszintén érdemes figyelembe venni az adatfeldolgozók szerepének növekedését, és adatkezelők és adatfeldolgozók közötti elhatárolások nehézségeit – e tényezőket a vonatkozó kötelezettségek újraosztásával lehetne orvosolni.[464] Megjelenik a jogirodalomban emellett az az álláspont is, miszerint egyes szabályokat ki kellene terjeszteni új szereplőkre, nevezetesen a készülékgyártókra és az informatikai rendszerek tervezőire is.[465]

A hozzájárulás gyakorlásával kapcsolatban is több érdekes elgondolás olvasható. Solove megjegyzi, hogy érdemes lenne olyan rendszeren gondolkodni, ahol a felhasználó globálisan tudna hozzájárulást adni, hogy ne kelljen a privacy-ügyeit

[458] Zanfir, 2014, 246-253.
[459] Moerel, 2012, 9.2 fejezet
[460] WP, 2010b, 7.
[461] Tene, 2010, 25.
[462] Pullet, 2010, 16-17.
[463] Kosta, 2013, 399. Míg ez a megoldás kétségtelenül jó választ adna arra a problémára, hogy sokszor az átlagos felhasználó is adatkezelőnek minősül, a Big Data jelenség egyik legfontosabb fejleménye, hogy a strukturált és nem strukturált adatok közötti hatásvonalat elmosni igyekszik, így az ez alapján történő kivételezés zsákutca lehet.
[464] Tene, 2010, 26.
[465] Poullet, 2010, 19.

„mikromenedzselnie”. Ezzel összefüggésben el is várná, hogy valaki azért felügyelje az adatkezelőket, és megvédje őt az esetleges sérelmektől.[466] Érdekes ötletként merül fel a kollektív hozzájárulás gondolata, melynek lényege, hogy egy adott csoport közösen adhatna vagy vonhatna vissza adatkezelési hozzájárulást, amely a csoport minden tagjára kötelező lenne, arra is, aki egyénként ezzel nem értene egyet. A gyakorlatban e megoldásnak ott lehet szerepe, ahol eleve működnek érdekképviseleti szervek: szakszervezetek, környezetvédelmi csoportok, diákcsoportok, stb. Az egyéni önrendelkezési jog annyiban megmaradna, hogy mindenki eldönthetné, átadja-e a hozzájárulás megadásának jogát a csoportnak vagy sem, illetve később konkrét esetben is opt-out jog illetné meg az egyes érintetteket.[467]

Igen szemléletes elgondolás Fuster, Gutwirth és De Hert javaslata, akik a kéretlen kommunikációval szembeni védelmi szabályokat terjesztenék ki a „kéretlen eligazgatásra”[468] is. A jelenséget legjobban egy konkrét példán lehet illusztrálni: a szerzők rendszerében ilyen "eligazgatásnak” minősül például, ha – a mindent átható technológia segítségével – az intelligens hűtőszekrény jelzi, hogy lassan elfogy a tej (esetleg küld erről egy sms-t), majd az ajtónyitáskor egy képernyőn megjelenik a közeli boltok tejkínálata, ajánlva persze egy eddig ismeretlen új márkát, amelyet egyetlen érintéssel meg is vehetünk – nem sokat tudva a rendszer működésének hátteréről.[469] Ésszerűnek tűnik biztosítani az ebből való kimaradás lehetőségét.[470]

A magyar jogirodalomban a második generációs szabályozásra adható lehetséges válaszokat Jóri András is részletesen elemzi. Ennek keretében kitér a technológia, elsősorban a privátszférát erősítő technológiák szerepére, az ipari önszabályozás, a szabványosítás és az adatvédelmi audit kérdésére, valamint a német jogban 1997-ben megjelent adattakarékosság elvére (amely nagyban hasonlít a ma igen népszerű „Privacy by Design” elvére).[471] Hegedűs Bulcsú az újgenerációs szabályozás jellemzőiként szintén az önszabályozás és a technológia (privátszférát erősítő technológiák és Privacy by Design elvének) szerepét emeli ki.[472]

3.3 A harmadik generációs szabályrendszer elvi kiindulópontjai

Az elmúlt években számos megoldási javaslat született az adatvédelem jövőjét illetően, amelyek igyekeztek – akár koncepció- és szemléletváltás sürgetésével, akár egy-egy jogintézményre vonatkozóan – reagálni az adatvédelmet ért kihívásokra. A leginkább átfogó javaslat – már csak jellegéből adódóan is – természetesen az Európai Unió

[466] Solove, 2013, 1901-1902.
[467] A koncepciót ld. részletesen Bygrave – Schartum, 2010, 169-172.
[468] A tanulmányuk címe is ez: From Unsolicited Communication to Unsolicited Adjustment
[469] A példa persze nem nagyon különbözik a korábban bemutatott technológiai jelenségek kapcsán leírtaktól, inkább a szerzők kéretlen kommunikációval párhuzamot vonó megközelítése érdekes.
[470] Fuster – Gutwirth – De Hert, 2010, 111.
[471] Jóri, 2009, 269-326.
[472] Hegedűs, 2013, 139-145.

Bizottsága által előkészített, és az Európai Parlament által első olvasatban számos módosítással elfogadott Rendelettervezet.[473]

Jelen fejezetben egy újgenerációs adatvédelmi szabályozás főbb elemeinek bemutatására teszek kísérletet. Nem kívánok – a dolgozatnak nem is célja – egy minden elemében részletezett és teljesen koherens koncepciót felvázolni, csak a főbb irányok elemzésére koncentrálok. Ennek során természetes módon merítek az említett szakirodalmi forrásokból, és különösen a Rendelettervezet előkészítő anyagaiból és a jelenlegi szövegtervezetből. A Rendelettervezetet nagyrészt e koncepció „mintaszabályozásának" tartom, amely persze nem jelenti azt, hogy minden részletszabályában megfelel annak. A következőkben áttekintem az újgenerációs szabályrendszer kiindulópontjait, majd főbb összetevőit, aminek során részletesen, kritikai megközelítéssel elemzem a Rendelettervezet szabályait.

3.3.1 Az érintett és az adatkezelő szerepe

A kiindulópontok közül elsőként azt kell eldönteni, hogy a szabályozás kitől várja elsősorban az egyének magánszférájának védelmét és az információs hatalommal szembeni korlátozást. A fenti eredmények azt mutatják, hogy az érintett ennek megvalósítására csak korlátozott mértékben képes, és sokaknak szándékában sem áll ezzel a kérdéssel különösebben foglalkozni, legalábbis olyankor, amikor a privátszférába történő behatolás nem érzékelhető közvetlenül. A másik potenciális szereplő az adatkezelők, akik sokkal inkább képesek a védelmet biztosítani, de gyakran ellenérdekeltek. A fogyasztói bizalom mértéke nemigen ellensúlyozza az adatvédelmi erőfeszítések költségeit – ez jól látszik a tisztán piaci alapú adatvédelmi megközelítés, és a különböző tanúsító-szervezetek működésének kudarcain is. Az adatkezelőket így alapvetően szabályozással – méghozzá az adatvédelmi tudatosságukat is növelő szabályozással – és a jelenleginél erősebb felügyeleti rendszerrel lehet rászorítani arra, hogy a személyes adatok védelméért az eddigieknél többet tegyenek.

Olyan szabályozási rezsimre van tehát szükség, amely reálisan számol az érintettek passzivitásával, illetve lehetőségeinek korlátaival, és sokkal kevésbé tekinti őket az adatvédelmi szabályozás főszereplőjének, mint eddig. Az adatvédelmi szabályozás súlypontjának el kell tolódnia a „milyen jogokkal élhet az érintett" kérdésétől a „milyen kötelezettségei vannak az adatkezelőknek" kérdése felé. Röviden: az „érintett-központú" szabályozás felől el kell mozdulni az „adatkezelő-központú" szabályozás felé.

Mindezt azonban lehetőleg nem úgy kell megtenni, hogy az érintett rendelkezési jogát széleskörűen korlátozó paternalista szabályokat alkot a jogalkotó: az érintettet nem megvédeni kell saját magától, hanem olyan, „mögöttes biztonságot" kínáló rezsimet kell kialakítani, amely hagyja, hogy az érintett döntsön a saját sorsáról, ha úgy szeretné, és képes is rá, de biztosítson megfelelő védelmet, ha egyébként van igénye a megfelelő védelemre, de valamilyen okból nem képes élni az egyébként szélesnek tűnő jogaival.[474]

[473] Itt is utalnom kell az Európa Tanács adatvédelmi egyezményének modernizálására (részletesen ld. a 1.2.2 fejezetet).

[474] Solove – a hozzájárulással kapcsolatos kritikai észrevételek mellett is – kifejezetten óva int a paternalista szabályoktól, de megjegyzi, hogy lehetséges megfelelő köztes szabályozási logika, ami „terelgeti" a

Mintaként leginkább a fogyasztóvédelmi és a különböző termékfelelősségi szabályok lehetnek irányadók: a fogyasztók széleskörű szerződési szabadsága mellett például egyes ÁSZF kikötések eleve vagy vélelmezetten tisztességtelennek minősülnek. Ha a fogyasztó nem is szentel túl sok figyelmet e dokumentumokat, az erre szakosodott szervek (állami hatóságok vagy civil szervezetek) igen.[475] A fogyasztók emellett nagyjából abban is biztosak lehetnek, hogy az általuk megvásárolt termékek megfelelnek bizonyos minimális biztonsági követelményeknek, amelyeket ráadásul legtöbbször az állam nem közvetlenül, csak közvetve, különböző tanúsító-szervezetek közbeiktatásával felügyel.

Végül, és erről eddig kevesebb szó esett, az érintetti kontroll szerepét legalább részben átvehetik a különböző alapjogvédő és „privacyféltő" civil szervezetek, vagy érintetti érdekképviseleti szervezetek, amelyek az adatvédelmi nyilatkozatok elemzésével, a kétes adatvédelmi gyakorlatot folytató szervezetekkel szembeni fellépéssel jelentős ellenőrző tevékenységet fejthetnek ki.

Az adatkezelők kötelezettségeinek középpontba állítása – amint azt korábban kifejtettem – nem azt jelenti, hogy az érintetti kontrollal, vagy az információs önrendelkezési joggal kapcsolatban visszalépésre lenne szükség. Nem az érintett pozíciója okozza az adatvédelmi szabályozás problémáit, hanem annak jelentős túlértékelése. Az érintett jelenlegi jogi pozíciója megtartandó, de megerősíteni nem érdemes, legalábbis hatékonyabb adatvédelmi szabályozás attól nemigen várható.[476]

E megközelítés ugyancsak nem érinti az alapjogi védelem létjogosultságát. A személyes adatok védelmének alapjogi megalapozottsága számos esetben – különösen a törvényekkel szabályozott állami adatkezelések esetén, ahol az érintett akaratának eleve jóval kisebb szerepe van – hatékony korlátja az információs hatalomnak. Emellett az alapvető jogokból objektív, intézményvédelmi kötelezettségek is származnak. Az „alapvető jogokból nemcsak egyéni, »szubjektív alapjogi igények« vezethetők le, hanem az alapjog mögött meghúzódó elvont érték, életviszony, szabadság biztosításának állami kötelezettsége is. Az alapjogok ún. objektív oldala alkotmányos intézményeket véd, az egyéni alapjogi igényektől független intézményvédelmi kötelezettséget ró az államra."[477] Ebbe a koncepcióba a szabályozás adatkezelők kötelezettségei felé történő eltolódása jól beleillik. Harmadszor pedig azt alapjogi védelem kifejez egy nagyon határozott értékválasztást, amely az adatvédelem és a magánszféra fontosságát üzeni akkor is, ha az adott jogviszonyban az alapjogi megközelítésnek nincs is gyakorlati hatása.

3.3.2 Transzparencia

Az összes szereplő számára kulcsfontosságú azonban az adatkezelések jelenleginél nagyobb átláthatósága. A technológiai változásokból egyértelműen az a tendencia

felhasználókat, anélkül, hogy elzárna előttük bármilyen lehetőséget (Solove, 2013, 1901. Ugyanakkor konkrét példákat ezzel kapcsolatban nem hoz).

[475] A fogyasztóvédelmi párhuzamról ld. még Rauhofer, 2013, 84.

[476] Néhány részletszabályra ugyanakkor szükség lehet annak érdekében, hogy az érintetti jogaival való gyakorlást elősegítse.

[477] A vonatkozó alkotmányjogi forrásokat összefoglalja Polyák, 2008, 23.

rajzolódott ki, hogy nemcsak az érintettek, de többször maguk az adatkezelők,[478] és nem mellékesen a felügyelőhatóságok is elvesztik a kontrollt a személyes adatok kezelése felett.

A transzparencia növelése egyrészt az adatkezelésekkel kapcsolatos egyértelmű tájékoztatás,[479] másrészt az adatkezelők átgondoltabb adatvédelmi politikára szorításával (pl. dokumentációs kötelezettségeinek előírásával és adatvédelmi tudatosságuk növelésével) érhető el.

3.3.3 Garanciális (tartalmi) szabályok erősítése

Az előző fejezetben is jeleztem, hogy a második generációs szabályozás során is megjelentek már olyan elvek, garanciák, amelyek az érintett hozzájárulásától vagy bármely más jogalaptól függetlenül alkalmazandók, pl. célhoz kötöttség követelménye (ideértve a cél a kezelt adatok kapcsán felmerülő szükségesség-arányosság kérdését is), adatminőség elve, adatfeldolgozás szabályai, adatbiztonsági szabályok stb. Ezen – inkább elvi – szabályok végrehajtása azonban meglehetősen nehézkes, könnyen kijátszható, és az adatkezelők, épp a nehezen számon kérhetőségük miatt, kevés figyelmet szenteltek e szabályoknak. E szabályok kapcsán elsősorban a részletek kidolgozására és a végrehajtás hatékonyságára kell koncentrálni.

3.3.4 Elszámoltathatóság

Az adatvédelem területén talán a legfontosabb újdonság az elszámoltathatóság alapú megközelítés, amely az adatkezelők belső szabályozásától, eljárási mechanizmusaitól várja az adatvédelmi elvek hatékonyabb végrehajtását. Az elszámoltathatóság elvével a következő fejezetben részletesen foglalkozom.

3.4 Az újgenerációs szabályrendszer főbb elemei

A fentiek elvi megközelítés alapján a kívánatos (és egyébként várható) adatvédelmi szabályozás változásai három fő területre koncentrálódnak Rövid felsorolásukat követően részletesen is elemzem az egyes pontokat, és áttekintem, hogy milyen szabályokat tartalmaz az új adatvédelmi rendelet tervezete, és hogy azzal kapcsolatban melyek a legfontosabb kritikai észrevételek.

1) Adatkezelők szerepének újragondolása

Az adatkezelők számára az elszámoltathatóság elvével kapcsolatban különböző, az eddigiekhez képest jóval részletesebben szabályozott kötelezettségek kell előírni, amelyek segítségével ténylegesen igazolhatják, hogy betartják és végrehajtják az adatvédelmi szabályokat. A kötelezettségeket olyan módon kell megállapítani, hogy az alkalmas legyen az adatkezelők tudatosságának növelésére. Összességében az

[478] Az adatkezelők tudatosságának növelése ezen a helyzeten változtathat. Vélhetően leginkább azokban az esetekben látják át az adatkezelők a belső folyamataikat, amelyekben különös (pénzügyi) érdekük fűződik az adatvagyon hasznosításához, ilyenkor azonban gyakran abban érdekeltek, hogy rajtuk kívül más ne pontosan lássa át ezeket a folyamatokat.

[479] E körben ki kell emelni a Rendelettervezet (később tárgyalt) egységes piktogramom alkalmazására vonatkozó szabályait, amely jó példa a transzparencia megteremtésére.

adatkezelőket belső szabályozási mechanizmusok kialakítására kell ösztönözni. A szabályozás hatályát nagyrészt ki kell terjeszteni az adatfeldolgozókra is.

Kulcsfontosságú e megközelítés során az adatkezelők differenciálása, azaz a szabályozási terhek megfelelő szétosztása. Az adatkezelések bizonyos jellemzői alapján a személyes adatok jogellenes kezeléséből, illetve az adatokat érintő incidensekből eredő kockázatok és az adatalanyokat érő várható hátrányok mértéke jelentősen eltérhetnek. Ezen eltéréseket hangsúlyosan figyelembe kell venni, ami tulajdonképpen az információbiztonság területén alkalmazott kockázatarányos védelem elvének az adatvédelmi szabályozásra történő kiterjesztését jelenti. A nem kellő differenciálás az egész adatkezelői kötelezettségen alapuló megközelítést értelmezhetetlenné teheti.

2) Az adatvédelmi felügyelet szerepének megerősítése

Meg kell erősíteni az adatvédelmi felügyeletet, méghozzá több szinten is. Mindenekelőtt felkészült (ideértve az informatikai felkészültséget is), független, és erős hatáskörökkel és bírságolási joggal felruházott adatvédelmi hatóságoknak kell az adatvédelem felügyeletét ellátni. A függetlenség kulcskérdés az állami adatkezelőkkel szembeni fellépés során, az erős hatósági eszközök pedig a piaci adatkezelőkkel szemben.

A hatóságok túlterhelésének elkerülése érdekében jelentősen erősíteni kell az egyéb felügyeleti módok, az adatvédelmi audit és tanúsítás intézményét. Egy adatkezelő teljes belső adatvédelmi szabályozásának és gyakorlatának áttekintése ugyanis jelentős erőforrásigénnyel jár, így célszerű e feladatokba piaci szereplőket is bevonni.

3) A technológia, illetve az adatbiztonság szerepének megerősítése

Az adatvédelmi szabályozásnak (újra) célul kell tűznie a technológia szabályozását, formálását. Egyértelművé kell tenni a közpolitikai (jogi) szabályozás elsődlegességét a technikai (praktikus értelemben vett) szabályozószerep felett, és a technológiát a jogszabályok végrehajtásának eszközéül kell használni.

3.4.1 Adatkezelők szerepének újragondolása

3.4.1.1 Az adatkezelők felelősségéről és elszámoltathatóságáról

Az adatkezelők felelősségének (responsibility) és elszámoltathatóságának (accountability) növelése évek óta élénk vita tárgya az adatvédelem jövőjéről szóló szakmai közbeszédben. Az elszámoltathatóság elve az európai adatvédelmi reform keretében is hangsúlyosan megjelenik: utal rá a 29-es munkacsoport adatvédelem jövőjéről szóló dokumentumában,[480] igen részletesen kifejtése kerül egy 2010-ben közzétett, kizárólag e témának szentelt véleményében,[481] majd megjelenik a Bizottsági Rendelettervezet előkészítő közleményében[482] is.

Az elszámoltathatósági elv bevezetésének fő célja a jogi követelmények konkrét adatvédelmi intézkedésekre történő lefordítása, és az adatvédelmi elvek szervezeti szintű

[480] WP29, 2009
[481] WP29, 2010b
[482] EB, 2010

beépítése, integrálása.[483] Az adatvédelem jövőjéről szóló dokumentum – kissé utópikusan – hangsúlyozza, hogy az adatvédelmi elveknek nem csupán az adatkezelő jogi osztálya által kipipálandó kötelezettségként kell megjelennie, hanem ténylegesen át kell hatnia az adott szervezet szervezeti kultúráját.[484] A dokumentum ugyanakkor nem ad eligazítást a tekintetben, hogy ez pontosan miként is valósulhatna meg. A magam részéről úgy látom, hogy a "checklist-compliance" egyrészt elkerülhetetlen, másrészt nem is feltétlenül jelent problémát, ha a szervezetek ellenőrző listák segítségével közelítik meg az (adatvédelmi) jogi megfelelőség kérdését, jelen disszertációban kifejezetten ehhez kívánok segítséget nyújtani. Egy jól kialakított módszertan ugyanis egyrészt csökkenti a megfelelés költségeit, másrészt nem törvényszerűen jár a kötelezettségek kiüresedésével, és azt sem jelenti, hogy le kell mondani az adatvédelmi elvek szervezeti kultúrába való beépítéséről. Utóbbinak több eszköze is lehet (pl. oktatás, workshopok, tájékoztató anyagok), ezek azonban szintén alapvetően "checklist" módszerrel teljesíthetők.

A 29-es munkacsoport a fenti célok érdekében az elszámoltathatóságot általános elvként javasolja jogszabályba iktatni, amelynek két fontos eleme, hogy (1) az adatkezelő megfelelő és hatékony intézkedéseket hajt végre a jogszabályban foglalt elveknek és kötelezettségeknek történő megfelelés biztosítása érdekében, amelyet (2) a felügyelő hatóság felhívására igazolni, bizonyítani is tud.[485] Ugyanakkor mind a munkacsoport, mind a Bizottság dokumentuma igen óvatosan közelít az elszámoltathatóság elv megvalósítása kapcsán felmerülő adatkezelői kötelezettségekhez: a munkacsoport szerint "az elszámoltathatóságról szóló rendelkezés nem jelent nagyobb újdonságot, és nagyobbrészt nem vezet be olyan kötelezettségeket, melyet nem voltak meg a már létező jogszabályokban is" és az "új rendelkezés nem irányul arra, hogy az adatkezelőket újabb elveknek vesse alá, hanem a már létezőeknek történő valós, hatékony megfelelést biztosítja",[486] míg a Bizottság így fogalmaz: az elv "nem az adatkezelők adminisztratív terheinek növelésére irányulna, mivel ezen intézkedések inkább olyan biztosítékok és mechanizmusok kialakítását helyezik előtérbe, amelyek révén hatékonyabban teljesülnek az adatvédelmi előírások". A Bizottság közleménye rögtön hozzáteszi, hogy emellett egyes adminisztratív formalitások – például az adatkezelések hatósági bejelentésének eltörlésével – csökkennek és egyszerűbbé válnak.[487]

Mindegyik dokumentum megnevez ugyanakkor – példálózó jelleggel – jó néhány, az elszámoltathatóság elvét megvalósító konkrét intézkedést is, például írásbeli és kötelező adatvédelmi politikák (szabályzatok) elkészítése, az adatkezelési eljárások feltérképezése (katalogizálása), adatvédelmi felelős kinevezése, adatvédelmi képzés szervezése, az érintett jogainak gyakorlására szolgáló belső eljárásrend és panaszkezelési mechanizmusok kialakítása, belső eljárások a biztonsági rendszer sérüléseinek kezelésére, adatvédelmi

[483] WP29, 2010b, 3. illetve WP29, 2009, 19.
[484] WP29, 2009, 19.
[485] WP29, 2010b, 10. A Bizottság közleménye az adatkezelők elszámoltathatóságának növelése melletti általános állásfoglalás mellett ezen eredmények figyelembevételét ígéri. EB, 2010, 12.
[486] WP29, 2010b, 10.
[487] EB, 2010, 12.

hatásvizsgálat elvégzése, a végrehajtást ellenőrző mechanizmusok kialakítása, külső audit és tanúsító szolgáltatás igénybevétele, a beépített adatvédelem elvének támogatása.[488]

Álláspontom szerint – a munkacsoport és a Bizottság dokumentumainak ezzel ellentétes megállapításaival szemben – ezen intézkedések jogi kötelezettségként történő potenciális bevezetése jelentős konkrét (kézzelfogható) adminisztratív többletterhet ró az adatkezelőkre a jelenleg hatályos szabályozáshoz képest. Ez akkor is így van, ha egyébként igaz, hogy tartalmilag valóban nem új adatvédelmi elvekről van szó, hanem e kötelezettségek inkább a jelenlegi szabályok tényleges érvényesülését szolgálják.

A Rendelettervezet jelentős lépéseket tesz az elszámoltathatóság elvének érvényesítése és adatkezelői kötelezettségek előírásának irányába. Mindenekelőtt az adatkezelés elvei között nevesíti, hogy az adatok feldolgozása az adatkezelő felelősségére történik, akinek biztosítania kell és igazolnia kell tudni az e rendelet rendelkezéseivel való összhangot (elszámoltathatóság).[489] A 22. cikk – az adatkezelő felelőssége és elszámoltathatósága cím alatt – részletezi az elszámoltathatóságból eredő követelményeket, és kimondja, hogy az adatkezelő mind az adatkezelés módjának meghatározása (azaz az adatkezelés megtervezésekor), mind az adatkezelés során „elfogadja azokat a megfelelő politikákat és megfelelő és igazolható technikai és szervezési intézkedéseket, amelyekkel biztosítja és átlátható módon igazolni tudja azt, hogy a személyes adatok feldolgozása e rendelettel összhangban történik.” A megfelelő politikák elfogadását a technika állására, a személyesadat-feldolgozás természetére, a feldolgozás kereteire, hatályára és céljaira, az érintettek jogait és szabadságait érintő kockázatokra, valamint a szervezet típusára tekintettel kell megtenni.

E rendelkezések végső soron valamilyen írásos dokumentum (szabályzat, nyilatkozat stb.), megalkotását írják elő, mivel csak így lehet a „politikák elfogadását” valóban igazolni egy esetleges jogvita vagy adatvédelmi hatósági eljárás esetén. Ebből az is következik, hogy a dokumentum hiánya adatvédelmi szankciókat vonhat maga után. Hiába nincs szó tartalmilag új adatvédelmi szabályról, amint azt az elszámoltathatóságról szóló előkészítő dokumentumok hangsúlyozzák, konkrét kötelezettségről, az adatkezelő által megteendő feladatról nagyon is szó van.

3.4.1.2 Az egyes compliance kötelezettségekről

3.4.1.2.1 Dokumentáció vezetése

A Rendelettervezet kötelezi az adatkezelőket és adatfeldolgozókat[490] rendszeresen felülvizsgált dokumentáció vezetésére.[491] A dokumentációnak az adatkezelő/adatfeldolgozó, illetve ha van, az adatvédelmi felelős neve, elérhetősége mellett az adatokat megszerző adatkezelőket, valamint mindazon adatokat tartalmaznia kell,

[488] WP29, 2009, 19-20., WP29, 2010b, 12., EB, 2010, 12-13.
[489] Rendelettervezet, 5. cikk (1) f)
[490] A Bizottság 2012-es szövegverziója még kivette volna a kötelezettség alól a kereskedelmi érdek nélkül személyes adatot kezelő természetes személyeket, és a 250 főnél kevesebb főt foglalkoztató vállalkozások/szervezetek, ha az adatkezelés csak a főtevékenységet kiegészítő folyamat. A Parlament által elfogadott szövegverzió ilyen kivételeket nem tartalmaz, az tehát minden adatkezelőre és adatfeldolgozóra kiterjed.
[491] Rendelettervezet, 28. cikk (1)-(2)

amelyekre a tájékoztatásnak ki kell terjednie. A Bizottság eredeti javaslatában jóval több adatkör szerepelt a dokumentáció tartalmára vonatkozóan, ez azonban a Parlamenti javaslatban átkerült a tájékoztatási kötelezettségek közé,[492] mivel az valójában „ugyanazon érme két oldala."[493]

A részletes tájékoztatási kötelezettséget is figyelembe véve, e szakaszok egyértelműen azzal a hatással járnak, hogy az adatkezelő kénytelen egyenként (az egyes adatkezelési célokként) feltárni és katalogizálni az összes adatkezelési tevékenységét, és ezt megfelelően dokumentálni. Ugyanakkor a dokumentálási kötelezettség előírása kiváltja a jelenleg hatályos irányelvben megtalálható, az egyes adatkezelések hatósági bejelentésére vonatkozó kötelezettséget.[494]

A többi, adatkezelőket terhelő kötelezettségekkel együtt e szabályok egyértelműen a transzparencia erősítését is szolgálják. Ugyancsak e tendenciába illeszkedik a tájékoztatási kötelezettséggel kapcsolatos új, az Európai Parlament által javasolt megoldás, amely bizonyos, kötelezően és egységesen használt piktogramok alkalmazását írja elő. Ezek segítségével az érintettek sokkal egyszerűbben és gyorsabban információhoz jutnak az adatkezelés lényegi – potenciálisan legérzékenyebb – kérdéseiről.[495]

3.4.1.2.2 Kockázatelemzés

A Rendelettervezet minden adatkezelő illetve adott esetben adatfeldolgozó számára előírja kockázatelemzés végzését annak érdekében, hogy megállapíthassák, vajon az adatkezelésük "valószínűsíthetően különleges kockázattal" jár-e. A valószínűsíthetően különleges kockázat eseteinek igen nagy jelentősége van a Rendelettervezet rendszerében, mivel számos további kötelezettség e feltételek fennállásának függvénye, ezek alapján történik tehát az adatkezelők terheinek differenciálása, amely kulcskérdés az általam felvázolt újgenerációs adatvédelmi szabályrendszerben.[496] A kockázatelemzést azonban minden adatkezelőnek el kell végezni, hogy egyáltalán megállapíthassa, hogy milyen további kötelezettségei lehetnek. A kockázatelemzést évente vagy az adatkezelésekkel kapcsolatos jelentős változás esetén meg kell ismételni, és – amennyiben nem kerül sor adatvédelmi hatásvizsgálatra – dokumentálni kell.[497]

3.4.1.2.3 Adatvédelmi irányítás (hatásvizsgálat és megfelelőségi vizsgálat)

Az új Rendelettervezet egyik legérdekesebb újítása az adatvédelmi hatásvizsgálat[498] és az adatvédelmi megfelelőségi vizsgálat kötelező bevezetése, mely intézkedéseket együtt az „adatkezelés teljes időtartamára kiterjedő adatvédelmi irányítás" cím alatt foglalja össze. A hatásvizsgálatot egy kivétellel minden „valószínűsíthetően különleges kockázattal járó adatkezelés" esetén el kell végezni, így a kötelezettség igen széles adatkezelői kört érint.[499]

[492] Rendelettervezet, 14. cikk
[493] LIBE, 2012, 86.
[494] Bizottsági Rendelettervezet, Indokolás, 3.4.4.1. pont
[495] Rendelettervezet, 13a cikk
[496] A „valószínűsíthetően különleges kockázat" eseteit és elemzését egyrészt az egyes kötelezettségeknél, másrészt, részletezve, az adatkezelők differenciálásáról szóló részben mutatom be.
[497] Rendelettervezet, 32a cikk, (4) bekezdés
[498] A tervezet angol nyelvű szóhasználatával: „data protection impact assessment" (DPIA).
[499] Rendelettervezet, 32a cikk, (3) bekezdés, c) pont

A hatásvizsgálat célja a tervezett adatkezelési műveletek érintettek jogai és szabadságai, különösen a személyes adatok védelméhez való joguk tekintetében várható hatásának vizsgálata.[500] A hasonló kockázatokat jelentő hasonló adatfeldolgozási műveletek esetében elegendő egyetlen hatásvizsgálatot elvégezni.[501] A hatásvizsgálatba – ha van – az adatvédelmi felelőst is be kell vonni.[502]

A vizsgálatnak ki kell terjednie az adatkezelés teljes időtartamára, a gyűjtéstől azok törléséig. A szöveg részletezi a hatásvizsgálat kötelező elemeit is, ezek

- a tervezett adatkezelés céljának, az esetleges jogos érdeknek a leírása,
- az adatkezelés célokhoz viszonyított szükségességének és arányosságának vizsgálata,
- az érintett jogaira vonatkozó kockázatok (ilyen különösen az esetleges diszkrimináció beágyazásának vagy felerősítésének kockázata), a kockázatok kezelésére és az adatminimalizálásra tervezett intézkedések,
- a személyes adatok védelmét szolgáló, például álnevesítéssel történő biztonsági intézkedések és mechanizmusok,
- a különböző adatkörök törlésére vonatkozó határidők meghatározása,
- a beépített és alapértelmezett adatvédelem elvének végrehajtásáról szóló magyarázat,
- a személyes adatok címzettjeinek (vagy címzettek kategóriájának) felsorolása,
- harmadik országba vagy nemzetközi szervezethez továbbítani tervezett adatok és a címzettek meghatározása, és a megfelelő biztosítékok igazolása,
- az adatfeldolgozás kereteinek vizsgálata.

Amennyiben a hatásvizsgálat magas szintű különleges kockázatot mutat, az adatkezelő köteles előzetesen konzultálni az adatvédelmi felelőssel, vagy – ha nincs ilyen – a felügyelő hatósággal.[503]

A szövegtervezet rendelkezik a hatásvizsgálat eredményeinek felülvizsgálatáról is, amely szükséges egyrészt az adatkezelések kapcsán felmerülő kockázatok változása esetén, de ettől függetlenül is legalább kétévente. Amennyiben a megfelelőségi vizsgálat – melybe úgyszintén be kell vonni az adatvédelmi felelőst is, ha van – nem megfelelést mutat, az adatkezelőnek/adatfeldolgozónak ajánlásokat kell tennie a helyzet rendezésére.[504] A Rendelettervezet tehát egy legalább kétévente elvégzendő tulajdonképpeni belső auditot írna elő az adatkezelők széles köre számára.

Az adatvédelmi illetve privacy-hatásvizsgálat elméleti és gyakorlati (módszertani) kérdéseinek az elmúlt években jelentős szakirodalma lett, és néhány, főleg angolszász jogrendszerben (Egyesült Államok, Ausztrália, Új-Zéland, Kanada, Egyesült Király) a

[500] A megfogalmazásból eredő nehézségekre már itt szeretném felhívni a figyelmet: a szöveg szerint nem csak a személyes adatok védelméhez való jog, hanem más, nem részletezett jogokra és szabadságokra tekintettel is el kell végezni a vizsgálatot.
[501] Rendelettervezet, 33 cikk, (1) bekezdés
[502] Rendelettervezet, 33 cikk, (3a) bekezdés
[503] Rendelettervezet, 34. cikk (2) bekezdés
[504] Rendelettervezet, 33a cikk

2000-es években[505] az egyes kormányzati szervekre vonatkozóan kötelező jogi követelményként is megjelent.[506]

A privacy-hatásvizsgálat definíciós kísérletei közül kiemelkedik az alábbi meghatározás: „olyan szisztematikus folyamat, amely minden érintett szereplő szempontjából azonosítja és értékeli egy projekt, kezdeményezés vagy tervezett rendszer magánszférára gyakorolt várható hatását, és keresi az esetleges negatív hatások elkerülésének vagy enyhítésének módját”[507]

Szükséges néhány terminológiai kérdést is tisztázni. A jogirodalomban eleinte a privacy-hatásvizsgálat („privacy impact assessment”, PIA) kifejezés terjedt el, újabban azonban megjelent – és a Rendelettervezetben is így szerepel – az adatvédelmi hatásvizsgálat, angol szóhasználattal: „data protection impact assessment” (DPIA) kifejezés is.[508] Az elnevezésbeli eltérések tartalmi különbséget is takarnak. Az adatvédelmi hatásvizsgálat (DPIA) a személyes adatok védelmére vonatkozó hatásokat, míg a privacy-hatásvizsgálat (PIA) ennél tágabb szempontrendszert, az érintett magánszféráját érintő hatásokat vizsgál. De Hert szerint ezért az adatvédelmi hatásvizsgálat inkább egy, az adatvédelmi szabályokra vonatkozó megfelelőség-ellenőrzés (compliance-check).[509]

A Rendelettervezet kifejezetten adatvédelmi hatásvizsgálatról rendelkezik, amelynek tartalma szerint azonban „a tervezett adatfeldolgozási műveleteknek az érintettek jogai és szabadságai, különösen a személyes adatok védelméhez való joguk tekintetében várható hatásának vizsgálatát” jelenti. Ez még a privacy-hatásvizsgálatnál is szélesebb vizsgálódási kört ölel fel, és ebben a formában a vizsgálat hatókörét teljesen parttalanná teszi.

A terminológiai különbségek ellenére a privacy-hatásvizsgálatra vonatkozó szakirodalom által felvetett kérdések és megállapítások nagyrészt az adatvédelmi hatásvizsgálatra is irányadóak. Az első gyakran felmerülő kérdés, hogy kötelezővé kell-e tenni az adatvédelmi hatásvizsgálat lefolytatását, és ha igen, milyen alanyi körben. Egyes államokban a jogszabályok kötelezően előírják a hatásvizsgálat lefolytatását az állami szervekre vagy azok egy részére. Ugyanakkor számos gyakorlati nehézséget is felvet a kötelezővé tétel, például a hatásvizsgálat hatókörének és alaposságának meghatározása: előfordulhat, hogy a PIA alanyai egy „egyoldalas checkbox-pipálós dokumentummal” teljesítettnek tekintik az adatvédelmi hatásvizsgálat lefolytatását.[510] A Rendelettervezet jelenlegi szövegezése szerint az adatvédelmi hatásvizsgálat – meglehetősen nehezen értelmezhető hatókörrel – széles körben válna kötelezővé az állami és az üzleti szféra adatkezelői számára egyaránt.

További potenciális szabályozási kérdések is felmerülnek, így például, hogy nyilvánosságra kell-e hozni az eredményét és/vagy kell-e hatósági jóváhagyás az

[505] A PIA módszertanok történetéről ld. Wright – De Hert, 2012, 8-10.
[506] Tipikusan egészségügyi adatok adatbázisba rendezése, adatbázisok összekapcsolása, biometrikus azonosítás bevezetése, új bűnüldözési célú adatgyűjtés és megfigyelés stb. kapcsán folytatnak adatvédelmi hatásvizsgálatot. Simon, 2008, 203-204.
[507] Clarke, 2011, 112. (saját fordítás). További definíciós kísérleteket ld. még Wright – De Hert, 5-8.
[508] A terminológiai különbségek oka, hogy az angolszász jogrendszerekben valóban a magánszférára gyakorolt hatásokat vizsgálják, míg az európai adatvédelmi rezsimbe a jogintézmény szűkebb hatókörrel, a személyes adatok védelmére vonatkoztatva, adatvédelmi hatásvizsgálatként importálható.
[509] Részletesen ld. De Hert, 2012, 34-40.
[510] Wright – De Hert, 2012, 28.

érvényességéhez.[511] A Rendelettervezet alapján sem a nyilvánosságra hozatal, sem a hatósági jóváhagyás nem kötelező, de a hatóság kérésére a hatásvizsgálat eredményeit az adatkezelőnek be kell tudni mutatnia.

Az adatvédelmi hatásvizsgálat kívánatos tartalmáról, módszertanáról gyakorlati tapasztalatok és néhány összegző forrás is rendelkezésre áll. Ezek alapján az adatvédelmi hatásvizsgálat egy meglehetősen összetett folyamat, igaz, a definíció kellően általános jellegére tekintettel adatvédelmi hatásvizsgálat elnevezéssel a legkülönbözőbb jellegű és alaposságú eljárásokat, egészen egyszerű (akár felületes) és valóban alapos és összetett elemzéseket egyaránt le lehet folytatni.

Több forrás egyetért abban, hogy a DPIA központi eleme a kockázatelemzés, amely régóta működő megközelítési mód a legkülönfélébb területeken.[512] A leginkább kézenfekvő természetesen az információbiztonság területén működő eljárások és azok gyakorlati tapasztalatainak hasznosítása, az adatvédelmi hatásvizsgálat módszertana során így célszerű lehet a már kialakított, sokszor szabványként is megjelenő módszerekből kiindulni.[513] A DPIA a kockázatelemzésnél azonban jóval többet jelent. A lefolytatás menetét egy szakértői anyag hét fázisra bontja: 1) a vizsgált projekt részletes leírása, 2) a projekt érintettjeivel (stakeholders) történő kommunikáció, 3) a kockázatelemzés, 4) a jogi megfelelés vizsgálata, 5) a kockázatok elkerülésére vagy csökkentésére és/vagy a jogi megfelelésre irányuló javaslatok megtétele, 6) a döntéshozatal és a javaslatok végrehajtása, valamint 7) a PIA külső felülvizsgálata (auditja).[514] Anélkül, hogy részletesen elemeznénk az adatvédelmi hatásvizsgálat módszertanát és lépéseit, jól látható, hogy egy alapos adatvédelmi hatásvizsgálat jelentős erőforrást és szakértelmet igényel, amely nem biztos, hogy minden adatkezelő számára rendelkezésre áll.

A Rendelettervezet meghatározza az adatvédelmi hatásvizsgálat főbb elemeit, amelynek egy része valójában inkább az adatkezelés katalogizálása (amelyet az adatkezelőnek egyébként is meg kellene tennie), más része azonban valóban segíti az adatkezelés kockázatainak felmérését. Megjegyzendő ugyanakkor, hogy a DPIA keretében végzett kockázatelemzés nem azonos a Rendelettervezet 32a pontjában foglalt kockázatértékeléssel. A Rendelettervezet alapján valójában kétszer kell a kockázatokat értékelni: először meg kell állapítani, hogy az adatkezelés beleesik-e a tervezet által „valószínűsíthetően különleges kockázattal járó" adatkezelési körök valamelyikébe (32a cikk), és egyáltalán szükség van-e adatvédelmi hatásvizsgálat lefolytatására, majd a DPIA keretében (33. cikk) is kell kockázatelemzést végezni. Ennek eredménye a jogi követelmények nagy részét nem érinti,[515] de egyrészt egyes – egyébként nehezen megfogható – elvek és intézkedések (például a privacy by design vagy a választott adatbiztonsági intézkedések, illetve az érdekmérlegelésen alapuló jogalap) alkalmazása és konkrét végrehajtása során az eredményt figyelembe kell venni, másrészt amennyiben a hatásvizsgálat magas szintű kockázatot jelez, az adatkezelő köteles a hatósággal előzetes

[511] Wright – De Hert, 2012, 27, 29.
[512] Az adatvédelmi hatásvizsgálatot gyakran ennél tágabb kockázatelemzési eljárások részeként folytatják le.
[513] De Hert – Kloza – Wright, 2012, 30-31, Wright et. al., 2013, 21-22.
[514] De Hert – Kloza – Wright, 2012, 27-32.,
[515] Azaz csekély kockázatra hivatkozva sem lehet az adatvédelmi elvek és kötelezettségek alól mentesülni.

konzultációt folytatni (amennyiben nincs kinevezett adatvédelmi felelős). Emellett a hatásvizsgálat eredménye – pontosan nem nevesített módon – az esetleges bírság kiszabása során is figyelembe veendő tényező. A kockázatok tényleges szintje és az alkalmazott intézkedések közötti konkrét kapcsolatról a Rendelettervezet egyébiránt nemigen rendelkezik, e szabályokat tartalommal csak a joggyakorlat töltheti ki. A fentiek fényében különösen nehezen érthető, hogy a Rendelettervezet – több más jogszabályhellyel szemben – miért nem rendelkezik további, akár a Bizottság, akár a leendő Európai Adatvédelmi Testület által kidolgozandó részletszabályokról (módszertanról).

Összességében az adatvédelmi hatásvizsgálat tervezett szabályai a jelenlegi formájában nehezen alkalmazhatók: a hatóköre parttalan, az alanyi köre túlzottan széles, mivel olyan adatkezelőkre is kiterjed, akik ennek megfelelő színvonalon vélhetően nem tudnak eleget tenni,[516] így a jogintézmény könnyen kiüresedhet. További részletszabályok és módszertani útmutató nélkül a kötelezettség tényleges tartalma igen nehezen mérhető fel, és egészen eltérő értelmezésekhez vezethet az adatvédelmi hatásvizsgálat terjedelmét, alaposságát és módszereit tekintve.

