Pécsi Tudományegyetem
Állam- és Jogtudományi Kar
Doktori Iskola

DR. SZŐKE GERGELY LÁSZLÓ

ADATVÉDELEM ÉS ÖNSZABÁLYOZÁS. ADATVÉDELMI IRÁNYÍTÁSI RENDSZER AZ ADATKEZELŐKNÉL

Doktori értekezés tézisei
Műhelyvitára szánt, nem végleges verzió

Témavezetők

Dr. Balogh Zsolt György, PhD,
tudományos főmunkatárs

Dr. Majtényi László,
az MTA doktora,
egyetemi tanár

Pécs 2014

1. A témaválasztás indokolása és a kitűzött kutatási feladat rövid összefoglalása

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.

A témaválasztást két együttes tényező, egy objektív folyamat mellett személyes indíttatás is indokolja, amelyek meghatározzák a disszertáció két nagy szakmai egységét 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. fejezet az új jogintézményeket és a Rendelettervezet[2] szövegét nem tételesen, hanem egy általam kidolgozott (elméleti) újgenerációs adatvédelmi szabályozási keretrendszerbe helyezve, kritikai szemlélettel elemzem.

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 informatikai biztonság területén, amelynek eredményei és szemlélete az adatvédelem területén is jól hasznosíthatók. Ennek érdekében az 5. fejezet az adatkezelők belső szabályozására, egy, az adatkezelők szintjén kialakítandó adatvédelmi irányítási rendszer kialakítására és annak főbb elemeire tesz javaslatot. Az adatkezelők szintjén megalkotott belső szabályozási eszközöket az önszabályozás egyik formájának tekintem, így a 4. fejezetben áttekintem az adatvédelmi önszabályozással kapcsolatos meglévő szabályokat és jogirodalmi nézeteket, ideértve az (ön)felügyeleti eszköznek tekinthető adatvédelmi audit és adatvédelmi tanúsítás jogintézményét is.

A fenti két tényező egymással szorosan összefügg. Az adatvédelmi reform egyik legfontosabb fejleménye éppen az adatkezelők szerepének előtérbe kerülése, a rájuk vonatkozó

[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 95/46/EK irányelv vagy adatvédelmi irányelv)

[2] 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.)

kötelezettségek növekedése és azok szigorúbb felügyelete. A korábbiakhoz képest várhatóan 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 elemzése, a jelenleg Európában zajló adatvédelmi reform egyes eredményeinek bemutatása és kritikai értékelése. Másodszor a dolgozat megoldást kínál a szabályozás jól látható tendenciáiból, az adatkezelők növekvő kötelezettségeiből eredő, adatkezelőket érintő kihívásokra egy adatvédelmi irányítási rendszer elemeinek bemutatásával.

2. A kutatás tézisei, az elvégzett vizsgálatok összefoglalása és kutatás módszertana

A disszertáció egymással szorosan összefüggő tézisei a következők.

1. Az adatvédelmi szabályozás fejlődésének egyik közvetlen mozgatórugója – több más, elsősorban politikai és gazdasági hatás mellett – az informatikai- és kommunikációs technológiák fejlődése, és e technológiák alkalmazása.
2. Az elmúlt évtized technológiai fejlődése az adatvédelmi szabályozást újra olyan kihívások elé állította, amelyre jelen formájában nem tud hatékony választ adni. Az adatvédelem alapjait érintő új megközelítésre és szabályozási koncepcióra van szükség.
3. Az új megközelítés központi eleme, hogy az „érintett-központú” szabályozás felől nagymértékben el kell tolódni az „adatkezelő-központú” szabályozás felé.
4. Ennek következtében a korábbiakhoz képest jóval nagyobb hangsúlyt kap az adatkezelők belső szabályozása, egy tudatosan felépített adatvédelmi irányítási rendszer, amely az önszabályozás egyik eszközének is tekinthető.
5. A belső szabályozással történő adatvédelmi megfelelés (compliance) korántsem triviális feladat, de kialakítható egy olyan általános módszertan, amely az adatkezelők számára útmutatásként szolgálhat.

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, rendszere, és hogy igazoljam az első tézist. 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 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 adatvédelmi szabályozás főbb elemeit, és ennek fényében elemzem az új adatvédelmi Rendelettervezet főbb rendelkezéseit. 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 szabályozásának eszközeit is.

