**SZEGEDI TUDOMÁNYEGYETEM
ÁLLAM- ÉS JOGTUDOMÁNYI KAR
DOKTORI ISKOLA**

Mészáros János

**Adatvédelem a XXI. században és
az internet világában**

PhD értekezés

Témavezető:

Prof. Dr. Paczolay Péter
tanszékvezető egyetemi tanár

Szeged

2017

Tartalomjegyzék

1. Alapvetés	5
1.1 Bevezetés.....	5
1.2 A téma kutatásának módszerei	12
1.3 A téma vizsgálatának hipotézisei	14
2. A személyiségi jogok, a magánszféra és az adatvédelem kapcsolata	16
2.1 A privacy és a magánszféra kapcsolata.....	16
2.1.1 Adatvédelem és a magánszféra védelme	21
2.1.2 Adatvédelem és az információs önrendelkezési jog	22
2.2 Az adatvédelem célja és helye a hatályos jogi szabályozásban	24
2.2.1 Az adatvédelem és az adatvédelmi jog fogalma	25
2.2.1 Személyiségi jogok.....	26
2.3 Az adatvédelem generációi	29
2.3.1 Az adatvédelem története	33
3. A személyes adatok védelméhez való jog ütközése alapvető jogokkal az Európai Unió Bíróságának joggyakorlatában	54
3.1 Az EU Bíróságának viszonya az alapvető szabadságokhoz és az alapjogokhoz	55
3.1.1 Az adatvédelmi irányelv érvényesülése az EU Bíróságának joggyakorlatában	56
3.1.2 A közérdekű adatok nyilvánosságának és a személyes adatok védelméhez való jognak az ütközése az EU Bíróságának joggyakorlatában	59
3.1.3 Személyes adatok védelméhez való jog és a szerzői jogok	60
3.2 Az EU Bíróság és a személyes adatok védelméhez való jog Lisszabon után	63
3.2.1 Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos, Mario Costeja González.....	64
3.2.2 Az Európai Unió Bíróságának Safe Harbort megszüntető ítélete.....	66
3.3 Következtetések összegzése az EU Bíróságának joggyakorlatáról.....	69
4. A felejtés joga és az internetes közvetítő szolgáltatók.....	71

4.1 Az adatkezelő és adatfeldolgozó meghatározásának szempontjai napjaink összetett adatkezelései során	71
4.1.1 Adatkezelő	71
4.1.2 Adatfeldolgozó.....	81
4.1.3 Az internetes közvetítő szolgáltatók.....	85
4.1.4 Az internetes kereső fogalma és működése	89
4.2 A felejtés joga.....	101
4.2.1 A technikai akadályok elhárítása	102
4.2.2 A felejtés joga az adatvédelmi irányelvben	110
4.2.3 A felejtés joga az adatvédelmi rendeletben	112
4.2.4 A felejtés joga és az internetes keresők	117
4.3 Az Európai Unió Bíróságának döntése a Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos, Mario Costeja González ügyben.....	120
4.4 A kérelmek elbírálásának problémái és a lehetséges megoldások	123
4.5 Következtetések	132
5. Adatvédelem a közösségi hálózatokon, különös tekintettel a Facebookon	135
5.1 A Facebook megalapítása és működése	136
5.2 Az érintett hozzájárulásával kapcsolatos problémák	146
5.3 Javaslatok a teljes értékű hozzájárulás eléréséhez	153
5.4 Javaslat egy rentábilis, „privacy by default” közösségi hálózat megvalósítására	154
5.5 A Személyes adatok profitra váltása	160
5.6 Facebook és a gyermekek adatvédelme	166
5.7 Fényképekkel és a felhasználó azonosításával kapcsolatos adatkezelések	170
5.8 Következtetések	178
6. Személyes adatok küldése az EU területéről az Egyesült Államokba, különös tekintettel az internetes keresőkre és a közösségi hálózatokra	180
6.1 Személyes adatok továbbítása harmadik államokba az Európai Unióból.....	184
6.1.1 Az érintett hozzájárulása.....	186

6.1.2 A személyes adatok továbbítását jogszabály vagy tagállami hatóság engedélyezi	189
6.1.3 Szerződés megkötéséhez vagy teljesítéséhez szükséges	190
6.1.4 Közérdek, jogi követelések létrejötte, érvényesítése vagy védelme	191
6.1.5 Nyilvántartásból történő továbbítás	192
6.1.6 Kötelező erejű vállalati szabályok	194
6.1.7 Általános szerződési feltételek	196
6.2 Privacy Shield	197
6.3 Következtetések	203
7. A személyes adat, mint adásvétel tárgya	205
7.1 A célhoz kötöttség és szükségesség elve, mint az adásvétel korlátja	208
7.2. Facebook és a WhatsApp	211
7.3 A Toysmart ügy	213
7.3.1 A tulajdonjogi és az alapjogi megközelítés	216
7.3.2 A „tulajdonjogi megközelítés” enyhébb változatának gyakorlati megvalósulása	217
7.4 Értékelő gondolatok	219
8. Összegzés és a dolgozat új eredményei	221
8.1 Összegzés	221
8.2 Új eredmények	231
Köszönetnyilvánítás	233
Irodalom	233

1. Alapvetés

1.1 Bevezetés

A XXI. században minimálisra csökkent az egyén döntési lehetősége a tekintetben, hogy részt vesz-e az online életben: egyetemeken az órákra és a vizsgákra való jelentkezés elektronikusan történik, a leveleink jelentős részét sem postán kapjuk már (csupán idő kérdése, hogy a hivatalos levelek is hasonló sorsra jussanak), a világban szétszóródott barátainkkal a kapcsolatot szociális hálózatokon és üzenetküldő szolgáltatásokon keresztül tartjuk.

Az állampolgár az információs társadalomban a "külvilág számára virtualizálódik", amely alatt azt értjük, hogy egyre több emberrel és szervezettel tart kapcsolatot teljes személytelenséggel, amely fordítva is igaz: a döntéshozó szervek felé csupán egy adathalmazként jelenik meg.

A virtualizálódás miatt különösen fontos, hogy az egyén kontrollal rendelkezhesen a külvilág felé róla áramló adatokról, mivel visszaélés esetén egy karrier törhet meg (pl. munkahelyi e-mail címmel nem kívánt levelek küldése, Egységes Tanulmányi Rendszerben tantárgyak vagy vizsgák leadása).¹

Az egyén digitális világban betöltött szerepének felértékelődése és a magánszférájának védelemre szorulása jelentik dolgozatom kiindulópontját, amelyet a magánszféra és az adatvédelem vizsgálatát követően az internet leggyakrabban használt szolgáltatásain (pl. Google, Facebook) keresztül tekintek át.

A privacy fogalmának meghatározása különösen nehéz, mivel a "privát" szó jelentése is országonként eltérő és koronként változik, ezért dolgozatomban annak történetét és az európai valamint az amerikai jogrendszerekben való érvényesülését vizsgálom meg, továbbá a meghatározásán túl a magánszférával való kapcsolatát elemzem, keresve az azonosságokat és az eltéréseket.

A magánszféra fogalmának tisztázása után az adatvédelemmel és az információs önrendelkezési joggal való kapcsolatát tekintem át.

Az alapjogok védelmével új kihívások és feladatok hárultak az Európai Unió Bíróságára, amelyek közül legfontosabb az EU Alapjogi Chartájának értelmezése, amely komoly

¹ Szabó Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, in: Információs Társadalom, szerk.: Simon Éva, Gondolat Kiadó, 2005. évfolyam 2. szám, 46.

nehézségekkel állította szembe a testületet a különböző hagyományokkal és értékrendszerrel rendelkező tagállamok tekintetében, amelynek során elengedhetetlen volt, hogy rendezze a viszonyát az Emberi Jogok Európai Bíróságával.²

2018-ig - az adatvédelmi rendelet hatályba lépéséig - az Európai Unió adatvédelmi irányelve jelenti az EU adatvédelmi szabályozásának keretét és egyben alapjait, amely az első ilyen szinten elfogadott jogszabály volt adatvédelem tárgyában.

Az irányelv elfogadásig eltelt 5 év során komoly viták folytak mind az EU szervei és tagállamai, mind a tudományos és gazdasági élet szereplői között, amelynek középpontjában az alapjogok és az EU négy szabadságának (személyek, áruk, szolgáltatások és a tőke szabad áramlása) konfliktusa állt.

Az EU adatvédelmi irányelve kettős, látszólag egymásnak ellentmondó célt hivatott megvalósítani: a személyes adatok szabad áramlását az Európai Unión belül, továbbá a magánszféra és a személyes adatok védelmét.³

A két cél közötti határvonal meghúzása a nemzeti jogalkotóknak is komoly feladat volt, ám a jogalkalmazásnak a mai napig is kihívást jelent a prioritás meghatározása.

Az Európai Unió elsődleges jogforrásaiban kitűzött egyik legfontosabb cél, a közös piac létrehozása - finomhangolásoktól eltekintve - megvalósult, amely az EU Bíróságának feladatkörére is hatással volt: egyre kevésbé fajsúlyos az alapvető szabadságok hangsúlyozása, míg az alapjogok védelme előtérbe került, amelyek között egyre nagyobb jelentőséggel bírnak az információs társadalommal kapcsolatos jogok.⁴

Az emberi jogok közösségi védelmének vonatkozásában az EU Bíróságára hárul a védelem határvonalának meghúzása a joggyakorlatban, a közösségi kompetenciák tekintetében⁵, amelyet dolgozatomban az EU Bíróságának legjelentősebb ügyein keresztül mutatok be.