3.4.1.2.4 Értesítési kötelezettség személyes adatok megsértése esetén

A jelenlegi szabályozáshoz képest a másik igen jelentős kötelezettség az adatvédelmi incidensek esetére bevezetendő – a hatósághoz vagy magához az érintetthez címzett – értesítési kötelezettség (data breach notification). Az Egyesült Államokban már létező, szigorú követelményként megfogalmazott jogintézmény 2009 óta az európai adatvédelmi jogban is ismert: a hírközlési szolgáltatókra a hatályos hírközlési adatvédelmi irányelv[517] már előírja e kötelezettséget.[518]

A Rendelettervezet az értesítési kötelezettséget általános, minden adatkezelőre kiterjedő követelményként tervezi bevezetni.[519] Mindenekelőtt meghatározza a személyes adatok megsértésének fogalmát is, ami „a továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, módosítása, jogosulatlan felfedése vagy az azokhoz való jogosulatlan hozzáférés”.[520] A személyes adatok megsértése esetén indokolatlan késedelem nélkül értesíteni kell a felügyelő hatóságot. Amennyiben az adatok megsértése várhatóan hátrányosan érinti az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét, valamint ha egyébként a hatóság a neki történ bejelentés alapján úgy ítéli meg, akkor az adatkezelőnek az érintettet magát is értesíteni kell. Nem kell ugyanakkor az érintettet értesíteni, ha az adatkezelő igazolja, hogy az incidenssel érintett adatokon olyan technológiai védelmi intézkedéseket hajtott végre, amely értelmezhetetlenné teszi az

[516] Simon Éva például – a magyar bevezetés lehetőségeit vizsgálva az állami szerveknél valamint azon piaci szereplőknél tenné kötelezővé, ahol adatvédelmi felelős kinevezése kötelező (Simon, 2008, 212.)
[517] A vonatkozó szabályokat a 2009/136/EK irányelv vezette be a hírközlési adatvédelmi (2002/58/EK) irányelv módosításával. A bejelentésre alkalmazandó intézkedések részleteit a 611/2013/EU bizottsági rendelet szabályozza.
[518] A hírközlési szolgáltatókra vonatkozó data breach notification szabályokat és a hazai implementálással kapcsolatos egyes kérdéseket részletesen ld. Bíró – Szádeczky – Szőke, 2011
[519] A data breach notification Németországban 2009 óta meghatározott adatokat kezelő szervezetekre vonatkozó követelményként jelenik meg, ld. BDSG 42a
[520] Rendelettervezet, 4. cikk 9. pont

adatokat mások számára. Az Európai Adatvédelmi Testület jogosult iránymutatásokat kidolgozni a részletszabályok tekintetében.[521]

A tervezett szabályok lényegében megegyeznek a jelenleg hírközlési szolgáltatókra vonatkozó szabályokkal. A kiterjesztést a Bizottság 2010-es közleménye már megfontolásra javasolta,[522] a 29-es munkacsoport 2011-ben elfogadott, egyébként a hírközlési szolgáltatók DBN kötelezettségét elemző munkadokumentuma pedig ezt üdvözölte, és javaslatokat is megfogalmazott. Ezek lényege abban állt, hogy először is a kötelezettséget minden adatkezelőre ki kell terjeszteni, mivel „a személyes adatok megsértése az a személyes adatok megsértése, függetlenül attól, hogy a szervezet egy szállító, bank, gyár, vagy a közszféra valamelyik szervezete", másodszor pedig változatlan tartalommal kell kiterjeszteni, mivel a hírközlési szektor kapcsán kiegyensúlyozott, a különböző érdekekre tekintettel lévő szabályozás született.[523] A dokumentum megfogalmazza a jogintézmény céljait is: egyrészt így az érintettek megtehetik a szükséges lépéseket a potenciális károk elhárítására (ezért kell gyorsan megtenni az értesítést, és ezért mellőzhető, ha az adatkezelő maga megteszi a megfelelő intézkedéseket), másrészt az adatkezelőket az adatbiztonság szintjének növelésére ösztönzi.[524] Ugyanakkor az ENISA 2011-ben kiadott tanulmánya jóval óvatosabb, és a kisvállalkozásokra történő kiterjesztést komoly kihívásnak nevezte, mivel azok gyakran nem rendelkeznek kellő erőforrással és tudással az adatok megfelelő biztosítására.[525]

A 29-es munkacsoportban foglalt célokkal alapvetően egyetértek. A data breach notification valóban alkalmas lehet a növekvő mértékű adatbiztonsági incidensek visszaszorítására, az érintettek számára pedig egyes esetekben kulcsfontosságú lehet a megfelelő intézkedések megtétele (pl. bankkártya letiltása új jelszóval történő regisztráció valamely szolgáltatásra, stb.) A hírközlési szolgáltatók kapcsán már több éve működő jogintézmény magyarországi tapasztalatai kapcsán azonban – vonatkozó szakirodalom hiányában konferencia-előadásokra támaszkodva[526] – több jogalkalmazási nehézségre is rá kell mutatni. Az indokolatlan késedelem nélküli bejelentést a végrehajtó jogszabályok rendszerint igen rövid határidővel, 24 órán belül várják el.[527] Emellett nincs igazán „alsó határa" az incidenseknek, a bejelentések jellemzően nem sok embert érintő, nagy volumenű adatlopásról, szivárgásról, vagy más „komoly" biztonsági incidensről, hanem egy-egy érintettet érintő kisebb hibáról, például egy téves előfizetői címre küldött számláról, vagy egy tévesen más előfizetőnél elszámolt kedvezményről szóló incidensről szól. Emellett az is világos, hogy a hírközlési szolgáltatók részéről komoly anyagi

[521] Rendelettervezet, 31-32. cikk. A szövegtervezet előír néhány további részletszabályt az értesítések tartalmára vonatkozóan.
[522] Ezt a kiterjesztésre vonatkozó különösebb indoklás nélkül tette, csak arra utalt, hogy „más ágazatokban (pl.: a pénzügyi szektorban) is fennáll az adatsértés veszélye, [így] a Bizottság megvizsgálja, hogy milyen módon terjeszthető ki [a hírközlésen kívüli] egyéb ágazatokra a személyes adatok megsértésére vonatkozó bejelentési kötelezettség." EB, 2010c, 7.
[523] WP29, 2011a, 10.
[524] WP29, 2011a, 9.
[525] ENISA, 2011, 6.
[526] Ld. Bényi Orsolya és Ádám Szilveszter 2014. április 17-én tartott előadásait (Bényi, 2014, Ádám, 2014)
[527] A 611/2013/EU bizottsági rendelet a „lehetőleg" 24 órán belül kitételt tartalmazza, a magyar szabályozás kötelezően írja elő a 24 órás határidőt. A Rendelettervezethez kapcsolódó végrehajtási szabályok persze ennél hosszabb határidőt is megállapíthatnak, a preambulum (67) bekezdése 72 órát javasol.

ráfordítást és szervezést igényel a bejelentések megtétele, különös tekintettel arra, hogy a 24 órás határidő miatt a bejelentést adott esetben munkaszüneti napokon is meg kell tenni.

E néhány gyakorlati nehézséget felvetése azt a célt szolgálja, hogy rámutassak arra, hogy – bár hatásosnak tűnő érvek felhozhatóak mellette – a kötelezettség módosítások nélküli, minden adatkezelőre egyformán történő kiterjesztése bizonyosan indokolatlan adminisztratív terhet ró a kisebb, az adatkezeléseket esetleg csak a főtevékenységét kiegészítő (járulékos) tevékenységként végző adatkezelőkre. Korábban a jogintézmény kiterjesztését szerzőtársaimmal így láttuk: „A magunk részéről egyetértünk a data breach notification jogintézményének kiterjesztésével olyan további adatkezelésekre is, amelyek esetében a biztonság megsértése számos magánszemély információs önrendelkezési jogát és érdekeit sértheti, ide értve például a bank-, egészségügyi, illetve esetlegesen az elektronikus kereskedelmi szektorban működő egyes szolgáltatókat is."[528] Nagyon is indokolt lehet tehát a jogintézmény kiterjesztése a hírközlési szolgáltatókon kívül másokra is, de korlátozott alanyi kört érintve: vagy egyes további szektorok adatkezelőire,[529] vagy – alkalmazkodva az új Rendelettervezet differenciálási logikájához – egyes „valószínűsíthetően különleges kockázattal járó adatkezelésekre", összességében olyan adatkezelőkre, akiknél a kezelt adatokkal kapcsolatos kockázatok valóban indokolják e szigorú szabályokat, és akik várhatóan meg is birkóznak az értesítési kötelezettséggel együtt járó teherrel. Emellett is mindenképp érdemes lenne kiszűrni a bagatell incidenseket.[530] Máskülönben ugyanis egyrészt az adatkezelők nem lesznek képesek eleget tenni minden bejelentésnek, és a jogintézmény részben papíros jog marad, másrészt ha úgy ahogy mégis sikerül eleget tenni, a felügyelő hatóságok több (tíz)ezer adatkezelőtől évente akár milliós nagyságrendű bejelentést is kaphatnak. Ennek feldolgozása vagy indokolatlanul sok értékes erőforrást köt le, vagy – és ez a valószínűbb – nyilvánvalóan semmilyen érdemi fellépést nem tesz lehetővé a hatóság részéről.[531]

3.4.1.2.5 Adatvédelmi felelős kinevezése és szerepe

A jelenleg hatályos irányelvhez képest jóval részletesebben szabályozná a Rendelettervezet az adatvédelmi felelős[532] jogállását. Viszonylag széles körben[533] kötelezné az

[528] Bíró – Szádeczky – Szőke, 2011, 48.

[529] Vagy még inkább a német minta alapján meghatározott típusú személyes adatot, pl. különleges adatot vagy pénzügyi adatot kezelő szervezetre.

[530] A bagatell ügyek kiszűrésénél is igen körültekintően kell eljárni. Az azonosításra szolgáló adatok (pl. online regisztrációhoz tartozó jelszavak) esetén például az érintettek számától függetlenül indokolt lehet az értesítési kötelezettség. A mostani szabályozás változatlan elfogadása esetén ugyanakkor bejelentési kötelezettség terhelné például a néhány főt foglalkoztató mikrovállalkozást (szóljon a példa egy asztalos kisüzemről), ha tévedésből valaki felbontja egy kollégája bérjegyzékét tartalmazó borítékát, vagy az ügyvezető elveszti az egyik megrendelője sajtpapírra felírt e-mail címét vagy telefonszámát (feltéve, hogy utóbbit széleskörű nyilvántartási rendszer, például az ügyféladatbázisába kívánta menteni). A bejelentést adott esetben hétvégén vagy ünnepnapokon is meg kellene tenni.

[531] Az ICO tartalmilag hasonló kritikáját idézi és elemzi Domokos, 2013, 27.

[532] Az angol szöveg "data protection officer" kifejezését a magyar szövegváltozatban „adatvédelmi tisztviselőnek" fordították, de a magyar terminológia – ideértve a jogszabályt és a jogirodalmat is – egyértelműen az „adatvédelmi felelős" fordulatot használja.

[533] Amennyiben az adatkezelést hatóság vagy állami szerv vagy olyan jogi személy végzi, aki több, mint 5000 érintettre vonatkozóan kezel adatokat, az adatkezelő/adatfeldolgozó fő tevékenységei olyan eljárásokat foglalnak magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerű nyomon követését igénylik, vagy az adatkezelő/adatfeldolgozó alapvető feladatai

adatkezelőket adatvédelmi felelős kinevezésére.[534] A tervezet részletezi az adatvédelmi felelős jogállását, feladat- és hatásköreit.

Rendelkezik az adatvédelmi felelős függetlenségéről, egyrészt meghatározva a megbízatás legrövidebb idejét, ami belső munkatárs esetén legalább 4 év, külső szolgáltató igénybevétele esetén legalább 2 év, másrészt további kötelezettségeket megállapítva az adatkezelő számára. Ennek keretében az adatkezelő köteles gondoskodni arról, hogy ne álljon fenn összeférhetetlenség, hogy az összes adatvédelmi ügybe megfelelően és időben bekapcsolódjon, és arról, hogy legyen valaki a felső vezetésben, aki felel az adatvédelmi megfelelésért, és akinek az adatvédelmi felelős közvetlenül tehet jelentést. Biztosítani kell emellett a megfelelő körülményeket (személyzetet, helyiséget felszerelést, egyéb forrásokat) is. A tervezet rögzíti, hogy az adatvédelmi felelős a kötelezettségét függetlenül látja el, és senkitől nem fogadhat el utasításokat.[535]

A feladat- és hatáskörök kapcsán az adatvédelmi felelősnek egyrészt az adatvédelemmel kapcsolatos figyelemfelhívási, tájékoztatási, tanácsadási szerepe, másrészt az adatvédelmi politikák végrehajtása, az adatvédelmi hatásvizsgálat dokumentumai, valamint a személyes adatok megsértéséről szóló értesítések kapcsán ellenőrzési szerepe, a munkatársak képzésén keresztül megvalósuló tudatosságnövelő szerepe, végül a hatósággal való kapcsolattartásban is jelentős szerepe van,[536] sőt, maga is kezdeményezheti valamely adatkezelés előzetes hatósági konzultációját.[537]

3.4.1.3 Az adatkezelők differenciálásáról

A Rendelettervezet a kockázatelemzés szabályai kapcsán rendezi az adatkezelők terheinek differenciálását. A kockázatelemzés célja, hogy az adatkezelők/adatfeldolgozók megállapíthassák, hogy az adatkezelésük "várhatóan különleges kockázatot" jelent-e.

A várhatóan különleges kockázat eseteit a tervezet tételesen felsorolja:

1) az adatkezelő bármely egymást követő 12 hónap alatt több mint 5000 érintett személyes adatait kezeli;
2) az adatkezelő különleges személyes adatot, tartózkodási helyre utaló adatot, illetve a gyermekekre vagy munkavállalókra vonatkozó, széleskörű nyilvántartási rendszerekben tárolt adatokat kezel;
3) olyan profilalkotásra kerül sor, amelyre az érintettre joghatással bíró vagy őt hasonlóan jelentős mértékben érintő intézkedések épülnek;
4) az adatkezelő egészségügyi ellátás nyújtására, járványügyi kutatásokra vagy mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó személyes adatokat kezel, ha az adatkezelésre meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor;

különleges adatra, tartózkodási helyre utaló adatra, illetve gyermekekre vagy munkavállalókra vonatkozó, széleskörű nyilvántartási rendszerekben tárolt adatok kezelését foglalja magában.

[534] Rendelettervezet, 35. cikk, (1) bekezdés

[535] Rendelettervezet, 35. cikk, (6)-(7) bekezdés, 36. cikk, (1)-(3) bekezdés

[536] Rendelettervezet, 37. cikk a)-h) pont

[537] Rendelettervezet, 34. cikk (2) bekezdés

5) a nyilvánosság számára hozzáférhető területek nagyarányú, automatizált nyomon követésére kerül sor;
6) olyan adatkezelési műveletekre kerül sor, amelynél az adatvédelmi felelős vagy a felügyelő hatóság – az Európai Adatvédelmi Testület jegyzékére figyelemmel – az előzetes konzultációt szükségesnek tartja;
7) az adatkezeléssel érintett személyes adatok megsértése (adatvédelmi incidens) várhatóan hátrányosan érintené az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét;
8) az adatkezelés jellegénél, alkalmazási területénél, illetve céljánál fogva az érintettek rendszeres és rendszerszerű nyomon követését igényli;
9) a személyes adatokat ésszerűen nem korlátozható, jelentős számú személy számára teszik hozzáférhetővé.

A tervezet az adatkezelőket érintő kötelezettségek egy részét a fenti feltételek valamelyikének fennállásához köti. Az 1-2 pont esetén az EU-n kívüli adatkezelőnek Unióban letelepedett képviselőt kell kijelölniük, az 1-8. pontban foglalt esetekben adatvédelmi hatásvizsgálatot kell készíteni, és az 1-2. és 8. pontban foglalt esetekben adatvédelmi felelőst kinevezni.

A Bizottság eredeti javaslata – összességében nehezen átlátható rendszerben – részben más szempontokat is javasolt a terhek differenciálására. Ilyen szempont volt például, hogy mentesült a dokumentációs kötelezettség alól a kereskedelmi érdek nélkül adatkezelést végző természetes személy és a 250 főnél kevesebbet foglalkoztató, az adatkezelést csak a főtevékenységét kiegészítő (járulékos) tevékenységként végző adatkezelő.

A szempontok egy része – például az érintettek követése, profilalkotás, vagy az ésszerűen nem korlátozható nyilvánosság szempontja – egyértelműen reagál az elmúlt évek technológiai fejlődésére. Az adatkezelők differenciálására vonatkozó szabályok alkalmazása azonban több elvi és gyakorlati nehézséget is felvet. A jelenleg megadott szempontok egy része objektív és egyértelmű, az adatkezelő könnyen megállapíthatja a fennállásukat (pl. az érintettek létszámára vagy a különleges adatok körére vonatkozó szempontok). Más részük legalább részben szubjektív, és joggyakorlat nélkül nehezen értelmezhető (széleskörű nyilvántartási rendszer, érintettet jelentősen érintő intézkedés a profilalkotás során, stb.), ami nem feltétlenül baj, de fennáll a veszélye a tagállamonként eltérő joggyakorlat kialakulásának.

Az is látható, hogy az adatvédelmi hatásvizsgálat igen széles adatkezelői körre terjed ki. Az érintettek követését és profilozást végző szolgáltatóktól[538] kezdve a nagyobb adatmennyiséget kezelő adatkezelőkön, egészségügyi szolgáltatókon, bűnügyi hatóságokon át egészen a közoktatási intézményekig és gyakorlatilag valamennyi munkáltatóig bezárólag. Igazán jelentős szűkítést tehát ez a szempontrendszer az adatvédelmi hatásvizsgálat kapcsán nem jelent.

[538] Ilyen adatkezelések lehetnek a szoftverekkel támogatott ügyfélértékelési, hitelbírálati eljárások, de akár egy vállalatirányítási rendszerben összegyűjtött személyes adatok is – ezek az üzleti élet nagyobb szereplői által viszonylag gyakran használt eszközök.

Az adatkezelők terhei közötti differenciálás álláspontom szerint az új, adatkezelő-központú adatvédelmi szabályozási rezsim egyik leglényegesebb kérdése. Egyrészt a web 2.0-es szolgáltatások kapcsán a természetes személy felhasználók is könnyen adatkezelői minőségben találhatják magukat, így kulcskérdés az ő mentesítésük megoldása a kötelezettségek egy jelentős része alól. Másrészt a megfelelő erőforrásokkal nem rendelkező, az adatkezelést a főtevékenységéhez képest gyakran mellékes tevékenységként végző kis- és középvállalkozások[539] is nehezen birkózhatnak meg az adatvédelmi megfelelésből eredő adminisztratív teherrel és többletköltséggel, ami versenyhátrányt okozhat számukra.[540] Ők ráadásul az esetlegesen megnövekedett fogyasztói bizalomból sem profitálhatnak, amelyre oly gyakran hivatkoznak az online szolgáltatások esetén.

Az eredeti elképzelések jóval jelentősebb differenciálást sugalltak. A 29-es munkacsoport elszámoltathatóság elvéről szóló, számos konkrét kötelezettséget is felsoroló véleménye a differenciálás kapcsán kifejti, hogy a „végrehajtandó intézkedések típusának meghatározása során nincs más lehetőség, csak a „méretre szabott" megoldások. A végrehajtandó konkrét intézkedéseket minden eset egyedi jellemzői és körülményei alapján kell meghatározni, különös figyelmet fordítva az adatfeldolgozással járó kockázatra és az adattípusokra.[541] Az „egy méret mindenkire jó" megközelítés csak olyan konstrukciókba kényszerítené az adatkezelőket, melyek nem megfelelőek a számukra, és amelyek kudarccal végződnének.[542]

A jelenlegi szabályozás változatlan elfogadásával éppen e kudarc látszik a legvalószínűbbnek. A differenciálás szabályait mindenképpen újra kell gondolni, hogy az e fejezetben felsorolt kötelezettségek alól szélesebb adatkezelői kört lehessen mentesíteni. A Bizottság eredeti javaslatában szereplő, a munkavállalók száma alapján történő (tulajdonképpen a kis- és középvállalkozásokat mentesítő) szempont nem vezet eredményre: az kizárólag a teherbíró-képességet igyekszik figyelembe venni, és egyáltalán nincs tekintettel az adatkezelésekkel járó kockázatokra.[543] A Bizottság eredeti verziójában szereplő másik szempontot, az „adatkezelés, mint a főtevékenységet kiegészítő (járulékos) tevékenység" fogalmát azonban érdemes lenne megtartani. A parlamenti szövegjavaslatból elsősorban a technológiai fejlődésre közvetlenül utaló, a követés, profilozás és monitorozás szempontjait, valamint az érintett adatkezelők számát figyelembe vevő szempontok lehetnének egy átgondolt differenciálási rendszer sarokkövei. A kötelezettségek túlzott személyre szabása ugyanakkor rugalmatlanná is teheti a rendszert, így indokolt a fenti

[539] Csak a szemléltetés kedvéért, pl. munkaügyi nyilvántartást vezető húsüzem, vagy "sarki fűszeres" az ügyfeleinek elérhetőségi adatait kezelő nyomda, a látogatók bérletét sorszám alapján rendszeresen ellenőrző fitneszterem.

[540] Számos országban – így Magyarországon is – a vállalkozások adminisztratív terheinek mértéke eltúlzott és kevésbé hatékony működést eredményez. Emellett a közvélemény részéről gyakran éri az EU szabályozási rendszerét a túlbürokratizáltság vádja is. Ezek ugyan nem jogi szempontok, de a néhol valóban ésszerűtlen adatvédelmi terhek mindkét jelenséget jelentősen tovább fokoznák, ami nem tartok kívánatosnak.

[541] A kockázat mértékét az adatkezelési művelet(ek) mérete, a feldolgozás tervezett célja, és a tervezett adattovábbítások száma határozhatja meg. Az adat fajtáját a dokumentum szintén javasolja figyelembe venni (WP29, 2010b, 14.)

[542] WP29, 2010b, 13-14.

[543] Egy kis- és középvállalkozás is kezelhet hatalmas mennyiségű és „érzékeny természetű" adatot, így – különösen, ha a tevékenységének jelentős része közvetlenül a személyes adatok valamilyen hasznosítására épül – joggal várható el tőlük akár jelentős adatvédelmi kötelezettségeknek való megfelelés is.

felsorolás 6. pontjában szereplő gumiszabály, miszerint az olyan adatkezelési műveletek is „valószínűsíthetően különleges kockázattal járnak” amelynél az adatvédelmi felelős vagy a felügyelő hatóság – az Európai Adatvédelmi Testület jegyzékére figyelemmel – az előzetes konzultációt szükségesnek tartja.

3.4.1.4 Értékelő gondolatok

A hatályos adatvédelmi szabályozáshoz képest legjelentősebb elmozdulást az adatkezelők elszámoltathatósága kapcsán előírt kötelezettségek jelentik.

A tervezet reagál az adatkezelők és adatfeldolgozók szerepének összemosódására, és a kötelezettségek jelentős részét mindkét szereplőre előírja. Ez alapvetően helyes irány, jellemzően az adatfeldolgozók rendelkeznek megfelelő szakértelemmel és eszközökkel az adatok megfelelő kezelésére, és ténylegesen igen nagy a szerepük az adatvédelem és adatbiztonság megvalósulásában.

Az elszámoltathatóságon alapuló szabályozás nagymértékben növeli az adatkezelések átláthatóságát, ami mind az adatkezelők, mind az adatkezelések felett kontrollt gyakorlók: az érintettek, felügyelő hatóságok és jogvédő szervezetek számára is alapvető fontosságú.

A szövegtervezet számos ponton egyértelműen arra irányul, hogy az egyes adatkezelőket és adatfeldolgozókat rászorítsa arra, hogy az adatkezeléssel kapcsolatos kérdésekre és belső szabályozásra a korábbinál lényegesen nagyobb hangsúlyt fektessenek. Ez jelentően növeli az adatkezelők tudatosságát, javítja az adatbiztonsági potenciált és csökkenti a jogellenes adatkezeléseket. Ugyanakkor jelentős compliance-költséget okoz az adatkezelőknek és adatfeldolgozóknak, és könnyen az adatvédelem „túladminisztrálásához” vezethet.

E hatásokat több eszközzel is csökkenteni lehet. Az egyik ilyen eszköz az adatkezelők szabályozási terheinek differenciálása, ami kulcskérdés az elszámoltathatóság alapú adatvédelmi rezsim működőképessége szempontjából. Bármennyire is mindent áthatóak a technológiai változások, számos adatkezelés esetén egyáltalán nem merülnek fel új kockázatok a 80-as, 90-es évekhez képest, így e területeken a belső szabályozással kapcsolatos adminisztratív kötelezettségek feleslegesek lehetnek. A Rendelettervezet jelentős lépést tesz a differenciálás terén, de számos, valóban bonyolult belső adminisztrációt igénylő kötelezettség (például a data breach notification, adatvédelmi hatásvizsgálat) még így is túlzottan széles alanyi kört érint. A differenciálás területén tehát további, egyes adatkezelők/adatfeldolgozók terheinek jelentős csökkentését eredményező lépésekre van szükség – az adatvédelmi szabályozás területén is érvényesítve az információbiztonság területén régóta ismert kockázatarányos védelem elvét: ha csekély a személyes adatokkal kapcsolatos jogsértések kockázata vagy a várható hátrány mértéke, indokolt lehet az adatvédelmi (adminisztratív) kötelezettségek számának csökkentése is.

Egy másik lehetséges eszköz a compliance-költségek csökkentésére olyan egyszerűen alkalmazható ellenőrző listák összefoglalása vagy módszertan kidolgozása, amely megkönnyíti az adatkezelők és adatfeldolgozók számára a rájuk vonatkozó kötelezettségek áttekintését és az azoknak való megfelelést. A dolgozat 4.5 fejezetében röviden áttekintem

a belső szabályozás „problématérképét”, a belső szabályozási rendszer kialakításának első lépéseit.

3.4.2 Az adatvédelmi felügyelet szerepének megerősítése

3.4.2.1 Az adatvédelmi hatóságok megerősítése

Az adatvédelmi felügyelőhatóságok működése kezdetektől fogva kulcseleme az európai adatvédelmi szabályozási rezsimnek. Államonként ugyan különböző elnevezéssel, jogkörökkel és szerepfelfogással rendelkeznek, de általános tendencia a hatásköreik folyamatos bővítése, és annak felvállalása, hogy az adatvédelmi jogsértéseket nem az csak egyén (bírósági) jogérvényesítésére bízzák.

A Rendelettervezet szabályozása jelentős további előrelépést mutat ezen a területen. A felügyelőhatóságokra vonatkozó rész az irányelv szabályaihoz képest jóval részletesebb. Az új szabályozás – már csak a jogforrási formája miatt is – jelentősen egységesítené a jelenleg egyébként mind függetlenség, mind feladat- és hatáskörök tekintetében meglehetősen különböző adatvédelmi felügyelőszervek jogállását. Az egységesítés azonban nem lenne akkora mértékű, mint más területeken. A Rendelettervezet szabályai ugyanis a hatóságok jogállása kapcsán korántsem annyira részletesek, mint az egyéb szabályokkal kapcsolatban, és a rendeleti forma ellenére a szabályait további tagállami szabályoknak kell megfelelő tartalommal kitölteni. Ez a tagállamok eltérő alkotmányos berendezkedése és hagyományai alapján akár védhető megoldásnak is tekinthető, de továbbra is fennáll annak kockázata, hogy a hatóságok tényleges „ereje” (például a függetlenség mértéke) tagállamonként eltér majd, és a nagy nemzetközi adatkezelők „forum shopping” keretében a kevésbé elszánt tagállami hatóság felügyelete alá igyekeznek tartozni.

3.4.2.1.1 Függetlenség

A Rendelettervezet mindenekelőtt részletezi a hatóságok függetlenségére vonatkozó szabályokat, és rögzíti, hogy „a felügyelő hatóság a ráruházott feladat- és hatáskörök gyakorlása során teljesen függetlenül és pártatlanul jár el” és hogy „a felügyelő hatóság tagjai feladatkörük ellátása során senkitől nem kérhetnek, és nem fogadhatnak el utasítást,” majd rendelkezik az összeférhetetlenség, és megfelelő erőforrások biztosításának szükségességéről. A hatóságok létrejöttével kapcsolatban a Rendelettervezet csak annyit deklarál, hogy azt a tagállam parlamentje vagy kormánya nevezi ki.[544]

A függetlenséggel kapcsolatban megjegyezzük, hogy az Európai Bíróság a jelenlegi szabályok alapján is igen szélesen értelmezi a hatóságok függetlenségére vonatkozó szabályokat. A vonatkozó osztrák, német és magyar ügyek kapcsán a bíróság részletezte a független jogállás egyes elemeit, amelyeket egyébként a Rendelettervezet szövegében is visszaköszönnek.[545] A függetlenség jelentőségét mutatja, hogy ez a követelmény – az alapjogi katalógusokban egyébként rendhagyó módon – az Alapjogi Charta szövegében is megjelenik.

[544] Rendelettervezet, 47-48. cikk
[545] Soós, 2012, 222. Az adatvédelmi biztos hivatalának megszűntetésével kapcsolatos magyar ügyről ld. még Majtényi, 2011, 113-114.

Tekintettel arra, hogy az állami szervek, mint a felügyelőhatóság által felügyelt szervek a legnagyobb adatkezelők közé tartoznak, a hatóság függetlensége kulcskérdés. Az adatvédelmi felügyelőhatóság vezetőjének megbízatását a kormányzati akarattól a lehető legtávolabb kell vinni, és lehetőleg a nemzeti parlamentek minősített többségi választásához kötni.

3.4.2.1.2 Feladat- és hatáskörök

Feladat és hatáskörök tekintetében a Rendelettervezet mind az „ombudsman-jellegű", mind „hatósági jellegű" hatáskörök kötelező előírását tartalmazza,[546] e tekintetben tehát a több államban is alkalmazott vegyes modell megvalósulását támogatja.[547] A tervezet igen nagy hangsúlyt fektet az egyes szankciók és a bírságolás lehetőségének és a bírság összegének meghatározására, és összességében az adatkezelő bevételéhez igazodó, akár egészen magas, az éves világméretű forgalom legfeljebb 5%-át kitevő bírság kiszabását is lehetővé teszi.[548]

A fenti szabályozási megoldás alapvetően helyes irányt követ. Az adatkezelések és az adatvédelmi jogsértések nagyfokú különbözősége változatos hatásköröket indokol, amely a figyelmeztetések és ajánlások kibocsátása mellett a nyilvánosság erejét használó és tudatosságnövelő eszközökön át a hatósági határozatban megtiltott adatkezelésekig és nagyösszegű bírságok kiszabásáig terjed.

3.4.2.1.3 Néhány további gondolat

Az adatvédelmi felügyelő hatóságok megerősített függetlensége és hatáskörei mellett néhány további olyan tényezőt is érdemes megemlíteni, amely szükséges az adatkezelők hatékony felügyeletéhez.

Hustinx arra hívja fel a figyelmet, hogy a hatósági feladatok során különös jelentősége lehet néhány nagy horderejű, jelentős erőforrást igénylő vizsgálat lefolytatásának, a felügyelőszerveknek megfelelő kapacitásokat kell erre fordítani.[549]

Ugyancsak felveti a hivatalból történő eljárások fontosságát.[550] A dolgozatban felvázolt modellben a hatósági szerepvállalás szintén proaktivitást feltételez, olyan szervezetet, amely nem csak az érintettek bejelentésére, hanem számos vizsgálatot hivatalból indít.

Végül rá kell mutatni, hogy az adatvédelmi vizsgálatok során nélkülözhetetlenné vált az informatikai, sőt az informatikai biztonsági szakismeret. Ezek alapos ismerete nélkül a vizsgálatok egy része egyszerűen nem végezhető el, az adatkezelő által megtett erőfeszítések nem értékelhetőek. A jogvédő és jogérvényesítő szervezetek azonban „gyakran híján vannak azon technológiai ismereteknek, amelyek szükségesek volnának

[546] Rendelettervezet, 52-53. cikk
[547] A hatósági hatáskörök megjelenése a korábban ombudsmanszerű tagállami felügyeleti szerveknél több országban – például Magyarországon is – épp az irányelvnek való megfelelés érdekében került be. Az ombudsmani és hatósági jogkörökkel is rendelkező ideális felügyeleti modellről, az információs biztosról ld. Jóri, 2010
[548] Rendelettervezet, 79. cikk.
[549] Hustinx, 2010, 136.
[550] Hustinx, 2010, 136. Hustinx összességében arra helyezi a hangsúlyt, hogy a hatóságoknak képesnek kell lenniük megfelelően priorizálni a feladat- és hatásköreik ellátása során.

ahhoz, hogy kampányszerű tiltakozások mellett komoly párbeszédre legyenek képesek az iparági szereplőkkel."[551] Pontos statisztikák a hatóságok személyi állományáról és annak végzettségéről és szakértelméről nem állnak rendelkezésemre, de az előző idézet alapján, valamint a magyarországi helyzetet nagyjából ismerve szinte bizonyos, hogy a legtöbb adatvédelmi felügyelő hatóságnak jelentős elmaradása van e területen.

3.4.2.2 Az adatvédelmi audit és tanúsítás támogatása

Az állami felügyeleti rendszert indokolt kiegészíteni további, az adatvédelmi megfelelés szakszerű ellenőrzésére képes, piaci alapon működő intézményekkel, auditáló- és tanúsító-szervezetekkel.

A Rendelettervezet igen jelentős lépést tesz az adatvédelmi audit és adatvédelmi tanúsítás elterjesztése felé, lényegében az adatkezelők jogává és a tagállami hatóságok kötelezettségévé téve az önkéntes adatvédelmi audit lefolytatását és egy egységes, "európai adatvédelmi címke" elnevezésű tanúsítvány kibocsátását.[552]

3.4.3 A technológia és az adatbiztonság szerepének megerősítése

A technológiai fejlődés adatvédelmi jogalkotásra gyakorolt hatását a történeti fejlődés és a paradigmaváltást sürgető tényezők kapcsán részletesen áttekintettem. Általánosan elfogadott megközelítés szerint a technológia fejlődése folyamatosan erodálja az egyének magánszféráját, amelyet jogi eszközökkel meg kell védeni. A technológia szabályozószerepe kapcsán mindenképpen utalnunk kell Lawrence Lessig munkásságára. Az amerikai jogász-filozófus professzor szerint a kibertér világában központi, meghatározó szerepet tölt be a „kód",[553] amely alatt az online közeg teljes infrastruktúráját érti: hardverek, szoftverek, az internetet működtető protokollok stb. A kód kényszerítő erejű szabályrendszerként meghatározza a kibertér törvényszerűségeit, a lehetséges és a nem lehetséges viselkedésformákat.[554] Az adatvédelem területén e problémát Dix így fogalmazza meg: „Az adatkezelők gyakran panaszkodnak arra, hogy nem tudnak az adatvédelmi szabályoknak megfelelni, mert a technológia nem alkalmas erre." Az adatvédelmi felügyelő hatóságok pedig utólag a már megtörtént jogsértést tudják csak szankcionálni – és egy vállalkozás sokszor inkább vállalja a büntetést.[555] Az informatikai infrastruktúra átalakítása ugyanis jelentős költségekkel jár.[556]

A fentiekre tekintettel számos olyan jogterületen, ahol a technológia fejlődése jogi kihívásokat okozott, megjelent az az evidensnek tűnő gondolat, hogy a technológiára nem

[551] A CEN/ISSS adatvédelmi szabványosítással kapcsolatos projektjének záródokumentumát idézi Jóri, 2009, 291.
[552] E témakörökkel azonban részletesen a 4. fejezetben foglalkozom, itt csupán megemlítem, hogy miként illeszkednek e jogintézmények az új adatvédelmi rezsimbe.
[553] Lessig remekül rájátszik a „Code" kettős jelentésére: kódexet (jogot) és informatikai értelemben vett kódot egyaránt jelent.
[554] Lessig, 2006, 5.
[555] Dix, 2010, 257-258.
[556] Egy korábbi tanulmányban egy gyakori példával illusztráltam a helyzetet: „hiába van pl. egy szervezetnél az adatvédelmi jogszabályoknak egyébként megfelelő belső szabályzat arra, hogy bizonyos adatokhoz csak meghatározott szervezeti egységek férhetnek hozzá, ha ezt nem támogatják az iktatórendszer jogosultsági beállításai, esetleg nem is lehet megadni jogosultsági korlátozásokat, akkor e szabály a gyakorlatban nem fog érvényesülni." Szőke, 2013, 111.

csak fenyegetésként, hanem a védelem eszközeként is lehet tekinteni. Példaként hozhatók a szerzői jog védelmére alkalmazott digitális jogkezelési rendszerek (DRM),[557] az online média gyermekekre gyakorolt káros hatásai kapcsán felmerülő címkézési-szűrési mechanizmusok, vagy a privátszférát erősítő technológiák (PET).[558] Ezekben az esetekben a technológia közvetlen szabályozószerepet tölt be, ezért igen izgalmas kérdés e szerepkör és a jog hagyományos szabályozószerepének egymáshoz való viszonya.[559]

3.4.3.1 A privátszférát erősítő technológiák (PET)

A „privátszférát erősítő technológiák" kifejezést először 1995-ben, a holland állam és az ontarioi adatvédelmi biztos hivatalának közös projektje során használták. Az azóta eltelt közel két évtizedben mit sem csökkent az érdeklődés az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások fejlesztése iránt. Az adatszivárgások, visszaélési botrányok száma jól mutatja, hogy komoly szerepet kaphat a technológiai megoldások alkalmazása az adatvédelem területén.[560]

A „Privacy Enhancing Technologies" az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőfogalma.[561] Egy ennél részletesebb meghatározás szerint „A PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az információs privacyt a személyes adatok kezelésének kiiktatásával vagy minimalizálásával védi, és így megakadályozza a személyes adatok szükségtelen vagy nemkívánatos kezelését, anélkül, hogy csökkentené az információs rendszer funkcionalitását."[562]

A privátszférát erősítő technológiáknak számtalan alkalmazási területe és konkrét megvalósulási formája van, az áttekintés érdekében érdemes Goldberg tipológiáját felidézni.

1. Az első csoportba tartoznak azok a PET-ek, amelyek a felhasználók anonimitását biztosítják az Interneten történő kommunikáció során, elrejtik személyes adatainkat a kommunikáció más résztvevői elől. Ilyenek például az anonim e-mailküldést lehetővé tevő „remailer"-ek, az egyéb anonimitást és pszeudoanonimitást biztosító rendszerek. Itt említhető az ún. Tor-projekt, amelynek célja, hogy az IP címek védelmét biztosítva a hagyományos Internettől részben független hálózat jöjjön létre, mely a létező infrastruktúrát és megoldásokat használja fel annak érdekében, hogy megakadályozza a hálózati forgalomba való beavatkozást, a cenzúra alkalmazását, vagy a hálózat felhasználóinak azonosítását.

[557] Digital Rights Management
[558] Privacy Enhancing Technologies. A magyar terminológiában többféle elnevezés, pl. a magánszféravédő-technológia is használatos. Székely Ivánt követve a privátszférát erősítő technológiák kifejezést használjuk, mivel így a magyar és angol rövidítés azonos (PET).
[559] A technológia és más – gazdasági, kulturális, politikai, - szabályozók kommunikációpolitikában és adatvédelmi szabályozásban betöltött szerepéről ld. Polyák – Szőke, 2014,
[560] Kiss, 2013, 113.
[561] Burkert, 1998, 125.
[562] Blarkom, Borking és Olk definíciójának magyar fordítása, Székely, 2008, 23.

2. A második csoportba tartoznak az olyan privátszférát erősítő technológiák, amelyek az online kommunikáció során átvitt tartalmat védik, elsősorban valamilyen titkosítási megoldással.

3. Végül a szerző említ néhány „egyéb online környezetben alkalmazott privátszférát védő megoldást", mint biztonságos online fizetési eszközök, adathalászat vagy cenzúrával szembeni eszközök.[563]

A PET megoldások használata ugyanakkor korántsem tömeges. Ennek okai, hogy a PET-ek használatához szükséges informatikai, technológiai ismeretek többnyire hiányoznak az átlagfelhasználóknál, illetve problémát jelenthet az is, hogy „általában nincs kézzelfogható eredménye a privátszférát erősítő technológiák alkalmazásának, ezért alacsony azok népszerűsége, kevésbé tudatosul egy átlagos felhasználóban, ha visszaéltek személyes adataival, mintha a fizikai világban érné kár."[564] Ezeken a PET megoldások előnyeinek népszerűsítésével, illetve azok minél inkább felhasználóbarát kialakításával (pl. könnyű telepíthetőséggel), és a vírusokkal, támadásokkal szembeni jelentős ellenálló-képesség biztosításával lehetne segíteni.[565] Emellett az adatkezelők üzleti érdekei is gyakran a PET-ek alkalmazása ellen szólnak, és akár a terjedésüket akadályozó lobbytevékenységtől sem riadnak vissza, mivel a személyes adatoknak az adatalanyok tudta és belegyezése nélküli felhasználása, elemzése, értékesítése komoly anyagi előnyt jelent számukra. Ugyancsak korlátozzák a PET-ek alkalmazását a szervezett bűnözés, illetve a terrorizmus ellen fellépő hatóságok és nemzetközi szervezetek,[566] a privátszférát védő technológiákat ugyanis nem egyszer valóban a számítógépes alvilág szereplői használják az elrejtőzés érdekében. Végül a felhasználói attitűdvizsgálatokra utalva itt is fel kell hívni a figyelmet a már említett privacy-paradoxonra: a magánszférával kapcsolatos aggodalmak nem feltétlenül csapódnak le tényleges cselekvésben, amely a PET eszközök használatának hiányában is megnyilvánul.

3.4.3.2 A Privacy by Design elv

A Privacy by Design, azaz a beépített adatvédelem fogalma az 1960-as években az építészetben jelent meg – az informatika világában csak az 1990-es évek közepe óta használják a kifejezést.[567] Az elv kidolgozása és elterjesztése – bár egyes elemeiben számtalan szerzőnél megjelent – kétségkívül Ann Cavoukian munkásságának köszönhető, aki a 90-es évektől foglalkozik e kérdéskörrel. Meg kell jegyezni, hogy a szakirodalom először egyértelműen a privátszférát erősítő technológiákkal foglalkozott, a beépített adatvédelem elve a PET eszközökkel kapcsolatos elméletek továbbgondolásaként, elvi szintre emeléseként jelent meg.[568]

---

[563] Goldberg, 2007. További alkalmazási területekről és eszközökről a magyar jogirodalomban ld. részletesen Székely, 2008, 23-25. valamint Jóri, 2005, 49-53.
[564] Kiss, 2013, 117.
[565] Kolter, Goldberg és Thiesse gondolatait összefoglalja, idézi és elemzi Kiss, 2013, 116-117.
[566] Székely, 2008, 32.
[567] Davies, 2010
[568] Simon Davies arra hívja fel a figyelmet, hogy a Privacy by Design elv mintegy reagál a 90-es években elsősorban az Egyesült Államokban megjelenő „Surveillance by Design" elvre, amelynek lényege épp a megfigyelési funkció kommunikációs technológiákba való olyan mértékű integrálása, amelynek segítségével a rendvédelmi szervek bármilyen adathoz hozzáférhettek. A szerző megjegyzi, hogy már a korai

Cavoukian meghatározása szerint a Privacy by Design lényegében egy filozófia, egy megközelítési mód, amely alapján a magánszféra-védelem szempontjait integrálni kell a különböző technológiák követelményrendszerébe (specifikációjába), azaz az adatvédelmi szabályozás elveit be kell építeni az adatkezelési technológiákba, mind a tervezés, mind a működtetés során. A Privacy by Design elv abból indul ki, hogy az informatikai infrastruktúra nagymértékben meghatározza az adatkezelő tényleges cselekvési szabadságát és lehetőségeit. Az elv ugyan eredetileg kifejezetten az infokommunikációs technológia kapcsán jelent meg, később azonban ez kiterjedt az üzleti folyamatok, sőt (visszatérve az építészeti gyökerekhez) a fizikai tervezés területére is.[569] Megjegyezzük, hogy az európai szabályozási tervekbe a beépített adatvédelem elve már kifejezetten e módosult hatókörrel került be: a követelményt nem csak a technológia kialakítása, de általában az adatkezelési folyamatok megtervezése során is figyelembe kell venni, a gyakorlatban persze e kettő között igen szoros az összefüggés.