Végül az 5. fejezet az adatvédelmi irányítási rendszer kialakításának a módszertanát tartalmazza. A fejezet a dolgozat legfontosabb új kutatási eredményeit tartalmazza, és deklarált célja, hogy praktikus segítséget nyújtson az adatkezelők számára az adatvédelmi megfelelés (compliance) eléréséhez.

3. A tudományos eredmények összefoglalása, és a hasznosítás lehetőségei

3.1 Kutatási eredmények

A dolgozat tárgyát és kutatási módszertanát meghatározó, valamint egyes alapfogalmakat tisztázó bevezetőt követően a 2. fejezetben részletesen áttekintettem az adatvédelem eddigi fejlődését, amelyet – elsősorban a könnyebb áttekinthetőség kedvéért – generációs felosztásban tárgyaltam, többször hangsúlyozva, hogy éles cezúra az egyes korszakok között nem húzható. 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 fokozták, összességében – potenciálisan vagy ténylegesen – folyamatosan szűkítve az egyének magánszféráját.

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, hogyan, és milyen mértékben közölnek másokkal magukról információt”.[3] 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[4] mutatott, összességében azonban megállapítható, hogy 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.”[5]

A fentiek alapján az látható, hogy a szabályozás közvetlenül reagált,[6] 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. A fejlődéstörténet áttekintése alapján a dolgozat első tézisét összességében megalapozottnak látom.

Megállapítottam emellett, hogy az állami adatkezelésekkel szemben nagyjából-egészében jól működött (és működik ma is) az adatvédelem szabályozása: 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.

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 adatvédelmi rezsim – annak ellenére, hogy a potenciális problémáival a szakirodalom már igen korán elkezdett foglalkozni – ugyanakkor egy ideig egészen jól bevált egy új technológia 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 azonban már látszódtak. Egyre terjedtek a „kevésbé látványos” adatkezelések, így például az online világban már a weblap

[3] 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.

[4] 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.

[5] Mayer-Schönberger, 1998, 227.

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

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, 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.

A 3. fejezetben először is az adatvédelmi szabályozást érő újabb kihívásokat tekintettem át, ideértve a web 2.0-től kezdve, a profilozáson és az azon alapuló targetált szolgáltatásokon át a Big Data és a mindent átható számítástechnika egymással szorosan összefüggő és egymást kölcsönösen erősítő jelenségéig. Az is látható, hogy 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. A technológiai fejlődés adatvédelmi szempontból egyértelműen abba az irányba hat, hogy az adatkezelések átláthatatlansága és az információs hatalom aszimmetriája tovább fokozódik, az érintetti kontroll tényleges lehetősége pedig drasztikusan csökken.

Ezt a tendenciát az elmúlt években végzett közvéleménykutatások alapos elemzése is alátámasztotta,[7] hangsúlyozva, hogy az adatkezelésekkel kapcsolatos aggodalmak és a kontroll vágya – egyes esetekben hamis biztonságérzettel párosulva – széles körben megjelenik. Igaznak bizonyult a privacy paradoxon jelensége is, azaz az érintettek tényleges magatartása nincs feltétlenül összhangban az aggodalmaikkal, de a „mindenki felelőtlenül megoszt mindent" klisé egyértelműen cáfolható. Jelentős az a kutatási eredmény is, miszerint nem elhanyagolható azok aránya (30-40%), akiket nemigen foglalkoztatnak az adatvédelemmel kapcsolatos kérdések, és nincs szándékukban különösebben foglalkozni a magánszféra-védelmük menedzselésével.

Ezt követően részletesen elemeztem a hozzájárulás központú – ahogy Solove fogalmaz a „privacy self-management"[8] alapú – megközelítés kritikáját is. Solove és több más szakirodalmi forrás elemzése azt mutatja, hogy a felhasználók nem tudják igazán megismerni az adatkezelés feltételeit, és ha meg is ismerik, 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.[9] Emellett strukturális problémák is fennállnak, 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

[7] A dolgozatban elsősorban az Eurobarometer által készített 2008-as és 2011-es eredményeket valamint néhány további, kifejezetten közvélenykutatások eredményeit összegző szakirodalmi forrást elemeztem.
[8] Solove, 2013.
[9] Solove, 2013, 1883-1888. Solove ezeket kognitív problémáknak nevezi.

magas érzékenységgel rendelkezik. Emellett a hatalmas adatmennyiségnek és az adatbányászati technikák folyamatos fejlődésének köszönhetően nem látható, 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.[10] E helyzetelemzéssel egyetértve összességében azt látom, hogy az adatkezeléssel kapcsolatos döntések meghozatala során az érintettnek sok esetben esélye sincs az előnyök és veszélyek helyes mérlegelésére.