Az idők kezdete óta az emberek számára a felejtés volt a természetes, míg a részletes emlékezés kivételes, különösen az analfabetizmus felszámolásáig. Napjainkban a technikának

² Gyenei Laura: Újabb kihívások az uniós emberi jogi bíráskodás területén, *Iustum Aequum Salutare* II. 2006/3–4, 85–99.

³ Az Európai Parlament és a Tanács 95/46/EK irányelve, 1 cikk, Az irányelv célja

(1) A tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében.

(2) A tagállamok nem korlátozhatják és nem tilthatják a személyes adatok tagállamok közötti szabad áramlását az (1) bekezdés értelmében biztosított védelemmel kapcsolatos indokok miatt.

⁴ Sionaidh Douglas Scott: Luxembourg and the growing European human rights acquis. *Common Market Law Review*, 2006/43, 661.

⁵ Takis Trimidas: The ECJ and the Draft Constitution: A Supreme Court for the Union? *Federal Trust Constitutional Online Paper* 05/04, <www.fedtrust.co.uk/uploads/constitution/05_04.pdf>

köszönhetően a helyzet megfordulni látszik: az emlékezés vált alapvetővé a digitális nyomaink miatt.

A felejtés joga folyamatosan ütközésben van az információhoz való joggal, és a mérleget az idő billentheti el közöttük: amennyiben egy információ aktuális, közérdekű és a társadalom joggal tarthat igényt rá, abban az esetben az információhoz való jog élvezhet elsőbbséget. Az idő múlásával azonban a kérdés már aktualitását vesztheti, az igények elévülhetnek és az egyén felejtéshez való joga kerülhet előtérbe.

A felejtés jogának életre hívói napjainkban az internetes keresők, a közösségi hálózatok és olyan közvetítő csatornák, amelyek lehetővé teszik az információ előkeresését és megosztását akkor is, ha az egy archívum mélyén van. Az információ, amely eddig adatmorzsákból volt összeállítható hosszas keresőmunka árán, így elérhetővé vált bárhol, bármikor, gyorsan és ingyen, akár inkognitóban is.

Dolgozatomban a felejtés jogának történeti és filozófiai hátterén túl az internetes keresőkön és a közösségi hálózatokon való érvényesülését vizsgálom meg.

Az EU Bíróságának Google Spain döntése⁶ több kérdést vet fel, amelyekre dolgozatomban a lehetséges megoldásokat keresem: az internetes keresők üzemeltetői hogyan állapíthatják meg az érintettek kéréseinek hitelességét, az adatok aktualitását és a közérdekűséget, továbbá egy magánszemély hogyan bizonyíthatná, hogy már nincsenek hitelekkel kapcsolatos problémái és nem jelent veszélyt a hitelezőkre (akiknek jogos érdekük tudni az adós fizetési képességéről és hajlandóságáról).

A közösségi hálózatok olyan kommunikációs platformok, amelyek lehetőséget nyújtanak a felhasználók számára, hogy a személyes adataikból, képeikből adatlapot (profil) hozzanak létre, amely azonosításukra szolgál, továbbá kapcsolatot létesítsenek más felhasználókkal és képesek legyenek saját – és sok esetben ismerőseik – kapcsolatrendszerét megtekinteni.

Az EU területén 2014-ben a közösségi oldalak használata jelentette az egyik leggyakoribb online tevékenységet. A 16–74 éves lakosság közel fele (46%) használta az internetet közösségi hálózatok (például a Facebook vagy a Twitter) böngészésére is⁷.

Több, mint egy milliárd felhasználójával a Facebook a világ egyik legnagyobb - nem állami - adatkezelője. Súlyát nem csupán a regisztrált felhasználók száma, hanem az általuk szolgáltatott

⁶ C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014. 05. 13.

⁷ Eurostat: Az információs társadalomra vonatkozó statisztika – háztartások és magánszemélyek (letöltés dátuma: 2016. április 25.) http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/hu

adatok mennyisége és minősége adja: az alapvető személyes adatoktól (pl. név, születési hely és idő) a különleges adatokig (pl. vallás, politikai nézetek) olyan információk tudhatóak meg a felhasználókról, amelyeket önként adnak meg, növelve annak hitelességét. A felhasználók ismerősein keresztül olyan kapcsolati háló rajzolható ki, amelyről másképpen – még titkosszolgálati eszközökkel sem - lehetne tudomást szerezni.

A felhasználók számának növekedését csak úgy tudja a vállalat fenntartani, hogy egyre több országban nyitja meg a lehetőséget a felhasználók regisztrálására. Egy új ország azonban nem csak felhasználói táborát és hirdetőket hoz magával, hanem egy új jogrendszert is, amelynek meg kell felelnie. Olyan nemzetközi szolgáltatást nyújtani azonban különösen nehéz, amely egységesen minden országban működőképes és az eltérő jogrendszereknek megfelel: a „modern” adatvédelmi jogszabályok egyre több országban jelennek meg és – főként az Európai Unió adatvédelmi elvárásai és standardjai miatt - folyamatosan szigorodnak.

Dolgozatomban a Facebook magánszférát érintő legfontosabb kérdéseit és problémáit helyezem vizsgálat alá, különösen az Európai Unió adatvédelmi szabályozásának a szemszögéből.

A közösségi hálózatok adatkezeléseikhez 3 jogalapot használhatnak fel alapvetően az Európai Unióban:

1. az érintett hozzájárulása,
2. az adatkezelés szerződés teljesítéséhez, vagy
3. az adatkezelő vagy adatfeldolgozó jogszerű érdekének érvényesítéséhez szükséges.

A „szerződés teljesítéséhez szükséges” jogalappal akkor élhetnek a közösségi hálózatok, ha az adatkezelés a szolgáltatás teljesítéséhez feltétlenül szükséges, így például az adatlap alapvető adatainak (név, nemzetiség) megadása és profilkép feltöltése.

A „jogszerű érdek érvényesítésével” csak korlátozott keretek között élhetne a közösségi hálózat, így például a rendszer és a többi felhasználó adatainak biztonsága érdekében, továbbá a „biztonság és megfelelő színvonalú szolgáltatás nyújtása” indokot is csak a valóban szükséges esetekben lennének jogosultak felhasználni.

Véleményem szerint minden egyéb adatkezelés esetén az érintett hozzájárulása lenne szükséges annak legitimálásához, amelynél a legfontosabb kérdés, hogy előzetes vagy utólagos is lehet-e (opt-in vagy opt-out), amelyre dolgozatomban a közösségi hálózatok esetében keresem a választ.

A felhasználó hozzájárulásának önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak, és félreérthetetlennek kell lennie, amely feltételek egyre kevésbé érvényesülnek az

internetes szolgáltatások – különösen a közösségi hálózatok – működése során, így fontosnak tartom probléma kimerítő elemzését, amelyet dolgozatomban a Facebookkal kapcsolatban végeztem el.

Az Európai Unió adatvédelmi jogának egyik alapvető célja, hogy minden adatkezelésnek legyen – legalább egy – felelőse, aki a közösségi és nemzeti adatvédelmi jogszabályok érvényesüléséről gondoskodik. Így került megalkotásra az adatkezelő intézménye, aki amely az adatkezelés célját és módját ténylegesen meghatározza.

Az életviszonyok jelentős részében könnyen megállapítható volt az adatkezelő és az érintett személye: egy mobilszolgáltatóval kötött szerződés, közvélemény kutatás, vagy bármilyen állami adatkezelés esetén egyértelműek a szerepek.

Az informatika fejlődése azonban megkönnyítette a távmunkát és a kiszervezések („outsourcing”) megvalósítását, amelynek következtében az adatfeldolgozások is jelentősen megváltoztak. Az olyan műveletek, amelyeket korábban egy szervezeten belül valósultak meg, napjainkban harmadik felek hajtják végre: saját jogi osztály helyett ügyvédi irodákat bízunk meg a cégek, a rendszergazdai teendőket és a honlap üzemeltetését is külsős informatikai cégek látják el.

Az internet elterjedésével együtt a közvetítő szolgáltatók szerepe is folyamatosan növekedett: a keresőszolgáltatások, szociális hálózatok, aukciós oldalak, tárhelyet és megosztást biztosító szolgáltatások alkalmazása magán és üzleti célra elterjedté vált. Az említett szolgáltatások esetében azonban könnyen elmosódhat a határvonal az adatkezelő és az adatfeldolgozó között, a szolgáltatók pedig törekednek saját felelősségüket minden téren (pl. adatkezelés, szellemi alkotások, adózás) minimalizálni, ezért különösen fontos a felhasználó érdekében a felelőségek és a szerepek elhatárolása, amelyre dolgozatomban több területen is törekedtem, különösen az internetes keresők és a közösségi hálózatok vonatkozásában.

Az Európai Unió, az Egyesült Államok és az ázsiai országok között a magánszférával kapcsolatos elvárásaikat tekintve komoly eltéréseket találhatunk, amelyet az adatvédelmi jogszabályaik is tükröznek.

Európában alapvető értéként jelenik meg az emberi méltóság és az egyén jogainak védelme, különösen a mindenható állammal és a társadalom többi tagjával szemben, amelyek a világháborúkból és a „mindent látó” szocialista államok emlékéből erednek, míg az Egyesült Államokban az egyéni szabadság a kiindulási pont, amely az individuum kibontakozását biztosítja az állam háttérbe szorításával.

Jól látható a különbség: a liberális piacgazdaság mellett elkötelezett amerikaiak szerint a szabadságra az állam tevékenysége jelentheti a legnagyobb veszélyt, míg az európaiak igénylik annak a védelmét⁸.