A Privacy by Design részletszabályainak kidolgozása alapvetően szintén Cavoukiannak köszönhető. Az általa megalkotott hét alapelv több mint 30 nyelven érhető el, köztük magyarul is.[570]

1) Reakció helyett proaktivitás, utólagos orvoslás helyett megelőzés. Fontos kiindulópont, hogy előre számolni kell a személyek magánéletébe beavatkozó eseményekkel, és meg kell akadályozni ezek bekövetkeztét, azaz a káros hatásokat nem utólag kell enyhíteni, hanem meg kell előzni.
2) Alapértelmezett adatvédelem. Lényeges momentum, hogy automatikus beállításokkal (úgy hogy az egyénnek ezért semmilyen külön lépést nem kell tennie) kell maximális védelmet biztosítani a magánszféra számára számítástechnikai környezetben vagy üzleti felhasználás során.
3) Tervezés során beépített adatvédelem. A Privacy by Design elv központi elemét adja az a követelmény, hogy a privacyvédelem szempontjait nem utólagos kiegészítésként, hanem már a tervezéstől kezdve figyelembe kell venni, amely így a számítástechnikai és üzleti alkalmazások integráns részévé válik anélkül, hogy a funkcionalitást korlátozná.
4) Teljes működőképesség. A Privacy by Design elvének alkalmazása integrálja az összes jogos érdeket és célt úgy, hogy a veszteségek és a profit ne csak kiegyenlítsék egymást, hanem a végeredmény pozitív mérleggel záruljon.
5) Teljes életciklusra kiterjedő védelem. Ha a Privacy by Design már az adatgyűjtés megkezdését megelőzően érvényesül, a hatékony biztonsági előírások az adatkezelés teljes ciklusát átfogják a kezdettől a végig. Az elv alkalmazása tehát elősegíti egy információ életútjának megfelelő kezelését a keletkezésétől a megszűnéséig.
6) Láthatóság és átláthatóság. A Privacy by Design elv az adatkezelés valamennyi résztvevőjét az alkalmazott technológiától vagy üzleti megoldástól függetlenül arra

telefonközpontok is rendelkeztek olyan technológiával, amellyel lehetőség nyílt az alkalmazottak teljesítményének és tevékenységének figyelemmel kísérésére. (Davies, 2010, 1-2.) Jelenleg az Edward Snowden által kiszivárogtatott dokumentumok nemzetközi visszhangja irányítja rá a figyelmet e problémára.

[569] Cavoukian, 2009, 3.

[570] Cavoukian, 2013.

sarkallja, hogy a megígért és kinyilvánított céloknak megfelelően járjon el (melyet független értékelésnek is alávethet). Az adatkezelési műveletek így a szolgáltató és a felhasználó számára is átláthatóak.

7) A felhasználó magánszférájának tisztelete. A Privacy by Design elve az adatkezelőtől egyértelműen azt követeli meg, hogy az érintett adatvédelmi érdekeit tartsa a legfontosabbnak, szigorú adatvédelmi előírások, megfelelő jelzések és felhasználóbarát megoldások használatával.[571]

Egyes kutatók szerint ezek az elvek jól átültethetőek a gyakorlatba is, mivel a megfogalmazott elvek többsége a jogkövető adatkezelők számára szinte magától értetődő,[572] a magam részéről ezt az optimizmust nem osztom: a gyakorlati alkalmazás jelentős nehézséget okoz, mivel a megfogalmazott elvek sokkal inkább egy szemléletet, hozzáállást tükröznek, mintsem olyan normatív követelményrendszert, amelynek betartása vagy be nem tartása könnyedén megállapítható.

Érdemes néhány szót szólni külön is az alapértelmezett adatvédelem és a beépített adatvédelem viszonyáról, e két elv gyakran ugyanis „párban" jelenik meg. A Privacy by Default elv a beépített adatvédelem koncepciójának részeként értelmezhető, annál szűkebb terjedelmű, és fő célja az adatvédelmi szabályok biztosítása a felhasználók passzivitása esetén is: „nincs szükség a felhasználó aktív közreműködésére ahhoz, hogy magánszféráját védje, hiszen a védelem a rendszer alapértelmezett részét képezi."[573] Összességében azonban az elv alkalmazása kapcsán komoly viták várhatóak, mivel tökéletesen ellentétes az online szolgáltatások során elterjedt és igen jól jövedelmező üzleti modellekkel.[574]

3.4.3.3 A technikai és szervezési intézkedések szabályozása

Az adatbiztonság megteremtéséhez szükséges technikai és szervezési intézkedések, valamint egyes, a technológia szerepéhez kötődő elvek jogszabályi követelményként való megjelenése természetesen nem újdonság.

3.4.3.3.1 Hatályos szabályozás

Az adatvédelem szabályozása kapcsán a rendszerek biztonságával, adatvédelem-barát kialakításával kapcsolatos legelső általános követelmények már az EU 1995-ös irányelvében megjelentek. „Az adatfeldolgozás biztonsága" alcímet viselő 17. cikk szerint: „A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a feldolgozás közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen. Tekintettel a technika vívmányaira és alkalmazásuk költségeire, ezen intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatfeldolgozás által jelentett kockázatoknak és a védendő adatok jellegének."

[571] Cavoukian, 2013, 2.
[572] Davies, 2010, 7.
[573] Davies, 2010, 7.
[574] A Privacy by Design elvéről ld. részletesen Böröcz – Szőke, 2013.

Az irányelv preambuluma már ekkor utalt a tervezési fázis fontosságára. A preambulum (46) bekezdése szerint a fenti követelménynek érvényesülnie kell mind a rendszer tervezésénél, mind az adatkezelési folyamat során, azaz a rendszereket már az adatvédelmi követelményeknek megfelelően kell tervezni. A holland adatvédelmi biztos például tudatosan a technológiai intézkedések elsődleges jellegét hangsúlyozza (a szervezeti intézkedésekhez képest) abból a megfontolásból, hogy azok hatásai nehezebben kerülhetők meg.[575]

Az információbiztonság jogi szabályozása kapcsán szakadék tapasztalható a jogalkotás és jogalkalmazás (jogászok) valamint az intézkedések végrehajtói (informatikusok) között.[576] Ennek oka, hogy a jogi követelmények mögötti technikai tartalom nem ismerhető fel könnyen, és ez nehezíti a PET-ekre vonatkozó szabályozás megalkotását. A követelmények felületesek, amelynek fő oka a technológiafüggetlenség, de a felületesség a jogalkalmazást rendkívüli módon megnehezíti.[577]

Jelentős elvi-filozófiai előrelépés volt a német Teledienstendatenschutzgesetz (TDDSG)[578] rendelkezése, amely már 1997-ben tartalmazta azt az – adattakarékosságnak nevezett – elvet, amely szerint a „távszolgáltatást nyújtónak olyan technikai eszközöket kell használnia, amelyek működtetése nem jár személyes adatok kezelésével, illetve a lehető legkevesebb személyes adat kezelésével jár, sőt, e szempontokat már az eszközök tervezésekor is figyelembe kell venni." A törvényszöveg azon rendelkezése, miszerint az adattakarékosság szempontját a tervezés során is figyelembe kell venni, mindenestre egybecseng a beépített adatvédelem legfontosabb jellemzőjével, a proaktivitás követelményével. Ez a rendelkezés később ugyan bekerült a német szövetségi adatvédelmi törvénybe[579] is,[580] de Európa-szerte egyelőre nem terjedt el.[581]

3.4.3.3.2 Az adatvédelmi reform eredményei

Mindenekelőtt a Rendelettervezetben továbbra is hangsúlyosan megjelenik az adatbiztonság szabályozása. A 30. cikk alapján „az adatkezelő és az adatfeldolgozó, a technika állására és a végrehajtás költségeire tekintettel, a 33. cikk szerinti adatvédelmi hatásvizsgálat eredményeit figyelembe véve végrehajtja a megfelelő technikai és szervezési intézkedéseket az [adatkezelés] kockázatainak megfelelő védelmi szint biztosítása érdekében." E szabályok kiinduló elvei azonosak a jelenlegi szabályozással, eszerint továbbra is megfelelő technikai és szervezési intézkedésekkel kell a személyes adatok biztonságát garantálni. Az adatbiztonsági szint kialakításánál az adatkezelőnek a technika állására, a végrehajtás költségeire és az adatvédelmi hatásvizsgálat eredményeire kell figyelemmel lenni. E szempontok jelenleg is megtalálhatók az irányelvben, és az

[575] Jóri, 2009, 290.
[576] Szádeczky, 2012. 326.
[577] Reidenberg, 1998, 584.
[578] Gesetz über den Datenschutz bei Telediensten (TDDSG) 1997 I 1871. 3. §
[579] Bundesdatenschutzgesetz (BDSG), 3. §
[580] Jóri, 2005, 65.
[581] Magyarországon azonban az adattakarékosság elve már 2004-ben megjelent szektorális szabályként az elektronikus kereskedelmi törvényben [ld. az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, 13/A. § (3) bekezdését].

információbiztonság szintjének meghatározása a gyakorlatban is ezen elvek mentén történik.[582] Az új tervezet az irányelvhez képest jóval részletesebb szabályokat tartalmaz arra nézve, hogy az adatbiztonsági intézkedéseknek milyen célokat kell elérnie. Mivel a szövegezés szerint a „biztonsági politikának" kell gondoskodnia e célokról, ez szintén nehéz másként értelmezni, mint úgy, hogy az adatkezelőknek írásban fellelhető adatbiztonsági politikával/szabályzattal kell rendelkezniük.

A privátszférát erősítő technológiákkal kapcsolatban az előkészítés során a Bizottság kifejezetten támogatta ezek elterjesztését. A 2007-es közleményében így fogalmaz: „A Bizottság úgy véli, hogy a magánélet védelmét erősítő technológiákat fejleszteni kell és szélesebb körben kell alkalmazni, […] a magánélet védelmét erősítő technológiák javítanák a magánélet védelmét és elősegítenék az adatvédelmi jogszabályoknak való megfelelést. A magánélet védelmét erősítő technológiák alkalmazása kiegészítené a meglévő jogi keretet és végrehajtási mechanizmusokat."[583] Az adatvédelmi reform kapcsán többen kiemelik, hogy a privátszférát erősítő megoldások használatát mind a felhasználók, mind az adatkezelők oldalán népszerűsíteni kell.[584] A Rendelettervezet szövegében ugyanakkor kifejezetten PET-re vonatkozó rendelkezések nincsenek, a megoldásokat az a preambulum is csupán egyszer említi. Egyes szerzők szerint az adatvédelmi szabványok és a PET-ek alkalmazásának kötelezővé tétele hangsúlyos elemként kellene, hogy megjelenjen a köztes szoftverek, az alkalmazás középrétegek (middleware) szabályozásában, elsősorban technológia semleges előírások formájában. Emellett a szövegtervezet elsősorban az adatkezelők és adatfeldolgozók oldaláról közelíti meg a PET-ek szabályozásának problémáját, de nem nyújt támogatást ahhoz, hogy a 2007-es Bizottsági koncepciónak megfelelően a technológia a felhasználók szélesebb köréhez juthasson el, több magánszemély védje ezek segítségével a magánszféráját.[585]

A reformfolyamat során a Privacy by Design elve is hangsúlyosan megjelent. A különböző társadalmi konzultációk eredményét összegző dokumentum szerint a résztvevő szervezetek jelentős része kifejezetten felhívta a Bizottság figyelmét a beépített adatvédelem, mint alapelv rendkívüli reformáló erejére is. Az elv lényegében az összes előkészítő dokumentumban szerepelt, és ennek megfelelően bekerült a Rendelettervezetbe is.[586]

---

[582] A szöveg kissé pontatlan, mivel a nyelvtani értelmezés alapján az adatbiztonsági kötelezettséget és a kockázatarányos védelem elvét is csak azon adatkezelőkre és adatfeldolgozókra írja elő, amelyek adatvédelmi hatásvizsgálatot végeztek, ez pedig nem minden esetben kötelező. E jogtechnikai hiba más jogértelmezési módszerekkel orvosolható, a rendelkezés nyilvánvalóan az adatvédelmi hatásvizsgálatra nem kötelezett szervezetekre is irányadó.

[583] Európai Bizottság, 2007, 4.

[584] Irion – Luchetta, 2013, 63.

[585] Kristina Irion, Giacomo Luchetta és mások gondolatait összefoglalja és elemzi, Kiss, 2013, 117-118. Meg kell jegyezni, hogy a privátszférát erősítő technológiák és a Privacy by Design elvének elterjedését jelentősen előmozdíthatná e témakörök műszaki és informatikai oktatásban való megjelenítése.

[586] Meg kell említeni, hogy a beépített adatvédelem elve általános követelményként, az adatbiztonságra vonatkozó korábbi szabályokat kiegészítve, megjelenik a magyar Infotv-ben is – megelőzve lényegében az EU jogalkotását. Az Infotv. 7. § (1) szerint „az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét." A törvény indokolása egyértelműen utal a beépített adatvédelem elvére: „A magánszféra védelmét szolgáló intézkedések figyelembevétele az adatkezelés folyamatában az ún. »privacy by design« elvének magyar szabályozásba illesztését célozza."

A Rendelettervezetben a „beépített és alapértelmezett adatvédelem” két általános kötelezettséget jelent az adatkezelő számára. Eszerint – az eredeti 2012-es szövegjavaslat alapján – „az adatkezelő – a technika állására és végrehajtás költségeire tekintettel – mind az adatkezelés módjának meghatározása, mind az adatkezelés során megfelelő technikai és szervezési intézkedéseket hajt végre oly módon, hogy az adatkezelés megfeleljen e rendelet követelményeinek, és biztosítsa az érintettek jogainak védelmét”.[587] Az Európai Parlament szövegjavaslata pontosítja és kiegészíti e követelményeket. A módosító javaslat szerint az intézkedéseket a jelenlegi technikai tudás, nemzetközi legjobb gyakorlat és az adatkezelés kockázata alapján kell megtenni, és az elvet az adatkezelés teljes életciklusa során alkalmazni kell. A javaslat kifejezetten utal arra, hogy a beépített adatvédelem elvének alkalmazása során figyelembe kell venni az esetleges adatvédelmi hatásvizsgálat eredményeit is.[588]

Emellett az adatkezelőnek – a Privacy by Default elv jegyében – „olyan mechanizmusokat kell végrehajtania, amelyek alapértelmezett módon biztosítják azt, hogy kizárólag az adatkezelés egyes konkrét céljaihoz szükséges személyes adatok kerülnek kezelésre, és különösen azt, hogy az adatgyűjtés vagy –tárolás [a Parlamenti javaslat alapján emellett az adattovábbítás] során az adatok mennyisége és az adattárolási időtartam tekintetében sem lépik túl az e célokhoz szükséges legkisebb mértéket. Ezeknek a mechanizmusoknak különösen azt kell biztosítaniuk, hogy a személyes adatok alapértelmezett módon ne váljanak határozatlan számú egyén számára hozzáférhetővé.”[589]

3.4.3.4 Értékelés

A tervezett szabályozás alapvetően helyes irányt követ. A PET kérdéskörét ugyanis többször az önszabályozás különböző eszközei kapcsán tárgyalják, míg mások a Rendelettervezet kapcsán szorgalmazták, hogy nevesítve is megjelenjen. A privátszférát erősítő technológiák helye az adatvédelmi szabályozásban a Privacy by Design elv alkalmazásával kerül helyre. Előbbi ugyanis csak egy eszköz, önmagában semleges, önálló szabályozószerepe nincs. A beépített és alapértelmezett adatvédelemnek azonban valóban elvi követelményként kell megjelennie, csakúgy, mint az adattakarékosság elvének. A privátszférát védő technológiák ezen elveknek való megfelelést szolgálják, és olyan konkrét eszközöket jelentenek, amelyek támogatása jogszabályi szinten – épp a technológiasemlegességre tekintettel – csak általános megfogalmazással lehetséges, akkor is, ha ez a gyakorlati alkalmazást nehezíti. Kívánatos ugyanakkor, hogy az adatvédelmi hatóságok egyedi, például épp a Privacy by Design elvét konkrét ügyben értelmező döntései nyomán kialakuló joggyakorlat, önszabályozó mechanizmusok (magatartási kódexek, szabványok), és az adatkezelők belső szabályai konkretizálják e szabályokat, és akár előírják konkrét PET alkalmazások használatát.

Összességében a Privacy by Design megközelítés annak biztosítására tesz ígéretes kísérletet, hogy a technológia és jog, mint két szabályozórendszer ne kioltsa, hanem erősítse egymást, és egyértelműen a technológiát állítsa a – társadalmi elvárásokat végső

[587] Bizottsági tervezet, 23. cikk (1)
[588] Rendelettervezet, 23. cikk (1)
[589] Rendelettervezet, 23. cikk (2)

soron kötelező normaként megjelenítő – jogi szabályozás szolgálatába, és megtartsa így a jogi szabályozás elsőbbségét. A privátszférát erősítő technológiák e célkitűzések megvalósításának első számú eszközei lehetnek, amely azonban önmagában nem igényel külön jogszabályi szintű szabályozást.[590]

3.5 Következtetések

A harmadik fejezetben először is áttekintettem az elmúlt 10-15 év technológiai változásait és azok személyes adatok védelmére gyakorolt hatását. A változások mértéke olyan jelentős, amelyre – számos szerző és az Európai Unió, mint jogalkotó szerv szerint is – a hatályos adatvédelmi szabályozás nem képest megnyugtató választ adni. Az erre vonatkozó szakirodalmi álláspontok elemzése alapján igazoltnak látom a dolgozat vonatkozó tézisét, miszerint: „Az elmúlt évtized technológiai fejlődése az adatvédelmi szabályozást (újra) olyan kihívások elé állította, amelyre jelen formájában nem tud hatékony választ adni. Ennek következtében az adatvédelem alapjait érintő új megközelítésre és szabályozási koncepcióra van szükség."

Az érintett adatvédelmi szabályozásban betöltött helyzetének részletes áttekintése (ideértve az elméleti kritikát és a felmérések eredményeit is), alapján az látszik, hogy tőle csak meghatározott esetekben várható, hogy az egyébként széleskörű jogaival élve az adatkezelések valódi korlátját jelentse; összességében jóval kisebb mértékben, mint amennyire a második generációs szabályozás támaszkodott erre.

A fejezet során részletesen kifejtettem, hogy olyan szabályozási megoldásra van szükség, amely az érintett passzivitása mellett (de nem az akarata ellenére) is képes megfelelő, mintegy „mögöttes" védelmet nyújtani. Ha a létrejövő új jogszabályi környezetben az adatkezelők elszámoltathatósága révén az adatkezelők átláthatósága, tudatossága és az adatvédelmi elvek adatkezelők szintjén történő végrehajtásának hatékonysága jelentősen nő, mindehhez a jelenleginél hatékonyabb felügyelet társul (az állami felügyelet kiegészítve a piaci alapon működő önkéntes adatvédelmi audittal és tanúsítással), és végül a technológiát valóban sikerül az adatvédelem „szolgálatába" állítani, akkor az érintett szerepétől függetlenül is magasabb védelmi szintet lehet garantálni. Tézisszerűen azt mondhatom, hogy „az új megközelítés központi eleme, hogy az »érintett-központú« szabályozás felől nagymértékben el kell tolódni az »adatkezelő-központú« szabályozás felé." Ez a hangsúlyeltolódás azonban nem jelenti sem az érintett jelenlegi jogi pozíciójának csökkentését, sem az adatvédelem alapjogi megközelítésének feladását.

Az elszámoltathatóság elvéből eredő kötelezettségek részletes áttekintése egyértelműen az adatkezelők belső szabályozásának növekvő szerepét mutatta. Az adatvédelmi szabályok betartásának igazolása csak dokumentált belső mechanizmusok kialakításával valósulhat meg. Ezek alapján igazolható a dolgozat következő tézise is, miszerint a „hangsúlyeltolódás következtében a korábbiakhoz képest jóval nagyobb szerepet kap az adatkezelők belső szabályozása."

[590] Az értékelés részben korábbi kutatási eredményeimen alapul, ld. erről Balogh – Kiss – Polyák – Szádeczky – Szőke, 2014, 45.

Ez a megközelítés ugyanakkor jelentősen növeli az adatkezelők compliance-költségeit és adminisztrációs terheit, és könnyen az adatvédelem túldokumentálásához vezethet. E hatást enyhítendő, egyrészt megfelelően differenciálni kell az adatkezelők között az egyes kötelezettségek tekintetében, másrészt olyan egyszerűen használható útmutatóra van szükség, amely hatékony segítséget jelent az adatkezelők számára a belső szabályozásuk kialakításában és a compliance kötelezettségeknek való megfelelésben.

4. ADATVÉDELMI ÖNSZABÁLYOZÁS, AUDIT ÉS TANÚSÍTÁS

Az előző fejezetek során áttekintettem az adatvédelem történeti fejlődését és a jelenleg zajló folyamatokat. Néhány tendenciák a sok bizonytalanság mellett is egyértelmű: az adatkezelés már jelenleg is, de a jövőben sokkal nagyobb mértékben támaszkodik az adatkezelők aktivitására, amely számukra jelentősen növekvő compliance kötelezettségként jelenik meg.

E tendenciák egyértelműen az önszabályozás különböző formáinak erősödése, valamint az auditálás illetve különböző címkéző-tanúsító rendszerek jelentőségének növekedése felé mutatnak. A korábbiakhoz képest jelentősen felértékelődik az önszabályozás egyik eszközének tekintett szervezeti (adatkezelői szinten kialakított) szabályozás. Az alábbiakban áttekintem az adatvédelmi önszabályozás lehetőségeit és korlátait, ideértve az adatvédelmi felügyelet sajátos intézményeként felfogható adatvédelmi audit intézményét is, majd kifejtem, hogy melyek lehetnek egy, a compliance kötelezettségekre tekintettel lévő belső szabályozási rendszer kiépítésének első lépései.

4.1 Az önszabályozási eszközök rendszerezése

4.1.1 A vonatkozó szakirodalom áttekintése

Az adatvédelem területén az önszabályozás kifejezés alatt a vonatkozó adatvédelmi szakirodalom szerzői különböző ön- és társszabályozási formákat és ellenőrző rezsimeket értenek, néhány közös pont azonban egyértelműen megállapítható. Ezek rövid áttekintését követően a dolgozat célkitűzéseit szem előtt tartó szempontok alapján rendszerezem az önszabályozás különböző formáit (eszközeit), és bemutatom azok főbb jellemzőit.

A külföldi irodalmat elemezve mindenekelőtt meg kell említeni Bennett és Raab felosztását. A szerzők az adatvédelmi önszabályozás eszközeinek (amelyek az ő megközelítésük alapján kizárólag önkéntes alapon működhetnek) az adatvédelmi nyilatkozatokat, a magatartási kódexeket, a szabványokat, és a tanúsító rendszereket értik, de – egyébként logikusan – e körben tárgyalják a Safe Harbour egyezményt is. A magatartási kódexek alatt mind szervezeti szintű (organizational code), mind az ágazati szintű (sectoral code) kódexet[591] értenek.[592] Később Bennett és Mulligan meghaladja ezt a felosztást, és meghatározza a Magatartási Kódex (Code of Conduct) főbb jellemzőit, elhatárolva azt a szervezeti szinten elfogadott – különböző elnevezésű – adatvédelmi dokumentumoktól.[593] Banisar a privacy védelmének modelljeiről írt, magyar nyelven is megjelent esszéjében az önszabályozás formáiként a cégek által kidolgozott szabályzatokat és az ágazati magatartási szabályokat említi, illetve az önszabályozás felügyelete kapcsán

[591] A szerzők valójában öt különböző típust különböztetnek meg: a szervezeti szintű és a szektorális kódex mellett az ún. funkcionális kódexeket, a technológiai kódexeket, és a szakmai kódexet, ezek azonban alapvetően a kódex funkciójából kiinduló, az első két kategóriához képest horizontális szempontok alapján képzett kategóriák.
[592] Bennett – Raab, 2006, p 151-175.
[593] Bennett – Mulligan, 2012, 12.

elemzi az önkéntes tanúsító rendszereket, az amerikai eredetű TRUSTe és a BBBOnline szolgáltatásait.[594] Az adatvédelmi önszabályozással foglalkozó irodalom rendszerint azonban nem törekszik az önszabályozás különböző eszközeinek rendszerezésére, csupán egy-egy területet vizsgál, és így – az adott tanulmány témájának megfelelően – az „amerikai típusú" iparági önszabályozást, a tanúsító rendszereket, a kötelező vállalati szabályokat, a Safe Harbour Egyezményen alapuló rendszert, vagy éppen az adatkezelők szintjén megteendő intézkedések összességét érti önszabályozás alatt.

Az adatvédelmi reform során fontos előkészítő szerepet játszó, az adatvédelem átfogó megközelítéséről szóló bizottsági közlemény önszabályozás alatt a magatartási kódexek elfogadását érti, és ugyanebben a fejezetben, de külön nevesítve utal a tanúsító rendszerek bevezetésére is.[595] A Rendelettervezet logikája szintén ezt a sémát követi, egy szakaszon belül, de külön nevesítve (és külön cikkekben) rendelkezik eljárási szabályzatokról (magatartási kódexekről) és a tanúsítás lehetőségéről – az önszabályozás kifejezés a tervezet szövegében nem szerepel.[596]

A magyar jogirodalomban – az Egyesült Államok adatvédelmi rendszerére történő rövid kitekintéseket leszámítva – részletesen csak Jóri András foglalkozik az önszabályozás kérdésével, aki erre az eszközre, mint a második generációs szabályozás kihívásaira adható (végül inkább sikertelen) válaszkísérletre tekint, ugyanakkor nem célja a témakör átfogó, rendszerező szemléletű megközelítése. Jóri először az Egyesült Államokból eredő tanúsító rendszer, a TRUSTe szolgáltatásait elemzi és kritizálja, mivel annak „megoldásai és korlátai is jellemzőek az ipari önszabályozási törekvések többségére",[597] majd a szabványosítási törekvésekkel foglalkozik.

Meg kell jegyezni, hogy az önszabályozási rendszerek értékelése, kritikája során mind a külföldi, mind a magyar szerzők alapvetően az Egyesült Államok rendszerére koncentrálnak, ahol az önszabályozás törvényi szabályozási háttér nélkül, annak pótlására (még inkább annak elkerülésére) alakult ki, és viszonylag kevés szó esik az „európai típusú" önszabályozás, és különösen a szervezeti szintű önszabályozás elemzéséről, értékeléséről.

Végül meg kell említeni, hogy kiterjedt irodalma van az adatvédelmi audit jogintézményének, amellyel a dolgozat során részletesen foglalkozom. Az auditálás azonban alapvetően egy speciális (ön)felügyeleti eszköz, amely akár önszabályozás, akár állami szabályozás keretében elfogadott normáknak való megfelelés „mérésére" is alkalmazható, sőt, nem egyszer állami szervek, adatvédelmi hatóságok végzik e tevékenységet, igaz minden esetben önkéntes alapon, az adatkezelő kifejezett kérésére.

4.1.2 Az egyes önszabályozási eszközök rendszerezése

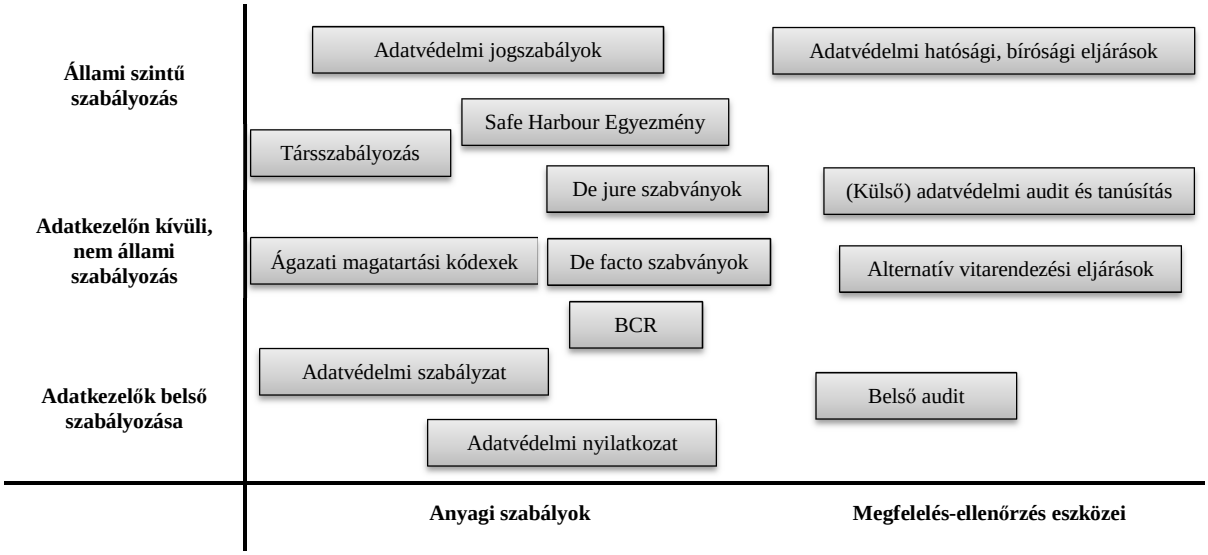
Az első fejezetben már utaltam arra, hogy a szakirodalomban is gyakran összemosódnak az önszabályozás során a normaalkotásra és a szabályok kikényszerítésére szolgáló mechanizmusok. Az első a követendő magatartási forma, azaz az anyagi szabályok

[594] Banisar, 2001, p 23-27.
[595] Európai Bizottság, 2010b, 13. (2.2.5 pont)
[596] Rendelettervezet, 38-39. cikk
[597] Jóri, 2005, 53.

előírását, míg a második e normák kikényszeríthetőségének eszközeit (és annak eljárási szabályait) jelentik. Utóbbiba mind a szabályoknak való megfelelés ellenőrzése (compliance-check), mind a jogkövetkezmények alkalmazása beletartozik.

E felosztáshoz hozzávehető egy másik szempont, nevezetesen az, hogy az adott anyagi szabályok milyen szinten kerülnek elfogadásra, és a szabályoknak való ellenőrzést milyen szinten működő szervezet folytatja le. Ez alapján megkülönböztethetünk állami szintű szabályozást, ami alatt az állami szervek által elfogadott, általánosan kötelező, és adott esetben állam által kikényszerített szabályokat (röviden: jogszabályokat) értek, önszabályozás, azaz az adatkezelőn kívüli szerv által elfogadott, rendszerint önkéntesen alkalmazott nem állami szabályozást, végül az adatkezelők szintjén elfogadott szabályozást.

Ezek alapján, számos összetett vagy „határeset" jellegű jogintézményt és eszközt elismerve nagyjából az alábbi, éles határvonalaktól mentes koordinátarendszer vázolható fel:



1. sz. ábra. Az (ön)szabályozási eszközök csoportosítása

A koordinátarendszerrel kapcsolatban fontos néhány magyarázó megjegyzést tenni.

Az anyagi szabályoknál az egyes szintek meghatározása az elfogadó/kibocsátó szervezet szintjére utal.

- Az adatvédelmi jogszabályokat az állam szervei alkotják.
- A Safe Harbour egyezmény speciális helyzetű, mivel annak követése önkéntes alapon, az Egyesült Államokban önszabályozást jelentő keretek között történik, ugyanakkor állami szerv (az FTC) felügyeli a betartását, és egy „államközi"[598] megállapodás határozza meg a követendő normákat, és speciális joghatást, az Európai Unió jogi aktusa egyes szabályainak való megfelelést[599] biztosít a Safe Harbour szabályok követőinek.[600]

[598] Valójában egy szupranacionális szerv és egy szövetségi állam közötti szerződésről van szó.
[599] Nevezetesen az adatvédelmi irányelv megfelelő szintű védelemre vonatkozó szabályainak való megfelelést biztosítja.
[600] A Safe Harbour természetéről részletesen ld.4.2.1.1.2 fejezet

- A társszabályozás speciális önszabályozás forma, amelynél viszonylag jelentős az állam szerepe, meghatározhatja az elérendő célokat, esetleg formálisan is jóváhagyja, vagy állami kényszerítőerőt kapcsol a szabályok be nem tartásához.[601]
- A szabványok tekintetében a szakirodalom megkülönböztet de jure szabványt, amelyet valamely elismert szabványügyi szervezet bocsátott ki, valamint de facto szabványt, amelyet „általában széles körűen elismert nemzetközi civil szervezetek vagy kormányzati intézmények, szabványosítási céllal, de a szabvány formai követelményeinek teljesítése nélkül alkotnak," [602] és a gyakorlatban kellően széles körben alkalmazzák őket.[603] E megkülönböztetés ugyanakkor nem érinti azt a tényt, hogy egyik esetben sem állami szerv általi elfogadásról van szó,[604] és a követésük minden esetben önkéntes.[605]
- Az ágazati magatartási kódexeket úgyszintén valamely nem állami szerv keretében fogadják el, alkalmazásuk önkéntes.
- Ugyancsak speciális jogi eszköz az ún. kötelező erejű vállalati szabályok (BCR),[606] amelyek egy (multinacionális) vállalatcsoport által elfogadott, azaz több adatkezelőre vonatkozó belső szabályrendszer, amelynek szintén speciális joghatása van, mivel ezek alkalmazása (csakúgy, mint a Safe Harbour esetén) az Európai Unió jogi aktusa egyes szabályainak való megfelelést is jelent.[607]
- Végül az adatkezelők által elfogadott adatvédelmi nyilatkozatok és szabályzatok viszonylag könnyen elhelyezhetők e rendszerben, az adatkezelők belső szabályozásának minősülnek, bár a gyakorlatban itt is elképzelhető átfedés az adatkezelőn kívüli normákkal, például egy ágazati mintaszabályzat változtatás nélküli átvétele esetén.

Az anyagi szabályokra való utalás kapcsán meg kell jegyezni, hogy az említett szabályozási eszközök magatartási szabályok előírása mellett gyakran eljárási normákat is tartalmaznak, a táblázatban azonban kifejezetten az adott szabályozási eszköz anyagi jogi szabályaira kívántam utalni.[608] A helyzetet ugyanis árnyalja, hogy a megfelelés-ellenőrzés egyes eszközeire vonatkozó eljárási szabályokat potenciálisan bármelyik szinten elfogadott szabályrendszer tartalmazhatja, így például állami szabályozás, magatartási kódex vagy szabvány is előírhat külső vagy belső auditra vonatkozó szabályokat. A megfelelés-értékelés eszközeinek elhelyezése ugyancsak nincs közvetlen összefüggésben azzal, hogy milyen szintű szabályok kikényszerítését célozza. Az önszabályozás keretében az anyagi és eljárási normák néha ugyan (akár kötelező jelleggel is) összekapcsolódnak egymással, de

[601] Részletesen ld. 1.3.1 fejezetet
[602] Szádeczky, 2011, 75-76.
[603] Gyakran előfordul, hogy egy „de facto szabvány egy adott változata de jure szabvánnyá válik." Szádeczky, 2011, 76.
[604] Igaz, de jure szabványok esetén államilag elismert, köztestületként működő, a nemzeti szabványok elfogadására kizárólagos hatáskörrel rendelkező szervezet által alkotott/elfogadott szabályokról van szó, részletesen ld. a nemzeti szabványosításról szóló 1995. évi XXVIII. törvény vonatkozó rendelkezéseit.
[605] Ld. erről a nemzeti szabványosításról szóló 1995. évi XXVIII. törvény 6. § (1) bekezdést
[606] Binding Corporate Rules
[607] Ez az eszköz úgyszintén az adatvédelmi irányelv megfelelő szintű védelemre vonatkozó szabályainak való megfelelést biztosítja. Részletesen ld. 4.3.3 fejezet
[608] Azaz a táblázat szempontjából az adatvédelmi jogszabályok alatt anyagi jogi szabályokat, a szabványok alatt magatartási szabályt tartalmazó, normatív szabványokat stb. kell érteni.

ez korántsem szükségszerű. Az adatvédelmi audit, mint megfelelőség-értékelési mechanizmus például bármilyen normarendszernek: állam által alkotott szabályoknak, iparági kódexnek, szabványnak vagy az adatkezelő belső szabályozásának való megfelelést is vizsgálhatja (és a gyakorlatban vizsgálja is).

Az egyes eljárási eszközöknél így a „szint" besorolása inkább arra utal, hogy milyen szintű szervezet (állami szerv, adatkezelőn kívüli nem állami szerv, vagy az adatkezelő maga) folytatja le az adott eljárást.

- Az adatvédelmi hatósági és bírósági eljárásokat minden esetben állami szervek folytatják le.
- A külső adatvédelmi audit és tanúsítás esetén a helyzet összetettebb. Azt minden esetben az adatkezelőtől különböző szerv végzi, de ez – az adott jogszabályi környezettől függően – piaci szereplő vagy hatóság is lehet. Ideális esetben a hatóság által lefolytatott audit esetén is jól elhatárolhatók a közhatalmi jogosítványok, és az önkéntes alapon – kvázi-szerződéses keretek között lefolytatott audit eljárás.[609]
- Az iparági önszabályozási kódexekhez kapcsolt alternatív vitarendező fórumok szintén az adatkezelőtől különböző, nem állami szervek.
- A belső auditot az adatkezelő szervezet folytatja le.

A negyedik fejezet további részében az állami szintű szabályozás és jogérvényesítés szabályait kivéve – a táblázatban foglalt területeket vizsgálom részletesen. A kutatás során kitérek az egyes eszközökkel kapcsolatos elhatárolási kérdésekre, a jogintézmények kritikai elemzésére és a gyakorlati alkalmazás nehézségeire is. Egy-egy fejezetet szánok az adatkezelőn kívüli, nem állami normaalkotás elemzésére, az adatkezelők belső szabályozására, majd külön fejezetben tárgyalom az adatvédelmi audit és tanúsítás szabályait.[610]

4.2 Adatkezelőn kívüli, nem állami szabályozás

4.2.1 Magatartási kódexek

A magatartási kódexek az önszabályozás egyik legjelentősebb eszközei, akár az adatvédelem, akár bármely más területen, és – rendszerint, de nem feltétlenül – valamilyen szakmai (érdekvédelmi) szervezet égisze alatt készülnek. A magatartási kódex főbb jellemzői az alábbiakban foglalhatók össze:

- kodifikált formában létezik;
- egynél több adatkezelőre (jellemzően adatkezelők egy meghatározott csoportjára) vonatkozik;
- szélesebb hatókörű, mint egy adatkezelő rövid adatvédelmi nyilatkozata;

[609] E témakörről és a magyar megoldásról részletesen ld. 4.4.6.2 fejezet
[610] E fejezetben térek ki a belső audit jogintézményére is. Az alternatív vitarendezési eljárásoknak külön fejezetet nem szentelek, arra a magatartási kódexek és a tanúsító-rendszerek bemutatása kapcsán térek ki.

- célközönsége mind az adatkezelő szervezet munkatársai, mind a potenciális érintettek.[611]

A magatartási kódexek szerepe jelentősen eltérő lehet attól függően, hogy van-e általános vagy az adott szektorra nézve kötelező állami szektorális szabályozás: amennyiben nincs, úgy a magatartási kódexnek inkább az állami szabályozást helyettesítő (elkerülő) funkciója van (pl. Egyesült Államok), míg szigorú állami szabályozás mellett inkább azt végrehajtó, kiegészítő feladata lehet (pl. európai államok).

4.2.1.1 A magatartási kódexek szerepe az Egyesült Államokban

4.2.1.1.1 Iparági önszabályozás

A 2.3.4 fejezetben röviden bemutattam az Egyesült Államok adatvédelmi rendszerét. Ennek lényege, hogy egy átfogó, minden adatkezelőre kiterjedő adatvédelmi szabályozás helyett csak egyes nevesített szektorokra vonatkozó szabályok találhatók, míg más területeken az állam tudatosan a piaci szereplőkre hagyja, hogy a kérdést önszabályozás vagy szerződéses viszonyrendszer keretében rendezzék. Ez a szabályozási modell több más Európán kívüli államban sem ismeretlen, így azokon a területeken, ahol az adott szektorra nézve nincs állami szabályozás, az európainál lényegesen nagyobb hangsúlyt kap az önszabályozás, elsősorban az iparági magatartási kódexek és a különböző tanúsító-rendszerek alkalmazása. A 90-es évektől kezdődően Kanadában a biztosítási szektor vagy a kábeltelevíziós piac, az Egyesült Államokban a csomagküldés és más direktmarketing technikák szabályozása, a bankszektor, és az elektronikus kereskedelem adatvédelmi szabályozása alapult az érintett érdekvédelmi szervezet magatartási kódexén.[612]

Az önszabályozásnak számos előnye, így az iparági szakértelem, a szabályozás rugalmassága és nagyobb hatékonysága, vagy a felhasználók bizalmának megnyerése az adatvédelmi magatartási kódexek területén is érvényesül,[613] a szakirodalom azonban összességében inkább kudarcnak ítéli az Egyesült Államok önszabályozási törekvéseit. Ennek egyik oka, hogy az iparág szereplői a saját érdekeinknek megfelelően eleve igen alacsony védelmi szintet biztosítanak, ráadásul ennek betartását is alig-alig felügyelik. Ha pedig jelentős erőfeszítéseket kívánnak a vállalt intézkedések, akkor versenyhátrányba kerülhetnek azok a vállalkozások, amelyek vállalják ezeket, ráadásul úgy, hogy a rendszerből kimaradók egyébként élvezik az iparág iránti bizalom előnyeit („free riders").[614] Végül az iparági önszabályozási törekvések megbukhatnak az érintettek adatvédelmi igényeinek hiányán és ezzel összefüggésben piaci szereplők üzleti logikáján is: a fogyasztók nem igénylik a magasabb szintű védelmet, nem hajlandóak kisebb extra költséget sem viselni az esetlegesen magasabb védelmi szintért cserébe, így a vállalkozások számára egyszerűen nem éri meg a törvényi minimumnál magasabb védelmi szintet biztosítani.[615]

[611] Bennett – Mulligan, 2012, 12.
[612] Bennett – Mulligan, 2012, 6.
[613] Ld. erről Swire, 1997, 8-9.
[614] Banisar, 2001, 26. Bennett – Raab, 2006, 156.
[615] Az adatkezelők ezzel kapcsolatos motivációit ld. Ilten – Guagnin – Hempel, 2012, 240-241. Hasonló kritikák fogalmazott meg Schwartz is, idézi Jóri, 2005, 63-64.