Természetesen számos elvi és gyakorlati érv hozható az információs önrendelkezési jog és az érintetti kontroll fontossága mellett is.[11] A közvéleménykutatások eredményei szintén összetett képet mutatnak: az érintettek egy részének tényleg nincs szándékában különösebben foglalkozni a magánszféra-védelmének menedzselésével, egy másik része pedig hiába szeretné, számos esetben – ilyen olyan okokból – érdemben nem képes kontrollt gyakorolni a személyes adatai kezelése felett. 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. És bár ez nem túlzottan széles réteg, 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.

A technikai és társadalmi 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 összefoglalása 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. Az adatvédelem alapjait érintő új megközelítésre és szabályozási koncepcióra van szükség."

A kutatás eredményeit figyelembe véve arra jutottam, hogy meg kell haladni az adatvédelmi szabályozás túlzott érintett-központúságát. Ez nem jelenti azt, hogy az érintetti kontrollal, vagy egyes országokban 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 nagyjából-egészében meg kell tartani, tudomásul véve, hogy tényleges korlátként csak ritkán funkcionál. Különösebben megerősíteni e pozíció jogi helyzetét[12] nem érdemes, az esetleges erősítésétől hatékonyabb adatvédelmi szabályozást várni pedig kifejezetten tévút.

Olyan szabályozási rezsimre van szükség, amely reálisan számol az érintettek passzivitásával, illetve lehetőségeinek korlátaival, és a jelenlegihez képest sokkal kevésbé tekinti őket az adatvédelmi szabályozás főszereplőjének. Az „érintett-központú" szabályozás felől el kell

[10] 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.

[11] Ld. például ezzel kapcsolatban Szabó Máté Dániel elemzését: Szabó, 2012, 30-32. Az információs önrendelkezési jog részleteiről ld. továbbá Majtényi 2006, 168-175.

[12] A jelenleg is fennálló jogok aktívabb gyakorlása

mozdulni az „adatkezelő-központú” szabályozás felé. Mindezt azonban nem az érintett rendelkezési jogát széleskörűen korlátozó paternalista szabályokkal, hanem olyan „mögöttes biztonságot” kínáló jogszabályi környezettel kell megoldani, amelyik 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. 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. 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 tanúsítószervezetek közbeiktatásával felügyel. E megközelítés nem érinti az alapjogi védelem létjogosultságát. 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 egy újgenerációs adatvédelmi szabályozás főbb elvi elemeit, és ezen elvi modellhez mérten elemeztem az új adatvédelmi Rendelettervezet egyes rendelkezéseit. Az újgenerációs szabályozás pillérei három pontban foglalhatók össze.

1. Az adatkezelők szerepének újragondolása.

   Az összes szereplő számára kulcsfontosságú azonban 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 kötelezettségek kell előírni, amelyek segítségével ténylegesen igazolhatják, hogy betartják és végrehajtják az adatvédelmi szabályokat.

   Kulcsfontosságú azonban e megközelítés során az adatkezelők differenciálása, azaz a szabályozási terhek megfelelő szétosztása, mivel az adatkezelések bizonyos jellemzői alapján az azzal kapcsolatos kockázatok jelentősen eltérhetnek. Ezen eltéréseket hangsúlyosan figyelembe kell venni, ami tulajdonképpen az informatikai biztonság 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

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 azonban a piaci alapon működő (ön)felügyeleti módozatok, az adatvédelmi audit és tanúsítás intézményét. Egy komplex adatvédelmi irányítási rendszer 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. Privacy by Design megközelítés éppen arra 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 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.

A fenti pontokat összefoglalva az látszik, hogy ha

- a létrejövő új jogi rezsimben az adatkezelők elszámoltathatósága révén az adatkezelők 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 lehet magasabb védelmi szintet garantálni.

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 tartalmaz.

Az elszámoltathatóság elvének jegyében számos új kötelezettséget ír elő nemcsak az adatkezelők, hanem és adatfeldolgozók számára is. Utóbbi üdvözlendő fejlemény, mivel sokszor inkább 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. Jelentős előrelépés várható tehát az „adatkezelő-központú” szabályozás irányába. Az elszámoltathatóság elvének való megfelelés azzal is jár, hogy az egyes adatkezelők és adatfeldolgozók kénytelenek az adatvédelem belső

szabályozásra a korábbinál lényegesen nagyobb hangsúlyt fektetni. Ez jelentően növeli az adatkezelők tudatosságát, javítja az adatbiztonsági potenciált és csökkenti a jogellenes adatkezeléseket. Ezen eredmények alapján igazolható a dolgozat negyedik tézise, miszerint „a korábbiakhoz képest jóval nagyobb hangsúlyt kap az adatkezelők belső szabályozása, egy tudatosan felépített adatvédelmi irányítási rendszer, amely az önszabályozás egyik eszközének is tekinthető."