Az Egyesült Államok abban a szerencsés helyzetben van, hogy a legnagyobb szoftver és technológiai óriásoknak (pl.: Google, Apple, Microsoft) a területén van székhelye.

A gazdasági szempontokon túl adatvédelmi kérdések is felmerülnek: milyen jogalapon és hogyan kezelik a hatalmas IT cégek a világ összes országából rendelkezésükre álló személyes adatokat. A szeptember 11-én elkövetett terrortámadásokat komoly magánszférát érintő változások követték: az NSA botrány rámutatott, hogy nemzetbiztonsági érdekekre és egy bírósági ítéletre hivatkozva bárkinek a személyes adataihoz és levelezéséhez hozzáférhetnek az amerikai titkosszolgálatok.

Mivel dolgozatom vezérfonala a magánszféra érvényesülése az internet világában - különösen a Facebook és a Google relációjában - így az USA adatvédelmi jogi szabályozásának vizsgálata megkerülhetetlenné vált a probléma elemzése során.

Az USA és az EU adatvédelmi szabályai, elvárásai jelentősen különböznek egymástól, ezért a két rendszer áthidalására és az USA-ba történő adattovábbítás megkönnyítése céljából jött létre a „Safe Harbor – Biztonságos Kikötő” rendszer.

Maximilian Schrems, egy osztrák állampolgár 2013-ban panaszt nyújtott be az Ír Adatvédelmi Hatósághoz a Facebook ellen, miután Edward Snowden által nyilvánosságra kerültek az Egyesült Államok által végzett korlátlan adatgyűjtések.

Az Ír Adatvédelmi Hatóság elutasító határozatát a panaszos megtámadta bíróságon (the High Court of Ireland), amely előzetes döntéshozatali eljárást kezdeményezett az EU Bíróságán, ahol különösen jelentős ítélet született: a Safe Harbor érvénytelensége került megállapításra.

A Safe Harbor nélkül különösen felértékelődik azon megoldások szerepe, amelyek lehetőséget teremtenek a személyes adatok küldésére az Egyesült Államokba. Dolgozatomban ezért vizsgálat alá helyeztem a lehetséges adatküldési módokat, különösen a felhasználó hozzájárulását és a Privacy Shieldet.

A cél az adatkezelés legfontosabb aspektusa, amelynek megváltozása új adatkezelést eredményez. Például a hitelkártya tulajdonosokat az American Express sorolta be vásárlási szokásaik alapján⁹, és a személyes adatokat marketing céljából használta fel, az eredeti

⁸ Péterfalvi Attila: Adatvédelem és információszabadság a mindennapokban, HVG-ORAC Lap- Könyvkiadó Kft., Budapest, 2012, 39.

⁹ Dwyer v. American Express, 652 N.E.2d 1351 (Ill. App. 1995)

adatkezelés céljától eltérően, amely egy új adatkezelést eredményezett, megfelelő jogalap nélkül¹⁰.

A célhoz kötöttség az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája¹¹. Az adatkezelésnek minden szakaszában meg kell felelnie a céljának, amely nem csak az adatkezelő és harmadik személyek relációjában kötelező szabály, hanem az adatkezelő szervezetén belül is. Ebből következően az adatkezelő szervezetében is csak azok férhetnek hozzá a személyes adatokhoz, akiknek ez feltétlenül szükséges, és munkájuk az adatkezelés céljához kapcsolódik, amelyből következően aggályos, hogy a Google és Facebook leányvállalatainak (WhatsApp, Youtube stb.) felhasználói adatbázisához korlátlanul hozzáfér. A célján túlterjeszkedő és megfelelő jogalap nélküli adatkezeléseket különösen a Facebook esetében vizsgálom meg dolgozatomban, az adatkezelési szabályzat és gyakorlat hiányosságaira és problémáira rámutatva.

A személyes adatainkat könnyedén - pár kattintással - „eladhatjuk” a népszerű és mindennapjainkat megkönnyítő szolgáltatások használatáért cserében, azonban azokat vissza már nem vásárolhatjuk, így különösen fontos az információs társadalomban a kockázatok ismerete és magas szintű védelem biztosítása a jog és technológia által, amelynek bemutatására és kidolgozására törekedtem dolgozatom megírása során.

¹⁰ Daniel J. Solove – Paul M. Schwartz: Privacy, Information and Technology, Wolters Kluwer Law & Business, New York, 2011, 425.

¹¹ 15/1991. (IV. 13.) AB határozat

1.2 A téma kutatásának módszerei

Jelen dolgozat alapját négy éves kutatási tevékenységem képezi, amelynek jelentős részét külföldi egyetemeken folytathattam hazai és nemzetközi ösztöndíjalapok, valamint témavezetőm támogatásának köszönhetően.

Kutatási témám aktualitását az adja, hogy globálisan az üzleti- és magánélet egyre jelentősebb része helyeződik át a digitális világba, a számítástechnika fejlődésének és az internet elterjedésének köszönhetően, amelyben a legnépszerűbb programok (Windows, Apple OS) és szolgáltatások (Facebook, Google, LinkedIn) használata nehezen megkerülhető, így például egy összetett szöveges dokumentumot csak Microsoft Wordben lehet megszerkeszteni lemondások nélkül, amely csak Windows és Apple eszközökön fut teljes szolgáltatáskínálattal. A legnépszerűbb szolgáltatások és oldalaknak használata során a felhasználók a személyes adataikat rendelkezésre bocsátják, így olyan helyzet alakul ki, amely során a felhasználónak egy, a személyes jogától idegen államban székhellyel rendelkező vállalatnak kell a személyes adatait átadni, a minimális alternatívával rendelkező szolgáltatásaikért cserébe.

A felhasználó így védelemre szorul, amelynek szintjéről és módjáról a jogtudomány, a jogalkotók és a jogalkalmazás részéről jogrendszerenként eltérőek a vélemények és a szabályozási modellek.

Az adatvédelemi jog gyökerei a magánjogban találhatók meg, azonban az alkotmányos védelem erősödése „elközjogiasítja” azt. Dolgozatomban a magánszféra alkotmányos védelmén túl elsősorban magánjogi oldalról közelítem meg az adatvédelem érvényesülését és jogi szabályozását.

A magánszféra és a személyes adatok védelmét az alkotmányjog, polgári jog és büntetőjog anyagi jog szabályain keresztül vizsgáltam meg, eljárásjogi szabályokat kizárólag a személyes adatok megsértése esetén alkalmazható jogérvényesítéssel kapcsolatban érintettem.

Dolgozatom megírása során törekedtem a mértékadó hazai és nemzetközi szakirodalom bemutatására és kritikus értékelésére, a tudományos feldolgozáshoz történeti, jogtörténeti, komparatív, leíró/kutató, analitikus tudományos módszereket alkalmaztam.

Összehasonlító jogi vizsgálataim során az Európai Uniót kívül különösen az Egyesült Államok jogrendszerére koncentráltam, mivel a digitális világ legjelentősebb vállalatai ezen állam területén rendelkeznek székhellyel.

A hatályos szabályozás elmélete (law in book) mellett dolgozatomban kiemelt figyelmet fordítottam a jogalkalmazási gyakorlat (law in action) bemutatására, azon belül is különösen az

Európai Unió Bíróságának ítélkezésére, mivel döntései (pl. Google Spain, Safe Harbor megszüntetése)¹² különös jelentőséggel bírnak az EU állampolgárok személyes adatainak kezelésével kapcsolatosan, továbbá az Egyesült Államok és az Európai Unió között fennálló kapcsolatokban adatvédelem terén.

Dolgozatom első része tartalmazza a magánszféra védelmének történeti és jogfilozófiai hátterét. Szociológiai megközelítésből az internetnek és a közösségi hálózatoknak a társadalom magánszféra iránti igényére gyakorolt hatását vizsgáltam meg, mivel a városiasodás után — véleményem szerint — az emberi kapcsolatokra az interneten történő kapcsolattartás gyakorolta a legnagyobb hatást globális szinten.

Dolgozatomban kitérek a technika és a jog kapcsolatának vizsgálatára is, amelynek során elsődleges célom az, hogy átlátható logikai tagolással rámutassak napjaink gyakorlatában felmerülő vitás kérdésekre és nehézségekre, valamint egyes jogalkotási és jogalkalmazási problémákra.

A dolgozat célja a személyes adatok védelmének bemutatása az online környezetben, különös hangsúlyt fektetve a Facebook és a Google adatkezeléseire.

A fenti vizsgálati módszerek alkalmazásától az uralkodó tézisek igazolását vagy cáfolását várom, továbbá célom, hogy egyes szabályozási nehézségek kiküszöbölésére, egyszerűsítésére, ill. gyakorlati problémák megoldására javaslatkísérletet tegyek.

A kutatásaim egyes részeredményeit felhasználtam előpublikációim, ill. tudományos előadásaim során, és törekedtem arra, hogy az így megszerzett szakmai ismereteket, visszajelzéseket és tapasztalatokat maradéktalanul felhasználjam a doktori értekezésemben.

¹² C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Court of Justice of the European Union, 2014. 05. 13.
C-362/14 Maximilian Schrems v Data Protection Commissioner, Court of Justice of the European Union, 2015. 10. 07.