4.2.1.1.2 Safe Harbour Egyezmény

A magatartási kódexekkel történő önszabályozás és tanúsítás igen sajátos területe az Egyesült Államokban a Safe Harbour egyezményen alapuló adatvédelmi szabályrendszer önkéntes követése. A Safe Harbour rendszer bemutatásán keresztül jól érzékeltethető a 4.1 fejezetben felvázolt csoportosítás komplexitása, az egyes jogintézmények szerves összefonódása, így indokolt röviden bemutatni e mechanizmust.

A sajátosságok közül mindenekelőtt kiemelendő, hogy 1) az Egyesült Államok Kereskedelmi Minisztériuma által 2000-ben kiadott „Safe Harbour adatvédelmi elvek" nem kifejezetten valamely szektorra, hanem a hiányzó általános adatvédelmi szabályozás pótlására jöttek létre; 2) az irányelvek önkéntes követésének fő motivációja és hozadéka, hogy az EU megfelelő szintű védelemmel rendelkezőnek ismeri el a Safe Harbour elveket alkalmazó adatkezelők számára történő adattovábbítást;[616] 3) az elvek alkalmazását az adatkezelők kizárólag az Európai Unióból érkező személyes adatokra nézve vállalják;[617] 4) a szabályrendszer betartását állami szerv, az FTC felügyeli (ha nem is túl hatékonyan), a be nem tartásukat „tisztességtelen vagy megtévesztő kereskedelmi eljárás vagy gyakorlat"-ként szankcionálhatja.[618]

A Safe Harbour rendszerhez való csatlakozás vagy önértékelésen alapul, azaz a szervezet kidolgoz a maga számára a Safe Harbour adatvédelmi elveknek megfelelő adatvédelmi nyilatkozatot, és nyilatkozik ezek alkalmazásáról,[619] vagy valamelyik adatvédelmi tanúsító szervezethez fordul (pl. TRUSTe, BBBonline), amelyek szintén kínálnak „Safe Harbour csomagokat," és megfelelően tanúsíthatják az elvek alkalmazását.[620]

A Safe Harbour elvek anyagi jogi szabályai összességében nem túl szigorúak, és olyan elveket tartalmaznak, amelyek nagyrészt már az OECD 1980-as dokumentumában is megjelentek (amelyek azonban egyébként nem kötelezőek). A tájékoztatás elve, a harmadik félnek történő adattovábbítás, vagy az eredeti céltól eltérő célra való felhasználás esetén a választás lehetőségének biztosítása,[621] a hozzáférés és helyesbítés joga[622] a teljes szabályozatlansághoz képest lényegesen magasabb védelmet nyújt, de az EU védelmi szintjét messze nem éri el.

A Safe Harbour egyezmény értékelése a kezdetektől fogva ellentmondásos. Az egyezmény elfogadása egyáltalán nem ment könnyen,[623] az első szövegtervezetek kapcsán a tagállamok mellett a 29-es adatvédelmi munkacsoport is aggályait fejezte ki, megjegyezve, hogy a megállapodásban foglalt védelmi szintnek legalább az OECD 1980-as adatvédelmi

[616] Ld. erről Európai Bizottság, 2000
[617] Az amerikaiak személyes adatai tehát ezen vállalkozások esetén sem feltétlenül esnek védelem alá.
[618] Bennett – Raab, 2006, 168.
[619] A részleteket ld. Bennett – Raab, 2006, 168.
[620] Európai Bizottság, 2000, I. melléklet
[621] Különleges adat esetén megerősítő vagy kifejezett választási lehetőséget, azaz opt-in rendszerű hozzájárulási lehetőséget kell biztosítani.
[622] A Safe Harbour kódex anyagi jogi szabályait ld. EB, 2000, I. melléklet
[623] A tárgyalások a várthoz képest alaposan elhúzódtak, Európai oldalon a különböző szereplők (Bizottság, Európai Parlament, adatvédelmi hatóságok, tagállamok) közötti ellentétek, és nagyon is jogos aggályok lassították a megegyezést. A tárgyalások részleteiről, az egyes intézmények szerepéről ld. Farrell, 2002

elvei által biztosított szintet el kellene érnie[624] – ez végül nagyjából megvalósult. Az egyezmény inkább elkerülhetetlen politikai kompromisszumnak, mintsem ténylegesen az európaival azonos védelmi szint biztosításának tekinthető. A kritikák között említhető, hogy hiányzik a felügyelet azokon a területeken, amelyeken az FTC-nek nincs hatásköre eljárni, így például a bank- és távközlési szektorban.[625] A Bizottság 2004-ben közzétett értékelése[626] szerint a szabályok végrehajtása sem zökkenőmentes: a vizsgált, az önértékelés alapján elvileg a Safe Harbour követelményeknek megfelelő adatkezelők egy részének egyáltalán nem volt hozzáférhető az adatvédelmi politikája, egy másik része pedig nem tudta sikerrel implementálni a Safe Harbour elveket a saját adatkezeléseire. A bizottsági jelentés a felügyeletet ellátó szerv, az FTC fokozottabb, proaktív szerepvállalását sürgette.[627] A Safe Harbour megállapodással kapcsolatos kritikus hangok az utóbbi időben felerősödtek az Edward Snowden nevével fémjelzett lehallgatási botrány következtében. A Bizottság, erre is[628] tekintettel, 2013-ban újabb értékelést tett közzé, amelyben a rendszerrel kapcsolatban több hiányosságot is megállapított, és számos javaslatot fogalmazott meg.[629] A kritikai észrevételek azonban a megállapodás hatályát nem érintik. A Safe Harbour megállapodást érintő kritikák súlyát elsősorban az a speciális körülmény adja, hogy ezek alapján az Európai Unió tagállamaiból történő adattovábbítás megfelelő védelmi szintű államban történő adattovábbításnak minősül, de a felvetett problémák (különösen a végrehajtás nehézkességével kapcsolatban) az önszabályozás nehézségeire is rámutatnak.

A Safe Harbour egyezmény jól mutatja a bevezető fejezetben kialakított rendszer komplexitását: a Safe Harbour szabályrendszere az amerikai vállalkozások számára önkéntesen vállalható, iparágtól független önszabályozási mechanizmus, amelynek feltételeit azonban nemzetközi együttműködés eredményeként állami (ideértve az Európai Uniót is) szervek dolgozták ki. A Safe Harbour szabályaihoz tanúsítvány is kapcsolódhat, amelyet azonban nem előz meg alapos adatvédelmi audit, végül egy állami szerv, az FTC felügyeli a normarendszer betartását, és alkalmaz adott esetben „állami" szankciókat az adatkezelőkkel szemben.

4.2.1.2 Magatartási kódexek az európai adatvédelmi jogban

Európában az adatvédelem jogi környezete egészen más: az adatvédelmi irányelv elfogadása megteremtette a többé-kevésbé egységes európai szabályozást, amely egyrészt – úgy tűnik – kevésbé teszi szükségessé az önszabályozás különböző formáit, másrészt egészen más szerepet is szán az önszabályozó mechanizmusoknak, mint az Egyesült Államok adatvédelmi rendszere. Európában ugyanis jellemzően nem az állami szabályozást helyettesítő, sokkal inkább azt kiegészítő, pontosító, „végrehajtási szabály" jellegű szerepet tölthetnek be az önszabályozás különböző formái.

[624] WP29, 1999, 3.
[625] Kierkegaard, 2005, 4.
[626] European Commission, 2004
[627] A Bizottság jelentését elemzi Kierkegaard, 2005, p 3-4.
[628] A dokumentumban megjelölt egyik felülvizsgálati oka az „Egyesült Államok hírszerzési programjairól a közelmúltban napvilágra jutott információk, amelyek újból megkérdőjelezik azon védelem szintjét, amelyet a védett adatkikötőre [Safe Harbour] vonatkozó szabályozás garantálni látszott."
[629] EB, 2013, p 20-22.

Az európai adatvédelmi irányelv elvi szinten támogatja az önszabályozás bizonyos formáit: a 27. cikk kifejezetten utal eljárási szabályzatok (magatartási kódexek)[630] elfogadásának lehetőségére: a „tagállamok és a Bizottság ösztönzik az irányelvnek megfelelően a tagállamok által elfogadott nemzeti rendelkezések helyes végrehajtásának elősegítésére szánt eljárási szabályzatok kidolgozását, figyelembe véve a különböző ágazatok egyedi jellemzőit." Az irányelv a kódexek kidolgozói számára megteremti azt a lehetőséget is, hogy azokat véleményezés céljából a nemzeti adatvédelmi hatóság vagy – amennyiben közösségi kódextervezetről van szó – a 29-es munkacsoport elé terjesszék,[631] amelyek kötelesek a kódex és a nemzeti jog összhangját vagy annak hiányát megállapítani.[632] Európai szintű elismerésben egyelőre csak Európai Direkt és Interaktív Marketing Szövetség[633] kódexe részesült.

Az irányelv szövegezéséből egyrészt az látható, hogy e szakaszok az ágazati, azaz az adott ágazat több szereplőjére kiterjedő magatartási szabályok kidolgozását támogatják, másrészt az irányelv e kódexeknek alapvetően végrehajtási-szabály szerepet szán, amely a meglévő jogi keretek egy-egy szektorra való adaptálását jelenti, nem pedig tartalmilag új normák megalkotását.

Az adatvédelmi reform során a magatartási kódexek kérdése – kiegészülve az adatvédelmi tanúsításra vonatkozó utalással – a Bizottság 2010-es közleményében is megjelenik. A Bizottság a Magatartási Kódexekben továbbra is az adatvédelmi szabályok érvényesítésének eszközét látja, elismerve, hogy az irányelv önszabályozásra vonatkozó rendelkezéseit ritkán használták az érdekeltek. Ezen beismerés ellenére az Európai Parlament által jóváhagyott Rendelettervezet nagyjából-egészében a hatályos irányelv szabályozásához hasonlóan rendelkezik magatartási kódexek létrehozásáról,[634] azaz sem az Európai Bizottság, sem az EP nem javasolt jelentős újításokat. A jelenlegi szabályhoz képest különbség azonban, hogy már nemcsak az iparági kódexek kidolgozását, hanem a tagállami hatóság által kidolgozott kódex elfogadását is ösztönzi az európai jogalkotó, azaz a normaalkotást akár a hatóságra is rábízná, egy sajátos társszabályozási rendszert alkotva ezzel. A tervezet felsorol néhány tipikus szabályozási tárgykört is e kódexek számára. Így azok rendelkezhetnek a tisztességes és átlátható adatgyűjtés és adatfeldolgozás feltételeiről, a fogyasztók jogainak tiszteletben tartásáról, a nyilvánosság és az érintettek tájékoztatásáról, az érintetti jogok gyakorlásáról, a gyermekek tájékoztatásáról és védelméről, a harmadik országokba vagy nemzetközi szervezetek részére történő adattovábbításról, az adatkezelőre vonatkozó szabályzatokkal való összhang nyomon követésére szolgáló mechanizmusokról, az érdekellentétek megoldására irányuló peren kívüli eljárásokról.[635] A kódexek kidolgozói számára továbbra is fennállna az a lehetőség,

[630] Az angol szöveg „Code of Conduct" kifejezésének sokkal inkább megfelel magyar fordításként a „magatartási kódex" kifejezés így a továbbiakban ezt használjuk.
[631] A 29-es munkacsoport ki is dolgozta a benyújtás és elfogadás menetét. Érdekesség, hogy a munkacsoport „„ahol releváns", a tagállami joggal való összhangot is vizsgálja. WP29, 1998, 4.
[632] 95/46/EK irányelv, 27. cikk
[633] Federation of European Direct and Interactive Marketing (FEDMA)
[634] Rendelettervezet, 38. cikk (1)
[635] Rendelettervezet, 38. cikk (1)

hogy azokat véleményezés céljából a nemzeti adatvédelmi hatóságok, illetve a Bizottság[636] elé terjesszék, amelyek kötelezően véleményt formálnak a kódex jogszabályi megfeleléséről.[637]

Európában nem igazán terjedtek el az iparági magatartási kódexek, amely nemcsak az átfogó törvényi szabályozásnak, de a számos területen fennálló szektorális szabályozásnak is köszönhető: az Európán kívüli országok iparági kódexei tipikusan azokat a területeket fedik le (direkt marketing, hírközlési szolgáltatások, pénzügyi szektor), amelyeket az Európai államok szektorális adatvédelmi törvényekkel szabályoznak.

Valódi pozitív példa azonban Hollandia, ahol az adatvédelmi önszabályozás fontos szerepet tölt be az adatvédelmi rezsimben. Az önszabályozás gondolata már az adatvédelem korai történeti szakaszában, az 1970-es években felmerült, és az 1988-as adatvédelmi törvényben is szerepelt e lehetőség.[638] Hollandiában összesen legalább egy tucat iparági kódex részesült hatósági jóváhagyásban, amely – kimondatlanul – tulajdonképpen egyfajta minőségjelző is.[639] A holland önszabályozással kapcsolatos előnyök és hátrányok nem különböznek attól, amit részben a bevezető fejezetben, részben e fejezet során bemutattam, az elterjedtség egyik oka kétségtelenül kulturális eredetű lehet.[640] A holland önszabályozás rendszerét újabban az Egyesült Államok adatvédelmi szabályozása számára is követendő mintának tekintik.[641]

Magyarország akár ellenpélda is lehet. A jogalkotó egyáltalán nem implementálta az adatvédelmi irányelv önszabályozásra vonatkozó szakaszait, és valóban nincsenek iparági adatvédelmi kódexek. Az adatvédelmi biztos 1997-es beszámolója ezt alapvetően sajnálatos fejleménynek tekinti, mivel „az önszabályozás élőbbé, szervesebbé teszi az adatvédelem fejlődését."[642] Ezzel elvben egyetértve úgy látom, hogy önmagában a magatartási kódexek hiánya nem okozott jelentős fennakadást az adatvédelmi szabályok érvényesülésében. Az adatvédelmi jogalapok szűkre szabása azt is eredményezte, hogy nagyon nagyszámú szektorális szabályozás született, és ugyan van néhány terület, ahol a szektorális szabályozás nagyon is hiányzik/hiányzott (pl. a munkahelyi adatkezelések és a sajtó adatkezelése területén), ezeken a területeken azonban az adatvédelmi biztos majd hatóság esetjoga részben kitöltötte a szabályozás hiányából eredő űrt.

Az persze előfordulhat, nemcsak Magyarországon, hanem máshol is, hogy azokon a területeken, ahol egyébként – az adatvédelemtől függetlenül – van valamilyen önszabályozás, ott az adatvédelmi kérdések is megjelennek. Jó példa erre a Magyar Tartalomszolgáltatók Egyesületének Tartalomszolgáltatási Kódexe,[643] amelynek 2. számú

[636] A 29-es munkacsoport utódjának tekinthető Európai Adatvédelmi Testület helyett tehát a Bizottsághoz kerülne e hatáskör. Igaz, a megfelelőség kimondó bizottsági döntés a Testület véleményének kikérését követően születhetne csak meg.
[637] Rendelettervezet, 38. cikk. (2)-(3) bekezdés
[638] Hustinx, 2002, 285. Az irányelvbe tulajdonképpen a holland minta alapján került be az önszabályozás lehetősége.
[639] Hustinx, 2002, 285.
[640] Hirsch, 2013, 122-125.
[641] Ld. erről és a holland rendszerről részletesen Hirsch, 2013.
[642] ABI, 1998, 31.
(http://abi.atlatszo.hu/index.php?menu=beszamolok/1997/II/6)
[643] MTE Tartalomszolgáltatási Kódex

melléklete részletes adatvédelmi szabályokat tartalmaz. A Kódex tárgyalja többek között a naplózott adatok, a cookie-k, regisztrációs adatok, a nyilvános kommunikációban közzétett adatok, valamint a linkek adatvédelmi szabályozását. Sőt, az MTE szabályzata tartalmaz egy előminősítési eljárást is,[644] melynek keretében egy ad hoc bizottság vizsgálja az adott szervezet működésének a Kódexszel foglalt összhangját, ideértve természetesen az adatvédelmi szabályokat is. Ez azt jelenti, hogy az egyesületi tagság és annak közzététele a szolgáltatásban egyfajta adatvédelmi minőségjelzőként is szolgál – a szolgáltató csak akkor jogosult, ha garantálja a Kódexben előírt magas adatvédelmi színvonalat.[645] Megjegyzendő, hogy az adatvédelmi biztos egy alkalommal (egy válaszlevélben) hivatkozik is az MTE etikai kódexére, amely alapján tehát az adott ügyben releváns jogforrásnak ismerte el annak rendelkezéseit.[646]

4.2.1.3 Értékelés

A fentieket röviden értékelve úgy tűnik, hogy állami szabályozás nélkül az önszabályozás nem tud kellő hatékonysággal működni, részletes állami szabályozás mellett pedig nincs igazán igény az iparági önszabályozásra. Az adatvédelmi irányelv és az új Rendelettervezet szabályai ugyan széles teret adnak e szabályozási formának, de ezzel a mozgástérrel eddig alig éltek az érintett szervezetek. Ugyanakkor az új Rendelettervezet – amint azt korábban részletesen elemeztem – alapvetően az adatkezelők belső szabályozásának erősítését célozza, amely, mintegy alulról építkezve, erősítheti az ágazati önszabályozást is. Az adatvédelem súlypontjának az adatkezelők belső szabályozása felé való elmozdulásának hatására tehát kialakulhatnak szektor-specifikus megoldások is, például egy-egy ágazat érdekvédelmi szervezete igyekszik egységesíteni a belső szabályozás kialakításának elveit, főbb pontjait, vagy mintaszabályzatok/mintadokumentációk formájában segíti az adatvédelmi irányítás rendszer kialakítását.

4.2.2 Szabványosítási törekvések

Az önszabályozás egy másik lehetséges iránya a szabványosítás. A szabványosítás tulajdonképpen egységesítésre irányuló törekvés, és története a 20. század kezdetéig nyúlik vissza.[647] A szabványosítás, mint fogalom „olyan tevékenység, amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen."[648] Az eredménye elősegíti a technológiai együttműködést, egységesíti például a terminológiát, a vizsgálati módszereket és a betartandó követelményeket. A szabványosítás nemzetközi, regionális, nemzeti és akár vállalati szinten is értelmezhető.[649] Amint korábban is uatltam rá, megkülönböztethetők de jure szabványok, amelyet valamely elismert szabványügyi

[644] A részletes szabályait a 4. sz. melléklet tartalmazza.
[645] Balogh – Jóri – Polyák, 2002, 298.
[646] ABI, 2005
[647] Szádeczky, 2011, 73. Magának a szabványosításnak a technikája természetesen jóval korábbi, de ekkor kezdek elterjedni először a nemzeti, majd a nemzetközi szabványosító és tanúsító szervezetek. A szabványosítás történetéről ld. még Winn, 2010, 192-194.
[648] Az ISO/IEC Guide 2:2004 szabvány fogalmát idézi Szádeczky, 2011, 74.
[649] Szádeczky, 2011, 74.

szervezet bocsátott ki, valamint de facto szabványok, amelyek e feltételnek nem felelnek meg, de a gyakorlatban széles körben alkalmazzák őket.[650]

A szabványok alkalmazása az információbiztonság „tipikus" szabályozási formája,[651] így az adatvédelmi szabványok építhetnek e terület tapasztalataira. Már a 90-es években megjelentek az adatvédelem területét szabályozó első szabványok, elterjedtségük azonban jóval elmarad az informatikai biztonsági és információbiztonsági szabványokhoz képest – a műszaki jellegű követelmények általában véve könnyebben szabványosíthatók, mint az eltérő kulturális hátterű, és jelentős etikai töltettel rendelkező adatvédelmi követelmények. Az adatvédelmi szabványok leginkább az információbiztonsági irányítási rendszerekre vonatkozó, azaz a folyamatokra koncentráló szabványokból meríthetnek.

Az adatvédelmi szabványok jelentőségét Bennett és Raab szerint az adja, hogy a szabványok nemcsak előírják a követendő normákat, intézkedéseket, hanem egy olyan eljárást is kínálnak, amely keretében a szervezetek igényelhetik a szabályok betartásának objektív tesztjét is, azaz kapcsolódik hozzá megfelelőség-értékelés (conformity assessment) is.[652] További fontos szempont, hogy a normát kidolgozó és kibocsátó szervezet – regisztráció alapján – szabványok kiadására jogosult szervezet.[653] E megállapítások azonban pontosításra szorulnak. Kétségtelen, hogy az audit eljárások a gyakorlatban gyakran szabványokhoz kapcsolódnak, de a megfelelőség-értékelési mechanizmusok egyébként bármely más szabályozási formához is kapcsolthatók – legyen az magatartási kódex vagy állami szabályozás,[654] azaz ez nem értékelhető elhatárolási szempontként a magatartási kódexekhez képest. A szabványügyi szervezet által történő elfogadás pedig csak a de jure szabványokra igaz, amiből az is következik, hogy a de facto szabványokat és az adatvédelmi magatartási kódexeket e szempont alapján sem lehet elhatárolni.

A legelső adatvédelmi szabványt a Kanadai Szabványügyi Tanács (Standards Council of Canada) bocsátotta ki 1996-ban, megpróbálva egységesíteni a különböző magatartási kódexek rendelkezéseit. A szabványhoz való csatlakozás önkéntes volt, de a csatlakozott szervezetek számára kötelező szabályként funkcionált – a szabályok betartását rendszeres audit keretében ellenőrizték az erre akkreditált szervezetek. A szabvány ugyanakkor nem terjedt el igazán, viszonylag kevés vállalkozás csatlakozott a rendszerhez, majd a legfontosabb elemei jogszabályi követelményként is megjelentek.[655]

A szabványosítással kapcsolatos legjelentősebb eredmények között említhető az Európai Szabványügyi Bizottság[656] Információs Társadalom Szabványosítási Rendszer[657] (CEN/ISSS) keretében 2000-ben indult, „Európai adatvédelmi szabvány kezdeményezés"

[650] Szádeczky, 2011, 76.
[651] Részletesen ld. Szádeczky, 2011, 130-158.
[652] Bennett – Raab, 2006, 159-160., megismétli Bennett – Mulligan, 2012, 11.
[653] Dumortier – Goemans 2000, 29., Bennett – Mulligan, 2012, 11.
[654] Ezen összetett viszonyrendszerről ld. a 4.1 fejezetet
[655] Bennett – Raab, 2006, 160-161. További japán és ausztrál szabványosítási kísérletekről ld. Bennett – Raab, 2006, 162-163.
[656] European Committee of Standardization (CEN)
[657] Information Society Standardization System (ISSS)

elnevezésű[658] projekt, amelynek célja kifejezetten az európai adatvédelmi irányelvvel összhangban álló szabvány kidolgozása, vagy legalábbis a kidolgozás lehetőségeinek feltárása volt.[659] A projekt zárójelentése[660] számos releváns megállapítást tartalmaz a szabványosítás lehetőségeiről és korlátairól, az adatvédelmi auditálással kapcsolatos kérdésekről, és a privátszférát erősítő technológiákról. A dokumentum végül arra a következtetésre jut, hogy a globális és átfogó szabvány kialakítása nem időszerű,[661] de konszenzus alakult ki arról, hogy további lépéseket kell tenni egyrészt a témát illető elemzések, másrészt önkéntes iránymutatások (guidance) kidolgozása terén.

Ennek eredményeként született meg 2005-2006-ban egy öt, majd 2010-ben egy további három dokumentumból álló informális szabványcsomag, ún. CEN Workshop Agreement.[662] A 2005-2006-os dokumentumok egyrészt a privátszférát erősítő technológiák és privacymenedzsment-rendszerek,[663] valamint az adatvédelmi irányelv 17. cikkének megfelelő, az adatfeldolgozó által garantált adatbiztonsági szabályokra vonatkozó mintaszerződés kapcsán,[664] másrészt – és ez a dolgozat szempontjából jelentősebb – adatvédelmi audit keretrendszerről szóló[665] kvázi-szabványokat állapít meg. A CEN tehát a szabványosítás kapcsán igen nagy hangsúlyt fektet az adatvédelmi audit kérdéskörére is. A 2010-es csomag legfontosabb eleme az adatvédelmi jó gyakorlatot összefoglaló, CEN CWA 16113:2010 jelzetű dokumentum.

Végül érdemes megemlíteni az ISO/IEC 29100 szabványt,[666] amely azonban nem alkalmas teljes adatvédelmi kockázatelemzésre, vagy egy adatvédelmi irányítási rendszer kialakítására, mivel csak az adatvédelmi terminológia és adatvédelmi alapelvek egységesítésére törekszik,[667] (illetve meghatározza az adatkezelések potenciális szereplőit és feladataikat).[668] Összességében tehát e szabvány csak az alapvető, definíciós kérdésekben kaphat szerepet.

4.3 Az adatkezelők belső szabályozása

Az önszabályozás további lehetséges – a fentieket nem kiváltó, inkább kiegészítő – eszköze az adatkezelő szintjén elfogadott szabályozás (policy, szabályzat, eljárásrend stb.), amelyek hatálya nem egy-egy ágazatra/iparágra, csupán az adott szervezetre, vagy szervezetcsoportra (pl. vállalatcsoportra) terjed ki. Ezen eszközre különösen igaz Banisarnak általában az önszabályozásra tett megállapítása, miszerint annak jelentőségét az adja, hogy a „cégeknél senki sem tudja jobban, hogy milyen adatokat gyűjtenek, illetve

[658] Initiative on Privacy Standardization in Europe (IPSE)
[659] Jóri, 2009, 288.
[660] CEN, 2002
[661] A jelentés összefoglalását ld. Jóri, 2009, 289-295.
[662] Winn, 2010, 198-199.
[663] CEN CWA 15263:2005
[664] CEN CWA 15292:2005
[665] CEN CWA 15262:2005, CEN CWA 15499-1:2006, CEN CWA 15499-2:2006
[666] ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework
[667] Wright et. al., 2013, 134.
[668] A szabvány rövid leírását ld:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123 [2014.02.20.]

hogyan használják fel azokat. A gazdasági társaságoknak komoly részt kell vállalniuk a hatékony adatvédelem feltételeinek megteremtésében”.[669]

A hatékony adatvédelem megvalósulásához elengedhetetlen információbiztonság területén a belső szabályozásnak igen nagy a jelentősége, ami abból ered, hogy az információs technológiák alkalmazása először szigetszerűen az egyes szervezet szintjén kezdődött.[670] Szádeczky úgyszintén kiemeli, hogy „komoly előnye a belső szabályozásnak bármely külső szabályhoz képest, hogy jobban képes illeszkedni a szervezet sajátosságaihoz.”[671] Ideális esetben az információbiztonság és az adatvédelem belső szabályozása kölcsönösen egymásra támaszkodva, és az egyes területeken kialakult jó gyakorlatokból kölcsönösen merítve valósulhat meg.

Amint azt a 3.4 fejezetben részletesen kifejtettem, az új adatvédelmi szabályozási rezsimben az adatkezelők szintjén elfogadott szabályok kiemelt jelentőségűek, így érdemes röviden áttekinteni, hogy a jelenlegi adatvédelmi szakirodalomban miként jelenik meg e témakör, és milyen főbb rendszerezési, elméleti és gyakorlati problémák merülhetnek fel.

A különböző adatkezelők által kiadott adatvédelmi tárgyú dokumentumok kapcsán meg kell jegyezni, hogy „e dokumentumokra nincs kialakult kanonizált elnevezési rendszer. Nem pontosan definiált kifejezések keringenek széles körben […] hogy valahogy leírják a számtalan jogon kívüli [szabályozási] eszközt, amely a magánszférával kapcsolatos kötelezettségek fejlesztésére, adoptálására és végrehajtására használnak.”[672]

E forgatagba a szakirodalmi források segítségével megkísérlek némi rendszert vinni, az adatvédelmi dokumentumokat csoportosítani, és a köztük lévő elhatárolásokat megtenni. Az adatkezelők belső adatvédelmi szabályait ezek alapján alapvetően három csoportba sorolom: 1) adatvédelmi nyilatkozat, 2) adatvédelmi szabályzat, és 3) kötelező erejű vállalati szabályok (BCR).

4.3.1 Adatvédelmi nyilatkozat

Az adatkezelők szintjén elfogadott szabályozás egyik típusának tekinthetők az adatvédelmi nyilatkozatok, amelyek az Egyesült Államokban jelentek meg a 80-as évektől kezdődően, és ma is használatosak. Az adatvédelmi nyilatkozatok később online környezetben szerte a világon elterjedtek. A vállalkozások az Egyesült Államokban rendszerint az OECD alapelvek vagy a Fair Information Policy Practices elveinek alkalmazását vállalják, de e vállalások mögött nincsenek részletesen kidolgozott belső szabályok, és nincs érdemi felügyelete sem. Azaz e nyilatkozatok – szemben egy részletesen kidolgozott szabályzattal – érdemben nem befolyásolják az adott szervezet belső működését. Bennett és Raab a fentiek mellett is fontos szerepet tulajdonít az adatvédelmi nyilatkozatoknak, mivel az érintettek számára hasznos, ha egy vállalkozás tömören és közérthetően közli az adatvédelmi politikája főbb elemeit.[673] A nap, mint nap elérhető számtalan online

[669] Banisar, 2001, 24.
[670] Szádeczky, 2011, 77.
[671] Szádeczky, 2011, 78.
[672] Bennett – Mulligan, 2012, 9. (Saját fordítás.)
[673] Bennett – Raab, 2006, 153-154.

adatvédelmi nyilatkozat egészen biztosan jelentős szerepet játszik az érintettek adatvédelmi tudatosságának növelésében is.

Az adatvédelmi nyilatkozatok funkciója – az adott állam adatvédelmi jogától függően is – többrétű. Először is a szolgáltatók adatvédelmi politikájának kommunikációs eszközeként szolgálnak, azaz inkább marketingszerepük van. Nem egyszer valamely nagyobb adatvédelmi botrány hatását kívánja a vállalkozás enyhíteni adatvédelmi politika elfogadásával.[674] Másrészt jogilag is releváns tájékoztató szerepük van: azon államokban, ahol az adatkezelés egyik jogalapja az érintett tájékozott hozzájárulása, a megfelelő tájékoztatás az érvényes hozzájárulás feltétele.[675] Ugyanakkor egyes szerzők felhívják a figyelmet arra, hogy a hosszú és gyakran homályos adatvédelmi nyilatkozatok láttán felmerül a gyanú, hogy az érintettek egyértelmű tájékoztatása helyett inkább az adatkezelő mozgásterének biztosítása e nyilatkozatok elsődleges célja. Ezt alátámasztja egy kutatás, amely arra jutott, hogy a privacy policyk többsége inkább „privacy-t felfaló" (privacy consuming), és nem a privacy-t védő (privacy supporting) nyilatkozat, és gondosan úgy van megfogalmazva, hogy a felhasználók elfogadják a privacy-t elfogyasztó feltételeket is.[676]

A fenti funkciókból eredően az adatvédelmi nyilatkozatok jogi státusza is eltérő lehet. Az adatok kezelésével kapcsolatos rendelkezések felfoghatók egyrészt az adatkezelő egyoldalú jognyilatkozatának (kötelezettségvállalásának), aminek különösen azokban az országokban (pl. az Egyesült Államokban) van jelentősége, ahol egy adott területen az állami szabályozás nem biztosítja a személyes adatok védelmét. Emellett az adatkezelő és az érintett között létrejött szerződéses viszony részévé is válhat, amelynek megsértése tulajdonképpen szerződésszegést jelent. Végül, mint említettük, a tájékozott hozzájárulás elvét követő országokban (például az Európai Unió tagállamaiban), az adatvédelmi nyilatkozat valójában az a tájékoztatás, amely alapján a felhasználó az adatkezeléshez hozzájárul. A hozzájárulás tartalma tehát azokra az adatkezelési műveletekre terjed ki, amelyek az adatvédelmi nyilatkozatban szerepelnek, így a nyilatkozat az érintett egyoldalú jognyilatkozatának – a hozzájárulásnak – a tartalmaként is felfogható. Ennek megsértése azt vonja maga után, hogy a hozzájárulás érvénytelen lesz, az adott, a nyilatkozatban foglaltakon túlterjeszkedő adatkezelésnek legalábbis nem lehet jogalapja. Amennyiben nincs más jogalap,[677] ez jogellenes adatkezelést valósít meg, függetlenül a felek között fennálló szerződéses viszonytól. Meg kell jegyezni, hogy az adatvédelmi nyilatkozat tényleges jogi helyzetét csak az adott ügy összes körülményének, különösen a kezelt adatok körének, a nyilatkozat megfogalmazásának, és az általános szerződési feltételek ismeretében lehet megállapítani.

[674] Bennett – Raab, 2006, 153-154.
[675] E rendszerekben a jogszabályok részletesen előírják, hogy a tájékoztatásnak mire kell kiterjednie. Az adatvédelmi nyilatkozatoknak e szempontokra ki kell térnie.
[676] Jøsang – Fritsch – Mahler, 2010, 133-134.
[677] Megjegyezzük, hogy a tájékoztatási kötelezettség más jogalapok esetén is kötelező, a tájékoztatás elmaradása így ekkor is jogsértő lehet, de attól még az adott jogalap az adatkezelés érvényes jogalapja lehet. Ilyen eset lehet például az, ha az adatvédelmi nyilatkozat nem tájékoztat arról, hogy az adatok – törvényben meghatározott esetekben – továbbíthatók a rendőrség vagy más hatóság részére.

A privacy policyk alkalmazása a gyakorlatban korántsem problémamentes. Az adatvédelmi nyilatkozat, mint a hozzájárulást tartalommal kitöltő dokumentummal kapcsolatos problémákat a hozzájáruláson alapuló adatvédelmi rezsim kritikája kapcsán részletesen elemeztem.

4.3.2 Adatvédelmi szabályzat

Bennett és Raab a szabályzatokat (privacy codes) határozottan elkülöníti az adatvédelmi nyilatkozatoktól, mivel a szabályzatok konkrét iránymutatást adnak az adatvédelmi elvek érvényesítéséhez szükséges viselkedés és eljárások tekintetében, azaz szabályokat állapítanak meg a tagvállalatokra vagy a munkavállalókra. A szervezetek által elfogadott szabályzatok elsősorban a nagy, jól szervezett, médiaérdeklődésre is számot tartó, és várhatóan sok fogyasztói panasszal szembenézni kénytelen vállalkozásoknál gyakoriak.[678] A szabályzat tehát – szemben egy adatvédelmi nyilatkozattal – nem csak annak kinyilatkoztatása, hogy mit csinál az adatkezelő, hanem annak is, hogy azt pontosan hogyan csinálja.[679]

Megemlítendő, hogy jelenleg is több európai adatvédelmi törvény kötelezően írja elő bizonyos szervezetek számára belső adatvédelmi (és adatbiztonsági) szabályzat elfogadását és/vagy belső adatvédelmi felelős kinevezését.[680]

Az adatvédelmi szabályzat a szervezet belső szabályozásának legfontosabb eleme, amely nemcsak egy adott adatkezeléssel kapcsolatos összefoglalót tartalmaz, hanem képes részletesen szabályozni az adatkezeléssel kapcsolatos belső eljárásrendeket, a hozzáférési jogosultságokat, az adatkezeléssel kapcsolatos feladat- és hatásköröket, az adatvédelmi szabályok megsértésének belső jogorvoslati fórumait stb. Ideális esetben a központi adatvédelmi szabályok végrehajtási szabályaiként funkcionálhatnak. Az adatvédelmi szabályzat tehát az adatkezelők belső szabályozásának alapvető jogforrása.

4.3.3 Kötelező erejű vállalati szabályok (BCR)

Az adatkezelők belső szabályozásának egyik speciális területe a kötelező erejű vállalati szabályok alkalmazása.

A „kötelező erejű vállalati szabályok (Binding Corporate Rules – BCR) olyan multinacionális vállaltcsoportok által elfogadott belső szabályozó-együttesek (magatartási kódex, szabályzat stb.), melyek egységesen, az adatkezelő illetve adatalany nemzetiségétől függetlenül, az adott vállalat különböző EGT-n kívüli országokban is elhelyezkedő egységei közötti adatáramlás szabályozására szolgálnak.”[681]

A BCR-ek, mint önszabályozási eszközök sajátossága először is abban rejlik, hogy a hatályuk nem egy adatkezelőre, hanem egy vállalatcsoportra – adatkezelők és

[678] Bennett – Raab, 2006, 155.
[679] Bennett – Mulligan, 2012, 9.
[680] Ld. például Magyarországon az Infotv. 24. §-át, amely szerint belső adatvédelmi felelőst kell kinevezni és adatvédelmi és adatbiztonsági szabályzatot kell elfogadni az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő adatkezelőnél, a pénzügyi szervezeteknél, és az elektronikus hírközlési és közüzemi szolgáltatóknál; ill. Németországban a BDSG. 4f-4g pontjait a belső adatvédelmi felelősről.
[681] Liber, 2011, 181.

adatfeldolgozók csoportjára – terjed ki, így az adatkezelők szintjén és az adatkezelőn kívüli szabályozási eszközök között „félúton” helyezkednek el. Specialitását másodszor az adja, hogy a BCR-ek elfogadását egy speciális cél: a harmadik országba történő adattovábbítás motiválja, így kifejezetten az a célja, hogy magánjogi eszközökkel (egyoldalú kötelezettségvállalással) pótolja a megfelelő szintű védelmi szabályokat. Harmadik sajátossága, hogy épp a harmadik országba történő adattovábbítással összefüggésben a 29-es munkacsoport igen részletes szabályokat dolgozott ki a BCR-ek kívánatos tartalmára nézve, megkülönböztetve az adatkezelők közötti adattovábbítást és az adatfeldolgozónak történő adatátadás szabályait. A 29-es munkacsoport dokumentumaiból egyértelműen kiderül, hogy igen részletes belső szabályozást vár el az adott vállalatcsoporttól. A BCR-eknek az adatvédelem anyagi jogi szabályainak (azaz az irányelv fontosabb szabályainak megismétlése) mellett ki kell térnie – a teljesség igénye nélkül – az érintetti jogok gyakorlásának módjára, a belső panaszkezelési mechanizmusokra, a megfelelés-ellenőrzés és esetleges audit módjára stb.[682] A BCR legfontosabb eleme azonban az Európai Unión belüli vállalat kötelező felelősségvállalása a vállalatcsoport többi tagja által végzett tevékenységéért is. A kötelező vállalati szabványokat a tagállami adatvédelmi hatóság hagyja jóvá, és betartásukat is ők felügyelik.[683]

A kötelező erejű vállalati szabályok alaposan kidolgozott adatvédelmi szabályzatként is felfoghatók, így az erre vonatkozó tartalmi és módszertani kérdésekkel kapcsolatos tapasztalatok és jó gyakorlat hasznosítható az egyéb adatvédelmi szabályzatok megalkotása során.

4.4 Adatvédelmi audit és adatvédelmi tanúsítás

Az adatvédelmi auditálás, tanúsítás (és hozzá kapcsolódó címkézés) lényegében a fent említett különböző típusú szabályozáshoz, állami szabályozáshoz, önszabályozás/társszabályozás keretében elkészült szabályozókhoz és az adatkezelők szintjén elfogadott szabályokhoz kapcsolódó ellenőrzési-felügyeleti rendszerként értelmezendő. Az auditálás valójában egy módszertan, egy technika, amely potenciálisan bármilyen szabályrendszernek való megfelelést vagy nem-megfelelést megállapíthat.

Mindenekelőtt érdemes áttekinteni az auditálással kapcsolatos alapfogalmakat, az audit/tanúsítás típusait, és az adatvédelmi auditálás előnyeit, hátrányait. Ezen áttekintéshez a vonatkozó – elsősorban külföldi – szakirodalmat, a tanúsításával kapcsolatos ISO szabványokat, és a már létező adatvédelmi audit módszertanokat használom.

4.4.1 Adatvédelmi audit és tanúsítás fogalma

Bár a jogirodalomban, illetve több különböző, adatvédelmi auditra vonatkozó módszertanban közvetlenül is szerepel az adatvédelmi audit fogalma, érdemes megnézni mindenekelőtt az ISO 9000:2005 jelzetű szabvány – meglehetősen semleges – irányítási rendszerekre vonatkozó audit fogalmát. Eszerint: „az audit auditbizonyítékok nyerésére és

[682] Ld. részletesen WP, 2008
[683] Liber, 2011, 182.

ezek objektív kiértékelésére irányuló módszeres, független és dokumentált folyamat annak meghatározására, hogy az auditkritériumok milyen mértékben teljesülnek."[684]

Az adatvédelmi audit meghatározásakor CEN Workshop Agreement egyik dokumentumára támaszkodunk. Eszerint az adatvédelmi audit egy módszeres és független vizsgálat annak meghatározására, hogy az adatkezeléssel kapcsolatos tevékenységek összhangban vannak-e a szervezet adatvédelmi szabályaival (policy-vel) és az EU adatvédelmi irányelvének követelményeivel.[685]

E két meghatározás segítségével megkísérlek egy harmadik, mindkét fogalom alapvető elemeit felhasználó definíciót alkotni. Eszerint az adatvédelmi audit egy független, auditbizonyítékok[686] gyűjtésén és objektív értékelésén alapuló, módszeres[687] és dokumentált vizsgálat annak meghatározására, hogy egy szervezet adatkezelési tevékenysége[688] megfelel-e az e tevékenységre irányadó szabályoknak.[689]

Az auditálást rendszerint (de nem szükségszerűen) tanúsítás is követi, amelynek során az auditjelentés és auditbizonyítékok ismételt vizsgálata és értékelése alapján a tanúsító-szervezet dönt egy meghatározott időszakra szóló tanúsítvány kiadásáról. A tanúsítást tehát minden esetben megelőzi az audit folyamata.