A tervezett rendelkezések ugyanakkor jelentős compliance-költséget okoznak, és könnyen az adatvédelem „túladminisztrálásához" vezethetnek. 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. A Rendelettervezet jelentős lépést tesz a differenciálás terén, de számos, valóban bonyolult belső adminisztrációt igénylő kötelezettség (például az adatvédelmi hatásvizsgálat vagy a data breach notification) egyértelműen túlzottan széles alanyi kört érint. A differenciálás területén tehát további, egyes adatkezelők/adatszolgáltatók terheinek jelentős csökkentését eredményező lépésekre van szükség – érvényesítve az informatikai biztonság területén régóta érvényesülő kockázatarányos védelem elvét.

A Rendelettervezet nagymértékben megerősíti az adatvédelmi felügyelő hatóságok szerepét, hatósági jogkörökkel és bírságolási joggal felruházva azokat. Ez meglátásom szerint egyértelműen helyes irány, de a megerősített jogok mellett fontos a felügyelőhatóságok aktív szerepvállalása is, amelyet a szabályozás önmagában nem képes garantálni. Egyetértek Peter Hustinx felvetésével, aki arra hívja fel a figyelmet, hogy a hatósági feladatok során különös jelentősége lehet néhány nagy horderejű, jelentős erőforrást igénylő vizsgálat lefolytatásának, valamint a rendszeres hivatalból történő eljárásoknak.[13] Végül rá kell mutatni, hogy az adatvédelmi vizsgálatok során nélkülözhetetlenné vált az informatikai, sőt az informatikai biztonsági szakismeret. Ezek 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 ahhoz, hogy kampányszerű tiltakozások mellett komoly párbeszédre legyenek képesek az iparági szereplőkkel."[14] Pontos statisztikák a hatóságok személyi állományáról és annak végzettségéről és szakértelméről nem állnak rendelkezésemre, de az idézett források alapján, és a magyarországi helyzetet nagyjából ismerve szinte bizonyos, hogy a legtöbb adatvédelmi felügyelő hatóságnak jelentős elmaradása van e területen.

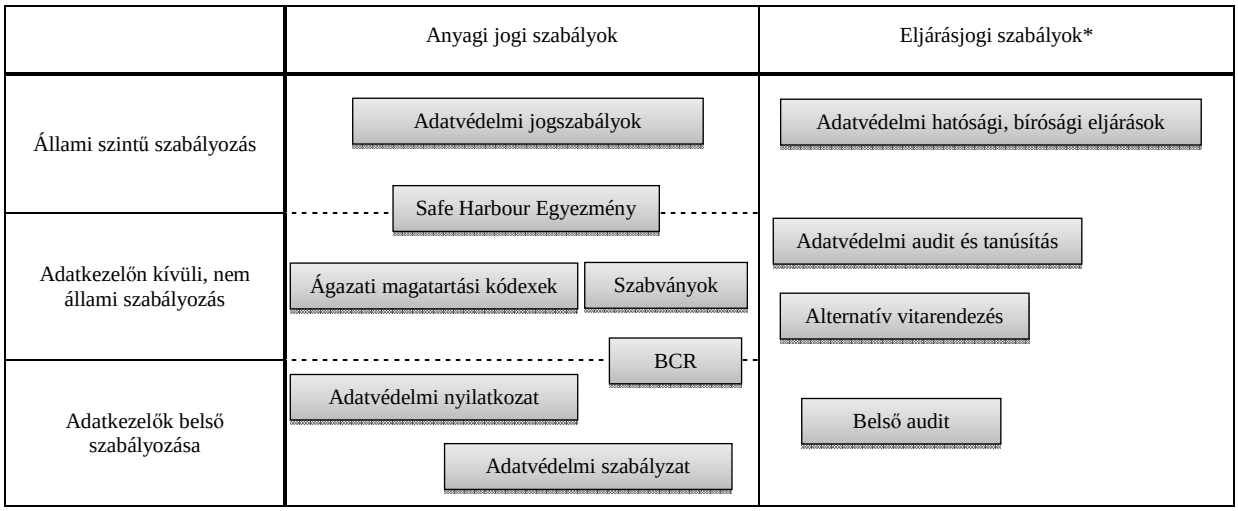
A Rendelettervezet ugyancsak jelentős előrelépést tesz a technológia és jog szabályozószerepének tisztázásában. A Privacy by Design megközelítés annak biztosítására tesz ígéretes kísérletet, hogy a technológia és jog, mint két szabályozórendszer ne kioltsa, hanem erősítse egymást, és egyértelműen a technológiát állítsa a – társadalmi elvárásokat végső soron kötelező normaként megjelenítő – jogi szabályozás szolgálatába, és megtartsa így