1.3 A téma vizsgálatának hipotézisei

1. A magánszféra tágabb kategória, mint az adatvédelem, továbbá az információs önrendelkezési jog és az adatvédelem nem egyeznek meg teljesen egymással. A disszertáció során igazolom továbbá, hogy az információs önrendelkezési jog folyamatosan gyengül, amelyet az adatvédelmi jog erősítésével lehet ellensúlyozni.
2. Az Európai Unió Bíróságának joggyakorlatában az alapjogok védelme (köztük a magánszféra és a személyes adatok védelme) folyamatosan erősödik az alapvető szabadságokkal (személyek, áruk, szolgáltatások és a tőke szabad áramlása) szemben.
3. A felejtés jogának érvényesítéséhez 3 területen szükséges megoldást találni, amelyekre a dolgozatomban javaslatokat teszek:
 - a) határvonalat húzni az adatkezelők és adatfeldolgozók között az online környezetben,
 - b) az érintettek törlésre vonatkozó kérelmeinek tartalmi vizsgálatához támpontok kialakítása egyéb szektorokban alkalmazott módszerekkel,
 - c) az elbírálás eljárásának a kialakítása oly módon, hogy az felhasználóbarát, átlátható, továbbá az uniós és nemzeti hatóságoknak minél kevesebb terhet jelentő legyen.
4. A Facebook adatkezelései jelentős részéhez jogalapként az érintett hozzájárulását használja fel, azonban a hozzájárulás alapvető követelményei (önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak és félreérthetetlennek kell lennie) nem érvényesülnek maradéktalanul, így feltételezem, hogy az uniós jogszabályoknak nem felel meg a Facebook által legtöbb esetben alkalmazott jogalap.
5. A Facebook és a közösségi hálózatok részére létezik alternatív megoldás annak biztosítására, hogy adatbányászat és viselkedés alapú reklámozás alkalmazása nélkül is megfelelő mértékű bevételre tegyenek szert. A Facebook felhasználónkénti bevételét és működését megvizsgálva keresem a megoldást arra, hogy lehetséges lenne-e a bevétel szintjének megtartása mellett a felhasználók személyes adatait a célhoz kötöttség és szükségesség elvének megfelelően kezelni.
6. Az online szolgáltatásokat biztosító vállalatok adásvétele adatvédelmi szempontból aggályos, mivel a tulajdonosváltással együtt az adatkezelés céljára és módjára befolyással lévő

személy is megváltozik, amely a kihatással lehet az érintettek jogaira, megfelelő szabályozás és korlátozás nélkül. Különösen érintettek az uniós állampolgárok adatai, amelyek csak megfelelő védelemmel juthatnának el a felvásárlással érintett legnagyobb vállalatokhoz az Egyesült Államokba.

2. A személyiségi jogok, a magánszféra és az adatvédelem kapcsolata

2.1 A privacy és a magánszféra kapcsolata

Az angol nyelvben használt "privacy" lefordítása egy szóval nem lehetséges, így célszerű a történeti kialakulásán keresztül, hazai és külföldi jogtudósok munkáinak segítségével bemutatni annak jelentését.

A privacy fogalmának meghatározása különösen nehéz, mivel a "privát" szó jelentése is országonként és koronként változik. 2000 évvel ezelőtt publikus illemhelyek voltak Ephesusban¹³, napjainkban pedig a magánszféránk durva megsértésének számít, ha valaki a kerítésünk lécei között leskelődik.

Az ókori Rómában a "privát személy" kifejezést negatív értelemben használták arra a személyre, aki nem vett részt a közügyek gyakorlásában, melynek több oka is lehetett: nem volt rá képes (jogosult), vagy nem szándékozott élni a legfontosabb állampolgári jogával (melyet a társadalom akkor negatívan ítélt meg).

A magánszférával kapcsolatos társadalmi felfogásra szignifikáns hatással volt a városiasodás: a jobb megélhetés reményében városokba vándorló vagy csupán a pezsgő kulturális életre vágyó emberek önként feladták a privát szférájuk egy részét, amikor beköltöztek a sokszor zsúfolt metropoliszokba.

Az urbanizálódás hatványozottan hatott a magánszféra ellen: a városi lét a tömegtájékoztatást is átalakította, az új gazdasági és kulturális közösség táptalajjal szolgált az újságírásnak, később a média minden formájának. Megfigyelhető ugyanakkor, hogy a nagyvárosokban az emberek tömege és fizikai közelsége szellemi eltávolodást is jelent: míg a kis településeken egymásról mindent tudnak a lakosok, ez egy 100 ezer fős városban már nem mondható el.

A magánszféra iránti igény nem csupán egy emberi vágy, hanem az élőlények jelentős része által támasztott alapvető igény: még azonos fajkon belül is komoly harcot eredményezhet, ha a fajtárs átlépi a képzeletbeli határt. A magánszféra folyamatos megsértése olyan betegségekhez is vezethet, mint a magas vérnyomás, keringési elégtelenségek, vagy pánikbetegségek.

¹³ Ephesusz (latinul Ephesus, hettita nyelven: Apasza[sz, Apašaš]) görög polisz volt Kis-Ázsia nyugati partvidékén. Ma Törökországban helyezkedik el, török neve Efes.

A magánszféra jogi védelmének kialakulása javarészt az amerikai jogfejlődés eredménye, melyet az európai jogrendszerek átvettek és azt napjainkra már meg is haladták.

A magánszféra meghatározásának első mérföldköve Samuel D. Warren és Louis Brandeis nevéhez fűződik, akiknek 1890-ben jelent meg a "The Right To Privacy" (A magánszférához való jog) című műve a Harvard Law Review kiadványban. Cikkükben a személyiség sérthetetlenségéből kiindulva, több jogeseten végigvezetve arra vonatkozóan tettek javaslatot, hogy a magánszféra megsértésével okozott lelki és érzelmi szenvedés nem vagyoni kártérítésre adhatson alapot.

A magánszférához való jogot abszolút szerkezetű jogviszonyként határozták meg: "Arra a következtetésre kell tehát jutnunk, hogy az így védett jogok - bármilyen legyen is valójában a természetük - nem szerződésekből vagy különös bizalmi viszonyból eredeztethető jogok, hanem a világ ellenében érvényesíthető jogok"¹⁴

Szerintük a védett jogi tárgy a lelki és érzelmi állapot, mely független a társadalom értékítéletétől, így elhatárolták a magánszféra védelmét a rágalmazástól és a becsületsértéstől.¹⁵

Warren és Brandeis tanulmányukban kifejtik továbbá, hogy a privacy nem más, mint a jog arra, hogy egyedül legyünk ("right to be let alone"), mely alatt azt értették, hogy az egyén kizárhatja a külvilágot.

Warren és Brandeis tanulmányukban amellet foglaltak állást (a technika akkori állása miatt), hogy a magánszféra megsértése főként írásban alapozhat meg jelentős érdeksérelmet, szóban csak kivételesen, így a nem vagyoni kártérítés is csak az írottan megvalósított magánszféra sértés esetén állapítható meg, szóbeli esetén pedig csak abban az esetben, ha tényleges kár is felmerült.¹⁶

Egy emberöltővel később a magánszféra fogalmát Alan Westin tágabban határozza meg: az egyének, csoportok és intézmények azon joga, hogy eldöntsék: mikor, hogyan és milyen terjedelemben adnak ki információt magukról másoknak.¹⁷

Westin szerint minden egyén folyamatosan részt vesz társadalmi életviszonyokban, melynek során az információk megtartása és azok közlése iránti vágy között egyensúlyoz, az adott társadalmi környezet és szociális normák függvényében.

¹⁴ Samuel D. Warren and Louis Brandeis: The Right To Privacy, Harvard Law Review, 1890, 1-10.

¹⁵ Simon Éva: Egy XIX századi tanulmány margójára, in: Információs Társadalom, szerk.: Simon Éva, Gondolat Kiadó, 2005. évfolyam 2. szám

¹⁶ Jóri András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2009, 15.

¹⁷ Alan Westin: Privacy and Freedom, New York: Atheneum, 1967. 116-140.

David Flaherty ötvözi Warren, Brandeis és Westin elméletét: szerinte a privacy jog az egyedülléthez és hozzánk kötődő információk kontrolljához.¹⁸

Szabó Máté szerint a privacy nem más, "mint az egyén joga ahhoz, hogy magáról döntsön. A magyar jogirodalomban, alkotmánybírósági gyakorlatban és a jogrendszer más területein is ismert jogról van tehát szó, az önrendelkezés szabadságáról, arról, hogy mindenki maga döntheti el, mi lesz a saját sorsa, mit tesz magával, testével és a rá vonatkozó ismeretekkel."¹⁹

Daniel J. Solove és Roger Clarke írásai is tükrözik, mennyire eltérő aspektusokból lehetséges a privacy meghatározása: Solove elsősorban a privacy-t sértő behatásokból és azok védelméből indul ki, míg Clarke a privacy egyes elemeit az érintett személyéből kiindulva határozza meg, majd a lehetséges veszélyeket azt követően vázolja fel.

A két megközelítés közti különbségre hasonlatként hozható fel az emberi élethez való jog és az emberölés tényállásának büntetőjog általi meghatározása.

Solove²⁰ a privacy fogalmának megragadásához és annak védelme érdekében az arra veszélyt jelentő behatásokat sorolja fel a privacy egyes aspektusai szerint. Így például az adatgyűjtéshez párosítja a megfigyelést és a vallatást, az adatkezeléshez a felhasználó azonosítását, biztonsági problémákat és az adatok céltól eltérő további felhasználását, az adatokhoz való nyilvánosságra hozatala esetében azok megváltoztatását és a zsarolást, valamint a magánszférába való behatolás főbb eseteit vizsgálja meg.

Roger Clarke a privacy 4 dimenzióját különíti el. A személyes vagy a test magánszférája (privacy of a person, bodily privacy) az emberi test integritását jelenti elsősorban, amelyet olyan behatások sérthetnek, mint például az orvosi kezelés, vagy a bántalmazás.