4.4.2 Az audit/tanúsítás típusai

4.4.2.1 Terméktanúsítás és rendszertanúsítás

Mind a minőségirányítási rendszerekkel, mind az adatvédelmi auditálással foglalkozó szakirodalom megkülönbözteti a különböző eszközök, termékek tanúsítását (terméktanúsítás) valamely irányítási rendszer tanúsításától (rendszer-audit vagy rendszertanúsítás).[690]

Valamely eszköz (termék) tanúsítása biztosítékot jelent arra, hogy a termék megfelel a vonatkozó jogszabályoknak, az előírt szabványoknak és egyéb dokumentumoknak (szerződésben előírt követelményeknek).[691] Termékek esetén a tanúsítást nem audit, hanem vizsgálat előzi meg, amely „egy vagy több jellemző [megkülönböztető tulajdonság]

[684] MSZ EN ISO 9000:2005, 34.
[685] CEN, CWA 15262:2005, 8. Az Egyesült Királyság Információs Biztosa által kiadott kézikönyv lényegében ezzel azonos fogalmat alkalmaz, ld. ICO, 2001, 1.4.
[686] Ilyen auditbizonyíték lehetnek például a szabályzatok, eljárásrendek, utasítások, tájékoztatók, szerződések adatvédelmi rendelkezései, személyes adatokat érintő panaszok, jegyzőkönyvek, szóbeli interjún alapuló információk stb.
[687] Az audit módszeressége lényegében azt jelenti, hogy azt meghatározott szabályok és folyamat alapján kell végrehajtani. Berényi – Szintay – Tóthné, 2011
[688] A „tevékenység" kifejezést a lehető legtágabban értve ide értjük az adatkezelésre vonatkozó dokumentumok meglétét, a tényleges adatkezelési műveleteket, a rendszer fejlesztésével kapcsolatos terveket stb.
[689] A „tevékenységre irányadó szabályokat" szintén tágan értve ide tartozik minden olyan dokumentum, amely az adatkezeléssel kapcsolatos szabályt állapít meg: törvények és más jogszabályok, magatartási kódexek, policy-k, szabályzatok, szerződési feltételek stb.
[690] A minőségügyi kérdésekkel foglalkozó szakirodalom az audit tárgy alapján emellett nevesíti még az eljárásauditot (folyamatauditot), és a személyauditot (Berényi – Szintay – Tóthné, 2011), ezekkel azonban a disszertáció tárgyára tekintettel nem foglalkozom.
[691] Szigeti – Végső – Kiss, 2003, 6.2.

valamely eljárás szerinti meghatározása".[692] Az adatvédelem területén ez tulajdonképpen az adatfeldolgozási hardver- és szoftver-termékek adatvédelmi és adatbiztonsági megbízhatóságának vizsgálatára és adott esetben tanúsítására irányuló eljárás, amely jelentősen megkönnyítheti az adatvédelmi szempontból megbízható eszközök kiválasztását is.[693]

A rendszer-audit célja, hogy – a fenti definícióval összhangban – egy szervezet adatkezelésekkel kapcsolatos tevékenységét értékelje. A rendszer-auditként értelmezett adatvédelmi audit feltételezi valamilyen irányítási rendszer kialakítását, amely integrálja és konkretizálja az adatkezelővel szemben a szabályozás alapján fennálló kötelezettségeket.[694]

Meg kell jegyezni, hogy a termékvizsgálatra és –tanúsításra, valamint a rendszerauditra és –tanúsításra különböző módszertanok és eljárási szabályok (szabványok) vonatkoznak. A disszertációban az adatvédelmi audit alatt kizárólag rendszer-auditot értek.

4.4.2.2 Belső, beszállítói és külső audit

Az auditot végző személy/szervezet alapján megkülönböztethető belső, beszállítói és külső audit.

A belső audit során az adott adatkezelő szervezet maga végzi el a vizsgálatot és az értékelést, amelyről dokumentációt készít.[695] Ha egy szervezet rendelkezik belső adatvédelmi felelőssel vagy más adatvédelemért felelős szervezeti egységgel, akkor a belső audit gyakran e személy vagy szervezeti egység feladata. A belső audit jellemzően nem jár együtt külön tanúsítvány kibocsátásával, de előfordul, hogy valamely tanúsítvány több éven keresztül történő használatához előfeltétel a meghatározott időszakonként lefolytatott belső audit.

Az ún. beszállítói auditra rendszerint akkor kerül sor, ha egy szervezet kiszervezi az adatkezelés tevékenységét, és szeretne meggyőződni a partner adatvédelmi rendszerének megfelelőségéről.[696]

Végül a külső audit során a szervtől elkülönült, független szerv végzi el az auditot: ez lehet az adott állam adatvédelmi hatósága (Magyarország mellett néhány európai országban is találunk erre példát) vagy piaci szereplő. Előfordul, hogy az adatvédelmi auditálásban érdekelt szervezetek valamely más, például információbiztonsági vagy minőségirányítási rendszerek tanúsításával kapcsolják össze az adatvédelmi tanúsítás szolgáltatás igénybevételét is.[697]

---

[692] MSZ EN ISO 9000:2005, 33.
[693] Balogh – Jóri – Polyák, 2002, 390.
[694] Az adatvédelmi audit, mint rendszeraudit, és ezzel összefüggésben Roßnagel audit-koncepciójának részletes elemzését ld. Balogh – Jóri – Polyák, 2002, 334-340.
[695] ICO, 2001, 1.5. Az ICO dokumentuma ezt „First Party Audit"-nak nevezi.
[696] ICO, 2001, 1.5. Az ICO „Second Party Audit" vagy „Supplier Audit" elnevezést használ.
[697] ICO, 2001, 1.5-1.6. Az ICO „Third Party Audit" elnevezést használ. Az egyes audit-típusok ICO dokumentumon alapuló magyar nyelvű összefoglalását ld. még Balogh – Jóri – Polyák, 2002, 382-383.

4.4.2.3 Alkalmassági audit és megfelelőségi audit

Az ICO adatvédelmi audit kézikönyve, és az azt elemző magyar kutatás alapján megkülönböztethető ún. alkalmassági audit (adequacy audit) és megfelelőségi audit (compliance audit).

Az alkalmassági audit annak megállapítására irányul, hogy az adatkezelő szervezetnél található különböző dokumentumok: szabályzatok, policy-k, gyakorlati útmutatások, stb. megfelelnek-e a központi adatvédelmi jogszabályok előírásainak. Az auditálás ezen szakasza nem feltétlen igényel helyszíni vizsgálatot, csupán az iratok áttekintésével jár.

A megfelelőségi audit célja annak megállapítása, hogy az adatkezelő szervezet tényleges működése (adatkezelési gyakorlata) megfelel-e a dokumentált szabályzatoknak és a jogszabályoknak. Ezen eljárás megköveteli a helyszíni vizsgálatok elvégzését, és rendszerint a munkatársaktól való információgyűjtést is.[698]

Nyilvánvaló, hogy lényegesen alaposabb a megfelelőségi audit, mivel az a tényleges helyzet feltárására és értékelésére irányul, nem csak a dokumentáció törvényességének vizsgálatára.

Megjegyezzük, hogy hasonló szempontrendszer szerint három típusba is sorolható az megfelelőség-értékelés. Bennett és Raab nevesíti a „policy-megfelelést" (compliance of policy), amely lényegében egyet jelent az alkalmassági audit eredményeként fennálló megfeleléssel. Az „eljárások megfelelősége" (compliance of procedure) a szerzők szerint azt igazolja, hogy az adott szervezet megfelelő eljárásokkal implementálja és végrehajtja a szabályzatait, míg a harmadik típus, a „gyakorlat megfelelősége" (compliance of practice), azt igazolja, hogy az adott szervezet tényleges tevékenysége megfelel a rá vonatkozó szabályzatoknak.[699] Utóbbi lényegében megegyezik a megfelelőségi audittal.

4.4.3 Az adatvédelmi tanúsítás előnyei, hátrányai – az érintett szervezetek motivációja

Első ránézésre is egyértelmű, hogy az adatvédelmi tanúsításhoz szükséges auditálásra való felkészülés azt feltételezi, hogy az adott szervezet alaposan megvizsgálja az adatkezeléssel kapcsolatos dokumentumait és gyakorlatát, így az adatvédelmi audit intézménye nagyban hozzájárul az adatkezelők adatvédelmi tudatosságának, érzékenységének erősítéséhez. Az auditálás feltételezi az adatvédelmi elképzelések, célkitűzések rendszerezett rögzítését, és a megvalósítás eszközrendszerének előzetes felvázolását is. Ellenérvként felhozható, hogy az önkéntes audit nem alkalmas az adatvédelmi színvonal általános, széles körű javítására, mivel abban valószínűleg azok az adatkezelők vesznek részt, akik korábban is magas színvonalú védelmet biztosítottak, és kimaradnak belőle azok, akik az adatvédelmi követelményekre kisebb hangsúlyt helyeznek.[700]

Emellett jelentős motivációs tényező lehet az adatkezelők számára, hogy a sikeres auditáláshoz kapcsolódó tanúsítvány megfelelő kommunikációja alkalmas az ügyfelek

[698] ICO, 2001, 2.2-2.3., Balogh – Jóri – Polyák, 2002, 384-385., NAIH, 2013, 4.
[699] Bennett – Raab, 2006, 259.
[700] Alexander Roßnagel, koncepcióját és annak Hans-Ludwig Drews és Hans Jürgen Kranz általi kritikáját idézi Balogh – Jóri – Polyák, 2002, 329.

illetve az állampolgárok adott szervezet felé megnyilvánuló bizalmának növelésére is.[701] A német jogirodalomban megjelenő álláspont szerint az adatvédelmi erőfeszítések potenciálisan akár jelentős versenyelőnyt is jelenthetnek,[702] az adatvédelem „piaci alapú" amerikai rendszerével kapcsolatos kritikák, valamint a piaci alapon működő tanúsító-rendszerek nehézségei azonban alapvetően azt mutatják, hogy a fogyasztók adatvédelmi tudatossága sokszor felülértékelt.

További motivációként értékelhető a jogellenes adatkezelésből eredő hátrányok, elsősorban a hatósági bírság elkerülése. Az egyre komplexebbé váló adatkezelések áttekintése növekvő kihívást jelent az adatkezelő szervezetek számára, márpedig alapos vizsgálat és értékelés nélkül az adott szerv nem lehet biztos benne, hogy valamennyi adatkezelése valóban jogszerű. Az auditálásból következő előny lehet a szervezeten belüli folyamatok ellenőrizhetőbbé válása is,[703] azaz az adatkezelési folyamatok „rendbetétele" jól illeszkedhet az adott szervezet általános irányítási rendszerének fejlesztéséhez is. Az európai adatvédelmi jog fejlődése egyértelműen abba olyan irányba mutat, amely feltételezi az adatkezelők saját adatkezelési rendszerükhöz való, az eddigieknél sokkal tudatosabb hozzáállását is, mivel az elszámoltathatóság elvének keretében eleve számos belső mechanizmus és dokumentációs kötelezettség merül fel. Ezen erőfeszítések megtételére álláspontom szerint kötelező szabályozás nélkül nehezen vehetőek rá az adatkezelők – a jelenlegi szabályozási rezsimben az adatvédelmi rendszer tudatos kiépítése csak a nagyvállalatok világára jellemző. Amennyiben azonban a jogszabályi környezet az adatvédelmi irányítási rendszer kiépítésére ösztönöz, vagy legalább egyes elemeinek megalkotását kötelezővé teszi, az adatvédelmi audit és egy tanúsítvány beszerzése ezen erőfeszítések kommunikálásaként, mintegy a „gyümölcsök leszedéseként" is felfogható.

Az információbiztonsággal foglalkozó iparág folyamatosan fejlődése is együtt járhat az adatvédelmi (jogi) kérdések előtérbe kerülésével. Az információbiztonsági szabványok ugyanis több esetben előírják a különböző jogi követelményeknek való megfelelést is, így az adatvédelmi kérdések kisebb-nagyobb mélységben való vizsgálata nem megkerülhető az információbiztonsági irányítási rendszerek auditálása során sem.

Végül érdemes megjegyezni, hogy az adatvédelmi audit intézményének jogszabályi szintű elismerése önmagában is jelentősen növelheti a jogintézmény iránti bizalmat illetve annak népszerűségét.

4.4.4 Adatvédelmi audit és adatbiztonság

Az adatvédelmi audit szempontjainak meghatározásában is fontos elem az adatbiztonság. Az adatbiztonsági követelmények egyben jogszabályi követelmények is, amiből az következik, hogy az – akár a hatóság, akár piaci szereplő által végzett – adatvédelmi auditálásnak és tanúsításnak valamilyen szinten ki kell terjednie az adatbiztonsági követelményekre is. Másik oldalról nézve megállapítható, hogy az információbiztonság

[701] A fogyasztói bizalomnak igen nagy jelentősége van olyan speciális területeken, mint például az elektronikus kereskedelem (ideértve a legkülönbözőbb online szolgáltatásokat).
[702] Balogh – Jóri – Polyák, 2002, 330-331.
[703] Thomas Königshofen gondolatait idézi Balogh – Jóri – Polyák, 2002, 331.

területén a szabványok alkalmazása és azok tanúsítása bevett szolgáltatásnak minősül,[704] és e szabványok rendre előírják a jogszabályi követelményeknek, például az adatvédelemre vonatkozó szabályoknak való megfelelést is, azaz egy információbiztonsági audit során is tekintettel kell lenni a jogszabályi környezetre. Ezek alapján célszerűnek tűnik az információbiztonsági irányítási rendszerek tanúsítása során alkalmazott auditálási-tanúsítási módszereket az adatvédelmi auditálás módszertanának kidolgozásakor hangsúlyosan figyelembe venni, e két terület ugyanis – ideális esetben persze – szükségszerűen ki kell, hogy egészítse egymást.

4.4.5 Az adatvédelmi audit és tanúsítás menete

Az adatvédelmi audit és tanúsítás részletes menete a gyakorlatban elég változatos lehet, van azonban a folyamatnak néhány olyan mérföldköve, amely szinte mindegyik módszertan alapján azonos. Az adatvédelmi audit jogintézményének megértéséhez érdemes e sarokpontokat vázlatosan áttekinteni:

1) Alapelvek meghatározása: Az adatvédelmi auditra jól alkalmazhatóak az irányítási rendszerek külső auditjára és tanúsítására vonatkozó ISO 17021[705] szerinti egyes általános előírások, úgymint a pártatlanság és függetlenség követelménye, és az összeférhetetlenség az auditált szervezet és az auditorok között. Gyakori problémát jelent a szakterületen, hogy a 17021 szabvány tiltja a tanúsító testület tanácsadási tevékenységét.[706] Ennek létjogosultságát a szakmai közvélemény is kritizálja. Véleményem szerint az adatvédelmi auditálás terén elegendő a személyi összeférhetetlenség biztosítása: vagyis az a személy, aki az adatvédelem belső szabályozásának kialakításában tanácsadóként részt vett, nem lehet az adott rendszer auditora.
2) A hatókör (scope)[707] meghatározása: Az auditálás/tanúsítás során az első legfontosabb kérdés a hatókör megállapítása,[708] azaz annak meghatározása, hogy az audit mely területekre (szervezeti egységekre) és mely adatkezelésekre terjed ki.
3) Auditterv elkészítése és végrehajtása: Az audittevékenységet egy előre kidolgozott menetrend alapján célszerű végezni, amelyet az auditterv foglal össze. Az auditterv kitér – többek között – az audit céljaira, az auditkritériumok és egyéb dokumentumok felsorolására, az audit területének (hatókörének) meghatározására, az auditcsoport tagjainak megnevezésére, felelősségére, a helyszíni audittevékenységek időpontjára, helyszínére, várható időtartamára stb.[709] Az audit két típusaként nevesített alkalmassági és megfelelőségi audit tulajdonképpen az audit fázisaiként is felfoghatók.[710] Az audit során tehát mind a dokumentumok megvizsgálására, mind helyszíni audittevékenységre szükség lehet az

[704] A leginkább elterjedt az információbiztonsági irányítási rendszerekre alkalmazandó ISO/IEC 27000-es szabványcsalád
[705] MSZ EN ISO/IEC 17021:2011. A belső auditra az MSZ EN ISO 19011:2011 jelzetű, „Útmutató irányítási rendszerek auditálásához (ISO 19011:2011)” című szabvány vonatkozik.
[706] MSZ EN ISO/IEC 17021:2011, 11.
[707] A hivatkozott szabvány magyar nyelvű változatában „az audit területe” fordítás szerepel.
[708] MSZ EN ISO/IEC 17021:2011, 20-21.
[709] MSZ EN ISO/IEC 17021:2011, 20-21.
[710] ICO, 2001, 3.9, 3.17

auditbizonyítékok gyűjtése érdekében. Auditbizonyíték lehet bármely, az adatkezelést érintő dokumentum vagy személyes interjú során szerzett bizonyíték.

4) Az audit megállapításai: Az audit eredményeként megállapítható a rendszer egyes elemeinek vagy egészének megfelelősége vagy nem-megfelelősége; emellett az auditjelentés tartalmazhat fejlesztési javaslatokat is. Nem-megfelelőség akkor állapítható meg, ha valóban van olyan előírt követelmény, ami nem teljesül, egy vagy több mulasztás okozza ezeket, és a nem-megfelelésre objektív bizonyítékok állnak rendelkezésre.
5) Az auditjelentés elkészítése: Az auditfolyamat utolsó állomása az auditjelentés elkészítése. A jelentés tartalmazza az audit legfontosabb paramétereit, (így annak célját, hatókörét, az ügyfél megnevezését), a lefolytatott helyszíni audittevékenység időpontját, helyszínét, az auditkritériumokat, valamint az audit megállapításait, bizonyítékait és következtetéseit.[711]
6) Tanúsítás: Az adatvédelmi audit előnyeinek egy része csak akkor realizálódik, ha az adatvédelem érdekében tett erőfeszítések, és az audit során ezt igazoló pozitív eredmények a nyilvánosság számára egyszerűen és könnyen kommunikálhatóak. Pozitív auditjelentés esetén szerencsés tehát az auditáláshoz meghatározott időre szóló tanúsítvány kiadását is kapcsolni. A tanúsítvány meglétét a legkönnyebben tanúsító védjegy (logó) alkalmazásával lehet kommunikálni.

4.4.6 Kitekintés: működő audit és tanúsító-rendszerek bemutatása

4.4.6.1 Kitekintés egyes külföldi megoldásokra

Az adatvédelmi hatóság által végzett adatvédelmi auditálás nem példa nélküli Európában. Az Egyesült Királyságban az információs biztos végez auditálási tevékenységet, amelyet – hasonlóan a Rendelettervezet javaslatához – külső szakember bevonásával is gyakorolhat. A biztos az adatkezelő hozzájárulásával a helyes adatvédelmi gyakorlat érvényesülését értékeli. Az angol adatvédelmi törvény szerint a személyes adatok kezelése során helyesnek tekinthető az a gyakorlat, amely a biztos szerint kívánatos az adatalany és mások érdekeire tekintettel, és megfelel az adatvédelmi törvény követelményeinek.[712] A biztos e jog gyakorlásához kidolgozta és 2001-ben kiadta az adatvédelmi audit módszertani kézikönyvét,[713] amelyet 2012-ben egy új iránymutatás (guide)[714] váltott.[715] Az auditálás célja a törvényi előírásoknak és a szervezet saját adatvédelmi rendszerének való megfelelés vizsgálata, a hiányosságok és gyengeségek feltárása, valamint információ szolgáltatása az adatvédelmi rendszer felülvizsgálatához. A saját adatvédelmi rendszer a törvényi előírásoknál szigorúbb követelményeket is megfogalmazhat. Az önkéntes auditálás végeredménye az adatkezelő, illetve a biztos tájékoztatása, iránymutatás kibocsátása az

[711] MSZ EN ISO/IEC 17021:2011, 26.
[712] Data Protection Act 1998 Art. 51
[713] ICO, 2001
[714] ICO, 2012
[715] A 2001-ben kiadott Adatvédelmi Audit Kézikönyv formálisan ugyan visszavonásra is került (ld. Morgan – Boardman, 2012, 58.), mivel azonban az újabb iránymutatásnál lényegesen részletesebb, fontos, e tanulmányban is többször hivatkozott jogirodalmi forrásként tekintünk rá.

adatkezelési gyakorlat előmozdítása végett, szankció alkalmazására természetesen nem kerül sor.[716]

Emellett pl. Németországban – ahol az adatvédelmi auditálás lehetősége régóta része a BDSG-nek – Schleswig-Holstein tartomány adatvédelem hatósága is végez (tartományi jog alapján) adatvédelmi auditálást az ebben önként résztvevő közjogi adatkezelőre vonatkozóan. Az eljárás célja annak vizsgálata, hogy az adatkezelő által önként meghatározott adatvédelmi célkitűzések az azokhoz rendelt intézkedésekkel megvalósíthatók-e. Az eljárás eredményeként a hatóság tanúsítványt bocsát ki, amely az állampolgár számára garancia arra vonatkozóan, hogy az adott közigazgatási szerv tudatos adatvédelmi tevékenységet végez.[717] Ez az eljárás összességben határozottan elválik az adatkezelés jogszerűségének hatósági ellenőrzésétől, alapvető célja a szervezeten belüli adatvédelmi tevékenység tudatosságának növelése, valamint az adatvédelemnek a törvényi garanciákat meghaladó színvonalú biztosítása.[718]

4.4.6.2 Az adatvédelmi audit szabályozása Magyarországon

Az új adatvédelmi törvény[719] egyik jelentős újdonsága, hogy rendelkezik az adatvédelmi audit jogintézményéről. Az auditálásra vonatkozó szakaszok az Infotv. első hatálybalépését követően egy évvel, 2013. január 1-én léptek hatályba – időt adva a NAIH számára a felkészülésre. A törvényi szabályozás összességében igen szűkszavú, az audit céljainak, módszerének, eljárásának részletes meghatározását az adatvédelmi hatóságra hagyja. Ennek megfelelően 2013 elején a Hatóság közzétette az adatvédelmi audit szolgáltatásával kapcsolatos szempontrendszerét,[720] amely a törvényszöveg által okozott bizonytalanságok egy részét rendezi. Az alábbiakban a jogszabályi környezetet és ezzel összhangban a hatóság által kibocsátott szempontrendszert együttesen elemezzük.

Az Infotv. szerint az adatvédelmi audit az adatvédelmi hatóság által, az adatkezelő kérelmére nyújtott szolgáltatás, amelynek célja a végzett vagy tervezett adatkezelési műveleteknek a hatóság által meghatározott és közzétett szakmai szempontok szerinti értékelésén keresztül a magas szintű adatvédelem és adatbiztonság megvalósítása.[721] A törvény egyértelművé teszi, hogy az auditálást a hatóság nem közigazgatási hatáskörben, hanem szolgáltatásként végzi, annak eredménye tehát nem lehet közigazgatási határozat. Az audit szempontrendszer kimondja, hogy a Hatóság az adatvédelmi audit keretében „csak” külső alkalmassági auditot végez, azaz az audit célja az adatkezelő adatvédelmi dokumentációjának a törvényhez mérése, és nem az adatkezelés tényleges gyakorlatának feltárása (megfelelőségi audit).[722]

Az audit, mint szolgáltatásnyújtás jelenlegi szabályozása azt is jelenti, hogy az adatkezelő oldalán nem keletkezik olyan jog, amely alapján egy adatkezelő valamely adatkezelését a

[716] Polyák – Szőke, 2011, 175.
[717] Polyák – Szőke, 2011, 174.
[718] Ld. az Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein honlapját, https://www.datenschutzzentrum.de/index.htm [2012.10.25.]
[719] Ld. részletesen Polyák – Szőke, 2011
[720] NAIH, 2013
[721] Infotv. 69. § (1)
[722] A megfelelőségi és alkalmassági auditról ld. NAIH, 2013, 4.

Hatóság köteles adatvédelmi audit alá vonni[723] (szemben a Rendelettervezet szövegezésével, amely az adatkezelők jogává tenné, hogy adatvédelmi tanúsítványt kérjenek valamely tagállami hatóságtól).

A hatóság az audit eredményét az auditról készített értékelésben rögzíti, amelyben javaslatokat fogalmazhat meg az adatkezelő számára.[724] Az értékelés tehát sem az adatkezelőre, sem a hatóságra nézve nem kötelező. Önmagában az értékelésben foglaltak nem teljesítése jogkövetkezményt nem von maga után, de a javaslatok megvalósítása a jogszerű működésnek sem garanciája. A törvény nem rendelkezik arról, hogy az adatvédelmi hatóság ad-e ki olyan tanúsítványt, amely szerint az adatkezelő, illetve az adott adatkezelés jogszerű. A Hatóság audit szempontrendszere erről szintén hallgat, de részletezi az értékelés elkészítésének menetét,[725] így összességében egyértelművé válik, hogy tanúsításra (tanúsítvány kiadására) nem kerül sor.

A törvényszöveg alapján önmagában nem lenne világos, hogy az auditálás során figyelembe vett értékelési szempontok mennyiben haladhatják meg a törvényi követelményeket.[726] E tekintetben az audit szempontrendszer közvetve eligazítást ad: a Hatóság csak alkalmassági auditot végez, így a belső szabályzatokat „méri" az Infotv. rendelkezéseihez – a törvényi előírásnál magasabb mércét viszont éppen a belső szabályzatok írhatnának elő, az ezeknek való megfelelés pedig csak megfelelőségi audit keretében lenne mérhető.

A hatósági audit szabályozásával kapcsolatban a legérzékenyebb kérdés az audit és más hatósági eljárások viszonya. Felmerül például a kérdés, hogy mi történik akkor, ha az adatvédelmi audit során a Hatóság jogellenes adatkezelést tár fel, illetve az, hogy miként biztosítható a különböző típusú eljárások egymástól való elválasztása.

A törvény kifejezetten rögzíti, hogy az adatvédelmi audit a hatóság egyéb hatásköreinek gyakorlását nem korlátozza. Így elvi szinten az sem kizárt, hogy az auditról készített értékelés nincs összhangban egy későbbi közigazgatási határozattal. A Hatóság audit módszertana igyekszik e kérdést rendezni, és kifejti, hogy az „auditra az adatkezelő számára nyújtott segítségként érdemes tekinteni", és „az a célja, hogy elősegítse az adatkezelő számára az adatvédelmi előírásoknak történő minél teljesebb megfelelést",[727] és a Hatóság az auditot nem bírságolást elősegítő eszköznek, hanem „figyelemfelkeltő, tudatosságot erősítő, mediáló" eszköznek tekinti. Amennyiben az adatvédelmi audit során jogellenes adatkezelésre derül fény, a Hatóság a végleges értékelés kibocsátása előtt megfelelő határidő tűzésével felszólítja az adatkezelőt a jogellenesség orvoslására. Ugyanakkor, ha az adatkezelő ennek nem tesz eleget, akkor a Hatóság fenntartja a jogot arra, hogy az audit keretein kívüli eszközzel kényszerítse ki a jogellenesség megszüntetését. Emellett, ha a Hatóság az adatvédelmi audit keretében bűncselekményt

[723] NAIH, 2013, 11.
[724] Infotv. 69. § (4)
[725] NAIH, 2013, 13.
[726] A külföldi példák arra mutatnak rá, hogy az adatvédelmi hatóság által végzett auditálás is legalább részben az adatvédelem törvényi előírásait meghaladó, az adatkezelő önkéntes vállalásain alapuló adatvédelmi követelmények teljesítésének minősítésére irányul.
[727] NAIH, 2013, 5.

észlel, vagy olyan információkat talál, amelyek alapján kötelező az adatvédelmi hatósági eljárást megindítani, akkor a Hatóság az adatkezelő értesítése mellett a szükséges intézkedéseket megteszi. Mindenképpen pozitívum a személyi összeférhetetlenség biztosítása: az audit szempontrendszer rögzíti, hogy a Hatóság adatvédelmi auditban résztvevő munkatársai az adatkezelővel szemben indított adatvédelmi hatósági eljárásában nem vehetnek részt.[728]

Álláspontom szerint a különböző eljárások közötti „átjárhatóság" kezelése korántsem megnyugtató, ez a probléma elsősorban a törvényi szabályozásból következik. Jelenleg úgy tűnik, hogy a jogintézmény kockázata éppen az, hogy a hatósági és nem hatósági jogköröket a jogalkotó nem tudta következetesen szétválasztani, és az adatkezelő kénytelen annak kockázatát vállalni, hogy a Hatóság jogellenes adatkezelést tár fel, és ezért végső soron akár bírsággal is sújtja az adatkezelőt.[729] Erre a gyakorlatban egyelőre azért kicsi az esély, mivel a Hatóság jelenleg csak alkalmassági auditot végez, azaz az adatkezelő ténylegesen megvalósuló gyakorlatát nem, csak a dokumentáció törvénynek való megfelelését vizsgálja.

Más jogterületeken[730] az auditálást rendszerint nem valamely hatóság végzi, hanem szakmai, gazdasági szervezetek, és legfeljebb e szervezet ellenőrzését, regisztrációját látja el az ágazati hatóság. Az auditálás eredménye általában egy olyan tanúsítvány, amely valamely minőségi követelményrendszernek való megfelelést igazol. A tanúsítvány feltétele lehet bizonyos tevékenység végzésének, de adott esetben kizárólag valamely feltételezett piaci előny kapcsolódik hozzá. Az auditálás intézményének törvénybe foglalása ugyanakkor nem zárja ki a piaci alapon működő adatvédelmi auditálás és tanúsítás lehetőségét, amelynek jelentős előnye lehet például a tanúsító szerv általi felelősségvállalás, amely kiterjedhet – a tanúsítás által meghatározott területen – a tanúsított szerv által esetlegesen okozott kárért, vagy a szervezetet ért adatvédelmi bírságokért való helytállásért is.

A létező európai példák, és az új európai Rendelettervezet „hibrid" megoldása mellett is azt gondolom, hogy az adatvédelmi auditálást elsősorban piaci szereplők által szerencsés végezni. Ez esetben mindenképpen biztosítható az auditált vállalkozás adatainak bizalmas kezelése, a hatósági ellenőrzéstől teljes mértékben elkülönült auditálási és tanúsítási folyamat, valamint – a polgári jogi szabályok alapján – egyértelművé tehetők a tanúsítvány kibocsátásával vállalt felelősségi kérdések. Az adatvédelmi auditálás és tanúsítás jól illeszthető a már létező információbiztonsági szabványokkal kapcsolatban kialakult gyakorlatba, az ezeknél alkalmazott módszerek nagyrészt az adatvédelmi jogi auditnál is alkalmazhatók. Véleményem szerint szerencsésebb lett volna a hatályos szabályozás helyett a piaci szereplők által végzett adatvédelmi tanúsítás feltételeit törvényben rögzíteni. Ilyen feltételek lehetnek például a tanúsítást végző szervek nyilvántartásba vételi kötelezettsége, az auditorrá válás meghatározott feltételekhez kötése, a felelősségi

[728] NAIH, 2013, 16.
[729] Határozott kritikát fogalmaz meg ezzel kapcsolatban Majtényi László is (Majtényi, 2011, 113.)
[730] Ld. például 2009. évi CXXXIII. törvény a megfelelőségértékelő szervezetek tevékenységéről; 2001. évi XXXV. törvény az elektronikus aláírásról

kérdések szabályozása. Ennek hiányában a piaci alapú adatvédelmi audit jelenleg a polgári jog általános szabályai szerint végzett tanácsadási tevékenység keretében folytatható.

Ugyanakkor a jelenlegi magyar törvényi szabályozás az adatkezelők kifejezett kérésére történő hatósági auditról rendelkezik, így megfér egymás mellett a hatóság által végzett és a piaci alapon végzett auditálás intézménye. Az adatkezelők az egyes eljárások előnyeit és hátrányait (ideértve az audit és a hatósági eljárások egymáshoz való viszonyából eredő kockázatot is) egyaránt mérlegelve eldönthetik, hogy számukra melyik auditáló szervezet kívánatos. A hatóság eljárása elsősorban az állami, önkormányzati szervek számára lehet vonzó (egyes külföldi szabályozási minták kizárólag állami szervek számára teszik lehetővé a hatósági által végzett auditálást), amelyeknek üzleti titkai nincsenek, és forrásaik szűkössége miatt a piaci alapon végzett auditálás nem feltétlenül elérhető számukra.

4.4.6.3 Adatvédelmi tanúsító-rendszerek

A fenti példák mellett vannak tisztán piaci alapon működő, for-profit tanúsító-rendszerek is, amelyek elsősorban az Egyesült Államokban tevékenykednek.

A legismertebb ilyen szervezet a TRUSTe,[731] amelynek fő célja, hogy bizalmat keltsen az online szolgáltatók adatvédelmi politikája iránt. A szervezet mind az iparági szereplőktől, mind a kormányzattól független. A TRUSTe által kiadott logót a különböző tanúsítási szolgáltatások által támasztott feltételeknek megfelelő, illetve a vitarendezési eljárásnak magukat alávető adatkezelők használhatják. A logót látva a felhasználó könnyen informálódhat arról, hogy az oldal meghatározott adatvédelmi elveket követ, illetve panaszával meghatározott vitarendező fórumhoz fordulhat.[732] A TRUSTe szolgáltatásai tanácsadásra, auditra, vitarendezésre és tanúsításra is kiterjednek, ugyanakkor maga nem dolgozott ki önálló magatartási kódexet, hanem más szervezet által kidolgozott szabályrendszereknek vagy iparági „legjobb gyakorlatoknak”[733] való megfelelést igazol, így a szolgáltatásai között szerepel a Safe Harbour egyezménynek, a gyermekek internetes védelméről szóló jogszabálynak vagy éppen az APEC[734] határokon átnyúló adatvédelmi szabályainak[735] való megfelelés tanúsítása.[736]

A TRUSTe felügyeleti tevékenysége keretében alapos auditot ugyan nem folytat, de gyakran regisztrál és megad bizonyos adatokat partnerei oldalain, hogy e próbaregisztrációval ellenőrizhesse az adatvédelmi elvek betartását.[737] Panasz esetén azonban szélesebb jogorvoslati lehetőségek állnak rendelkezésre. A TRUSTe szankciórendszere keretében az elveket be nem tartó adatkezelőket felszólíthatja az adatvédelmi politikája módosítására, vagy arra, hogy azt vesse alá harmadik fél által

[731] A tanúsító-szervezet honlapja: www.truste.com
[732] Jóri, 2005, 54.
[733] Megjegyezzük, hogy a tanúsítás során a legjobb gyakorlatra történő utalás igen bizonytalanná teszi a tanúsító logó mögötti tényleges szabályrendszer tartalmát, a fogyasztók ugyanis vélhetően nincsenek tisztában a legjobb gyakorlat tartalmával, ami ráadásul átláthatatlanul változhat is.
[734] Asia-Pacific Economic Cooperation
[735] Cross Border Privacy Rules
[736] Ld. erről a TRUSTe honlapját: http://www.truste.com/industry-solutions/b2c-brands [2014.05.22.]
[737] Bennett – Raab, 2006, p 164-165.

végzett auditnak, súlyosabb esetben a felügyelő hatósághoz (az Egyesült Államokban az FTC-hez) fordulhat, végül visszavonhatja a logó használatának jogát.[738]

Egy másik jelentős tanúsító-szervezet a BBB Online,[739] amelynek működése nagymértékben hasonlít az imént bemutatott modellhez. A Safe Harbour tanúsítási szolgáltatást leszámítva a weblapjuk alapján azonban nem egyértelmű, hogy az adatvédelem területén pontosan milyen szabályok/elvek betartását várják el a tanúsított szervezetektől. A legkomolyabb követelményeket kétségkívül a WebTrust nevű tanúsító-szervezet támasztja, amely azzal is jár, hogy kevesebb adatkezelő használja a rendszerüket.[740]

A tanúsító-rendszerek legnagyobb előnye, hogy elvileg alkalmasak arra, hogy egyszerűen (és gyorsan) informálják a fogyasztót az adott adatkezelő adatvédelmi megfeleléséről, és segítenék az informált döntéshozatalát.[741]

Ugyanakkor számos kritikai észrevétel is tehető. Mindenekelőtt látható, hogy ezeknél a rendszereknél az alapos auditáláshoz és szigorú szabályok következetes érvényesítéséhez képest a tanúsítvány kiadása, és – a tanúsító-szervezetek üzleti logikájából következően – a tanúsító védjegy minél szélesebb körű alkalmazása áll a középpontban. Honlapjaik alapján igen nehéz megtudni, hogy pontosan milyen adatvédelmi követelményeknek kell megfelelniük a logót használó szervezeteknek, néhol csak a „legjobb gyakorlatra" való utalás található. A tanúsítás során a legfőbb követelmény az, hogy az adatkezelőknek legyen valamilyen adatvédelmi politikájuk, amit be is tartanak, és ami megfelel bizonyos (nem túl szigorú) privacy-alapelveknek. Jellemzően e rendszerek keretében tehát nem készül önálló magatartási kódex, hanem már kidolgozott normarendszernek, például a már említett Fair Information Principles Practices-nek kell megfelelni. A tanácsadás és a megfelelés ellenőrzése (kvázi audit) és a tanúsítás nem válik el élesen egymástól. A szabályozás teljes hiányához képest a tanúsítvánnyal rendelkező vállalkozások bizonyosan magasabb védelmi szintet garantálnak, de ez jellemzően nem éri el az európai jogszabályi követelmények szintjét.

Ráadásul minél szigorúbbak a csatlakozás feltételei, minél magasabb védelmi szintnek kell megfelelni, és ezáltal minél magasabb lehetne a fogyasztói bizalom, annál kevesebb adatkezelő fog a rendszerhez csatlakozni. Az adatkezelők így a nyereségérdekelt és versengő szolgáltatók közül inkább egy csekélyebb (akár minimális) követelményeket támasztó tanúsító-szervezetet választanak.[742]

További releváns kritika, hogy a valóságban egyik sem ért el széleskörű elfogadottságot, így ironikus módon, minél több van belőlük, annál jobban összezavarja a fogyasztókat.[743] Célszerű lenne ezért a versengő hitelesítő programok értékelésének szempontjait

[738] Jóri, 2005, 55. A vitarendezési eljárásról ld. részletesen Jóri, 2005, p 55-56.
[739] A szervezet weblapja: www.bbb.org
[740] Bennett-Raab, 2006, 166-167.
[741] Több, az adatvédelmi szabályozást érintő kritikai észrevételnek eleme, hogy a fogyasztó nehezen és jelentős energiaráfordítással szerezhet csak kellő információt az adott szolgáltató adatvédelmi politikájáról és az annak való megfelelésről.
[742] Bennett – Raab, 2006, 167.
[743] Bennett – Raab, 2006, 167.

ugyancsak szabványba foglalni.[744] A tanúsító rendszerek gyengéje továbbá, hogy mivel nem túl elterjedtek, ezért a rendszerek legfőbb (és amúgy ritkán alkalmazott) szankciója, a logó használatának visszavonása nem hatékony, a felhasználók ugyanis nem hiányolják azt.[745]

4.4.7 Az adatvédelmi audit és tanúsítás a Rendelettervezetben

4.4.7.1 A Rendelettervezet szövegjavaslata

Újdonságként került be a 2012-es bizottsági szövegtervezetbe egy adatvédelmi tanúsítással és címkézéssel kapcsolatos cikk, amely szerint (meglehetősen soft law jellegű megfogalmazással) a tagállamok, valamint a Bizottság – különösen európai szinten – ösztönznék olyan adatvédelmi tanúsítási mechanizmusok és adatvédelmi címkék és jelzők létrehozását, amelyek segítségével az érintettek gyorsan fel tudják mérni az adatkezelő és az adatfeldolgozó által biztosított adatvédelem szintjét.[746] Ugyanakkor e „szándéknyilatkozat" komolyságát mutatta, hogy a Bizottság felhatalmazást kapott volna az adatvédelmi tanúsítási mechanizmusokra vonatkozó szempontok és követelmények meghatározása érdekében további jogi aktusok elfogadására.[747]

Az Európai Parlament által elfogadott javaslat azonban ennél lényegesen továbbmegy. Az új 39. cikk szerint bármely adatkezelő vagy adatfeldolgozó ésszerű, az adminisztratív költségeket figyelembe vevő díj ellenében bármely uniós felügyelő hatóságot felkérheti annak tanúsítására, hogy a személyes adatok feldolgozása megfelel e rendeletnek, (különösen az adatkezelő és az adatfeldolgozó kötelezettségeire és az érintettek jogaira vonatkozó szabályoknak). A tanúsításnak önkéntesnek, megfizethetőnek, valamint hozzáférhetőnek kell lennie.[748]

Ezek a rendelkezések tehát kötelezik a tagállami hatóságokat arra, hogy audit-szolgáltatást nyújtsanak az adatkezelők számára, ráadásul rögtön „versenyhelyzetbe" is hozva őket, mivel az adatkezelők bármely tagállam hatóságához fordulhatnak (ennek legfeljebb a nyelvi korlátok szabhatnak határt egyes adatkezelőknél).

A versenyhelyzetet enyhítendő a tervezet együttműködést és az eljárási díjak harmonizálását írja elő,[749] ami ugyanakkor egyes kevésbé fejlett EU tagállamokban akár irreálisan magas díjakat is eredményezhet. Mindegyik tagállami hatóság azonos feltételek teljesítését tanúsító, egységesen „európai adatvédelmi címke"[750] elnevezésű tanúsítványt és címkét bocsát ki. A tanúsítvány addig érvényes, amíg a tanúsított adatkezelő vagy adatfeldolgozó adatfeldolgozási műveletei maradéktalanul megfelelnek a rendeletnek, legfeljebb azonban öt évig. Az érvényes és érvénytelen tanúsítványok nyilvános elektronikus nyilvántartásban bárki számára hozzáférhetőek.[751]

[744] Jóri, 2005, 58.
[745] Schwartz gondolatait idézi Jóri, 2005, 63.
[746] Bizottsági tervezet, 39. cikk (1) bekezdés
[747] Bizottsági tervezet, 39. cikk (2) bekezdés
[748] Rendelettervezet, 39. cikk (1a)-(1b)
[749] Rendelettervezet, 39. cikk (1c)
[750] "European Data Protection Seal"
[751] Rendelettervezet, 39. cikk (1e)-(1h)

A Rendelettervezet gondol a hatósági kapacitások szűkösségére is, ezért lehetővé teszi számukra, hogy harmadik félként eljáró, akkreditált ellenőröket (lényegében piaci szereplőket) vegyen igénybe az auditálás során. A Rendelettervezet előír néhány általános jellegű minimumfeltételt, miszerint e szereplőknek megfelelő képzettséggel kell rendelkezniük és pártatlannak (összeférhetetlenségtől mentesnek) kell lenniük. A piaci szereplők közreműködése mellett a „végleges tanúsítást" és a tanúsítvány kibocsátását a hatóság végzi el.[752]

Végül az új szövegváltozat is felhatalmazást ad a Bizottságnak további jogi aktusok elfogadására, valamint az Európai Adatvédelmi Testületnek arra, hogy valamely műszaki szabvány rendelettel való összhangját megállapítsa.[753]

4.4.7.2 A tervezett rendelkezések értékelése

Meg kell jegyezni, hogy a tervezett Rendelet elfogadása a Európai Parlament márciusi döntése ellenére igen lassan halad, és jelentős módosítások várhatóak, ugyanakkor a változások iránya egyértelmű: az új európai adatvédelmi szabályozási keretek között az adatvédelmi auditnak és tanúsításnak a korábbinál lényegesen nagyobb szerepe lehet.

A jelenlegi szövegtervezet egy sajátos, a hatósági tanúsítási modell és a piaci szereplők által végzett tanúsítási modell között „félúton" elhelyezkedő, hibrid megoldásra tesz javaslatot. Továbbra is szerencsésebbnek tartanám az adatvédelmi hatóságok szerepének csökkentését. A tanúsítást piaci szereplőkre kellene bízni azzal, hogy az audit és tanúsítás személyi és szervezeti feltételeire, részletes menetére, a megfizethetőség érdekében akár az eljárási díjak maximalizálására közös és kötelezően alkalmazandó szabályok készülnének.