[13] Hustinx, 2010, 136. Hustinx összességében arra helyezi a hangsúlyt, hogy a hatóságoknak képesnek kell lenniük megfelelően priorizálni a feladat- és hatásköreik ellátása során.
[14] A CEN/ISSS adatvédelmi szabványosítással kapcsolatos projektjének záródokumentumát idézi Jóri, 2009, 291.

a jogi szabályozás elsőbbségét. A privátszférát erősítő technológiák e célkitűzések megvalósításának első számú eszközei lehetnek.

A 4. fejezet az adatvédelmi önszabályozás kérdését tárgyalja, mivel az adatkezelők belső szabályozása az önszabályozás egyik formájának tekinthető. E fejezetben rendszerező módszert követve tekintem át az adatvédelmi önszabályozás fontosabb eszközeit.

Ennek keretében megkülönböztettem egyrészt az anyagi jogi és a megfelelés-ellenőrzésre szolgáló eljárásjogi normákat, másrészt az állami, az adatkezelőn kívüli nem állami, és az adatkezelők belső szabályozásának szintjét, majd e mátrixban elhelyeztem az egyes önszabályozásra szolgáló eszközöket:



A negyedik fejezet következtetései során rámutattam az egyik önszabályozási forma, az ágazati magatartási kódexekkel kapcsolatos nehézségekre is, ami – úgy tűnik – szigorú állami szabályozás nélkül nem hatékony (amerikai modell), részletes állami szabályozás mellett viszont nem különösebben elterjedt (európai modell). Utóbbin az adatvédelem újabb tendenciái sem látszanak érdemben 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 – az adatkezelői szintre tolódik.

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, a működésüket már-már ellehetetlenítő problémára igyekszik megoldást kínálni. Az audit módszertan elemzése az utolsó fejezet előkészítésének is tekinthető: az adatkezelők adatvédelmi irányítási rendszerét mindenképpen úgy célszerű kialakítani, hogy az könnyen auditálható legyen, azaz egyértelműen megállapítható legyen egyes követelményekkel kapcsolatban azok teljesülése vagy nem teljesülése. Mivel azonban az adatvédelem szabályozása részben absztrakt elveket tartalmaz, ez korántsem triviális feladat.

Végül a dolgozat 5. fejezete az adatvédelmi irányítási rendszer fogalmának meghatározását és a kiépítésének módszertanát tartalmazza. Az irányítási rendszer módszertanának szükségszerűen általánosnak kell lennie, mivel így széles körben hasznosulhat. A módszertan alkalmazása 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. Ezzel együtt biztosítani kell, hogy a módszertant alkalmazó adatkezelők valóban elérhessék a jogszabályoknak való megfelelést, azaz kitérjen minden lényeges kérdésre. Ebben az értelemben a módszertan adatvédelmi problématérképnek is tekinthető. E fejezet a dolgozat legfontosabb új kutatási eredményeit tartalmazza, és deklarált célja, hogy praktikus segítséget nyújtson az adatkezelők számára az adatvédelmi compliance eléréséhez.

3.2 A dolgozat új eredményei és azok hasznosítása

A dolgozatban részletesen összefoglalom az adatvédelmi szabályozás történetét, a technológia-társadalmi változások kontextusába is helyezve. Ilyen szemléletű és ilyen részletes 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 adatvédelmi önszabályozás témaköre szintén nem túl hangsúlyos, sem a magyar, sem az angol nyelvű külföldi jogirodalomban. Ez ugyanakkor nem 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 talán legjelentősebb új kutatási eredménye az 5. fejezetben található, az adatvédelmi irányítási rendszer kialakítására szolgáló módszertan, amely új szempontokat és megközelítési módot ad hozzá az adatvédelmi szakirodalomhoz. Hasonló módszertan Magyarországon még nem készült.