Az egyén magatartásának, viselkedésének a magánszférája (privacy of personal behaviour) alatt az érintett olyan védendő és a külvilág számára akarata nélkül meg nem osztandó cselekményeit értjük, mint például a politikai és vallási meggyőződésének a gyakorlása, amely a publikus helyekre is kiterjedhet.

A kommunikáció magánszférája (privacy of personal communication) alatt az egyén azon jogát jelenti, hogy eldöntse, mely személyekkel osztja meg a véleményét és gondolatait anélkül, hogy azt mások lehallgatnák, elolvasnák²¹.

¹⁸ David Flaherty: Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, U.S.: The University of North Carolina Press. 1989, 86-110.

¹⁹ Szabó Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, in: Információs Társadalom, szerk.: Simon Éva, Gondolat Kiadó, 2005. évfolyam 2. szám, 46.

²⁰ Daniel J. Solove: Understanding Privacy, Harvard University Press, 2008. 104.

²¹ Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997. <http://www.rogerclarke.com/DV/Intro.html>

A személyes adatok magánszférája (privacy of personal data) az adatvédelmet fedi le, amely az érintett személyes adatait védi olyan esetben is, amikor azokat más személy kezeli.

Rachel L. Finn, David Wright, Michael Friedewald a privacy 7 típusát határozzák meg, kiegészítve Clarke kategóriáit.

A személyes magánszféra hasonlóan Clarke meghatározásához, az emberi testet és az avval kapcsolatos információkat védi (pl. genetikus kódok és biometrikus tulajdonságok). Clarke magatartással és viselkedéssel kapcsolatos magánszférája kiterjesztésre kerül a cselekvés magánszférájával (privacy of behaviour and action), és magában foglalja az egyén olyan szenzitív viselkedését, mint a politikai és szexuális preferenciái, cselekedetei. A publikus helyen való véleménynyilvánítás és viselkedés nehezen ragadható meg, mivel a társadalom biztonságával összeütközésbe kerülhet, továbbá esetenként eldöntendő, hogy egy helyszín teljesen, vagy részlegesen publikus.

A kommunikáció magánszférája Finn, Wright és Friedewald elméletében hasonlít a Clarke által leírtakhoz, amely a kommunikáció szabad és lehallgatás nélküli áramlását biztosítja, továbbá a legtöbb demokratikus állam által biztosított és általában csak megfelelő biztosítékok mellett lehetséges az attól való eltérés. A véleménynyilvánítás szabadságához a magánszférának ezen aspektusa elengedhetetlen.

Finn, Wright és Friedewald kiterjeszti Clarke személyes adatokkal kapcsolatos magánszféráját a képmás védelmével. A magánszféra ezen kategóriája az ő elméletükben is az adatvédelmet jelenti, amely biztosítja, hogy csak az arra jogosultak férhessenek hozzá a személyes adatokhoz, és az érintett kontrollal rendelkezzen azok felett.

Az új technológiák egyre jelentősebb veszélyt jelentenek a „gondolatok és érzések” magánszférájára (privacy of thoughts and feelings), amely így külön kategóriát képvisel. Az embereknek joguk van ahhoz, hogy a gondolataikat és érzéseiket úgy osszák meg egymással, hogy annak illetéktelenek általi hozzájutásától ne féljenek. A gondolat szabadsága az egyik alapvető emberi jog. Itt a személyes magánszférával szemben – amely az egyén testét védi – az ember szellemi védelméről van szó. Szintén el kell különíteni a gondolat és az érzések szabadságát a cselekvés szabadságától és annak védelmétől, mivel nem minden gondolat vezet cselekedethez (fordítva is igaz lehet, ahogy sok esetben gondolkodás nélkül cselekszenek)²².

²² Rachel L. Finn, David Wright, Michael Friedewald: Seven Types of Privacy, European Data Protection: Coming of Age, 2013.

A privacy meghatározásában jelentős továbbá, hogy pozitív, vagy negatív oldalról közelítjük-e meg. Napjaink legátfogóbb privacy elemzését a Typology of Privacy²³ című írásban találhatjuk, amelyben a szerzők negatív oldalként a „jog az egyedülélthez” (being let alone), míg pozitív oldalként a „önfejlesztés, önrendelkezés” (self-development) határozzák meg. A negatív oldal a személyes zónától a publikusig haladva a következő skálán kerül meghatározásra: az emberi test, a személyes tér, kommunikáció és tulajdon magánszférája.

A pozitív oldalon szintén a személyes zónától a publikusig haladva: intellektuális, döntés, társulás, és magatartás magánszférája.

A pozitív és a negatív oldalt, a privát és publikus részeket összeköti az információs magánszféra a szerzők elemzésében.

A digitális technológia jelentősen megváltoztatta a magánszféránk határait: bár az életünk jelentős része az otthonunk falai között zajlik, egy részét már virtuálisan éljük, mely újra publikussá, mások számára könnyen elérhetővé teszi életünk ezen aspektusát.

Nincs döntési lehetőségünk a tekintetben, hogy részt veszünk-e a digitális életben: egyetemeken az órákra és a vizsgákra való jelentkezés elektronikusan történik, a leveleink jelentős részét sem postán kapjuk már (csupán idő kérdése, hogy a hivatalos levelek is hasonló sorsra jussanak), a világban szétszóródott barátainkkal a kapcsolatot szociális hálózatokon és üzenetküldő szolgáltatásokon keresztül tartjuk. Fontos változás továbbá, hogy a munkahelyünkön is számítógépeken dolgozunk, melyek rendszerint hálózatba vannak kötve és interneteléréssel rendelkeznek, mellyel még az irodában is digitális lenyomatokat hagyunk magunk után, melynek segítségével munkatársaink, feletteseink, akár jövőbeni munkáltatóink is több információt tudhatnak meg rólunk.

Szabó kifejti, hogy nem csupán az egyén fizikai léte, hanem a rá vonatkozó adatok is védelmet igényelnek, mivel az egyén az információs társadalomban a "külvilág számára virtualizálódik". Egyre több emberrel és szervezettel tart az egyén kapcsolatot teljes személytelenséggel, mely fordítva is igaz: a döntéshozó szervek és személyek felé csupán egy adathalmazként jelenünk meg.

A virtualizálódás miatt különösen fontos, hogy az egyén kontrollal rendelkezessen a külvilág felé áramló - hozzá kapcsolható - adatokról, mivel azok határozzák meg az életének egyre jelentősebb részét. Ha valaki elveszti a kontrollt, vagy az adatait mások felhasználják, avval egy karriert meg lehet törni (pl.: munkahelyi e-mail címmel nem kívánt levelek küldése, Egységes Tanulmányi Rendszerben tantárgyak vagy vizsgák leadása, átrendezése).

²³ Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski, and Maša Galič: A Typology of Privacy, 2016. 69-70.

Ugyanakkor a vázolt folyamat nem egyoldalú: az egyén nem csupán arról dönthet, hogy adatokat milyen minőségben és mennyiségben ad ki magáról a kívüllágnak, hanem azt is meghatározhatja, hogy a kívüllágot mennyire engedi be a magánszférájába, mely által a magánszféra "többet jelent, mint a háborítatlan magánélethez való jog".²⁴

A magánszféra kiterjesztésének egyik jelentős új lépése a számítógépes rendszerek alkotmányos védelmének biztosítása, amelyet a Német Alkotmánybíróság mondott ki ítéletében, amely két hagyományos magánszféra védelem (az otthon és a kommunikáció) között helyezkedik el, mivel a számítógépek és az okos eszközök a kommunikációnak egyre jelentősebb részét tárolják el, a hagyományos papír alapú levelezéssel összehasonlíthatatlanul nagyobb mennyiségben²⁵. A Bíróság előtt lévő ügy a nemzetbiztonsági szervek által alkalmazott trójai falovakkal volt kapcsolatos²⁶, amely során a bíróság kimondta, hogy a személyi számítógépek (és a rajtuk tárolt adatok) nincsenek megfelelően védve az otthon és a telekommunikáció magánszférájának védelme által, így ez a magánszférának egy nyitott végét jelenti. Olaszországban szintén hasonló folyamat indult meg, azonban ott még nem alkotmányos szinten, hanem a büntetőjog által a számítógépes rendszerbe való illetéktelen behatolás a birtokháborításhoz hasonlóan.

A Kanadai Legfelsőbb Bíróság döntésében²⁷ szintén elismerte a számítógépes rendszerek védelmének fontosságát, mivel olyan mennyiségű és minőségű információt tárolnak, amelyet az érintettek jelentős része nem képes, vagy nem akar kontrol alatt tartani.

2.1.1 Adatvédelem és a magánszféra védelme

Az adatvédelem meghatározása előtt elengedhetetlen, hogy tisztázzuk a viszonyát a magánszféra védelemmel és az információs önrendelkezési joggal: az adatvédelem intézményét kizárólag a magánszféra védelmén belül értelmezhetjük, míg az információs önrendelkezési jogot az adatvédelmen belül helyezhetjük el.

²⁴ Szabó 2005, 49.

²⁵ Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorváne, Tomislav Chokrevski, and Maša Galič, 2016. 30.

²⁶ BVerfG [German Constitutional Court] 27 February 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007

²⁷ R. v. Vu, [2013] SCR 657, para. 24 (2013) ("Computers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search.")

A magánszféra védelmének előző fejezetben történt meghatározása után kijelenthetjük, hogy az a személyiségvédelemnek egy nehezen körülhatárolható, széles területét fedi le, mely egyértelműen tágabb, mint az adatvédelem²⁸.

Péterfalvi Attila adatvédelmi biztosként ebben a kérdésben a saját hatáskörét szűkítve úgy foglalt állást, hogy olyan esetben nem jár el, melyben bár a magánszféra megsértése megállapítható, viszont a személyes adatok megsértése már nem.