A Rendelettervezetben foglalt javaslat azonban két ponton nagyon jól reagál a tanúsító-szervezetek kapcsán felvetett problémákra: először is egyértelművé teszi, hogy az auditálás a Rendeletnek való megfelelést vizsgálja, elejét véve azoknak a – főleg az ezredforduló környékén Németországban lefolytatott – vitáknak, hogy az auditálás vajon a jogszabályi követelményeknél szigorúbb előírások meglétét feltételezi vagy sem. Ugyanakkor az amerikai tanúsító-szervezetek kapcsán épp az ellenkező probléma merült fel: valójában nem mindig lehet pontosan tudni, hogy milyen normarendszernek felelnek meg a tanúsítványnal rendelkező vállalkozások, de az szinte bizonyos, hogy nem túl szigorú szabályoknak. A magam részéről a Rendelettervezet megközelítésével egyetértek: az adatvédelem jogszabályi szintű követelményei Európában – különösen a Rendelettervezet elfogadása esetén – kellően szigorúak, az annak való megfelelés önmagában magas adatvédelmi szintet biztosít. E szint előírása indokolt, ennél magasabbat azonban várhatóan kevesen tudnának teljesíteni. A javaslat másik igen előremutató eleme az egységesítés: a közös normának (a Rendeletnek) való megfelelés egységes címkével való jelölése ugyanis megszünteti a tanúsítványok közötti versenyt, vagy legalábbis kiemelt helyzetet biztosít egy konkrét tanusítványnak. Ez a tanúsítórendszerek kapcsán felvetett problémákat nagyrészt orvosolja: a felhasználók nem vesznek el a különböző tanúsítványok között, és a várhatóan széles körű alkalmazás miatt a tanúsítvány visszavonása valós szankció lehet.

[752] Rendelettervezet, 39. cikk (1d)
[753] Rendelettervezet, 39. cikk (1i)-(2)

4.5 Lépések egy belső szabályozási rendszer kiépítése felé

4.5.1 Bevezető gondolatok

Az előző fejezetekben részletesen áttekintett tendenciák egyik következménye, hogy megnő az adatvédelem belső, intézményi szintű szabályozásának jelentősége. Erre tekintettel indokolt lehet a belső szabályozási rendszer kialakításához vezető út – deklaráltan a teljesség igénye nélküli[754] – főbb mérföldköveinek kijelölése. E fejezet, mintegy problématérképként funkcionálva, segítséget jelenthet az adatkezelők számára a compliance kötelezettségeknek való tervszerű megfeleléshez.

Ezen áttekintés szükségszerűen általános, mivel így széles körben hasznosulhat. Az áttekintés független az adott adatkezelő jellemzőitől (állami szerv vagy piaci szereplő, méret, szervezeti felépítés stb.), valamint az éppen aktuális pozitív jog részletszabályoktól, így annak változása esetén, illetve a különböző európai államokban is alkalmazható. Ennek érdekében a fogalmak, problémakörök és követelmények tekintetében alapvetően a hatályos adatvédelmi irányelv rendelkezéseiből indulok ki, utalva olykor a tagállami (és különösen a magyar) eltérő szabályok lehetőségére, valamint alkalmanként előretekintve az új adatvédelmi rendelettervezet szabályaira is.

E fejezet célja, hogy bemutassa azokat a kérdésköröket, amelyekre egy adatkezelőnek vagy adatfeldolgozónak a belső szabályozásának kialakítása során figyelmet kell szentelnie. Az egyes adatvédelmi értelmezési problémákra csupán felhívom az adatkezelők figyelmét, nem kívánom – és egy adott adatkezelés részletes ismerete nélkül nem is lehetséges – e problémákat megoldani. Elsősorban tehát arra koncentrálok, hogy hogyan tudja az adatkezelő megtenni azokat az első lépéseket, amelyek végső soron biztosítják az adatkezelések törvényességét.[755]

A belső szabályozás kialakításának főbb pillérei:

1) az adatkezelések katalogizálása;
2) az adatvédelmi kötelezettségek számbavétele;
3) a dokumentáció elkészítése;
4) a végrehajtás belső mechanizmusainak kialakítása (azaz a működés hozzáigazítása a szabályokhoz).

4.5.2 Az adatkezelések katalogizálása

Az adatkezelők első feladata mindenképpen az adatkezeléseik feltárása, azok katalogizálása. E nélkül nem lehetséges az alkalmazandó szabályok kiválasztása sem. Az adatkezelőnek mindenekelőtt meg kell állapítania, hogy

[754] A belső szabályozási rendszer minden kérdésre kitérő áttekintése csak egy meghatározott konkrét adatkezelőnél lenne lehetséges, mivel az adatkezelésre számtalan szektorális szabály is vonatkozik, amelyek jelentősen befolyásolják egy adatkezelő jogait és kötelezettségeit.

[755] A fejezet során részletezett lépések részben korábbi kutatási eredményekre támaszkodnak. Egy 2011-2012 során folytatott, a munkahelyi adatvédelemre vonatkozó kutatás keretében kutatótársaimmal, Dr. Rátai Balázzsal és Dr. Szádeczky Tamással kidolgoztuk egy (munkahelyi adatvédelmet szabályozó) magatartási kódexet adott szervezeti keretek közé történő implementálásának néhány lépését. Ennek eredményeit ld. Rátai – Szádeczky – Szőke, 2012

- hozzáfér-e személyes adatnak minősülő adathoz;
- végez-e velük olyan műveletet, ami adatkezelésnek vagy adatfeldolgozásnak minősül;
- a szervezet adatkezelőnek vagy adatfeldolgozónak minősül-e;
- az adatkezelésnek melyek a főbb jellemzői (célja, jogalapja, további körülményei).

Hangsúlyozandó, hogy a katalogizálást elvileg a tervezett adatkezelésekre – amennyiben azonban ez korábban elmaradt, úgy persze a már folyamatban lévő adatkezelésekre – kell elvégezni.

A fentiek alapján az adatkezelő kap egy statikus képet a (tervezett) adatkezeléseiről. Érdemes emellett egy, az adatok életútját feltérképező, dinamikus képet mutató elemzést is végezni, amely végigköveti az adat útját attól a ponttól kezdve, hogy az adatkezelő először hozzáfér az adott adatokhoz, egészen addig, amíg ez a hozzáférés megszűnik (adatéletciklus-elemzés).

4.5.2.1 Személyes adat és a különleges adat meghatározása

A hatályos adatvédelmi irányelv alapján személyes adat „az azonosított vagy azonosítható természetes személyre (érintettre) vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén.”[756] A magyar Infotv. ugyan külön határozza meg az érintett és a személyes adat fogalmát, de tartalmilag teljesen megfelel az irányelv rendelkezéseinek. A Rendelettervezet a hatályos irányelv fogalmával lényegében megegyező definíciót tartalmaz.[757]

Az elsőre egyszerűnek és igen tágnak tűnő definíció kapcsán a legfontosabb gyakorlati kérdés az ún. abszolút és relatív értelmezés kérdése. A (szélsőségesen) abszolút értelmezés szerint személyes adatnak minősül egy adat, ha az adat és a személy közötti kapcsolat elvileg megteremthető. Amennyiben tehát az érintett akár több különböző adatkezelőnél lévő adatok segítségével, több lépésben, különböző technikai eljárásokkal (például titkosított adatok dekódolásával), de végül is azonosítható, akkor – függetlenül attól, hogy az adott adatkezelőnek van-e tényleges vagy jogszerű lehetősége erre – az adatot személyes adatnak kell tekinteni. Ez az értelmezés a személyes adat fogalmát igen tágra szabja. A relatív értelmezés szerint egy adat személyes adat jellegét az adatkezelő szempontjából kell vizsgálni: amennyiben az adatkezelő ténylegesen nem képes az általa kezelt adatokat az érintetthez kötni, úgy az adat e vonatkozásban (ezen adatkezelőnél) nem minősül személyes adatnak.[758]

Valójában e két értelmezés között számtalan köztes megközelítés lehetséges. Az irányelv preambuluma szerint annak meghatározására, hogy egy személy azonosítható-e, minden

[756] 95/46/EK 2. cikk a) pont
[757] Az azonosíthatóság szempontjai közé bekerült a név, a helymeghatározó adatok, és a nemi identitás, a felsorolás példálózó jellegére tekintettel ez azonban nem jelent érdemi változást (Rendelettervezet, 4. cikk 2. pont). A Rendelettervezet bevezetni tervezi az „álneves adat” és a „kódolt adat fogalmakat (Rendelettervezet 4. cikk 2a és 2b pont), igaz, összességében igen kevés „enyhítő” szabályt fűz az ilyen adatok kezeléséhez.
[758] Az abszolút és relatív értelmezésről ld. Majtényi, 2006, 110-113., Jóri, 2005, 101-104.

olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy ésszerűen feltehetően felhasználna az említett személy azonosítására.[759] A 29-es munkacsoport véleménye alapján jelentősége lehet többek között az adatkezelés céljának: ha az adatkezelő célja az esetleges azonosítás, úgy akkor is személyes adatnak kell tekinteni a kezelt adatokat, ha a tényleges azonosításra csekély reális esély van. Emellett fontos szempont lehet, hogy az azonosítást milyen technológiával és milyen költséggel lehet elvégezni, és e költség milyen arányban áll az adatkezelő által elérni kívánt céllal: „egy dinamikus próbáról van szó, és tekintetbe kell venni a[z adatkezelés idején] hozzáférhető csúcstechnológiát, valamint a fejlesztés lehetőségeit is azon időszak tekintetében, amelyre vonatkozóan az adatokat [kezelik].”[760] Végül praktikus korlátja lehet az azonosításnak, ha ahhoz más adatbázisokhoz való jogosulatlan hozzáférés vagy a titoktartási szabályok megsértése szükséges.[761] Az EU irányelve tehát tulajdonképpen egy „köztes” értelmezést követ, amely végül is teret enged a különböző tagállami szabályozásokra.[762] Összességében a gyakorlatban a konkrét adatok és tervezett műveletek összes körülményét mérlegelve lehet megállapítani, hogy a kérdéses adatok személyes adatoknak minősülnek-e.

Az adatvédelmi jogszabályok egyes személyes adatokra eltérő szabályokat állapíthatnak meg, ezek azonosítása szintén fontos része az adatkezelések katalogizálásának. A legfontosabb ilyen kategória a különleges adatok köre, amely az irányelv szerint felöleli a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkozó adatokat.[763] A különleges adatokon kívül is egyes ágazatokban számos további személyesadat-kategória található (a magyar jogban például különböző szakmai titkok, vagy a közérdekből nyilvános személyes adatok stb.), amelyre szintén tekintettel kell lenni, mivel nagymértékben meghatározzák, hogy a kezelt személyes adatokra milyen további jogszabályi követelmények vonatkoznak.

4.5.2.2 Az adatokon végzett műveletek és a szerepkör meghatározása

Amennyiben az adott szervezet arra jutott, hogy az általa hozzáfért adatok személyes adatnak minősülnek, úgy a következő fontos kérdés, hogy az azon végzett műveletek adatkezelésnek/adatfeldolgozásnak minősülnek-e.

Az irányelv szerint adatkezelésnek (az irányelv szóhasználatában adatfeldolgozásnak) minősül „a személyes adatokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés, továbbítás,

[759] 95/46/EK (26) preambulum-bekezdés. Az angol szöveggel szemben a magyar fordításból az ésszerűségre utalás kimaradt.
[760] WP29, 2007, 17. Az eredeti szöveg „adatfeldolgozás” terminológiát az idézetben „adatkezelés” kifejezésre cseréltük.
[761] Részletesen ld. WP29, 2007, 17-28.
[762] Ennek fényében talán nem meglepő, hogy a személyes adat abszolút-relatív értelmezése Európa szerte különböző. Néhány nemzeti példát ld. Polyák – Szőke, 2011, 157-158.
[763] 95/46/EK, 8. cikk. A különleges adatok köre tagállamonként némiképp eltérő lehet, a magyar szabályozás például az irányelvben felsoroltakon felül különleges adatnak tekinti a kóros szenvedélyre vonatkozó személyes adatokat, valamint a bűnügyi személyes adatokat is.

terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés".[764] A magyar adatvédelmi jog megkülönbözteti az adatkezelés és adatfeldolgozás fogalmát. Az adatkezelés fogalma lényegében megegyezik az irányelvével,[765] míg adatfeldolgozás alatt az Infotv. az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzését érti, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.[766] A magam részéről egyetértek Jóri András megállapításával, miszerint az adatkezelés – adatfeldolgozás tartalma az adatokon végzett műveletek alapján nem, csak az azt végző alanyok alapján határolható el egymástól. Egy adott műveletről önmagában nem lehetséges megmondani, hogy éppen adatkezelésnek vagy adatfeldolgozásnak minősül, az csak az azt végző személy vagy szervezet pozíciója alapján ítélhető meg.[767] A szerepkörök elhatárolásához egyébként sincs szükség magának a tevékenységnek a megkülönböztetésére, az az irányelvben és a magyar jogban is ismert adatkezelő-adatfeldolgozó fogalompáros segítségével megtehető.

Az irányelv szerint adatkezelő „az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját; ha a célokat és módokat egy adott nemzeti vagy közösségi jogszabály határozza meg, az adatkezelőt vagy a kinevezésére vonatkozó külön szempontokat ez a nemzeti vagy közösségi jogszabály jelöli ki",[768] míg adatfeldolgozó „az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely személyes adatokat dolgoz fel az adatkezelő nevében".[769]

Az adatkezelő és adatfeldolgozó között alapvetően szerződéses viszony áll fenn, a magyar jog alapján az adatfeldolgozói szerződést írásba is kell foglalni. Az adatfeldolgozó az adatkezelő utasításai alapján jár el, és érdemi döntést az adatkezeléssel kapcsolatban nem hozhat. A gyakorlatban az adatfeldolgozói jogviszony vagy magának az adatkezelésnek a kiszervezését jelenti, vagy olyan kiszervezett tevékenységhez kapcsolódik, amelyek során személyes adatokhoz való hozzáférésre is sor kerül. Fontos megjegyezni, hogy az adatfeldolgozónak történő adatátadás nem minősül adattovábbításnak és adatkezelési műveletnek, így ehhez önmagában nem szükséges külön jogalap. Az adatfeldolgozó számára a személyes adatokhoz való hozzáférés lehetőségét a szerződéses jogviszony biztosítja. Az adatfeldolgozó azonban saját célból adatkezelést nem végezhet, mivel ez esetben adatkezelőnek minősülne.[770]

[764] 95/46/EK, 2. cikk, b. pont
[765] A magyar jogszabály hosszabb példálózó felsorolást tartalmaz.
[766] Infotv. 3. § 10. és 17. pontok
[767] „Van-e olyan művelet, amely az adatkezelés körébe tartozhat-e, ám az adatfeldolgozás körébe nem? Van-e olyan adatfeldolgozási művelet, amely egyben ne minősülne adatkezelési műveletnek is? Álláspontunk szerint nincs: a két fogalom […] azonos terjedelmű. (Jóri, 2005, 154.)
[768] 95/46/EK, 2. cikk, d) pont
[769] 95/46/EK, 2. cikk, e) pont
[770] Ld. még az irányelv 17. cikk (3) bekezdését és az Infotv. 10. §-át.

4.5.2.3 Adatkezelés céljának és jogalapjának meghatározása

Amennyiben egy szervezet sikeresen azonosította az általa kezelt/feldolgozott személyes adatokat és tisztázta, hogy adatkezelőként (és nem adatfeldolgozóként) jár el, a katalogizálás következő lépése az adatkezelés céljának meghatározása, kissé leegyszerűsítve annak a kérdésnek a megválaszolása, hogy miért kezeli az adott személyes adatokat.

Az adatkezelési célok meghatározása kulcsfontosságú. Egyrészt ezek száma határozza meg az adatkezelések számát, azaz az adott szervezet adatkezeléseit alapvetően a célok alapján lehet elhatárolni egymástól, másrészt a célok szoros összefüggésben állnak az adatkezelés jogalapjával és az alkalmazandó jogszabályokkal is.

Az adatkezelési célok áttekintése kapcsán – mintegy nulladik lépésként – az adatkezelőnek meg kell határoznia, hogy az adatokat nem csupán a „természetes személyként, kizárólag személyes célra, vagy háztartási tevékenysége keretében”[771] végzi-e. Ez esetben ugyanis az adatkezelés kikerül az adatvédelmi jog tárgyi hatálya alól, és az adott természetes személy mentesül az adatvédelmi szabályok betartása alól. Megjegyzendő, hogy a nem természetes személy adatkezelőkre ez a kivételszabály nem alkalmazható.

Az adatkezelés céljának meghatározása elsőre egyszerűnek tűnhet ugyan, de a gyakorlatban korántsem az. A célok meghatározása során mindenekelőtt tekintettel kell lenni az ágazati adatvédelmi szabályokra, amelyek a legtöbb esetben tételesen meghatározzák a szabályozott adatkezelések célját – ez esetben az adatkezelőnek nincs mozgástere, az adatkezelési célok a jogalkotó döntésén alapulnak. Előfordulhatnak olyan esetek, amikor a jogszabály nem rendelkezik külön adatkezelési célokról, ebben az esetben a jogszabály által szabályozott jogviszony adja meg az adatkezelés célját.

Amennyiben az adatkezelés jogalapja nem jogszabály, az adatkezelőnek lényegesen szélesebb mozgástere van az adatkezelési célok meghatározásában. Különösen igaz ez a hozzájáruláson alapuló adatkezelésekre.

Az adatkezelés jogalapja kapcsán az adatvédelmi irányelv hat lehetőséget nyújt az adatkezelők számára. A 7. cikk szerint személyes adat akkor kezelhető, „ha

1) az érintett ahhoz egyértelmű hozzájárulását adta; vagy
2) az adatfeldolgozás olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges; vagy
3) az adatfeldolgozás az adatkezelőre vonatkozó jogi kötelezettségnek teljesítéséhez szükséges; vagy
4) feldolgozásuk az érintett létfontosságú érdekei védelméhez szükséges; vagy
5) az adatfeldolgozás közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges, vagy

[771] 95/46/EK, 3. cikk, (2) bekezdés. Az Infotv. tartalmilag azonos szabályát ld. Infotv. 2. § (4) bekezdés

6) az adatfeldolgozás az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettnek [a személyes adatok védelméhez fűződő joga]."

A jogalapok megválasztása sok esetben korántsem egyszerű feladat, és az adatkezelés jellegét nagymértékben meghatározza. A 2-4) pont viszonylag egyértelmű, az 5. pontban foglalt közérdekből történő adatkezelések pedig a tagállamok belső jogán, azaz jogszabályi felhatalmazáson alapulnak, amelyek rendszerint körülírják az adatkezelés feltételeit.

A hozzájáruláson alapuló adatkezelésnél kiemelendő egyrészt a tájékoztatás szerepe, amely – mivel az érintett az abban foglalt feltételekkel történő adatkezeléshez adja a hozzájárulását – teljes egészében meghatározza az adatkezelés körülményeit. Másrészt hangsúlyozni kell a hozzájárulás önkéntességét, amelynek körülményeit egy jogvita esetén a felügyelőhatóságok rendszerint alaposan vizsgálnak, és ami azt is jelenti, hogy a hozzájáruláson alapuló adatkezeléseknél az adatkezelőnek számolnia kell a hozzájárulás esetleges visszavonásával is.

A 6. pontban foglalt, érdekmérlegelésen alapuló adatkezelés lényegében az adatkezelőre bízza annak eldöntését, hogy a feltételek fennállnak-e, vagy sem. Ez, különösen más jogalap hiányában akár „kibúvónak" is tűnhet az adatkezelő számára, de az érdekmérlegelés szempontjai alapvetően kidolgozottak,[772] és az ezzel kapcsolatos döntéséért az adatkezelő természetesen felelősséggel tartozik. Így az érdekmérlegelésen alapuló adatkezeléseknél alapos körültekintés indokolt.

Előfordulhat, hogy egyes nemzeti jogszabályok (így például a magyar Infotv. is)[773] az egyes jogalapokat ettől némiképp eltérően határozzák meg. Az Európai Unió bírósága azonban az érdekmérlegelésen alapuló jogalap kapcsán kimondta, hogy a jogalap alkalmazásához fűzött további feltételek ellentétesek az irányelvvel, és az irányelv vonatkozó szakaszának (7. cikk f) pont) a tagállamokban közvetlen hatálya van.[774]

4.5.2.4 Adatkezelés további körülményeinek meghatározása

A katalogizálás során az adatkezelés célja és jogalapja mellett meg kell határozni az adatkezelés további körülményeit, így

- az érintettek körét és számát;
- a kezelt adatok körét (azonosító és leíró adatok);
- az adatok forrását (azaz azt, hogy miként kerültek az adatkezelőhöz)
- az adatkezelés módját (papír alapú, elektronikus, vagy vegyes);
- az adatkezelés helyét (akár fizikai akár virtuális értelemben, pl. egy weblap megjelölésével);
- az adatkezelés időtartamát (amelyet előírhat jogszabály, a hozzájárulás részét képező tájékoztatás, de az adatkezelés végét jelentheti a cél megvalósulása, illetve amennyibe az cél adatkezelés célja folyamatos, a hozzájárulás visszavonása is);

[772] Ld. erről részletesen: WP29, 2014
[773] Infotv. 5-6. §§
[774] C-468/10. és C-469/10. sz. egyesített ügyek. Az ítélet elemzését részletesen ld. Halász, 2012

- az adatokon végzett adatkezelési műveleteket.

Az utolsó pont kapcsán fel kell hívni a figyelmet egy kifejezetten „érzékeny” adatkezelési műveletre, a rendszeres vagy eseti adattovábbításra vonatkozó speciális szabályokra. Kiindulópontként az mondható, hogy az adattovábbítás, mint adatkezelési művelet ugyanazokkal a jogalapokkal lehetséges, mint bármely más adatkezelés. Különös szabályok vonatkoznak ugyanakkor a harmadik országba, azaz az Európai Gazdasági Térség (EGT) tagállamain kívülre történő adattovábbításokra, amelyekre az adatkezelőknek tekintettel kell lenniük.

4.5.3 Az adatvédelmi kötelezettségek számbavétele

Az adatkezelések katalogizálását követően érdemes vázlatosan, mintegy felsorolásszerűen („checklist-szerűen”) áttekinteni az adatkezelőkre vonatkozó főbb kötelezettségeket. Az adatkezelések számbavétele azért is különösen fontos az adatkezelőknél, mivel számos további adatvédelmi kötelezettségnek csak ennek segítségével tudnak eleget tenni, ugyanakkor egy alapos és naprakészen tartott „leltár” jelentősen meg is könnyíti e kötelezettségek teljesítését.

Az adatkezelő szempontjából a konkrét kötelezettségek összegyűjtésére a dokumentáció kialakításával párhuzamosan – az adatkezelőkre vonatkozó külső normák összegyűjtését követően – kerül sor. Meg kell jegyezni, hogy az ágazati szabályozások miatt általános jelleggel lehetetlen a kötelezettségek listáját a teljesség igényével összeállítani,[775] így jelen fejezetben az általános európai adatvédelmi szabályozásból eredő legfontosabb, alapvető kötelezettségek összegyűjtésére vállalkozom, utalva egyes esetekben a magyar jogra és a várható új összeurópai szabályozásra is.[776] Az egyes kötelezettségek rövid összefoglalását követően táblázatba foglalva utalok a kötelezettség tartalmának hatályos és várható jogforrására is.

Ezek alapján egy adatkezelő kötelezettségei az alábbiakban foglalhatók össze.[777]

1) Az alkalmazandó jog meghatározása.[778] Az adatkezelőnek, adatfeldolgozónak mindenekelőtt el kell döntenie, hogy mely állam jogát kell alkalmaznia, amely egy multinacionális vagy határokon átnyúló szolgáltatást nyújtó szervezet esetén nem is feltétlenül egyértelmű. A Rendelettervezet megalkotása jelentős lépés lehet az egységes európai szabályozás megtétele felé.

[775] A teljes lista csak a konkrét adatkezelések katalogizálása és a vonatkozó szabályok számbavételével lehetséges. Elképzelhető például, hogy egy meghatározott ágazatban tevékenykedő szervezetre az adott ágazatot érintő részletszabályok vagy a felügyelőhatóság valamely iránymutatása, joggyakorlata ró személyes adatot is érintő kötelezettséget, illetve valamely ágazati törvény az adatvédelem általános rendelkezéseit lex specialis-ként akár felül is írhatja.

[776] Itt is meg kell említenem, hogy a Rendelettervezet elfogadása illetve a végleges szöveg tartalma egyelőre bizonytalan, a jelenlegi tervezethez képest akár jelentős változások is elképzelhetők.

[777] A kötelezettségek egy többé-kevésbé logikus időrendi sorrendet mutatnak, sok esetben azonban a kötelezettségek csak egymásra tekintettel, párhuzamosan zajló folyamatokként teljesíthetőek. A lista tartalmazza a hatályos jog alapján még nem létező, de a Rendelettervezet alapján várható kötelezettségeket is, amelyeket a táblázatban dőlt betűvel jeleztem.

[778] irányelv, 4. cikk, Infotv. 2. § (1)-(3), Rendelettervezet, 3 cikk

2) Bejelentési kötelezettség.[779] A hatályos adatvédelmi rezsim egyik jelentős adminisztratív eszköze az adatkezelések – számos kivétellel megtört – felügyelő hatósághoz történő, az adatkezelés főbb jellemzőire vonatkozó bejelentési kötelezettsége. Az adatkezelések katalogizálását követően e szabályoknak könnyedén eleget lehet tenni, de sokszor felesleges adminisztratív tehernek tűnik. A Rendelettervezet – alapvetően az átláthatóságot biztosító számos más kötelezettségre tekintettel – eltörölni tervezi a bejelentési kötelezettséget.
3) Dokumentáció elkészítése és vezetése.[780] Részben épp a bejelentési kötelezettség kiváltására a Rendelettervezet kötelezi az adatkezelőket és adatfeldolgozókat rendszeresen felülvizsgált dokumentáció vezetésére.[781] Jelenleg ilyen kötelezettség expressis verbis nincs ugyan előírva, de egyrészt a hatósági bejelentés, másrészt az érintettek tájékoztatása miatt az adatkezelőnek mégiscsak át kell tekintenie az adatkezeléseit akkor is, ha azt nem foglalja össze „külön" dokumentációként.
4) Kockázatelemzés.[782] Az EU új adatvédelmi rendeletének tervezete alapján az adatkezelőknek kockázatértékelést kell végeznie,[783] hogy eldönthesse, hogy a tervezett adatkezelés "valószínűsíthetően különleges kockázattal" jár-e. Ez több további kötelezettséget (pl. adatvédelmi hatásvizsgálat vagy adatvédelmi felelős kinevezése) is megalapozhat.
5) Uniós képviselő kijelölése.[784] A Rendelettervezetre vonatkozó javaslat szerint az Európai Unión kívül letelepedett azon adatkezelők, amelyekre az alkalmazandó jog szabályai szerint az EU adatvédelmi joga kiterjed, kötelesek – meghatározott, a kockázatértékelés során megállapított feltételek teljesülése esetén – uniós képviselőt kijelölni.
6) Adatvédelmi felelős kinevezése.[785] Az adatvédelmi irányelv jelenleg lehetőségként utal az adatvédelmi felelős kinevezésére. Több tagállam, például Magyarország, meghatározott feltételek fennállása esetén kötelezően előírja adatvédelmi felelős kinevezését, és meghatározza a jogállásának főbb elemeit. A Rendelettervezet ezen a téren is jelentős előrelépést tesz, és a jelenleginél jóval szélesebb körben írja elő adatvédelmi felelős kinevezését, aki egy szervezeten belül kétségkívül a belső adatvédelmi szabályozás kialakításának és ellenőrzésének kulcsszereplője.
7) Adatvédelmi irányítás.[786] Az új Rendelettervezet egyik legjelentősebb újítása az adatvédelmi hatásvizsgálat és a rendszeresen elvégzendő adatvédelmi megfelelőségi vizsgálat (kvázi belső audit) kötelező bevezetése, mely intézkedéseket együtt az „adatkezelés teljes időtartamára kiterjedő adatvédelmi irányítás" cím alatt foglalja össze. A hatásvizsgálatot egy kivétellel minden

[779] Irányelv, 18-19. cikk, Infotv. 65-68. §§
[780] Rendelettervezet, 28. cikk
[781] Részletesen ld. a 3.4.1.2.1 fejezetet
[782] Rendelettervezet, 32a. cikk
[783] Részletesen ld. a 3.4.1.2.2 fejezetet
[784] Rendelettervezet, 25. cikk
[785] Irányelv, 18. cikk (2), Infotv. 24. § (1)-(2), Rendelettervezet, 35-37. cikk
[786] Rendelettervezet, 33-33a. cikk

„valószínűsíthetően különleges kockázattal járó adatkezelés” esetén el kell végezni, így a kötelezettség igen széles adatkezelői kört érint.[787]

8) Adatbiztonsági intézkedések megtétele.[788] Mind a hatályos, mind a várható új szabályozási rezsimnek hangsúlyos eleme az adatbiztonsági intézkedések megtétele, azaz megfelelő technikai és szervezési intézkedések végrehajtása a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében. Itt kell megemlíteni a beépített adatvédelem (Privacy by Design) követelményét,[789] amely jelenleg az irányelv még nem, de egyes nemzeti jogok (pl. a magyar jog) már nevesíthetnek, és amely az új szabályozás egyik fontos újítása is lesz. Bár maga az elv kellően általános, az új szabályozási keret lényege éppen abban áll majd, hogy az adatkezelőnek igazolnia kell tudnia, hogy milyen intézkedéseket tett meg ezen elvek érvényre juttatásáért. Összességében a megfelelő adatbiztonság tényleges kialakítása – gyakran egy ennél tágabb információbiztonsági rendszer részeként – elsősorban belső szabályozás, különböző szabványok és „jó gyakorlatok” kialakításával lehetséges.[790]
9) Adatvédelmi és adatbiztonsági szabályzat elfogadása.[791] A hatályos irányelv nem írja elő kifejezetten szabályzatok elfogadását, de a nemzeti jogalkotásban lehet erre példa, a magyar Infotv. – meghatározott adatkezelők számára – például előírja ezt a kötelezettséget. Az Rendelettervezet pedig szintén rendelkezik majd arról, hogy az adatkezelőknek „megfelelő politikákat” kell elfogadnia, ami az elszámoltathatóság követelményével összhangban értelmezve (miszerint az adatkezelőnek igazolnia kell tudnia az adatvédelmi szabályok betartását) írásbeli dokumentum megalkotásának kötelezettségét jelenti.
10) Előzetes ellenőrzés.[792] Jelenleg az irányelv lehetővé teszi, hogy a tagállamok meghatározzanak olyan adatkezelési műveleteket, amelyek különös kockázatot jelenthetnek, és amelyek esetén előzetes ellenőrzésre kerülhet sor. Az új Rendelettervezet – előzetes konzultáció elnevezéssel – szintén előírja, hogy meghatározott feltételek esetén a felügyelőhatósággal az adatkezelést megelőzően konzultálni kell.
11) Tájékoztatási kötelezettség.[793] A hatályos és a jövőbeni szabályozás is előírja az érintettek részletes tájékoztatását, amely minden jogalap „használata” esetén kötelező, de a hozzájáruláson alapuló adatkezeléseknél – a tájékozott hozzájárulás elve alapján – a tájékoztatás egyben meghatározza az adatkezelés körülményeit és terjedelmét is.
12) A célhoz kötöttség követelményének megtartása.[794] Az adatkezelés céljának és az adott célhoz szükséges adatkörök „egyszeri” meghatározása mellett e

[787] Részletesen ld. 3.4.1.2.3 fejezetet
[788] Irányelv, 16-17. cikk, Infotv. 7. §, Rendelettervezet, 30. cikk
[789] Infotv. 7. § (1), Rendelettervezet, 23. cikk
[790] Az adatbiztonságról és a beépített adatvédelem elvéről részletesen ld. 3.4.3.2 és 3.4.3.3 fejezeteket
[791] Infotv. 24. § (3), Rendelettervezet, 22. cikk, (1)-(1a)
[792] Irányelv, 20. cikk, Infotv. 68. § (3)-(5), Rendelettervezet, 34. cikk
[793] Irányelv, 10-11 cikk, Infotv. 20. §, Rendelettervezet, 13a-14. cikk
[794] Irányelv, 6. cikk (1) b-c. e., Infotv. 4. § (1)-(2), Rendelettervezet, 5. cikk, (1) b), c), e)

követelménynek az adatkezelés teljes folyamatát át kell hatnia. Az adatkezelőnek tartózkodnia kell a már kezelt személyes adatok eredetitől eltérő célra való felhasználásától, kivéve, ha arra egyébként szintén van valamilyen jogalapja.

13) Adatok pontosságának és időszerűségének (naprakészségének) biztosítása.[795] E követelmény a kezelt adatok minőségét hivatott biztosítani, a jelenlegi és a várható szabályozási rezsimben lényegében azonos tartalommal. A jogalkotó alapvetően az adatkezelőre bízza ezen elvek végrehajtását, de míg jelenleg ezzel kapcsolatban nincsenek előírva kézzelfogható követelmények, a várható szabályozás keretében az adatkezelőnek igazolnia kell tudnia, hogy miképpen biztosítja az adatok pontosságát és – amennyiben szükséges – az időszerűségét.
14) Érintetti jogok gyakorlásának biztosítása.[796] A jelenlegi, érintetti kontrollt középpontba helyező adatvédelmi szabályozás egyik kulcseleme az érintetti jogok: a tájékoztatáshoz, helyesbítéshez, törléshez és tiltakozáshoz való jog biztosítása. E jogosítványok a „másik oldalon" kötelezettségként jelenik meg. Az adatkezelőnek egyrészt ki kell alakítania valamilyen mechanizmusokat e jogok érvényesítésére, másrészt – és ez sokkal jelentősebb erőfeszítést igényel – úgy kell(ene) kialakítania az adatkezeléseinek technikai feltételeit, hogy az érintettek követelése valóban teljesíthető legyen. Ez különösen a törléshez való jog esetén okoz kihívásokat. Az érintetti jogokhoz kapcsolódik két további kötelezettség is. Először is tájékoztatni kell a személyes adatok címzettjeit arról, ha az érintett az adatok törlését vagy helyesbítését kérte.[797] Másrészt annak érdekében, hogy az érintettet az adattovábbításokról is tájékoztatni lehessen, adattovábbítási nyilvántartást kell vezetni.[798] A Rendelettervezet a jelenlegi jogosítványokat az adathordozhatósággal tervezi kiegészíteni, amely jelentős fejlesztési feladatot jelenthet egyes adatkezelőkre.
15) Átvett adatok kezelésére vonatkozó speciális szabályok.[799] A magyar Infotv. tartalmaz néhány speciálisnak tűnő, de az általános adatvédelmi szabályokból valójában különböző szabályt a más adatkezelőtől adattovábbítás során átvett adatok kezelésével kapcsolatban. Ennek lényege, hogy az átvevő adatkezelő köteles az adatokat az adattovábbítás során megadott esetleges (pl. cél, időtartam stb. tekintetében fennálló) korlátozásoknak megfelelően kezelni.
16) Adatvédelmi incidenssel kapcsolatos értesítési kötelezettség.[800] A jelenlegi szabályozáshoz képest igen jelentős többletkötelezettséget jelent az adatvédelmi incidensek esetére a Rendelettervezet által minden adatkezelőre kiterjeszteni tervezett[801] – a hatósághoz vagy magához az érintetthez címzett – értesítési

[795] Irányelv, 6. cikk (1) d., Infotv. 4. § (4), Rendelettervezet, 5. cikk, (1) d)
[796] Irányelv, 12-14. cikk, Infotv. 14-18., 21. §§, Rendelettervezet, 15-19. cikk
[797] Irányelv 12. cikk c), Infotv. 18. § (1), Rendelettervezet, 13. cikk. Az irányelv alapján e kötelezettség csak az érintett erre irányuló kérelme esetén áll fenn, a magyar és a tervezett EU szabályozás azonban – kivételekkel megtörve ugyan, de – az érintett kérelmétől függetlenül előírja.
[798] Irányelv, 12. cikk a) Infotv. 15. § (2), Rendelettervezet 15. (1) c). A hatályos irányelv alapján elegendő a címzettek kategóriáiról tájékoztatni az érintettet, amihez nem feltétlenül kell az adattovábbításokról nyilvántartást vezetni.
[799] Infotv. 9. §
[800] Rendelettervezet, 31-32. cikk
[801] A hatályos jogi környezetben a data breach notification csak a hírközlési szolgáltatókat terheli.

kötelezettség (data breach notification). Az e kötelezettségnek való megfelelés igen jelentős erőfeszítést és összetett belső mechanizmusok kialakítását kívánja meg az adatkezelő részéről.[802]

17) Automatizált egyedi döntésekre vonatkozó szabályok betartása.[803] A jogrendszer az érintetteket érintő, kizárólagosan „gépi" döntéshozatallal szembeni védelme érdekében korlátozó rendelkezéseket tartalmaz az ún. automatizált egyedi döntésre vonatkozóan: az csak meghatározott feltételekkel, megfelelő tájékoztatás mellett lehet jogszerű. Az erre vonatkozó szabályok az új Rendelettervezetben is hangsúlyosan megjelennek, az ilyen típusú döntéssel megtámogatott adatkezelési folyamatos adatkezelőinek tehát e korlátozásokra is tekintettel kell lenni.
18) Harmadik országba történő adattovábbítás szabályainak betartása.[804] Végül meg kell említeni, hogy mind a hatályos, mind a tervezett adatvédelmi keretrendszerben jelentős hangsúlyt kap az EGT országokon kívülre történő adattovábbítás kérdése. Ezen adatkezelési műveleteknek speciális jogalapjai és eljárási szabályai vannak, amelyeket – bizonyos feltételek fennállása, pl. az adatátvevő adatkezelő államának nem megfelelő szintű állami szabályozása esetén – éppen belső szabályozásban, kötelező vállalati szabályokban vagy szerződéses formában kell rögzíteni.

	Kötelezettség megnevezése	**Kötelezettségre vonatkozó szabályok**		
		Hatályos szabályozás		**Jövőbeni szabályozás**
		Irányelv	**Infotv.**	**Rendelettervezet**
Adatkezelés megkezdése előtt	Alkalmazandó jog meghatározása	4. cikk	2. § (1)-(3)	3 cikk
	Uniós képviselő kijelölése	-	-	*25. cikk*
	Bejelentési kötelezettség	18-19. cikk	65-68. §§	-
	Dokumentáció előkészítése (vezetése)	-	-	*28. cikk*
	Kockázatértékelés	-	-	*32a. cikk*
	Adatvédelmi felelős kinevezése	18. cikk (2)	24. § (1)-(2)	35-37. cikk
	Adatvédelmi irányítás (hatásvizsgálat és felülvizsgálat)	-	-	*33-33a. cikk*
	Adatbiztonsági intézkedések Privacy by Design	16-17. cikk -	7. § 7.§ (1)	30. cikk 23. cikk
	Adatvédelmi és adatbiztonsági szabályzat elfogadása	-	24. § (3)	22. cikk, (1)-(1a)
	Előzetes ellenőrzés	20. cikk	68. § (3)-(5)	34. cikk

[802] E kötelezettség minden adatkezelőre történő bevezetését nem tartom indokoltnak, mivel indokolatlan adminisztratív terhet ró a kisebb, az adatkezeléseket esetleg csak a főtevékenységét kiegészítő (járulékos) tevékenységként végző adatkezelőkre. Részletesen ld. 3.4.1.2.4 fejezetet
[803] Irányelv, 15. cikk, Infotv. 11. §, Rendelettervezet, 20. cikk
[804] Irányelv, 25-26. cikk, Infotv. 8. §, Rendelettervezet, 40-45. cikk

	Tájékoztatási kötelezettség	10-11 cikk	20. §	13a-14. cikk
Adatkezelés alatt	Célhoz kötöttség követelménye	6. cikk (1) b-c. e.	4. § (1)-(2),	5. cikk, (1) b), c), e)
	Adatok pontosságának és időszerűségének biztosítása	6. cikk (1) d.	4. § (4)	5. cikk, (1) d)
	Érintetti jogok gyakorlásának biztosítása	12-14. cikk	14-18., 21. §§	15-19. cikk
	A címzett adatkezelő értesítése a helyesbítésről, törlésről	12. cikk c)	18. § (1)	13. cikk
	Adattovábbítási nyilvántartás	12. cikk a)	15. § (2)	15. cikk (1) c)
	Átvett adatok kezelésére vonatkozó speciális szabályok	-	9. §	-
	Adatvédelmi incidenssel kapcsolatos értesítési kötelezettség	-	-	*31-32. cikk*
	Automatizált egyedi döntésekre vonatkozó követelmények	15. cikk	11. §	20. cikk
	Harmadik országba történő adat-továbbítás szabályainak betartása	25-26. cikk	8. §	40-45. cikk

2. sz. ábra. Az adatvédelmi kötelezettségek összefoglalása

4.5.4 A dokumentáció összeállítása

A belső szabályozás kialakításához mindenképpen szükséges a vonatkozó kötelező normák áttekintése és az azokkal összhangban álló belső dokumentáció kialakítása.[805] E két lépés időzítése jelentősen eltér egymástól. A külső normák áttekintése időrendben az adatkezelések katalogizálásával párhuzamosan, esetleg azt követően történik,[806] és értelemszerűen megelőzi az adatvédelmi kötelezettségek áttekintését, mivel a vonatkozó kötelezettségek éppen e forrásokban találhatók. A belső dokumentáció kialakítására a kötelezettség-katalógus összeállítását követően, a következő fejezetben áttekintett tényleges végrehajtási intézkedésekkel párhuzamosan zajlik, a dokumentumok elkészítése a folyamat szerves része.

1) Külső normák áttekintése

A külső normák mindenekelőtt a személyes adatok védelmére vonatkozó jogszabályokat, az ezek értelmezését segítő joggyakorlatot, valamint az adatkezelőn kívül elfogadott önszabályozási eszközöket jelentik. E jogforrások meglehetősen széles kört érinthetnek, ugyanis nem csak az általános és szektorális adatvédelmi normákat, hanem az egyéb, eredetileg nem kifejezetten adatvédelmi célú, de a személyes adatokat érintő normákat is jelentik.

2) Belső dokumentáció kialakítása

[805] Ld. erről Rátai – Szádeczky – Szőke, 2012, 304.

[806] Ideális esetben egy szervezet ismeri a tevékenységére vonatkozó normákat, ami gyakran meghatározza az adatkezelés körülményeit is. Nem kizárt azonban, hogy az adott szerv éppen az adatkezelések katalogizálása, a szükségesnek vélt adatkezelések tervezése vagy a tényleges adatkezelések feltárása során fedezi fel, hogy valamely jogszabályt alkalmaznia kell.

A belső dokumentációhoz különféle elnevezésű és funkciójú dokumentumok tartozhatnak, így például stratégiák, küldetésnyilatkozatok, szabályzatok, utasítások, tájékoztatók, policy-k, etikai kódexek, cselekvési tervek, eljárásrendek, munkaszerződések, adatfeldolgozói szerződések, hozzájárulás-nyilatkozatok, munkaköri leírások, hatóságokkal való kommunikáció dokumentumai, incidensekről, bejelentésekről, adattörlésről (selejtezésről), adattovábbításról készült jegyzőkönyvek, belső ellenőrzésről készült jegyzőkönyvek, jelentések, az adatkezelésre használt infrastruktúra jellemzőire vonatkozó információk stb.[807] E dokumentumok egyrészt a végrehajtási cselekmények elrendelését, másrészt az elvégzett cselekmények igazolását szolgálják.