A dolgozat új eredményei mindenekelőtt gazdagítják a hazai adatvédelmi jogirodalmat és kiindulópontként szolgálhatnak az adatvédelem legújabb tendenciáinak további kutatásához. Számos lábjegyzetbe került megjegyzés vagy pontosítás kifejezetten ezt a célt szolgálja.

A Rendelettervezet elfogadása esetén a dolgozat eredményei a jogalkalmazók segítségére is lehetnek: a dolgozat számos potenciálisan felmerülő értelmezési kérdésre, anomáliára rávilágít, egyes problémák esetén megoldási javaslatot is kínálva.

Az eredmények hasznosulhatnak emellett az oktatásban is, az adatvédelmi jog tananyagának szinte mindenhol része az adatvédelem történeti fejlődése, amelyet a disszertáció igen részletesen tárgyal.

Végül a doktori kutatás eredményei közvetlenül az adatkezelők mindennapi gyakorlatában is hasznosulhatnak. Az adatvédelmi irányítási rendszer módszertanának kidolgozása kifejezetten azt a célt szolgálja, hogy segítse az adatkezelőket az – várhatóan egyre fokozódó – adatvédelmi compliance-kötelezettségeknek való tervszerű megfelelésben.

4. Az értekezés témakörében készült publikációk

[1] Balogh, Zsolt György – Polyák, Gábor – Rátai, Balázs – Szőke Gergely László (2012): Privacy in the Workplace, in: Balogh, Zsolt György et. al. (eds.): Studia Iuridica Auctoritate Universitatis Pécs Publicata 150. Essays of Faculty of Law University of Pécs. Yearbook of 2012. University of Pécs, Faculty of Law, Pécs, 2012. pp. 9-40.

[2] Balogh, Zsolt György – Polyák, Gábor – Rátai, Balázs – Szőke Gergely László (2012): Munkahelyi adatvédelem a gyakorlatban, Infokommunikáció és jog, 2012. 3. szám pp. 95-104.

[3] Balogh, Zsolt György – Falk, Hagedorn – Kiss, Attila – Polyák, Gábor – Rátai, Balázs – Szőke Gergely László (2012): Comparative Report on the Regulation of Workplace Privacy in Germany and in Hungary, in: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest, pp. 25-161.

[4] 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.

[5] 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.

[6] Böröcz István – Szőke Gergely László (2013): A beépített adatvédelem (Privacy by Design) elve, Infokommunikáció ás jog, 3. sz. pp. 120-125.

[7] 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.

[8] 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.

[9] Polyák Gábor – Szőke Gergely László (2013): A személyes adatok védelme és a közérdekű adatok nyilvánossága. Jegyzet PTE ÁJK Igazságügyi ügyintéző szakos hallgatók számára, Kézirat, PTE ÁJK Elektronikus tananyag, p. 24.

[10] 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.

[11] Szőke Gergely László (2008): Szembenézés helyett (recenzió Trócsányi Sára: Forradalom az irattárban. Az információs kárpótlás jogi aspektusai c. könyvről), *Infokommunikáció és jog*, 2008. augusztus, pp. 176-177.

[12] Szőke, Gergely László (2010): Privacy Protection, in.: Balázs Rátai – Péter Homoki – Gábor Polyák – Judit Schvéger – Balázs Szemes – Gergely Szőke – Sándor Tasnádi – András Tóth: Cyber Law in Hungary, Kluwer Law International

[13] Szőke Gergely László (2011): Közterületi kamerázás az Európai Unióban, JURA 2. sz, pp. 192-206.

[14] Szőke, Gergely László (2012, ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest, p. 342.

[15] 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.

[16] Szőke Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése, Infokommunikáció és jog, 3. sz. pp. 107-112.

[17] Szőke Gergely László (2014): Az önszabályozás, audit és tanúsítás lehetőségei és korlátai az adatvédelem területén, Infokommunikáció és jog, 1. sz. pp. 14-20.

5. A tézisekhez felhasznált források

[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

[2] 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 (a továbbiakban bizottsági Rendelettervezet)

[3] 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.

[4] Jóri András (2009): Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs

[5] Majtényi László (2006): Az információs szabadságok, Complex, Budapest

[6] 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.

[7] 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.]

[8] Szabó Máté Dániel (2012): Az információs hatalom alkotmányos korlátai, Miskolci Egyetem, Miskolc

[9] Westin, Alan F. (1967): Privacy and freedom, Atheneum, New York