"Úgy gondolom, hogy a személyes adatok védelméhez fűződő jog - bár tudjuk, hogy szinte minden személyes adat - általában szűkebb, mint a privacy vagy a magánélethez fűződő jog védelme, és én itt hatáskörömet nem értelmezem kiterjesztően. Azokban az esetekben foglalom tehát állást, amelyek személyes adatok kezeléséhez kapcsolódnak, de ettől még a vizsgált eljárás adott esetben a privacyt vagy a magánélethez való jogot sértheti."²⁹

Jóri András szerint is az adatvédelem a privacy keretein belül értelmezhető: "a magánszféra védelmének számos – jogi és jogon kívüli – eszköze, módja különböztethető meg, és maga a fogalom a jelenségek jóval szélesebb tartományára értelmezhető, mint az adatvédelem – az adatvédelem csak a magánszféra védelmének keretein belül, mint a magánszféra-védelem adott társadalmi és technikai körülmények között létrejött jogi eszköze értelmezhető."³⁰

2.1.2 Adatvédelem és az információs önrendelkezési jog

Az adatvédelem tágabb kategória, mint az információs önrendelkezési jog, melyet az első adatvédelmi törvények még nem biztosítottak az érintett számára, ugyanakkor az információs önrendelkezési jognak is vannak olyan aspektusai, melyek nem fedhetők le az adatvédelmi joggal.

Az önrendelkezési jog alapján megilleti az egyént az a jog, hogy döntsön a rá vonatkozó információk nyilvánosságra hozataláról, míg az adatvédelmi jog elsősorban az adatkezelőnek állít korlátokat az adatok kezelésével kapcsolatban.³¹ Az egyén azon jogára vonatkozóan, hogy nyilvánosságra hozhasson magáról bármilyen információt, az adatvédelmi jog korlátot nem állapít meg, csupán az adatkezelőnek írja elő a jogalapokat³² (hozzájárulás, vagy jogszabály

²⁸ Anita L. Allen: Unpopular Privacy, Oxford University Press, New York, 2011. 4-5.

²⁹ Interjú Péterfalvi Attila adatvédelmi biztossal, in: Fundamentum, 2004. 4. szám, 40-41.

³⁰ Jóri, 2009, 15.

³¹ 15/1991. (IV. 13.) AB határozat, 20/1990. (X. 4.) AB határozat

³² Rhona K. M. Smith: International Human Rights, Oxford University Press, Oxford, 2003, 269.

engedélye). Kijelenthetjük, hogy ebben az esetben az információs önrendelkezési jog és az adatvédelmi jog nem fedik egymást³³.

1. ábra: Az adatvédelem és az információs önrendelkezési jog viszonya

Szabó Máté tágabb értelmezése szerint az információs önrendelkezési jog magába foglalja az egyén kívülág megismeréséhez való jogát is, melyet az adatvédelem közvetlenül szintén nem korlátoz.³⁴

Az adatvédelem tágabb jelentését az adatbiztonság követelményéből is levezethetjük: az adatvédelem része az adatbiztonság követelménye, mely alatt olyan szervezési és technikai követelményeket értünk, melynek az adatkezelő köteles eleget tenni (pl.: csak meghatározott személyek férhetnek hozzá az adatbázishoz egyéni jelszóval, vírusirtó és tűzfal telepítése). Az adatbiztonság követelménye túlmutat az érintett információs önrendelkezési jogán: az adatbiztonság nem csak attól véd, hogy illetéktelenek hozzáférhessenek az adatainkhoz, hanem az adatok megsérülése, megsemmisülése ellen is. Szabó Máté szerint is "itt egyértelműen az adatok fizikai és jogi védelmén van a hangsúly, nem pedig az önrendelkezésen, az alany döntési szabadságán".³⁵

Fontos megjegyezni, hogy több olyan kötelező adatszolgáltatás esetén (pl.: születés, halálozás, népszámlálás), melynél az információs önrendelkezési jog háttérbe szorul a közérdek miatt, az adatvédelmi és adatbiztonsági szabályok ugyanúgy érvényesülnek, mint a nem kötelező adatkezelések esetén.

Az Alkotmánybíróság több határozatában is kiemelte, hogy az információs önrendelkezési jog alapjog, azonban nem abszolút jog, mivel törvény korlátozhatja azt. A korlátozás csak akkor alkotmányos, ha a korlátozás megfelel az Alaptörvényben támasztott követelményeknek.³⁶

³³ Ian Kerr – Valerie steeves – Carole Lucock: Lessons From The Identity Trail, Oxford University Press, New York, 2009, 303-17.

³⁴ Szabó 2005, 53.

³⁵ Szabó 2005, 54 p.

³⁶ 2/1990. (II. 18.) AB határozat, 5/1991. (IV. 13.) AB határozat, 46/1995. (VI. 30.) AB határozat

2.2 Az adatvédelem célja és helye a hatályos jogi szabályozásban

Az EU Adatvédelmi irányelve a magánszféra védelméből kiindulva, azon belül jelöli meg az adatvédelem helyét:

*"A tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében."*³⁷

Magyarország Alaptörvényének VI. cikke a privát szféra védelmével egy csoportban helyezi védelem alá a személyes adatokat.

(1) Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák.

(2) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.

(3) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi.

Nemzeti szabályozás szintjén az információs önrendelkezési jogról és az információszabadságról szóló törvény nevesíti is az érintett magánszféráját és az irányelvet követve azon belül helyezi el a személyes adatok védelmét.

*"E törvény célja az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák..."*³⁸

Az EU adatvédelmi rendelte már szűkebben fogalmaz, nem helyezi el az adatvédelmet a magánszféra védelmén belül elméleti jelleggel:

³⁷ Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (1995. október 24.), I. Fejezet, 1. cikk, (1) bek.

³⁸ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, 1. §

*"Ez a rendelet a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi."*³⁹

2.2.1 Az adatvédelem és az adatvédelmi jog fogalma

Az adatvédelem megalkotása mögött legfőképp az a filozófia húzódik, hogy a titokszféra védelme már nem elegendő, melynél messzebb kell menni, a védelemnek minden személyes adatra ki kell terjednie.⁴⁰

Az adatvédelem és az adatvédelmi jog tudományos meghatározásához hazai és külföldi jogtudósok elméleteit használtam fel, a különböző jogrendszerekből eredő megközelítések különbözőségét figyelembe véve.

A fogalmi meghatározásokban egybevág, hogy az adatvédelem az érintett természetes személy jogait védi közvetlenül vagy közvetetten.

Majtényi László szerint „Az adatvédelem a személy, az ember, más szóval: az adatalany védelmét, nem pedig magának az adatnak a védelmét jelenti”⁴¹

Ha figyelembe vesszük, hogy az adatbiztonság követelménye is közvetetten az érintett jogait védi, a szerzők meghatározása időtállóan tekinthető. Fontos megjegyezni, hogy az internet fejlődése, térnyerése és folyamatos változása (pl. a felhő alapú technológia elterjedése) miatt az adatbiztonság követelménye előtérbe került, így az újabb szabályozások egyre jelentősebb részét teszik ki a technikai és szervezési követelmények, melyek az adatok védelmét fokozottan biztosítják, az érintett érdekében.

Lothar Determann fogalmi meghatározása⁴² átmenetet képez az európai és az amerikai megközelítés között. Az adatvédelmi szabályok mindennapi alkalmazására készült könyvében az alábbiak szerint határozza meg az adatvédelmi jog fogalmát (az információs önrendelkezési jogból kiindulva):

"Olyan jogszabályok, melyek célja, hogy megvédjék az érintett azon képességét, hogy rendelkezessen azon adatokról, információkról, melyek hozzá köthetőek, beleértve az európai típusú szabályozásokat (melyek a személyes adat mindenféle kezelését és feldolgozását

³⁹ Javaslat az Európai Parlament és a Tanács rendeletére a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet), 1. cikk (2) bek. (Brüsszel, 2012.01.25.)

⁴⁰ Jóri 2009, 9.

⁴¹ Majtényi László: Adatvédelem, információs szabadság, Alkotmány- és Jogpolitikai Intézet, Budapest, 1997, 6.

⁴² Lothar Determann: Determann's Field Guide to International Data Privacy Law Compliance, Edward Elgar Publishing Limited, 2012. 10-11 p.

szabályozzák), és az angolszász típusú szabályozásokat (az egyén azon jogának védelme, hogy egyedül lehessen)"⁴³

A Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján található adatvédelmi szótárban az alábbi meghatározást találjuk:

"Személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége"⁴⁴

Az adatvédelem és az adatvédelmi jog tudományos megfogalmazását Jóri András meghatározásával zárnám le, mely teljes körűen és időt állóan határozza meg a jogintézményt: "Az adatvédelem jellemzője, hogy a magánszféra védelmén belül értelmezhető az alábbiak szerint:

- a) az adatvédelem minden esetben a személy magánszférájának jogi védelmét jelenti, amely
- b) az 1970-es évektől az elektronikai forradalom által egyre általánosabbá váló automatizált adatfeldolgozás veszélyeire válaszul jelent meg Európában, és
- c) az általa nyújtott jogi védelem tartalma a fogalom megjelenése óta többször is jelentősen változott, illetőleg jelenleg is folyamatosan változásban van."⁴⁵

2.2.1 Személyiségi jogok

Az ember magánszférájának polgári jogi védelmét a személyiségi jogok biztosítják. A személyiségi jogok szerkezete a tulajdonjog mintájára megalkotott, abszolút szerkezetű jogviszony, mely a konkrét jogosult és a végtelen számú ismeretlen kötelezett között áll fenn. Ahogy a dolog tulajdonosának jogait, úgy a személyiségi jogokat is felsorolni lehetetlen. A technika és az internet fejlődésével párhuzamosan új személyiségi jogok is keletkeznek, melyekre a védelem automatikusan kiterjed.