4.5.5 A belső végrehajtási mechanizmusok kialakítása

A fentieket követően az adatvédelmi szabályok tényleges érvényesülését csak az biztosítja, ha az imént részletezett dokumentumokban foglaltak a gyakorlatban – „reálcselekmények" szintjén is – megvalósulnak, amelyet szintén kívánatos valamilyen formában dokumentálni, ez ugyanis egy esetleges auditálás és tanúsítás során auditbizonyítékként használható. Biztosítani kell tehát a szabályok szervezeti szinten történő végrehajtását, az adatkezelő tényleges működésének szabályokhoz való igazítását.

Egyes források, illetve az adatvédelmi tanácsadók e folyamatot gyakran adatvédelmi compliance stratégiának nevezik. Morgan és Boardman szerint a stratégia két legfontosabb eleme a politikák és eljárások kidolgozása, valamint a megfelelő személyzet kinevezése.[808]

A gyakorlati tapasztalatokat is figyelembe véve – a teljesség és egy komplett irányítási rendszer kialakításának igénye nélkül – véleményem szerint három kulcselemet érdemes figyelembe venni a belső szabályozás kialakítása során.

1) Szervezeti és személyzeti kérdések

Tisztázni kell, hogy az adott szervezetrendszeren belül pontosan melyik szervezeti egység milyen adatkezelési műveleteket végez, az adott műveleteknek ki a felelős vezetője, és ki jogosult az adatkezelések belső ellenőrzésére. Az egyes adatvédelemmel kapcsolatos feladatokat egyértelműen jelezni kell a szervezeti felépítésről szóló dokumentációban.[809] Amennyiben egy szervezet a célhoz kötöttség követelménye vagy más szempont alapján a szervezeten belül is korlátozza a személyes adatokhoz való hozzáférési jogosultságokat, úgy rendezni kell a hozzáférési jogosultságokra és a belső adattovábbításra vonatkozó szabályokat. Az egyes adatkezelésekkel kapcsolatos belső szervezeti kérdéseket célszerű az adatkezelések katalogizálása során is rögzíteni.

A személyzeti kérdésekkel kapcsolatban kiemelendő, hogy az egyes munkavállalók szintjén is egyértelművé kell tenni az adatkezeléssel kapcsolatos feladatokat és felelősségi viszonyokat, amelyeknek a munkaszerződésekben és a munkaköri leírásokban is meg kell jelennie.

[807] Más kontextusban, de a potenciális dokumentumokról ld. még Rátai – Szádeczky – Szőke, 2012, 307-308.
[808] Morgan – Boardman, 2012, 88.
[809] Ez lehet Szervezeti és Működési Szabályzat (SZMSZ), vagy bármilyen olyan dokumentum, amely a szervezeten belüli szervezeti egységeket és azoknak a feladat- és hatásköreit szabályozza.

Jelentőségénél fogva külön is hangsúlyozni kell az adatvédelmi felelős szerepét, akinek az adatvédelem belső szabályozásának kialakításában, működtetésében és felügyeletében is kulcsszerepe van. Az Infotv. egyes adatkezelőknél és adatfeldolgozóknál[810] kötelezővé teszi közvetlenül a szerv vezetőjének felügyelete alá tartozó, jogi, közigazgatási, informatikai vagy ezeknek megfelelő felsőfokú végzettséggel rendelkező adatvédelmi felelős kinevezését,[811] de természetesen bármely más szervezetnél is lehetőség van erre. A belső adatvédelmi felelős feladatai a következők:

- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- ellenőrzi az adatkezelésre vonatkozó szabályok és az adatbiztonsági követelmények megtartását;
- kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
- elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
- vezeti a belső adatvédelmi nyilvántartást;
- gondoskodik az adatvédelmi ismeretek oktatásáról.

A feladatokból látható, hogy az adatvédelmi felelős szerepe összetett, egyszerre lát el tanácsadó, tudatosság-növelő és oktató, valamint ellenőrző feladatkört.

Az adatvédelmi felelős feladatkör ellátásának módja szervezetenként változó, a feladatokat elláthatja akár egy több főből álló osztály, egy kizárólag e feladatkört betöltő, vagy akár egy egyébként más munkakört is betöltő személy. Az adatvédelmi felelősi feladatok ki is szervezhetők, nincs akadálya annak, hogy megbízási jogviszonyban azokat az adatkezelőtől/adatfeldolgozótól különböző személy vagy szervezet lássa el.

2) Eljárásrendek kialakítása

A második elem a megfelelő belső eljárásrendek kialakítása, az adatkezeléssel kapcsolatos folyamatok beillesztése a szervezet működési rendjébe. Az eljárásendek kiterjedhetnek többek között:[812]

- az adatvédelmi hatásvizsgálat lefolytatására, eljárására, módszertanára;
- az érintetti jogok gyakorlására, azaz arra, hogy az érintett pontosan hogyan kap előzetes, és hogyan kérhet később tájékoztatást, illetve hogyan kérheti adatai helyesbítését és törlését, ennek a szervezet mennyi időn belül tesz eleget, ki hozza meg az erre vonatkozó döntéseket, ki a felelős az érintett valamint az adatokat esetleg átvevő harmadik fél értesítéséért, stb.;

[810] Országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetve feldolgozó adatkezelőnél és adatfeldolgozónál, pénzügyi szervezetnél, elektronikus hírközlési és közüzemi szolgáltatónál
[811] Infotv. 24. § (1)
[812] A korántsem teljes lista Morgan és Boardman témalistája (Morgan – Boardman, 2012, x-xiv), a 29-es munkacsoport elszámoltathatóság elvéről szól véleményében kifejtett belső intézkedési javaslatai (WP29, 2010b, 12.), az előző pontban felsorolt adatvédelmi kötelezettségek számbavétele, valamint a saját gyakorlati tapasztalatok alapján készült.

- a belső jogorvoslati lehetőségekre, azaz arra, hogy az érintettek kihez fordulhatnak a szervezeten belül az esetleges jogszerűtlen adatkezelés esetén, ki és milyen eljárásban dönt az adott ügyben, stb.;
- a külső adattovábbítások rendjére, ideértve mind a belföldi (EGT-n belüli), mind a harmadik országba történő, és mind az eseti, mind a rendszeres adattovábbításokat;
- adatok pontosságának és időszerűségének (naprakészségének) biztosítására;
- az adatvédelmi és adatbiztonsági incidensek kezelésére, milyen adatbiztonsági intézkedésekkel igyekeznek megelőzni az incidenseket, mi történik az incidenst követően,[813] kit és milyen formában értesítenek erről, stb.;
- az adatvédelmi követelmények belső ellenőrzésére vonatkozóan;
- hatósággal való kommunikációra (az adatkezelés bejelentésétől kezdve az esetleges előzetes vagy későbbi ellenőrzésig);

3) Adatvédelmi és adatbiztonsági tudatosság növelése

Végül az adatvédelmi szabályok (és a compliance-stratégia) végrehajtásának fontos eleme a munkavállalók megfelelő tudatossága és elköteleződése, amelyet többféle eszközzel lehet növelni, például képzési programokkal, kézikönyvekkel illetve a témakör fontosságának belső üzenetekben, emlékeztetőkben való hangsúlyozásával.[814] A legjelentősebb eszköz kétségkívül a személyes adatok kezeléséért felelős munkavállalók belső képzése:[815] az adatvédelem és adatbiztonság alapelveinek megértésével a munkavállalók az előre nem látható helyzeteket is könnyebben kezelik.[816]

A fentieket összefoglalva látható, hogy az adatvédelmi szabályok belső végrehajtásának szervesen kell illeszkednie az adott adatkezelő mindennapi működésébe, a már kialakított üzleti folyamataiba. Ezeknek a részletes áttekintésére, egy teljes adatvédelmi irányítási rendszer kialakításának bemutatására e dolgozat keretein belül nincs mód, e fejezet célja csupán az lehetett, hogy felhívja néhány kulcskérdésre az adatkezelők figyelmét, és támpontot adjon az adatvédelmi elvek szervezeti implementálásához, és ahhoz, hogy a megtett intézkedések minként igazolhatóak. Az adatvédelmi szabályozás területén is „felfedezett", a jövőbeni szabályozást számos elemében átható új alapelv, az elszámoltathatóság (accountability) elve ugyanis éppen ezt a követelményt támasztja az adatkezelőkkel szemben.

[813] E folyamatokat célszerű a szervezetnél működő üzletmenet-folytonossági tervhez (Business Continuity Plan, BCP) igazítani. ha rendelkezik ilyennel.
[814] Morgan – Boardman, 2012, 103.
[815] A kérdéskör jelentőségét mutatja, hogy önálló szakirodalma is van: Rebecca Herold 540 oldalas könyvet szentelt e témának (Herold, 2011).
[816] Morgan – Boardman, 2012, 103. Az adatvédelmi és adatbiztonsági tudatosság növelésének további (közvetett) előnyeit, mint például a jogszabályi megfelelés biztosítását, az elszámoltathatóság elve alapján konkrét intézkedések igazolását, az érintettek bizalmának és a szervezet jó hírnevének növekedését ld. részletesen Herold, 2011, 7-18.

4.6 Következtetések

A 4. fejezetben az adatvédelem önszabályozási eszközeit, az adatvédelmi audit és tanúsítás főbb jellemzőit, valamint egy belső szabályozási rendszer kialakításának főbb pilléreit mutattam be.

Az adatvédelmi önszabályozásra vonatkozó szakirodalom jellemzően nem tartalmaz minden önszabályozási formára kiterjedő áttekintő csoportosítást, így a disszertáció jelen fejezetének célja elsősorban az volt, hogy rendszerezze az adatvédelmi önszabályozás különböző eszközeit. Ennek keretében megkülönböztettem először az anyagi szabályozást és a megfelelőség-ellenőrzésre szolgáló eszközöket, másodszor megkülönböztettem az állami, az adatkezelőn kívüli nem állami, és az adatkezelők belső szabályozási szintjét. Ennek megfelelő koordinátarendszerbe helyeztem az egyes önszabályozási eszközöket, ideértve a belső szabályozást, amely jól beleillett e rendszerbe, azaz igazolható a dolgozat vonatkozó tézise, miszerint az „adatkezelők belső szabályozása az önszabályozás egyik eszközének tekinthető."

A kritikai elemzés során rámutattam az ágazati magatartási kódexekkel kapcsolatos nehézségekre is. Az eddigiek alapján úgy tűnik, hogy ez az önszabályozási forma szigorú állami szabályozás nélkül nem hatékony (amerikai modell), részletes állami szabályozás mellett viszont nem elterjedt (európai modell). Utóbbin az adatvédelem fejlődési tendenciái nem látszanak változtatni: az állami (EU) szintű szabályozás várhatóan a jelenlegihez képest sokkal részletesebb lesz, nem várható a szektorális szabályok visszaszorulása sem, a végrehajtási szabályok egy jelentős része pedig – az elszámoltathatóság elvének szellemében – adatkezelői szintre tolódik. E tényezők mellett a „köztes" szint létjogosultsága várhatóan tovább csökken.

Részletesen elemeztem az adatvédelmi audit és tanúsítás elméleti hátterét és egyes megvalósulási formáit is. Ugyancsak kitértem a várható jövőbeni európai szabályozásra, amely jelen formájában igen ígéretes, és több, a tanúsító-rendszerekkel kapcsolatos, a működésüket már-már ellehetetlenítő problémára igyekszik megoldást kínálni.

A dolgozat egyik lényegi eleme az adatkezelők szintjén elfogadott szabályozás elemzése. Ennek jelentősége nagymértékben megnő az általam felvázolt újgenerációs adatvédelmi rezsimben, amelynek legalább részleges megvalósulása egyébként a közeljövőben reális. E fejezet során elemeztem a belső szabályozás egyes eszközeit (nyilatkozat, szabályzat) is.

Végül e fejezet végén – a teljesség igénye nélkül – iránymutatást adtam egy belső szabályozási rendszer kiépítéséhez, azonosítva a legfontosabb, az adatkezelő részéről várhatóan felmerülő problémákat, és felvázolva az első lépéseket. A kifejezetten gyakorlatorientált megközelítést alkalmazó fejezet célja, hogy problématérképként funkcionálva segítséget nyújtson az adatkezelők és adatfeldolgozók számára a compliance-kötelezettségeik áttekintéséhez, valamint az azoknak való, belső szabályozással történő megfeleléshez.

5. ÖSSZEGZÉS ÉS A DOLGOZAT ÚJ EREDMÉNYEI

5.1 Összegző gondolatok

A dolgozat tárgyát és kutatási módszertanát meghatározó, valamint egyes alapfogalmakat tisztázó bevezetőt követően a 2. fejezetben részletesen áttekintettem az adatvédelem eddigi fejlődését, hogy választ kapjak arra a kérdésre, hogy a technológia milyen hatást gyakorolt az adatvédelem fejlődésére, és hogy miként alakult ki az adatvédelem jelenlegi, „érintett-központú" rendszere. Ennek érdekében áttekintettem az elmúlt negyven-ötven év technológiai fejlődését, annak az egyén magánszférájára gyakorolt hatását, valamint az adott kor adatvédelmi szabályozásának főbb jellemzőit.

A szakirodalmi források elemzésével világossá vált, hogy a technológia fejlődésével egyre több olyan eszköz jött létre, amely a megfigyelés, az adatfeldolgozás, vagy az adatközlés hatékonyságát fokozta, összességében – potenciálisan vagy ténylegesen – folyamatosan szűkítve az egyének magánszféráját. E tendenciákra mind az első, mind a második generációs adatvédelmi szabályozás igyekezett reflektálni, más-más módszerekkel és hangsúlyokkal. Az első generációs szabályozás „adatkezelő-központúságát" a 80-as, 90-es években egy új megközelítés váltotta fel. Ennek során a jogalkotó alapvetően absztrakt szabályokat és elveket tartalmazó, a magánélet védelmét új – immár nemcsak az „intim" adatokra, hanem bármely természetes személyre vonatkozó adatra alkalmazandó – szabályokkal kívánta biztosítani, és az érintetti kontrollt előtérbe helyező szabályozást alakított ki. Az érintett tényleges szerepe ugyan tagállamonként kisebb-nagyobb eltéréseket mutatott, összességében azonban megállapítható, hogy európai adatvédelmi szabályozás logikája alapvetően „érintett-központúvá" vált.

Azt is megállapítottam, hogy az Internet megjelenése, és a 90-es évek közepétől kezdődő elterjedésére a szabályozás – alapvető logikáját tekintve legalábbis – nem reagált. Az absztrakt elveken nyugvó, érintetti kontrollon alapuló szabályozás azonban egy ideig egészen jól bevált az új technológiai környezetben is.

A 3. fejezetben először is az adatvédelmi szabályozást érő újabb kihívásokat tekintettem át, ideértve különösen a web 2.0-t, a profilozást és az azon alapuló perszonalizált szolgáltatásokat, és a Big Data és a mindent átható számítástechnika egymással szorosan összefüggő és egymást kölcsönösen erősítő jelenségét. A technológiai fejlődés egyértelműen csökkenti az adatkezelések átláthatóságát és növeli az információs hatalom aszimmetriáját, az érintetti kontroll lehetőségét pedig jelentősen szűkíti. Ezt az elmúlt években végzett közvélemény-kutatások alapos elemzése is alátámasztotta, hangsúlyozva, hogy az adatkezelésekkel kapcsolatos aggodalmak és a kontroll vágya – úgy tűnik, sokszor hamis biztonságérzettel párosulva – széles körben megjelenik. Igaznak bizonyult a privacy-paradoxon jelensége is, miszerint az érintettek tényleges magatartása nem adekvát az aggodalmaikkal. Ugyanakkor a „mindenki mindent felelőtlenül megoszt" klisé is egyértelműen cáfolható. Jelentős az a kutatási eredmény is, ami azt mutatja, hogy jelentős azok aránya (30-40%), akiket nemigen foglalkoztatnak az adatvédelemmel kapcsolatos

kérdések, és nincs szándékukban különösebben a magánszféra-védelmük menedzselésével törődni.

A technikai háttérrel és az érintetti attitűddel párhuzamosan részletesen elemeztem a hozzájárulás központú – ahogy Solove fogalmaz a „privacy self-management”[817] alapú – megközelítés kritikáját is. Az információs önrendelkezési jog fontosságát hangsúlyozó érveket is figyelembe véve arra jutottam, hogy meg kell haladni az adatvédelmi szabályozás érintett-központúságát. Ez nem jelenti azt, hogy az érintetti kontrollal, vagy az információs önrendelkezési joggal kapcsolatban visszalépésre lenne szükség, mivel a problémákat nem az érintett pozíciója, hanem annak jelentős túlértékelése okozza. Összességében tehát az érintett jelenlegi jogi pozícióját meg kell tartani, de tudomásul kell venni, és számolni is kell azzal, hogy az érintetti kontroll csak ritkán funkcionál az adatkezelések érdemi korlátjaként. Különösebben megerősíteni a pozícióját nem érdemes, az esetleges erősítésétől pedig egészen biztosan nem lehet hatékonyabb adatvédelmi szabályozást várni.

Olyan szabályozásra van tehát szükség, amely reálisan számol az érintettek passzivitásával, illetve lehetőségeinek korlátaival, és a jelenlegihez képest kevésbé tekinti őket az adatvédelmi szabályozás főszereplőjének. Amint azt tézisként is megfogalmaztam, az „érintett-központú” szabályozás felől el kell mozdulni az „adatkezelő-központú” szabályozás felé. Ezt azonban nem az érintettet korlátozó paternalista szabályokkal kell elérni, hanem olyan „mögöttes biztonságot” kínáló jogszabályi környezettel, amelyik biztosítja az érintett saját sorsáról (saját adatairól) való döntését, ha úgy szeretné, és képes is rá, de megfelelő védelmet biztosít, ha egyébként az érintettnek van igénye a magas szintű védelemre, de valamilyen okból nem akar vagy képes élni az egyébként igen széles jogosítványaival. Mintaként leginkább a fogyasztóvédelmi és a különböző termékfelelősségi szabályok lehetnek irányadók az ÁSZF-ekre vonatkozó szabályozás lényege, hogy ha a fogyasztó nem is szentel túl sok figyelmet e dokumentumoknak, az erre szakosodott szervek (állami hatóságok vagy civil szervezetek) igen. A fogyasztók emellett nagyjából abban is biztosak lehetnek, hogy az általuk megvásárolt termékek megfelelnek bizonyos minimális biztonsági követelményeknektanúsító-szervezet. Hangsúlyozni kell, hogy e megközelítés nem érinti az alapjogi védelem létjogosultságát. Igaz, az „adatkezelő-központú” szabályozás inkább az alapvető jogok objektív, intézményvédelmi kötelezettségeket is hangsúlyozó megközelítésbe illik bele, amely szerint az alapjogi védelem az egyéni alapjogi igényektől független intézményvédelmi kötelezettséget is ró az államra.

A 3. fejezetben – a jogirodalmi források és az EU adatvédelmi reformjának előkészítő dokumentumaira támaszkodva – felvázoltam az adatvédelmi szabályozás megújításának egy lehetséges útját, egy adatkezelő-központú újgenerációs adatvédelmi szabályozás főbb elemeit. Az újgenerációs szabályozás pilléreit három pontban foglaltam össze.

1) Az adatkezelők szerepének újragondolása.

[817] Solove, 2013.

Az összes szereplő számára kulcsfontosságú az adatkezelések jelenleginél nagyobb átláthatósága (transzparencia). A technológiai változásokból egyértelműen az a tendencia rajzolódott ki, hogy nemcsak az érintettek, de többször maguk az adatkezelők, és nem mellékesen a felügyelőhatóságok is elvesztik a kontrollt a személyes adatok kezelése felett. A transzparencia növelése – többek között – az adatkezelők átgondoltabb adatvédelmi politikára szorításával (pl. dokumentációs kötelezettségeinek előírásával és adatvédelmi tudatosságuk növelésével) érhető el.

Az adatvédelem területén is érvényesülnie kell az elszámoltathatóság alapú megközelítésnek, amely az adatkezelők belső szabályozásától, eljárási mechanizmusaitól várja az adatvédelmi elvek hatékonyabb végrehajtását. Az adatkezelők számára az elszámoltathatóság elvével kapcsolatban különböző, az eddigiekhez képest jóval részletesebben szabályozott kötelezettségeket kell előírni, amelyek segítségével ténylegesen igazolhatják, hogy betartják és végrehajtják az adatvédelmi szabályokat. Ennek keretében lényegesen megnő az adatkezelők belső szabályozásának jelentősége.

E megközelítés során azonban elengedhetetlen az adatkezelők differenciálása, azaz a szabályozási terhek megfelelő elosztása, mivel az adatkezelések bizonyos jellemzői alapján az azzal kapcsolatos kockázatok is jelentősen eltérhetnek. Ezen eltéréseket hangsúlyosan figyelembe kell venni, ami tulajdonképpen az információbiztonság területén alkalmazott kockázatarányos védelem elvének az adatvédelmi szabályozásban való megjelenését jelenti. A nem kellő differenciálás az egész adatkezelő-központú megközelítést tarthatatlanná teheti.

2) Az adatvédelmi felügyelet szerepének megerősítése

Az adatvédelmi felügyeletet több „szinten” is meg kell erősíteni. Mindenekelőtt felkészült (ideértve különösen az informatikai felkészültséget is), független, és erős hatáskörökkel és bírságolási joggal felruházott adatvédelmi hatóságoknak kell az adatvédelem felügyeletét ellátni. A függetlenség kulcskérdés az állami adatkezelőkkel szembeni fellépés során, az erős hatósági eszközök pedig a piaci adatkezelőkkel szemben. Erősíteni kell emellett a piaci alapon működő (ön)felügyeleti módozatok, az adatvédelmi audit és tanúsítás intézményét. Az adatkezelők belső szabályozási rendszerének részletes áttekintése ugyanis jelentős erőforrásigénnyel jár, így célszerű e feladatokba piaci szereplőket is bevonni.

3) A technológia, illetve az adatbiztonsági szerepének megerősítése

Az adatvédelmi szabályozásnak (újra) célul kell tűznie a technológia szabályozását, formálását. A Privacy by Design megközelítés éppen arra tesz merész kísérletet, hogy a technológia és jog, mint két szabályozórendszer egymást erősítse, és egyértelműen a technológiát állítsa a – társadalmi elvárásokat végső soron kötelező normaként megjelenítő – jogi szabályozás szolgálatába, megtartva a jogi szabályozás elsőbbségét. A privátszférát erősítő technológiák e célkitűzések megvalósításának első számú eszközei lehetnek.

A fenti pontokat összefoglalva az látszik, hogy az érintett szerepétől függetlenül lehetne magasabb védelmi szintet garantálni, ha:

- a létrejövő új jogi rezsimben az adatkezelők elszámoltathatósága révén az adatkezelők átláthatósága és tudatossága és az adatvédelmi elvek adatkezelők szintjén történő végrehajtásának hatékonysága jelentősen nőne,
- mindehhez a jelenleginél hatékonyabb felügyelet társulna (ideértve az állami felügyelet mellett a piaci alapon működő önkéntes adatvédelmi auditot és tanúsítást is),
- a technológiát végül valóban sikerülne az adatvédelem „szolgálatába" állítani.

A 3. fejezetben – az imént említett három pillér alapján – részletesen vizsgálom az EU adatvédelmi rendelet tervezetét is, amelyet a harmadik generációs szabályozás „mintaszabályozásának" tekintek. A Rendelettervezet mindegyik vizsgált területen jelentős előrelépést tesz, azonban jelen formájában egyértelműen az adatvédelem túldokumentálásával fenyeget. A Rendelettervezet ugyanis nem kellően differenciál az adatkezelők között, és így egyes kötelezettségeket – különösen a data breach notification és az adatvédelmi hatásvizsgálat lefolytatását – túlzottan széles adatkezelői kör számára írja elő.

A dolgozat egyik fontos következtetése, hogy a fenti megközelítés összességében jelentősen növeli az adatkezelők belső szabályozásának jelentőségét, az adatkezelők szemszögéből nézve pedig a compliance-költségeiket és adminisztrációs terheiket. E hatás enyhítésére olyan egyszerűen használható útmutatóra, módszertanra van szükség, amely hatékony segítséget jelent az adatkezelők számára a belső szabályozásuk kialakításában és a compliance kötelezettségeknek való megfelelésben.

A 4. fejezetben rendszerező módszert követve tekintettem át az adatvédelmi önszabályozás fontosabb eszközeit. Az önszabályozás rendszerében sikerrel helyeztem el az adatkezelők belső szabályozását, mint az önszabályozás egyik eszközét. A rendszerezés keretében megkülönböztettem egyrészt az anyagi szabályozást és a megfelelőség-ellenőrzésre szolgáló eszközöket, másrészt az állami, az adatkezelőn kívüli nem állami, és az adatkezelők belső szabályozási szintjét, majd ennek megfelelően elkészített koordinátarendszerbe helyeztem az egyes önszabályozási eszközöket.

A kritikai elemzés során rámutattam az egyik önszabályozási forma, az ágazati magatartási kódexekkel kapcsolatos nehézségekre is, ami szigorú állami szabályozás nélkül, például az Egyesült Államokban, nem hatékony, átfogó és részletes állami szabályozás mellett pedig, például Európában, nem különösebben elterjedt. Ezen az adatvédelem jövőbeni tendenciái sem látszanak változtatni, mivel az elszámoltathatóság elve alapján a végrehajtási szabályok egy része az adatkezelői szintre tolódik, ami tovább csökkenti a „köztes" szabályozói szint létjogosultságát.

Részletesen elemeztem az adatvédelmi audit és tanúsítás elméleti hátterét és egyes megvalósulási formáit. Ugyancsak kitértem a várható jövőbeni európai szabályozásra, amely jelen formájában igen ígéretes, és több, a tanúsító-rendszerekkel kapcsolatos, jelentős problémára igyekszik megoldást találni.

Végül a dolgozat 4.5. fejezete az adatkezelők belső szabályozási rendszerének alapvető lépéseit tartalmazza. A kifejezetten gyakorlatorientált fejezet célja, hogy kézzelfogható szempontokat adjon az adatkezelők számára a compliance-kötelezettségek teljesítéséhez és a belső szabályozásuk kialakításához. A fejezet fontos kiindulópontként szolgálhat további, az adatkezelők belső szabályozási rendszerét vizsgáló kutatások számára.

5.2 A dolgozat új eredményei

A dolgozatban részletesen összefoglalom az adatvédelmi szabályozás történetét, a technológia-társadalmi változások kontextusába is helyezve. Bár az adatvédelem történetéről többen is írtak, ilyen szemléletű és részletességű történeti összefoglaló magyar nyelven korábban nem készült.

A dolgozat kifejezetten hiánypótló az európai adatvédelmi reformfolyamat és az adatvédelem új elveinek és jogintézményeinek („privacy by design”, adatvédelmi hatásvizsgálat stb.) és a Rendelettervezet egyes újításainak bemutatása kapcsán. Az elmúlt néhány évben a magyar jogirodalomban alig jelentek meg e témakörökkel foglalkozó írások.

Bár az adatvédelem lehetséges irányairól, egy-egy témakör kapcsán felmerülő újításokról, vagy egy-egy új jogintézmény szükségességéről számtalan forrás található, egyértelműen a dolgozat új eredményének tekinthető az újgenerációs adatvédelmi szabályrendszer főbb elemeinek felvázolása. Az adatkezelő-központú szabályozási megközelítéssel kapcsolatos gondolatok és a compliance-szemlélet hangsúlyos megjelenése új színt jelent a magyar jogirodalomban, amely a személyes adatok védelmét nagyobbrészt (néhány kivételtől eltekintve) alapjogi megközelítésben, az érintett (ön)rendelkezési jogát elemezve közelítette meg.

Az adatvédelmi önszabályozás témaköre szintén nem túl hangsúlyos, sem a magyar, sem az angol nyelvű jogirodalomban. Ez ugyanakkor nem feltétlenül a témakör alulértékeltségét jelenti, az adatvédelmi önszabályozás gyakorlati jelentősége Európában valóban mérsékelt. A 4. fejezetben található, kifejezetten rendszerező igényű összefoglalás, és az adatkezelők belső szabályozásának e rendszerben történő elhelyezése mindenképp jelentős újdonság a hazai jogirodalomban.

Végül a dolgozat új kutatási eredménye az 4.5 fejezetben található, az adatkezelők belső szabályozásárához szükséges alapvető lépések összefoglalása, amely mintegy problématérképként funkcionál a belső szabályozás kialakításához. E fejezet új megközelítési módot ad hozzá az adatvédelmi szakirodalomhoz; hasonló áttekintés Magyarországon még nem készült.

6. ENGLISH SUMMARY

6.1 Historical overview

The birth of data protection regulation in Europe was directly linked to technological developments, and from the very beginning these developments challenged data protection law on a daily basis. In the '70s the development of information technology made it possible to apply computers to operate state-owned databases, and so personal information could be controlled by means of these digitalized databases much more rapidly, and different state registers could be merged and connected, showing many aspects of an individual's life; it was even possible to create personality profiles based on these. The threat to privacy at this time was connected to data processing by the state, often referred to as the 'Big Brother' effect based on Orwell's famous novel '1984'. These concerns drove the first data protection law in the world to be enacted in the Land of Hesse, Germany in 1970. This Act "set the course for all further discussions"[818] and served as an example for the legislation enacted in many Western European states (Sweden: 1973, Germany: 1976, Denmark, Norway France: 1978, etc.).[819]

In the 80s and 90s the world changed a great deal – also from the perspective of privacy risks. Various developments such as the spread of personal computers (first as standalone computers, later connected by the Internet), the wide-spread usage of computers in the business sphere, the new (direct) marketing techniques, and, still later, the development of online marketing (based on cookies and other tracking methods), as well as the increasing importance of customer relationship management (CRM) and enterprise resource planning (ERP), made evidenced that demand from the business sphere (sometimes referred to as "Little Brother") for personal data is at least as significant as a state's "natural intention" to collect personal data.

Later, from the middle of the 90s, the rapid expansion of Internet usage and the appearance of many online services set new challenges for regulators. The establishment of the "information society" became a political programme in the European Union, and so documents were adopted in this field, all emphasising the importance of privacy. As ensuring the legal protection of personal information plays an important role also in building trust in the field of online services, its legal regulation, and, in a broader sense, the entire privacy issue of the Internet became an important element of this broadened and vaguely defined phenomenon referred to as the "information society". Another significant trend at this time was the globalization of data processing, which generated the significant feature of trans-border data flow, so creating the need for international and European regulation.[820]

[818] Simitis, 1987, 5.
[819] Burkert, 2000, 48-50.
[820] Burkert, 2000, 51-53.

Considering the challenges to be faced and the general trends of the decade, I argued in this dissertation, that the data protection legislation introduced reflected them quite well. The focus of the regulation extended from governments to new subjects, to companies and organizations. In parallel, international and European laws were adopted which attempted to assure the legal certainty of international data flows, to strengthen the rights of the data subjects' and to introduce some new approach to legislation. One of the most important new concepts was developed by the German Constitutional Court in 1983, the concept of informational self-determination. This should be understood as "the authority of the individual to decide himself, on the basis of the notion of self-determination, when and within what limits information about his private life should be communicated to others".[821] However this right cannot be unlimited as the data subject has to accept limitations in the case of overriding general interest when this is incorporated into a law and is clear and proportional.

I drew up the conclusion, that although European countries followed different value approaches in the development of national data protection rules,[822] the data subjects' control and the consent (as legal ground for data processing) became a key issue. By the end of the last century data protection law became, by and large, "data subject oriented", with the consequence that the realization of the law has been strongly based on the activity and awareness of the data subjects.

6.2 Paradigm shift in data protection regulation

6.2.1 Current trends of technological development and attitudes to privacy

Currently, however, European data protection law is undergoing long awaited revision, and one of the most important aims of reform is to react appropriately to the latest technological developments and to the related social changes once more.[823] In the dissertation I pointed out, that during the last 10-15 years there have been further significant social, economic and cultural changes, like the emerging role of Web 2.0 technologies, the spread of ubiquitous computing, the "internet of things", and the sophisticated methods of profiling, and offering highly personalized content, the growing importance of cloud computing, mobile data processing (including location tracking), and Big Data technologies, etc.

The attitudes of the data subjects and data controllers are also changing. It seems, that most people tend to accept that disclosing personal information is an increasing part of modern life, but sometimes it causes discomfort for them. Despite their concerns about legal and fair data processing, their actual behaviors don't fit to their attitude (privacy-paradox). It also has to be emphasized, that many people, mostly youngsters are much more conscious while revealing personal data that it is usually considered. On the other hand, it is also

[821] Rouvroy – Poullet, 2010, 45.
[822] Burkert, 2000, 53-56.
[823] Reding, 2011, 3.

clear, that cca. 30-40% of the citizens don't have any concerns about their privacy, and don't willing to deal with their privacy management. All in all the results of the public opinion surveys show a quite complex picture, with significant or even huge national variances.

It seems that current legislation cannot respond to these challenges. I analyzed many critical opinions that have been published in the past few years concerning the current regulation, including criticism of the "data subject oriented" legal framework. Solove, for instance, summarized the main problems of the so called "privacy self-management" system. He points out first cognitive problems that "impair individuals' ability to make informed, rational choices about the costs and benefits of consenting" (user doesn't read privacy policies, or don't fully understand). Second, "and more troubling, even well-informed and rational individuals cannot appropriately self-manage their privacy due to several structural problems." The number of entities processing personal data makes it almost impossible to deal with every single issue. Besides this, "many privacy harms are the result of an aggregation of pieces of data over a period of time", and so data subjects cannot weigh the costs and benefits of revealing one or more single data.[824]

6.2.2 Key elements of a framework for a new generation of data protection

All in all both technology and citizens have changed so much, that these trends, as many authors suggests, clearly call for a new data protection regime, new laws with new concepts. In other words, it is time for a paradigm shift in data protection legislation. My aim in the dissertation was, among others, to draft the key elements of a framework for such a new generation of European data protection, at the same time comparing the European Commission's Proposal for Regulation to this concept.

The essence of the new regime will be to effectively protect individual privacy, even if their privacy awareness is low, and even if they do not take any steps to be protected by ensuring so-called "background protection". The new data protection regime should not count on the data subject's activity any more than previously; the new law should be "data controller oriented" instead of the current "data subject oriented" law. This does not mean, in my view, that the rights of the data subjects and/or the regulation of consent should be weakened, indeed, they should be kept, and detailed provisions concerning the realization of current rights would be useful, although it is unlikely that strengthening these rights would significantly increase the actual level of privacy protection.

This approach may be similar to that followed by consumer protection,[825] which also aims to protect the weaker party. This, for example, includes 'blacklisting' (a practice invariably regarded as unfair) which should trigger action by a strong consumer protection authority or NGOs. This means that, although freedom of contract is a generally important principle,

[824] Solove, 2013, 1880-1881.
[825] A similar approach is followed in many other sectors, e.g. food or any other product safety regimes.

but even if the consumer ignores the general terms and conditions, the authorities do not, and so consumers cannot enter into a totally unfair contract.[826]

In the dissertation I sketched the core elements of this new model of data protection regulation, which may be summarized in three points:

1) Rethinking the role of the data controllers whilst also distinguishing the duties of them;
2) Strengthening supervision
3) Regulating the technology as much as possible

6.2.2.1 Rethinking the role of the data controllers

Increasing the accountability of data controllers is an important issue in professional debate on the future of data protection regulation. The principle of accountability was expressed in detail in the opinion 3/2010 of Article 29 of the Working Party, and it arose again in the Commission's Communication on "a comprehensive approach on personal data protection in the European Union", which was one of the preparatory documents of the new data protection proposal. In both of these documents the approach to the principle was quite cautious: accountability was interpreted as a general principle, which does not impose cumbersome new legal requirements, but "aims at ensuring de facto, effective compliance with existing ones".[827] In my view these measures should be prescribed as legal requirements for some data controllers, whilst admitting that these are very concrete duties for data controllers which impose administrative burdens and cost – even if they are not new principles, but measures to ensure the realization of existing ones. The Proposal for Regulation clearly takes significant steps in this direction, imposing many new duties on data controllers and data processors. The proposed measures are suitable for ensuring the accountability principle, and will increase the actual level of privacy protection. This will arise, firstly, by enhancing the awareness of data controllers, so reducing unwanted or unnecessary data processing operations, and, secondly, by improving the transparency of data processing, which may be controlled by data subjects, and so (most importantly) making the tasks of data protection authorities and NGOs easier.

Once regulations impose new requirements on data controllers, we need to be able to distinguish among them in several ways. As Article 29 of the Working Party emphasises, the "one-size-fits-all" approach should be avoided, and, rather, the "specific measures to be applied must be determined, depending on the facts and circumstances of each particular case, with particular attention to the risk of the processing and the types of data."[828]

There are two main reasons for differentiating the duties of data controllers. First, it is important to avoid unnecessary administrative burdens and costs and the (potential) decrease in the competitiveness of smaller businesses processing a low volume of personal data, or processing personal data only as an activity ancillary to its main activities. Second, as mentioned above, millions of users can also be regarded as a data controller in some

[826] About the possible comparison parallel between future data protection rules and consumer protection rules, see also Rauhofer, 2013, 84.
[827] WP29, 2010b, 10.
[828] WP29, 2010b, 13.

cases, mostly due to user-generated content. It is crucial to make some difference regarding the duties of the "everyday users", even if they fall within the scope of the definition of 'data controller'.

6.2.2.2 Strengthening supervision

In the dissertation I interpreted of strengthening supervision in the field of data protection in two levels. First, the role of the national data protection authorities (DPAs) should be increased, and second, bigger emphasis should be laid on audit and certification schemes.

It should first be stated that data protection authorities operate in all Member States of the EU and their objectives of enforcement are very similar due to the implementation of Directive 95/46/EC. Data controllers may face severe sanctions in cases of a breach of personal data regulations under national laws, but those consequences are not always sufficiently transparent or standardized. Three issues should be considered while strengthening the DPAs position:

1) Enhance the independence of the authorities,
2) Extend the possible sanctions they may use, and empower and encourage them to impose a high amount of fines,
3) Ensure adequate expertise in the field of information technology, and mostly in IT security.

The role of self-regulation, internal regulation and various certification schemes are also expected to increase. Independent, third-party audits and certification may demonstrate the data controllers' commitment to respecting privacy.

The Proposal for a Regulation contains some advanced provisions in this field. It basically provides specification for the creation of codes of conduct similarly to the regulations contained in the Directive,[829] however, at the same time, it is a novelty that the Proposal incorporates an article on data protection certification and seals. The Parliament's Proposal grants the right for the data controllers to request (on a voluntary basis) any supervisory authority to certify that the processing of personal data is performed in compliance with the Regulation. The supervisory authority may accredit specialized third party auditors to carry out the auditing.[830]

6.2.2.3 Regulating the technology

The development of information technology plays a key role in jeopardizing privacy, so it's a quite obvious intention to try to use IT also for protecting privacy. Technology can enhance the level of data security, and increase the level of protection of personal data.

In the dissertation I summarized the development of privacy enhancing technologies (PETs) and the main idea of Privacy by Design, as developed by Ann Cavoukian. PETs are clear engineering approaches which focus on the positive potential of technology, on tools used to maintain anonymity, confidentiality, or control over personal information,[831] whilst

[829] Proposal for a Data Protection Regulation, Article 38, 1-3.
[830] Proposal for a Data Protection Regulation, Article 39, 1a-1g.
[831] Rubinstein, 2012, 1412.

PbD is a broader concept comprising several elements. Introducing Privacy by Design (PbD) to the personal data protection regulation will play a major role in forming a new legal framework - not only in the European Union, but also in Canada and the US. PbD has several definitions, but, it refers mainly to the concept that information and communications technologies and systems should be designed (and also operated) as taking privacy into account, even from the outset, as a default setting.

The proposal for a Data Protection Regulation would enact the Privacy by Design principle into Data Protection Law, but the actual implementation of the principle to practice arise many questions.

As a conclusion, in respect of the role of technology, these principles ease the compliance duties of data controllers - which leads to the better protection of data subjects, even given their inactivity or lack of interest in privacy. Setting strict rules for data controllers on applying technologies for personal data processing fairly fits the concept of a paradigm shift.

6.3 Self-regulation, audit and certification schemes in the field of data protection

The dissertation also focuses on the role of self-regulation and internal regulation in the field of data protection. In the fourth chapter I summarized and systematize the different means of self-regulation, dividing them into substantive norms and procedural means, and distinguishing three levels of adoption: 1) regulation adopted by the state, 2) regulation adopted by organizations above data controllers and 3) regulation adopted by data controllers. Thus, the internal regulation of a data controllers' was also placed in the self-regulation regime.

While summarizing the opinions found in the legal literature I also compared the role of the Code of Conducts in the US and in the EU. In the absence of a unified regulation at the federal level, industrial self-regulation (relating to data protection) plays an important role in the United States, which is founded on the business-based approach according to which the characters of business life are capable of developing a regulation that meets consumer requirements thereby preventing state regulation.[832] Still, self-regulation in the US generally regarded as a non-effective way to protect privacy – the quality of the protection fall behind the European one. As opposed to this, in Europe, the adoption of the Data Protection Directive has established a more or less harmonized European regulation, ensuring a quite high level of protection, which seems to hinder (to make it unnecessary) the wide-spread usage of Code of Conducts. Although Article 27 of the Data Protection Directive expressly lays down the possibility of adopting codes of conduct and enables the elaborators of codes to submit them to the opinion of the national data protection authority or to the Article 29 Working Party, so far only very few codes have been granted recognition at the European level.

[832] Jóri, 2005, 53.

In this chapter I also discussed the institutions of data protection audit and certification in detail: the basic notions relating to audit, types of audit/certification, and the advantages and disadvantages of them. I also analysed the expected changes in this field: the proposed provisions of the new Regulation would take a huge step forward in this field, and would grant the right for the data controllers to request (on a voluntary basis) any supervisory authority to certify that the processing of personal data is performed in compliance with the Regulation. The supervisory authority may accredit specialised third party auditors to carry out the auditing.[833]

Finally I pointed out the main important first steps how to establish internal data protection governance at data controllers' level. This may help the data controllers to comply with the increasing compliance duties planned to be imposed for them by the new European Data Protection Law.

[833] Proposal for a Data Protection Regulation, Article 39, 1a-1g.

7. IRODALOMJEGYZÉK

7.1 Jogszabályok

[1] Európa Tanács (1981): Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény

[2] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata 2012/C 326/01 (EUSZ)

[3] Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata 2012/C 326/01 (EUMSZ)

[4] Az Európai Unió Alapjogi Chartája (2010/C 83/02)

[5] A Bizottság 611/2013/EU rendelete (2013. június 24.) a 2002/58/EK európai parlamenti és tanácsi irányelv (elektronikus hírközlési adatvédelmi irányelv) szerinti személyes adatok megsértésére vonatkozó bejelentésre alkalmazandó intézkedésekről

[6] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

[7] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

[8] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

[9] Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról

[10] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

[11] 1995. évi XXVIII. törvény a nemzeti szabványosításról

[12] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[13] 62/1997. (XII. 21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről

[14] Act on the Protection of Personal Data Used in Teleservices (Gesetz über den Datenschutz bei Teleddiensten), Federal Law Gazette (Bundesgesetzblatt) 1997 I 1871.

7.2 Szakirodalmi források

[15] Andrade, Norberto – Monteleone, Shara (2013): Digital Natives and the Metamorphosis of European Society. The emerging behavioral trends regarding privacy and their legal implications, in: Serge Gutwirth – Ronald Leenes – Paul de Hert – Yves Poullet: European Data Protection: Coming of Age, Springer, pp. 119-144.

[16] Anthonysamy, Pauline – Greenwood, Phil – Rashid, Awais (2012): A Method for Analysing Traceability between Privacy Policies and Privacy Controls of Online Social Networks, in: Bart Preneel – Demosthenes Ikonomou (eds.): Privacy Technologies and Policy, pp. 187-202.

[17] Bakos Eszter – Krausz Miklós (2011): A kiskorúak védelme és az önszabályozás hatékonysága. Az RTL Klub Való Világ 4 című műsor szerkesztési alapelveire vonatkozó kódexe tükrében, Infokommunikáció és jog, 4. sz. pp. 149-153.

[18] Balogh Zsolt György (1998): Jogi informatika, Dialóg Campus, Budapest-Pécs

[19] Balogh Zsolt György (2004): Adatvédelem és információszabadság, Fundamentum, 4. szám, pp. 55-58.

[20] Balogh Zsolt György – Jóri András – Polyák Gábor (2002): Adatvédelmi „legjobb gyakorlat" kialakítása az elektronikus közigazgatásban, Kézirat, Pécsi Tudományegyetem, Állam és Jogtudományi Kar, Pécs

[21] Balogh Zsolt György – Kiss Attila – Polyák Gábor – Szádeczky Tamás – Szőke Gergely László (2014): Technológia a jog szolgálatában? – Kísérletek az adatvédelem területén, Pro Futuro – A jövő nemzedékek joga, 1. sz. pp. 33-45.

[22] Banisar, David (2001): A Privacy védelmének modelljei, in: Majtényi László (szerk.): Az odaátra nyíló ajtó, Adatvédelmi Biztos Irodája, Budapest

[23] Belovich, Steve, G. (2010): IT Security History & Architecture, IQware http://iqware.us/PDF_presentations/SecurityArticleBrief5-18-10.pdf [2014.04.02.]

[24] Benkőné Deák Ibolya– Bodnár Pál – Gyurkó György (2008): A gazdasági informatika alapjai, Perfekt, Budapest

[25] Bennett, Colin J. (1992): Regulating Privacy – Data Protection and Public Policy in Europe and the United States, Cornell University Press, Ithaca and London

[26] Bennett, Colin J. (1998): Convergence Revisited: Toward a Global Policy for the Protection of Personal Data, in: Philip E. Agre – Marc Rotenberg (eds.): Technology and Privacy: The New Landscape, Cambridge: MIT Press, pp. 99-124.

[27] Bennett, Colin J. (2005): Információpolitika és adatvédelem: a szabályozás nemzetközi fórumai. Információs Társadalom, 2. szám, pp. 74-97.

[28] Bennett, Colin J. – Raab, Charles D. (2006): The Governance of Privacy. Policy Instruments in Global Perspective, The MIT Press

[29] Berényi László – Szintay István – Tóthné Kiss Anett (2011): Minőségügy alapjai, Miskolci Egyetem, Vezetéstudományi Intézet http://www.szervez.uni-miskolc.hu/blaci/minmen/index.html [2012. 10.28.]

[30] Bíró János – Szádeczky Tamás – Szőke Gergely László (2011): A hírközlési szolgáltatók értesítési kötelezettsége a személyes adatok megsértése esetén (data breach notification), Infokommunikáció és jog 2. sz. pp. 46-49.

[31] Black, Edwin (2002): Az IBM és a Holokauszt, Atheneum 2000, Budapest

[32] Bodenschatz, Nadine (2010): Der Europäische Datenschutzstandard, Peter Lang, Frankfurt am Main

[33] Böröcz István (2014): Don't be evil. A Google adatvédelmi politikája az AdWords szolgáltatás tükrében, in: Drinóczi Tímea – Naszladi Georgina – Novák Barnabás (szerk.): Studia Iuvenum Iurisperitorum, Pécs, pp.147-174. http://sii.ajk.pte.hu/files/Studia_Iuvenum_Iurisperitorum_7_2014.pdf [2013.07.17.]

[34] Böröcz István – Szőke Gergely László (2013): A beépített adatvédelem (Privacy by Design) elve, Infokommunikáció ás jog, 3. sz. pp. 120-125.

[35] Brockdorff, Noellie – Appleby-Arnold, Sandra (2013): What Consumers think (paper presented at Online Privacy: Consenting to your Future International Conference, Malta) http://consent.law.muni.cz/storage/1365167549_sb_consentonlineprivacyconferencemarch2013-consentprojectresultswhatconsumersthink.pdf. [2013.07.17.]

[36] Brownsword, Roger (2010): Consent in Data Protection Law: Privacy, fair processing, and confidentiality, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer, pp. 83-110.

[37] Budai Balázs Benjámin (2009): Az e-közigazgatás elmélete, Akadémiai Kiadó, Budapest

[38] Burkert, Herbert (1998): „Privacy-enhancing technologies: Typology, critique, visions, in: Philip E. Agre – Marc Rotenberg (eds.): Technology and Privacy: The New Landscape, Cambridge: MIT Press, pp. 125-142.

[39] Burkert, Herbert (2000): Privacy – Data Protection. A German/European Perspective, in: Christoph Engel – Kenneth H. Keller (eds.): Governance of Global Networks in the Light of Differing Local Values, Baden-Baden: Nomos, pp. 44-69. http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf [2013.07.17.]

[40] Burkert, Herbert (2010): Towards a New Generation of Data Protection Legislation, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer, pp. 335-342.

[41] Bygrave, Lee Andrew – Schartum, Dag Wiese (2010): Consent, Proportionality and Collective Power, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer, pp. 160-161.

[42] Castells, Manuel (2005): Az információ kora. Gazdaság, társadalom és kultúra. I. kötet (A hálózati társadalom kialakulása), Gondolat-Infonia, Budapest

[43] Castelluccia, Claude (2012): Behavioural Tracking on the Internet: A Technical Perspective, in: Serge Gutwirth – Ronald Leenes – Paul De Hert – Yves Poullet (eds.): European Data Protection: In Good Health? Springer, pp. 21-33.

[44] Cavoukian, Ann (2008): Privacy in the clouds, in: Identity in the Information Society 1. sz. Springer, pp. 89-107. http://link.springer.com/content/pdf/10.1007%2Fs12394-008-0005-z.pdf [2013.11.22.]

[45] Cavoukian, Ann (2009): Privacy by Design. …Take the challenge. Information and Privacy Commissioner of Ontario, http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf [2014.03.20.]

[46] Cavoukian, Ann (2013): Privacy by Design. A hét alapelv, Ontario (Canada) Információs és Adatvédelmi Biztosa, http://www.privacybydesign.ca/content/uploads/2013/03/7foundationalprinciples-hungarian.pdf [2013.08.11.]

[47] Clarke, Roger (2011): An evaluation of privacy impact assessment guidance documents, International Data Privacy Law, 2. sz. pp. 111-120. http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.full.pdf [2013.12.10]

[48] Cuijpers, Colette – Koops, Bert-Jaap (2013): Smart Metering and Privacy in Europe: Lessons from the Dutch Case, in: Serge Gutwirth – Ronald Leenes – Paul de Hert – Yves Poullet (eds.): European Data Protection: Coming of Age, Springer, pp. 269-293.

[49] Custers, Bart –van der Hof, Simone – Schermer, Bart – Appleby-Arnold, Sandra – Brockdorff, Noellie (2013): Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law. http://script-ed.org/wp-content/uploads/2013/12/custers_et_al.pdf [2013.08.15.]

[50] Csink Lóránt – Mayer Annamária (2012): Variációk a szabályozásra. Önszabályozás, társszabályozás és szabályozó hatóság a médiajogban, Médiatudományi Intézet, http://mtmi.hu/dokumentum/310/MK3.pdf [2013.08.05.]

[51] Davies, Simon (2013): Why Privacy by Design is the next crucial step for privacy protection.

http://www.i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf [2013.10.17.]

[52] De Hert, Paul (2012): A Human Rights Perspective on Privacy and Data Protection Impact Assessment, in: David Wright – Paul De Hert (eds.): Privacy Impact Assessment, Springer pp. 33-76.

[53] De Hert, Paul – Kloza, Dariusz – Wright, David (2012): Recommendations for a privacy impact assessment framework for the European Union. PIAF project [A Privacy Impact Assessment Framework for data protection and privacy rights] http://piafproject.eu/ref/PIAF_D3_final.pdf [2013.07.17.]

[54] Dhillon, Gurpreet – Kolkowska, Ella (2011): Can a Cloud Be Really Secure? A Socratic Dialogue, in: Serge Gutwirth – Yves Poullet– Paul De Hert – Ronald Leenes (eds.): Computers, Privacy and Data Protection: an Element of Choice, Springer, pp. 345-360.

[55] Dix, Alexander (2001): A magyar információszabadság- törvény nemzetközi hatása – a brandenburgi modell és tapasztalatai, in: Majtényi László (szerk.): Az odaátra nyíló ajtó, Adatvédelmi Biztos Irodája, Budapest, pp. 69-76.

[56] Dix, Alexander (2010): Built-in privacy – no panacea, but a necessary condition for effective privacy protection, Identity in the Information Society, 2.sz. pp. 257-265. http://link.springer.com/article/10.1007%2Fs12394-010-0045-z#page-1 [2013.08.15]

[57] Dobos Balázs (2005): A magyarországi németek kitelepítése az 1941-es népszámlálás tükrében, Kisebbség Kutatás 3. sz. Lucidus Kiadó http://www.hhrf.org/kisebbsegkutatas/kk_2005_03/cikk.php?id=954 [2013.07.17.]

[58] Domokos, N. Márton (2013): Az EU új adatvédelmi szabályozása – avagy keep bangin' on the wall of Fortress Europe, Jogi Fórum http://www.jogiforum.hu/files/adatvedelem/Az_EU_uj_adatvedelmi_szabalyozasa.pdf [2014.05.05.]

[59] Dumortier, Jos – Goemans, Caroline (2000): Data Privacy and Standardization. Discusssion Paper prepared for the CEN/ISSS Open Seminar on Data Protection, K.U. Leuven, ICRI https://www.law.kuleuven.be/icri/publications/90CEN-Paper.pdf [2012. 10.20.]

[60] Farrell, Henry (2002): Negotiating Privacy across Arenas: The EU-US "Safe Harbor" Discussions, in: Adrienne Héritier (ed.): Common Goods: Reinventing European and International Governance, Rowman & Littlefield, Boston Way, Lanham, Maryland, pp. 105-126. http://www.utsc.utoronto.ca/~farrell/privacy1.pdf [2014.05.20.]

[61] Finn, Rachel L. – Wright, David – Friedewald, Michael (2013): Seven Types of Privacy, in: Serge Gutwirth – Ronald Leenes – Paul de Hert – Yves Poullet: European Data Protection: Coming of Age, Springer, pp. 3-32.

[62] Friedrichs, Günter – Schaff, Adam (1984): Mikroelektronika és társadalom - Áldás vagy átok, Statisztikai Kiadó Vállalat, Budapest

[63] Fuster, Gloria Gonzalez – Gutwirth, Serge – De Hert, Paul (2010): From Unsolicited Communications to Unsolicited Adjustments, in: Serge Gutwirth – Yves Poullet – Paul de Hert (eds.): Data Protection in a Profiled World, Springer, pp. 105-117.

[64] Galántai Zoltán (2003): E-privacy olvasókönyv, Arisztotelész, Budapest http://mek.oszk.hu/04100/04134/html/ [2013.07.17.]

[65] Gárdos-Orosz Fruzsina (2011): Alkotmányos polgári jog? Az alapvető jogok alkalmazása a magánjogi jogvitákban, Dialóg Campus, Budapest-Pécs

[66] Halász Bálint (2012): Személyes adatok kezelése hozzájárulás nélkül – egy uniós bírósági ítélet és következménye, Infokmmunikáció és jog, 1. sz. pp. 18-21.

[67] Hassan, Robert (2008): The Information Society, Polity Press, Cambridge

[68] Hegedűs Bulcsú (2013): Az adatvédelmi jog általános tanai, in: Tóth András (szerk.): Infokommunikációs jog II., Patrocínium, Budapest, pp. 128-219.

[69] Heinz Ervin – Lakatos Miklós (2004): A Központi Statisztikai Hivatal szerepe a német lakosság kitelepítésében, in: Czibulka Zoltán – Dr. Heinz Miklós – Dr. Lakatos Miklós (összeáll.): A magyarországi németek kitelepítése és az 1941. évi népszámlálás, Központi Statisztikai Hivatal Népszámlálási Főosztálya, Budapest http://www.nepszamlalas2001.hu/hun/egyeb/nemet/data/tartalom.html [2013.07.17.]

[70] Herendy Csilla (2010): A kereső, a dokumentumok és a user. A szemantikus web egy lehetséges nézőpontja, Médiakutató, 2010. tavasz http://www.mediakutato.hu/cikk/2010_01_tavasz/03_szemantikus_web [2014.03.20.]

[71] Herold, Rebecca (2011): Managing an Information Security and Privacy Awareness and Training Program, CRC Press, Boca Raton

[72] Hildebrandt, Mireille (2010): A New Type of Knowledge. Profiling the European Citizen. Cross-Disciplinary Perspectives, from Profiling the European Citizen, in: Mireille Hildebrandt – Serge Gutwirth (eds.): Profiling the European Citizens. Cross-Disciplinary Perspectives, Springer, pp. 17-30.

[73] Hildebrandt, Mireille – Gutwirth, Serge (2010): Concise Conclusions: Citizens out of Control, in: Mireille Hildebrandt – Serge Gutwirth (eds.): Profiling the European Citizens. Cross-Disciplinary Perspectives, Springer, pp. 365-368.

[74] Hirsch, Dennis D. (2013): Going dutch? Collaborative dutch privacy regulation and the lessons it holds for U.S. privacy law, Michigan State Law Review 83. sz. pp. 85-107. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393707 [2014.05.15.]

[75] Hustinx, Peter J. (2002): Co-regulation or self-regulation by public and private bodies – the case of data protection http://www.dutchdpa.nl/downloads_art/art_phu_2002_coregulation.pdf [2014.03.16.]

[76] Hustinx, Peter (2010): The Role of Data Protection Authorities, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer, pp. 131-137.

[77] Ilten, Carla – Guagnin, Daniel – Hempel, Leon (2012): Privacy Self-regulation Through Awareness? A Critical Investigation into the Market Structure of the Security Field, in: Serge Gutwirth – Ronald Leenes – Paul De Hert – Yves Poullet (eds.): European Data Protection: In Good Health? Springer, pp. 233-247.

[78] Irion, Kristina – Luchetta, Giacomo (2013): Online personal data processing and EU data protection reform. Brussels: Centre for European Policy Studies http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform [2013.11.23.]

[79] Jaquet-Chiffelle, David-Olivier (2010): Reply: Direct and Indirect Profiling in the Light of Virtual Persons, in: Mireille Hildebrandt – Serge Gutwirth (eds.): Profiling the European Citizens. Cross-Disciplinary Perspectives, Springer pp. 34-45.

[80] Jay, Rosemary – Hamilton, Angus (1999): Data Protection. Law and Practice, Sweet & Maxwell, London

[81] Jóri András (2005): Adatvédelmi kézikönyv, Osiris, Budapest

[82] Jóri András (2009): Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs

[83] Jóri András (2010): Az adatvédelmi és információszabadságért felelős biztos intézményéről, Fundamentum, 2. sz. pp. 20-32.

[84] Jóri András – Bártfai Zsolt (2005): Vitás kérdések az adatvédelmi törvény értelmezése körül, Infokommunikáció és jog, 5. sz. pp. 159-164.

[85] Jøsang, Audun – Fritsch, Lothar – Mahler, Tobias (2010): Privacy Policy Referencing, in: Sokratis Katsikas – Javier Lopez – Miguel Soriano (eds.): Trust, Privacy and Security in Digital Business, 7th International Conference, TrustBus 2010, Bilbao, Spain, August 30-31, 2010. Proceedings, Springer, pp. 129-140. http://link.springer.com/chapter/10.1007%2F978-3-642-15152-1_12#page-1 [2014.04.16.]

[86] Kardos Gábor (2003): Az emberi jogok nemzetközivé válása, in: Halmai Gábor – Tóth Gábor Attila (szerk.): Emberi jogok, Osiris, Budapest, pp. 66-80.

[87] Kierkegaard, Sylvia (2005): Safe Harbor Agreement –Boon or Bane?, Shidler Journal of Law, Commerce & Technology, 3. sz. http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/362/vol1_no3_art10.pdf?sequence=1 [2014.06.21.]

[88] Kiss Attila (2013): A privátszférát erősítő technológiák, Infokommuikáció és jog 3. sz. pp. 113-119.

[89] Kosta, Eleni (2013): Peeking into the cookie jar: the European approach towards the regulation of cookies, International Journal of Law and Information Technology, 4. sz. pp. 380–406.

[90] Kovács András – Polyák Gábor (2012): Alternatív piacszabályozási eszközök. A hatósági szerződések, valamint az ön- és társszabályozás térnyerése, Infokommunikáció és jog, 3. sz. pp. 123-126.

[91] Könyves-Tóth Pál – Székely Iván (ford.) (1991): Az NSZK Alkotmánybíróságának ítélete a népszámlálásról (1983), in: Könyves- Tóth Pál (szerk.): Informatika – Jog – Közigazgatás. Nemzetközi dokumentumok I., InfoFilia, Budapest pp. 6.1- 6.39

[92] Könyves-Tóth Pál (1992): A nyilvántartás nyilvánossága. Információs jogalkotás Magyarországon, Világosság 11. sz. pp. 807-815.

[93] Könyves-Tóth Pál (2013): Az Európai Unió új adatvédelmi rendeletének tervezete, Infokommunikáció és jog 1. sz. pp. 12-15.

[94] Kuner, Christopher (2012): The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Bloomberg BNA Privacy and Security Law Report, pp. 1-15. http://www.ico.org.uk/news/events/~/media/documents/future_of_dp_in_europe_2012/ico_event_future_of_dp_in_europe_2012_Chris_Kuner_article.ashx [2013.11.23.]

[95] Langheinrich, Marc – Finn, Rachel – Coroama, Vlad – Wright, David (2014): Quo Vadis Smart Surveillance? How Smart Technologies Combine and Challenge Democratic Oversight, in: Serge Gutwirth – Ronald Leenes – Paul de Hert (eds): Reloading Data Protection, Springer, pp. 151-182.

[96] Leenes, Ronald – Oomen, Isabelle (2010): The role of citizens. What can Dutch, Flemish and English students teach us about privacy?, in Serge Gutwirth – Yves Poullet – Paul De Hert, – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer, pp. 139-153.

[97] Leiner, Barry M. (2009): A Brief History of the Internet, ACM SIGCOMM Computer Communication Review, 5. sz. pp. 22-31. http://dl.acm.org/ft_gateway.cfm?id=1629613&ftid=608056&dwn=1&CFID=311242108&CFTOKEN=70276390 [2013.10.22.]

[98] Lessig, Lawrence (2006): Code, Version 2.0., New York, Basic Books, http://codev2.cc/download+remix/Lessig-Codev2.pdf [2014.03.16.]

[99] Liber Ádám (2011.): Személyes adatok nemzetközi továbbítása. Az új adatvédelmi törvény margójára, Infokommunikáció és jog 5. sz. pp. 179-186.

[100] Lussato, Bruno (1989): Az informatikai kihívás, OMIKK, Budapest

[101] Majtényi László (2002): Megőrizhető-e a magánélet az információs társadalomban?, in: Glatz Ferenc (szerk.): Információs társadalom és jogrendszer, MTA Társadalomkutató Központ, Budapest, pp. 95-104.

[102] Majtényi László (2003): Az információs jogok, in: Halmai Gábor – Tóth Gábor Attila (szerk.): Emberi jogok, Osiris, Budapest, pp. 577-635.

[103] Majtényi László (2006): Az információs szabadságok, Complex, Budapest

[104] Majtényi László (2011): „A képmutatás a bűn tisztelgése az erény előtt.” Az információs jogok a nemzeti együttműködés rendszerében, Fundamentum, 4. sz. pp. 106-115.

[105] Masuda, Yoneji (1988): Az információs társadalom, OMIKK, Budapest

[106] Mayer-Schönberger, Viktor (1998): Generational Development of Data Protection in Europe, in.: Philip E. Agre – Marc Rotenberg (eds.): Technology and Privacy: The New Landscape, The MIT Press, Cambridge and London, pp. 219-241.

[107] Mayer-Schönberger, Viktor (2009): Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, Princeton and Oxford

[108] Miller, Arthur, R. (1969): Personal Privacy in the Computer Age: The Challenge af a New Technology in an Information-Oriented Society, Michigan State Law Review 67. sz. pp. 1089-1246. http://heinonline.org/HOL/Page?handle=hein.journals/mlr67&div=75&g_sent=1&collection=journals#1103 [2012.11.20.]

[109] Moerel, Lokke (2012): Binding Corporate Rules, Corporate Self-Regulation of Global Data Transfers, Oxford University Press, Oxford

[110] Morgan, Richard – Boardman, Ruth (2012): Data Protection Strategy. Implementing Data Protection Compliance, Sweet & Maxwell, London

[111] Morton, Anthony (2014): “All my mates have got it, so it must be okay”: Constructing a Richer Understanding of Privacy Concerns, in: Serge Gutwirth – Ronald Leenes – Paul de Hert (eds): Reloading Data Protection, Springer, pp. 259-298.

[112] Movius, Lauren B. – Krup, Nathalie (2009): U.S. and EU Privacy Policy: Comparison of Regulatory Approaches, International Journal of Communication 3. sz. pp. 169-187. http://ijoc.org/index.php/ijoc/article/view/405/305 [2013.09.13.]

[113] Nagy Csongor István (2012): A fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlatot érintő vállalati önszabályozás perspektívái, Verseny és szabályozás, 1. sz. pp. 141-173. http://econ.core.hu/file/download/vesz2012/onszabalyozas.pdf [2013.09.15.]

[114] O’Reilly, Tim (2005): What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software http://oreilly.com/web2/archive/what-is-web-20.html [2014.03.20.]

[115] Pariser, Eli (2011): The Filter Bubble. What the Internet Is Hiding from You, The Penguin Press, New York

[116] Polefkó Patrik (2011): Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (4. rész), Infokommunikáció és jog, 1. sz. pp. 32-34.

[117] Polyák Gábor (2011): Technológiai determinizmus a kommunikáció szabályozásában, Információs Társadalom, 3. sz. pp. 31-47.

[118] Polyák Gábor (2002): Hatalom-leosztás, avagy önszabályozás az Interneten http://www.jogiforum.hu/letoltes/!/files/publikaciok/polyak_hatalom_leosztas.doc!1399376642!/publikaciok/63 [2013.09.13.]

[119] Polyák Gábor – Szőke Gergely László (2011): Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései, in: Drinóczi Tímea (szerk.): Magyarország új alkotmányossága, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs, pp. 155-177.

[120] Polyák Gábor – Szőke Gergely László (2014): Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére, in: Nemeslaki András (szerk.): E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek, Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kar, Budapest, pp. 65-89.

[121] Poullet, Yves (2010): About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?, in: Serge Gutwirth – Yves Poullet – Paul De Hert (eds.): Data Protection in a Profiled World, Springer, pp. 3-30.

[122] Racskó Péter (2014): Big Data a közigazgatásban, in: Nemeslaki András (szerk.): E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek, Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kar, Budapest, pp. 258-271.

[123] Raffai Mária (1997): Az informatika fél évszázada, Springer Hungarica, Budapest

[124] Rauhofer, Judith (2013): One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework, Journal of Law and Economic Regulation, 1.sz. pp. 57-84. http://ssrn.com/abstract=2260967 [2013.09.13.]

[125] Rauhofer, Judith (2014): Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age, Edinburgh School of Law Research Paper 6. sz. University of Edinburgh http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2389981 [2014.09.13.]

[126] Rátai, Balázs – Szádeczky, Tamás – Szőke, Gergely László (2012): Methodology to implement and audit of a Privacy Management System concerning monitoring in employment relationships, in: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest, pp. 301-310.

[127] Reidenberg, Joel. R. (1998): Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review, 3. sz. http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship [2013.08.23.]

[128] Reding, Viviane (2011): The upcoming data protection reform for the European Union, International Data Privacy Law, 1. sz. pp. 3-5.

http://idpl.oxfordjournals.org/content/1/1/3.full.pdf+html [2013.09.22.]

[129] Regan, Priscilla M. (1995): Legislating Privacy, University of North Caroline Press, Chapel Hill & London

[130] Robinson, Neil – Graux, Hans – Botterman, Maarten – Valeri, Lorenzo (2009): Review of the European Data Protection Directive, Rand Corporation, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf [2013.10.18.]

[131] Rodotà, Stefano (2010): Data Protection as a Fundamental Right, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer, pp. 77-82.

[132] Ropolyi László (2006): Az Internet természete: internetfilozófiai értekezés, Typotex, Budapest

[133] Rouvroy, Antoinette – Poullet, Yves (2010): The Right to Informational Self-Determination and the Value of Self-Deployment: Reassessing the Importance of Privacy for Democracy, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer, pp. 45-76.

[134] Rubinstein, Ira S. (2012): Regulating Privacy by Design, Berkeley Technology Law Journal, 26. sz. pp. 1410-1456. http://ssrn.com/abstract=1837862 [2013.11.20.]

[135] Rudgard, Sian (2012): Origins and historical context of data protection law, in: Eduardo Ustaran (ed.): European Privacy. Law and Practise for Data Protection Professionals, International Association for Privacy Professionals, pp. 3-17. https://www.privacyassociation.org/media/pdf/publications/European_Privacy_Chapter_One.pdf [2013.08.10.]

[136] Ruiter, Joep – Warnier, Martijn (2011): Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice, in: Serge Gutwirth – Yves Poullet– Paul De Hert – Ronald Leenes (eds.): Computers, Privacy and Data Protection: an Element of Choice, Springer, pp. 361-376.

[137] Schäfer, Georg E. (2013): History of Computer Science, BoD, Books on Demand, Norderstedt

[138] Simitis, Spiros (1987): The Hessian Data Protection Act, The Hessian Data Protection Commissioner, Wiesbaden

[139] Simon Éva (2005): Egy XIX. századi tanulmány margójára, Információs társadalom, 2. sz. pp. 32-43.

[140] Solove, Daniel, J. (2013): Introduction: Privacy Self-Management and the Consent Dilemma, Harward Law Review, 7.sz. pp. 1880-1903 http://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/ [2014.06.10.]

[141] Soós Andrea Klára (2012): Az adatvédelmi hatóságok „teljes függetlensége”: az Európai Unió Bíróságának gyakorlata, Infokommunikáció és jog, 5-6. sz. pp. 219-223.

[142] Sólyom László (1983): A személyiségi jogok elmélete, Közgazdasági és Jogi Könyvkiadó, Budapest

[143] Sólyom László (1988): Egy új szabadságjog: az információszabadság, Valóság, 9. sz. pp. 14-34.

[144] Sundmaeker, Harald – Guillemin, Patrick – Friess, Peter – Woelfflé, Sylvie (2010): Vision and Challenges for Realising the Internet of Things http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf [2013.08.10.]

[145] Swire, Peter P. (1997): Theory of Markets and Privacy http://www.ntia.doc.gov/print/page/chapter-1-theory-markets-and-privacy [2012.10.14.]

[146] Szabó Máté Dániel (2005): Kísérlet a privacy meghatározására a magyar jogrendszer fogalmaival, Információs Társadalom, 2. sz. pp. 44-54.

[147] Szabó Máté Dániel (2012): Az információs hatalom alkotmányos korlátai, Miskolci Egyetem, Miskolc

[148] Szádeczky Tamás (2008): Terrorizmus a kibertérben, Infokommunikáció és jog, 5. sz. pp. 200-205.

[149] Szádeczky Tamás (2011): Szabályozott biztonság: Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan, PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs

[150] Szádeczky Tamás (2012): The role of the technology. Auditing and certification in the field of data security, in: Szőke Gergely László (ed.): Privacy In The Workplace. Data Protection Law and Self-Regulation in Germany and Hungary, Budapest, HVG-ORAC, pp. 311-337.

[151] Szádeczky Tamás (2013): Az IT biztonság szabályozásának konfliktusa, Infokommunikáció és jog, 3. sz. pp. 151-155.

[152] Székely Iván (2002): Adatvédelem és nyilvánosság, in: Lajtha György (szerk.): Távközlő hálózatok és informatikai szolgáltatások, Hírközlési és Informatikai Tudományos Egyesület, Budapest, pp. 127-140. http://www.regi.hte.hu/data/upload/File/online/THIS/1.pdf [2014.10.24.]

[153] Székely Iván (2004): Adatvédelem és információszabadság, Fundamentum, 4. sz. pp. 47-54.

[154] Székely Iván (2008): Privátszférát erősítő technológiák, Információs Társadalom, 1. sz. http://pet-portal.eu/files/oldfiles/articles/2008/02/InfTars_PET.pdf [2014.03.17.]

[155] Székely Iván (2012): The Right to Forget, the Right to be Forgotten, in: Serge Gutwirth – Ronald Leenes – Paul De Hert – Yves Pullet (eds.): European Data Protection: In Good Health?, Springer, 2012, pp. 347-363.

[156] Székely Iván (2013): Jog ahhoz, hogy elfelejtsenek és töröljenek, Információs társadalom, Információs társadalom, 3-4. sz. pp. 7-27. http://www.infonia.hu/digitalis_folyoirat/2013/2013_34/i_tarsadalom_2013_34_szekely.pdf [2014.03.17.]

[157] Székely, Iván – Szabó, Máté Dániel – Vissy, Beatrix (2011): Regulating the future? Law, ethics, and emerging technologies, Journal of Information, Communication and Ethics in Society, 3. sz. http://publications.ceu.hu/sites/default/files/publications/szekely-szabo-vissyregulatingthefuture.pdf [2014.10.25.]

[158] Szigeti Tamás (2009): Az információs hatalom korlátozása tengeren innen és túl, Infokommunikáció és jog, 4. sz. pp. 159-165.

[159] Szigeti Ferenc – Végső Károly – Kiss István (2003): Minőségirányítási ismeretek, Nyíregyházi Főiskola http://mmfk.nyf.hu/min/index.htm [2012.10.28.]

[160] Sziklay Júlia (2009): 9/11 hatása a privacy amerikai értelmezésére, in: Sziklay Júlia (szerk.): Az információs jogok kihívásai a XXI. században, Adatvédelmi Biztos Irodája, Budapest

[161] Sziklay Júlia (2011): Az információs jogok kialakulása, fejlődése és társadalmi hatása, PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs

[162] Szőke, Gergely László (2012): Self-regulation, audit and certification schemes in the field of Data Protection, in: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest, pp. 287-300.

[163] Szőke Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése, Infokommunikáció és jog, 3. sz. pp. 107-112.

[164] Szőke Gergely László (2014): Az önszabályozás, audit és tanúsítás lehetőségei és korlátai az adatvédelem területén, Infokommunikáció és jog, 1. sz. pp. 14-20.

[165] Szurday Kinga (2009): 2001. szeptember 11-e következménye a személyes adatok védelmére vonatkozó politikára az Európai Unióban, in: Sziklay Júlia (szerk.): Az információs jogok kihívásai a XXI. században, Adatvédelmi Biztos Irodája, Budapest

[166] Tene, Omer (2011): Privacy: The new generations, International Data Privacy Law, 1. sz. pp. 15-27.

http://idpl.oxfordjournals.org/content/1/1/15.full.pdf+html [2013.09.12]

[167] Tene, Omer – Polotensky, Jules (2011): To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising, Minnesota Journal of Law, Science & Technology, 1. sz. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1920505 [2012.10.20.]

[168] Tene, Omer – Polotensky, Jules (2012): Big Data for All: Privacy and User Control in the Age of Analytics http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364 [2013.10.28.]

[169] Terwangne, Cécile (2014): The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data, International Review of Law, Computers & Technology, 2. sz. pp. 118-130. http://dx.doi.org/10.1080/13600869.2013.801588 [2014.10.23.]

[170] Tófalvy Tamás (2013): Média a törvényen túl? Önszabályozás a magyar írott médiában: előzmények, kontextus, lehetőségek, Médiakutató, 4. sz. pp. 85-95. http://www.mediakutato.hu/cikk/2013_04_tel/06_media_onszabalyozas.pdf [2014.06.18.]

[171] Turow, Joseph – Draper, Nora (2012): Advertising's new surveillance ecosystem, in.: Kirstie Ball – Kevin D. Haggerty – David Lyon (eds.): Routledge Handbook of Surveillance Studies, Routledge, London, pp. 133-140.

[172] Van Alsenoy, Brendan – Ballet, Joris – Kuczerawy, Aleksandra – Dumortier Jos (2009): Social networks and web 2.0: are users also bound by data protection regulations? Identity in the Information Society, 1. sz. pp. 65-79. http://link.springer.com/article/10.1007%2Fs12394-009-0017-3#page-1 [2013.10.01.]

[173] Varga János (2011): A „szűréstudók" felelőssége – Akik eldöntik, mit akarunk szabadon olvasni az interneten http://www.nyest.hu/hirek/a-szurestudok-felelossege-akik-eldontik-mit-akarunk-szabadon-olvasni-az-interneten [2014.06.18.]

[174] Walrave, Michele – Heirman, Wannes (2011): Disclosing or protecting? Teenagers' online self-disclosure, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Ronald Leenes: Computers, Privacy and Data Protection: an Element of Choice, Springer, pp. 285-307.

[175] Warren, Samuel D. – Brandeis, Louis D (1890): The Right to Privacy, Harvard Law Review 4. sz. pp. 193-220. http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/hlr4&id=205&terms=photograph#207 [2013.06.15.]

[176] Warren, Samuel D. – Brandeis, Louis D. (2005): A magánszférához való jog, Információs társadalom, 2. sz. pp. 7-31.

[177] Westin, Alan F. (1967): Privacy and freedom, Atheneum, New York

[178] Whitman, James Q. (2004): The Two Western Cultures of Privacy: Dignity versus Liberty, Yale Law Journal, 113. sz.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=476041 [2013.06.10.]

[179] Winn, J. K. (2010): Technical Standard as Data Protection Regulation, in: Serge Gutwirth – Yves Poullet – Paul De Hert – Cécile Terwangne – Sjaak Nouwt (eds.): Reinventing Data Protection?, Springer pp. 191-206.

[180] Z. Karvalics László (2003): Információ, társadalom, történelem, Typotex, Budapest

[181] Zanfir, Gabriela (2014): Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law, in: Serge Gutwirth – Ronald Leenes – Paul de Hert (eds.): Reloading Data Protection, Springer, pp. 237-257.

[182] Zágoni Miklós (2000): A technikától az etikáig: a technológiai neutralizmus kritikája http://orszagepito.hu/sites/all/files/orszagepito-hu/lapszam/2000-3/2000-3.pdf [2013.12.14.]

7.3 További források

[183] ABI (2005): Az adatvédelmi biztos 1790/A/2004 számú válaszlevele http://abi.atlatszo.hu/index.php?menu=beszamolok/2005/M/3&dok=1790_A_2004

[184] Ádám Szilveszter (2014): Egy új jogintézmény születése. A személyes adatok megsértésének szabályozása és gyakorlata az elektronikus hírközlésben, konferencia-előadás a XV. Infokommunikációs Szakmai Nap - Az adatvédelmi szabályozás tendenciái című konferencián 2014. április 17-én

[185] Bangemann-jelentés (1994): Europe and the global information society, Bangemann report recommendations to the European Council, http://www.epractice.eu/files/media/media_694.pdf [2014.04.12]

[186] Bényi Orsolya (2014): Adatvédelmi incidens szolgáltatói szemmel, konferencia-előadás a XV. Infokommunikációs Szakmai Nap - Az adatvédelmi szabályozás tendenciái című konferencián 2014. április 17-én

[187] Bizottsági Rendelettervezet: Javaslat - Az Európai Parlament és a Tanács Rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet), COM(2012) 11 final

[188] CEN (2002): Initiative on Privacy Standardization in Europe, Final Report CEN/ISSS Secretariat, Brussels http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/ipsefinalreportwebversion.pdf [2012.10.20.]

[189] CEN CWA 15262-2005: CEN Workshop Agreement on Inventory of Data Protection Auditing Practices,

[190] CEN CWA 15263-2005: CEN Workshop Agreement on Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization

[191] CEN CWA 15292:2005: CEN Workshop Agreement on Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)

[192] Charles Babbage Institute (2013): Report on the IBM Joint Data Security Studies https://wiki.umn.edu/CBI_ComputerSecurity/PubReportofIBMJointStudies [2013.07.17.]

[193] Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Jan Philipp Albrecht). Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011–C7-0025/2012–2012/0011(COD)). http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf [2013.08.15.]

[194] Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Jan Philipp Albrecht). Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011–C7-0025/2012–2012/0011(COD)). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN [2013.08.15.]

[195] Eurobarometer (2008a): Flash Eurobarometer 225, Data Protection - General Public, Country Specific Questionnaire Hungary http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf [2013.11.20.]

[196] Eurobarometer (2008b): Flash Eurobarometer 226, Data Protection - Data Controllers' Perceptions, Country Specific Questionnaire Hungary http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf [2013.11.20.]

[197] Eurobarometer (2011): Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [2013.09.17.]

[198] Európai Bizottság (1997): Konvergencia Zöld Könyv. A távközlési, média és információtechnológiai szektorok konvergenciájáról és ennek szabályozási kihatásairól, COM(97) 623 final

[199] Európai Bizottság (2000): A Bizottság határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott "biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről (2000/520/EK)

[200] Európai Bizottság (2007): A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak az adatvédelemnek a magánélet védelmét erősítő technológiák által történő ösztönzéséről COM(2007) 228 final

[201] Európai Bizottság (2010a): A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A szabadság, a biztonság és a jog érvényesülésén alapuló térség megvalósítása a polgárok szolgálatában, COM (2010) 171 végleges

[202] Európai Bizottság (2010b): A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és A Régiók Bizottságának. Az európai digitális menetrend. COM (2010) 245 végleges/2

[203] Európai Bizottság (2010c): A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. A személyes adatok európai unión belüli védelmének átfogó megközelítése, COM(2010) 609 végleges

[204] Európai Bizottság, (2013): A bizottság közleménye az Európai Parlamentnek és a Tanácsnak a védett adatkikötő működése az uniós polgárok és az EU-ban letelepedet vállalatok szempontjából, COM(2013) 847 final

[205] European Commission (1994): Europe's Way to the Information Society. An Action Plan. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM (94) 347 final

[206] European Commission (2000): eEurope 2002. An Information Society For All, COM (2000) 330 final

[207] European Commission (2004): Commission Staff Working Document – The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC (2004) 1323

[208] European Commission (2010): Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final

[209] European Commission (2012): Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (2012) 11 final

[210] eTForecast (2014): Worldwide PC market http://www.etforecasts.com/products/ES_pcww1203.htm [2014.02.14.]

[211] European Parliament – European Commission (2003): Interinstitutional Agreement on better law-making. European parliament, Council of the European Union, Commission of the European Communities (2003/C 321/01)

[212] European Union Agency for Fundamental Rights (2010): Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II. Luxembourg: Publications Office of the European Union,

http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf [2014.02.14.]

[213] IBM (2014): IBM AS/400 http://sysrun.haifa.il.ibm.com/ibm/history/exhibits/rochester/rochester_4010.html [2014.02.14.]

[214] ICO (2001): Data Protection Audit Manual, UK Information Commissioner's Office, http://www.privacylaws.com/documents/external/data_protection_complete_audit_guide.pdf [2012.11.20.]

[215] ICO (2012): Auditing data protection. A guide to ICO data protection audits. UK Information Commissioner's Office http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/guide_to_ico_data_protection_audits_v2.ashx [2012.11.20.]

[216] ICO (2013): Bring your own device (BYOD), ICO, http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.pdf [2014.10.24.]

[217] Irányelv tervezet: Javaslat - Az Európai Parlament és a Tanács irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, COM/2012/010 final (a továbbiakban irányelv-tervezet)

[218] József Attila (1980): Levegőt, in: József Attila minden verse és versfordítása, Szépirodalmi Könyvkiadó, Budapest, pp. 389-390.

[219] Kádár Ákos (2012): Buborékba zár az internet http://www.nyest.hu/hirek/buborakba-zar-az-internet [2014.06.18.]

[220] Kodak (2013): History of Kodak http://www.kodak.com/ek/US/en/Our_Company/History_of_Kodak/Milestones_-_chronology/1878-1929.htm [2013.08.22.]

[221] McDermott, John (2014): WTF is cross-device tracking? http://digiday.com/platforms/wtf-cross-device-tracking [2014.06.20.]

[222] MSZ EN ISO/IEC 17021:2011. Megfelelőségértékelés. Irányítási rendszerek auditját és tanúsítását végző testületekre vonatkozó követelmények

[223] MSZ EN ISO 9000:2005. Minőségirányítási rendszerek. Alapok és szótár

[224] MTE Tartalomszolgáltatási Kódex: Tartalomszolgáltatási Kódex a Magyar Tartalomszolgáltatók Egyesületének a tartalomszolgáltatásra vonatkozó működési, etikai és eljárási szabályzata (utolsó felülvizsgálat időpontja: 2009. október 21.), http://mte.hu/etikaikodex.html [2014.06.06]

[225] NAIH (2013): Szakmai szempontok az adatvédelmi audit végzéséhez

http://naih.hu/files/AdatvedelmiAuditSzakmaiSzempontokVegleges.pdf [2014.03.20.]

[226] OECD (1980): Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról (kivonatolt magyar nyelvű fordítás) http://www.oecd.org/sti/ieconomy/15590228.pdf [2013.09.13.]

[227] Stockholmi Program: A Stockholmi Program – a polgárokat szolgáló és védő, nyitott és biztonságos Európa (2010/C 115/01)

[228] The Boston Consulting Group (2012): The Value of Our Digital Identity. (Liberty Global Policy Series) http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf [2014.06.18.]

[229] The Economist Intelligence Unit (2013): Privacy Uncovered. Can private life exist in the digital age?, a report from The Economist Intelligence Unit http://www.economistinsights.com/analysis/privacy-uncovered/methodology [2014.05.12.]

[230] WP29 (1998): Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct (WP13)

[231] WP29 (1999): Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government (WP15)

[232] WP29 (2007): Opinion 4/2007 on the concept of personal data (WP 136)

[233] WP29 (2008): Working Document Setting up a framework for the structure of Binding. Corporate Rules (WP154)

[234] WP29 (2009): The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168)

[235] WP29 (2010a): 2/2010. számú vélemény a viselkedésalapú online reklámról (WP171)

[236] WP29 (2010b): 3/2010 vélemény az elszámoltathatóság elvéről (WP173)

[237] WP29 (2011a): Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments (WP184)

[238] WP29 (2011b): Opinion 15/2011 on the definition of consent (WP187)

[239] WP29 (2014): Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217)