Az "új" Polgári Törvénykönyv személyiségi jogokat védő generálklauzulája a védelem aktív oldalát hangsúlyozza a "régi" Ptk. passzív megközelítésével⁴⁶ szemben:

⁴³ "Laws intended to protect an individual data subject's ability to control information about him or herself, including European-style data protection laws (regulating any processing of any personal data) and common law privacy laws (protecting reasonable expectations of being left alone)."

⁴⁴ <http://www.naih.hu/adatvedelmi-szotar.html> (2014. jan. 5.)

⁴⁵ Jóri 2009, 16.

⁴⁶ 1959. évi IV. törvény a Polgári Törvénykönyvről, 75. § (1) A személyhez fűződő jogokat mindenki köteles tiszteletben tartani. E jogok a törvény védelme alatt állnak.

2:42. § (1) Mindenkinek joga van ahhoz, hogy törvény és mások jogainak korlátai között személyiségét szabadon érvényesíthesse, és hogy abban őt senki ne gátolja.⁴⁷

(2) Az emberi méltóságot és az abból fakadó személyiségi jogokat mindenki köteles tiszteletben tartani. A személyiségi jogok e törvény védelme alatt állnak.

2:43. § A személyiségi jogok sérelmét jelenti különösen

e) a magántitokhoz és a személyes adatok védelméhez való jog megsértése;

Az új Polgári Törvénykönyv alapján sem azonos a polgári jogi személyiségvédelem az alapjogok katalógusával. Kétségtelen, hogy számos alapjog, melyek elsősorban közjogi eszközökkel védettek (pl. az élethez, testi épséghez való jog büntetőjogi védelme), megsértésük személyiségi jogok védelme körében is szankcionálható, viszont eltérő jogi eszközökkel és eljárási szabályokkal.⁴⁸

A törvény nem határozza meg a személyiségi jogok fogalmát, ehelyett egy generálklauzulával védelem alá helyezi azt, szélesre tárva a védelem hálóját.

A személyiségi jogvédelem generális jellegére az Alkotmánybíróság is rámutatott: "Az általános személyiségi jog 'anyajog', azaz olyan szubszidiárius alapjog, amelyet mind az Alkotmánybíróság, mind a bíróságok minden esetben felhívhatnak az egyén autonómiájának védelmére, ha az adott tényállásra a konkrét, nevesített alapjogok egyike sem alkalmazható"⁴⁹. Az élethez és az emberi méltósághoz való jog lényegéből is következik, hogy a személyiségi jogok védelmének hatálya az emberi létezésből eredő bármely jogra kiterjed abban az esetben is, ha a jogalanyt ért sérelem a Ptk-ban nevesített vagy más jogszabályokban szabályozott személyhez fűződő jogok egyikének sem feleltethető meg. A személyhez fűződő jogok nem kategorizálhatók, mivel azok a személyiségnek az egyén viselkedésében, gondolkodásában és külső megjelenésében megnyilvánuló, értékminőségéből adódó sokszínűségét hivatottak védeni⁵⁰. Ez indokolhatja azt, hogy mind a „régí”, mind az „új” Ptk. csupán példálózó jelleggel sorolja fel a személyhez fűződő, illetve személyiségi jogokat.

⁴⁷ 2013. évi V. törvény, a Polgári Törvénykönyvről, 2:42. § [A személyiségi jogok általános védelme]

⁴⁸ Vékás Lajos (szerk.): A Polgári Törvénykönyv magyarázatokkal, CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2013, 56-57.

⁴⁹ 8/1990. (IV. 23.) AB határozat

⁵⁰ 34/1992. (VI. 1.) AB határozat

A bírói gyakorlat is számos védendő személyiségi jogot nevesített, mint például a teljes családi élethez⁵¹, illetve a családtervezéshez fűződő jogot⁵², míg a személyes adatok védelméhez való jogot az Alkotmánybíróság helyezte védelem alá információs önrendelkezési jogként⁵³.

A személyiségi jogok meghatározása elengedhetetlen az adatvédelem és az magánszféra védelmének szempontjából, ezért egy átfogó fogalmi meghatározást idéznék Lenkovics Barnabástól és Székely Lászlótól:

"A személyiségi jogok az embernek és a jogi személyeknek a társadalmi rendeltetésük betöltéséhez szükséges nem vagyoni értelemben vett integritást, háborítatlanságot, beavatkozástól mentes mozgásteret hivatott biztosítani, átlagosan tipizáltan a közfelfogáshoz igazodva, a konvenció által szükségtelennek minősített illetéktelen beavatkozások ellen."⁵⁴

⁵¹ 2043/2009. PEH

⁵² Legfelsőbb Bíróság 1/2008. PJE határozat

⁵³ 15/1991. (IV. 13.) AB határozat

⁵⁴ Lenkovics Barnabás - Székely László: A személyi jog vázlata, Eötvös József Könyvkiadó, Budapest, 2001, 100.

2.3 Az adatvédelem generációi

Első generáció

A számítástechnikai fejlődésének köszönhetően az 1960-as évekre lehetővé vált, hogy hatalmas adatbázisokat hozzanak létre az állampolgárok adatainak elektronikus kezelésére. Mivel a technológia nagyon drága volt, és a képzett szakemberek sem álltak rendelkezésre olyan szinten, mint napjainkban, ezért az üzemeltetőnek célszerűbb volt egy helyre összpontosítani az eszköz- és személyi állományát, majd azt távoli felhasználók számára elérhetővé tenni.⁵⁵

Az adatbázisok kombinálásának és kezelésének legegyszerűbb módja egy egységes és univerzálisan használható mesterséges azonosító kód alkalmazása volt (pl.: egy személyi szám) a közigazgatáson belül.

Az adatbázisok összekapcsolásának és az egységes azonosító kódok bevezetésének terve vezetett az adatvédelmi törvények első generációjának kialakulásához, melyek az állam információs túlsúlyának kiegyensúlyozására születtek meg.

Az első generációs adatvédelmi törvények a technológia és az adatkezelő szemszögéből közelítették meg a szabályozás tárgyát, mely az adatkezelést lehetővé tevő technológia volt, melynek alkalmazása során az átláthatóság és ellenőrizhetőség megteremtésére volt a legfőbb elérendő cél. Azért közelítették meg első sorban az adatkezelő szemszögéből az adatkezelést, mert a törvények legfőképpen azt szabályozták, hogy ki és milyen feltételekkel, mennyi ideig, hol és milyen személyes adatokat kezelhet⁵⁶.

Az első generációs törvények – az adatkezelőből való kiindulásuk miatt – még nem biztosították az információs önrendelkezési jogot az érintett részére, csupán olyan részjogosítványokat, mint a betekintéshez, vagy a helyesbítéshez való jog.

Összegzésként kijelenthetjük, hogy az első generációs adatvédelmi törvények célja az állam (azon belül is a végrehajtó hatalom) információs túlsúlyának csökkentése volt, a csekély számú, nagyméretű adatbázisok korában.

⁵⁵ A helyi, tagállami és szövetségi közigazgatás adatbázisainak együttes kezelését tervezték Németországban is.

⁵⁶ Ekkor, a „kevés és nagy” - főként állami - adatbázisok korában keletkezett az adatbázisok nyilvántartási kötelezettsége, mely az első generációs adatvédelmi szabályozás egyik jellemzője volt.

Második Generáció

Az első generációs adatvédelmi törvényeket – melyek a centralizált adatbankok szabályozására születtek – az informatika fejlődése meghaladta az 1980-as évektől. Az adattárolási és adatfeldolgozási lehetőségek megváltoztak: elterjedtek az otthoni számítógépek és a szerverek megfizethetőek lettek a kis- és középvállalkozások számára is, így az adattárolás a nagy állami és vállalati központokból fokozatosan áttevődött a mindennapi üzleti- és magánéletbe. Az egyre gyorsabb és olcsóbb processzorokkal, valamint növekvő tárolókapacitású merevlemezekkel a folyamat felgyorsult: a 90-es évek végére bárki tudott otthonában megfizethető áron komoly adatbázisokat kezelő technológiát üzemeltetni, melyre olaj volt olcsó és gyors internetet.

Mivel technikai fejlődés következtében az adatbázisok és az adatkezelők szabályozása nehézkessé vált, ezért a hangsúly áttevődött az érintettre: felruházták jogokkal az adatkezelés teljes időtartamára.

A második generáció kezdetének az információs önrendelkezési jog Német Alkotmánybíróság általi megfogalmazását tekinthetjük⁵⁷, melynek következtében a nemzeti törvényhozások felruházták az érintetteket azon joggal, hogy adataik kiadásáról és felhasználásáról maguk dönthessenek.

Az érintettek jogainak bővülésével egy időben egyszerűsödtek az adatbázisok üzemeltetőinek nyilvántartásba vétellel kapcsolatos kötelezettségei is, reagálva a kor kihívásaira a működőképességük érdekében.

Bár az információs önrendelkezési jog megfogalmazása és az érintett avval való felruházása az adatvédelmi jog legjelentősebb intézménye volt, a mindennapokban nem működött és nem működik úgy, ahogyan azt annak megfogalmazói elképzelték.

A gazdaságot és társadalmat olyannyira áthatják az elektronikus adatkezeléssel egybekötött szolgáltatások (pl.: Egységes Tanulmányi Rendszer, Neptun, munkahelyi hálózatok, email szolgáltatók, Skype), hogy nélkülük az egyetemi-, munkahelyi- és sokszor magánéletünket is komoly hátrányokkal tudnánk csak folytatni (pl.: Skype állásinterjúk). Az ilyen esetekben az érintett hasonló helyzetbe kerülhet, mint a fogyasztó a gazdasági erőfölényben lévő vállalatokkal szemben: vagy kénytelen megkötni a szerződést, vagy komoly hátránnyal jár számára annak elutasítása.⁵⁸

⁵⁷ A Német Alkotmánybíróság népszámlálás ítélete, BVerfG 65, 1, („Volkszählungsurteil”)

⁵⁸ Sokszor személyes adatok nem is voltak szükségesek a szerződés megkötéséhez és az áru vagy szolgáltatás nyújtásához, mégis kénytelen volt az érintett az alkupozió hiánya folytán az adatkezelő rendelkezésére bocsátani azokat.

Az érintettek jelentős része – napjainkig – nincsen tisztában a személyes adataira váró feldolgozási módokkal, azok piaci értékével, így az ilyen szerződések megkötése során sérül az alkupozíciója, mivel az adatkezelő tudja csak pontosan, hogy mi lesz a személyes adatok sorsa („knowledge gap”)⁵⁹.

A hozzájárulások jelentős részében az önkéntesség is kérdéses: az adatkezelő (pl. egy weboldal üzemeltetője) a szolgáltatás igénybevételét a személyes adatok megadásához és az adatkezelési irányelvek elfogadásához köti a szükségesség elvével ellentétesen („consent fallacy”).

Az információs önrendelkezési joggal operáló második generációs adatvédelmi törvények alkalmazása során érződtek különösen a fentebb vázolt problémák: az ügyek jelentős része „kimerült a jogalap formális vizsgálatában”, így „a hozzájáruláson alapuló adatkezelések esetén, főképp az üzleti forgalomban, a jogalkalmazó kényszermegoldásokkal, bonyolult és gyakran téves jogértelmezéssel próbálja segíteni az információs önrendelkezési jogának értéktelenségét tapasztaló, a nagy adatkezelő szervezeteknek kiszolgáltatott egyént.”⁶⁰

Harmadik generáció

A második generációra jellemző „technológia semleges” szabályozás a mindent átható internet, az automatizált adatfeldolgozás, és az érintett gyenge alkupozíciójára tekintettel megváltozott: az adatvédelmi szabályozás harmadik generációja az adott technológiára tekintettel, szektoriális szabályozás mentén is törekszik az önrendelkezési jog támogatására az iparág sajátosságait figyelembe véve.

A III. generáció kezdetének az 1997-es, távszolgáltatások adatvédelméről szóló német törvény elfogadását tekinthetjük (Teledienstschutzgesetz)⁶¹, mely olyan új elveket és intézményeket vezetett be az adatvédelmi jogba, mint az adattakarékosság elve, vagy az adatvédelmi audit.

Az adatvédelmi audit (hasonlóan más iparágakhoz) valamely eljárás vagy eszköz adatvédelmi szempontból való megfelelőségét vizsgálja egy független harmadik szervezet által.⁶²

A harmadik generáció további jellemzője, hogy az integráció mentén születtek a szabályozások az Európai Unió irányelvének köszönhetően, melynek hatása nem állt meg az EU határainál:

⁵⁹ Paul M. Schwartz: Privacy and Democracy in Cyberspace, 52 Vanderbilt Lawreview, 1999, 1660.

⁶⁰ Jóri 2009, 40.

⁶¹ Gesetz über den Datenschutz bei Telediensten, 1997. 07. 22.

⁶² Nemzeti Adatvédelmi és Információszabadság Hatóság és a magánszférában tevékenységet folytató szervezetek is végezhetnek adatvédelmi auditot. Az adatvédelmi auditról és annak szempontjairól az alábbi oldalon olvashat részletes információkat:

<http://www.naih.hu/files/AdatvedelmiAuditSzakmaiSzempontokVegleges.pdf>

több ország törvényhozása azt mintának tekintette, vagy kénytelen volt annak tekinteni az irányelv harmadik országokba irányuló adatküldésekre vonatkozó korlátozása miatt.

Az adattakarékosság elve alapján az adatkezelőnek kötelessége, hogy már az adatkezelés megkezdése előtt úgy tervezze a cél eléréséhez szükséges folyamatokat és eszközöket, hogy az minél kevesebb személyes adattal legyen elérhető, vagy – amennyiben az lehetséges – ne is használjon fel ahhoz személyes adatot.

Az adattakarékosság elve így több, mint az 1992-es és a hatályos adatvédelmi törvényben megfogalmazott szükségesség elve.⁶³

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény módosítása tartalmazta az adattakarékosság elvét német mintára.⁶⁴

Kijelenthetjük, hogy a harmadik generációs szabályozás az önrendelkezési joggal felruházott érintett és az adatkezelő közötti egyensúly helyreállítására született meg, az adatkezelő nagy szervezetek tevékenységének és technológiájának szabályozására.

⁶³ 1992. évi LXIII. törvény 5. § (2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.

2011. évi CXII. törvény 4. § (2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

⁶⁴ 2001. évi CVIII. törvény 13/A. § (3) A szolgáltató - a (2) bekezdésben foglaltakon túlmenően - a szolgáltatás nyújtása céljából kezelheti azon személyes adatokat, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek. A szolgáltatónak az egyéb feltételek azonossága esetén úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie az információs társadalommal összefüggő szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig.

2.3.1 Az adatvédelem története

A legrégebbi magánszféra védelmével kapcsolatos írásos emlék a Hippokratészi eskü, mely Kr. e. V. századból maradt fenn. Az eskü a Kósz szigetén élő orvos papoknak tartalmazott erkölcsi iránymutatást az orvoslással kapcsolatban, melyet Hippokratésznek, vagy valamelyik tanítványának tulajdonítanak.⁶⁵ Az eskü titoktartással kapcsolatos része:

"És ha olyat látok vagy hallok orvosi kezelés közben vagy akár a therapia körén kívül az emberek életéről, amit nem szabad kifecsegni, azt el fogom hallgatni, abban a véleményben, hogy az efféle dolgokat szent titkok módjára kell megőrizni."

A szöveg jelentőségét mi sem mutathatja jobban, mint hogy napjainkban is szinte ugyanerre az esküre (kisebb fordításbeli különbségekkel) kell az orvosoknak felesküdniük.

A Szegedi Tudományegyetem orvosi esküje így hangzik:

"Akár az orvosi szolgálat közben, akár azon kívül bármely titkot megtudok embertársaimról, azt – hacsak törvény nem követeli – senkinek fel nem fedem."

Az első magánszféra védelmét biztosító jogszabály az Angliában 1361-ben elfogadott Justices of the Peace Act⁶⁶, mely a hallgatóságot és a kukkolást szankcionálta.

Sokunk számára ismerős "az én házam az én váram" kifejezés, mely 1604-ből ered, a "Semayne" ügy ítéletéből. Az ügy rövid tényállása, hogy Londonban a seriff egy jogerős végzés birtokában az ajtó betörésével behatolt egy házba, hogy a végzésnek eleget tegyen. Sir Edward Coke bíró ítéletében az alábbiak szerint rendelkezett:

"Minden olyan esetben, mikor seriff a király képviseletében jár el, behatolhat a házba, hogy végrehajtsa a király, vagy az ő nevében hozott határozatot. De, mielőtt behatol, köteles tájékoztatni a belépés szükségességének okáról, és kérni, hogy nyissák ki az ajtót."

"A háza mindenkinek a saját vára és erődje"⁶⁷

A XIX. század második felében a fotográfia fejlődése és a sajtó átalakulása jelentősen megváltoztatta az emberek mindennapi életét. A fotográfia megjelenésekor egy fénykép elkészítése hosszas folyamat volt, mely során az alanynak akár több órán át kellett egy helyben ülnie. A technika fejlődésével azonban lehetővé vált a fotók azonnali elkészítése, mely komolyabb veszélyt még mindig nem jelentett a magánszférára, mivel a gépek drágák és nagyok voltak, azonban 1884-ben a Kodak bemutatta az első olyan fényképezőgépet, mely

⁶⁵ Farnell, Lewis R.: Greek Hero Cults and Ideas of Immortality. Kessinger Publishing, 2004, 234–279.

⁶⁶ The National Archives, United Kingdom, <http://www.legislation.gov.uk/aep/Edw3/34/1>

⁶⁷ Semayne's Case(1604) Michaelmas Term, 2 James I In the Court of King's Bench, first published in the Reports, volume 5, page 91a

kellően kompakt volt és megfizethető, hogy tömegesen elterjedhessen. A magánszférára leselkedő veszélyt növelte a bulvársajtó elterjedése is, mely az egyre növekvő eladási számokkal óriási bevételekre tett szert. Az új fényképezési technológia és az erősödő bulvársajtó találkozása komoly veszélyt jelentett a magánszférára, melyre a jogalkotónak lépnie kellett.

1888-ban nyújtottak be egy keresetet képmás jogosulatlan közzétételével kapcsolatban az Egyesült Államokban. Egy fotóstúdió az ügyfelük fotóját annak engedélye nélkül egy képeslapra helyezte rá, majd azt sokszorosította és árulta.⁶⁸ A bíróság az alperes fotóstúdiót eltiltotta a kép engedély nélküli felhasználásától.⁶⁹

Az adatvédelem és a magánszféra témájában a legjelentősebb tudományos munka Samuel D. Warren és Louis Brandeis nevéhez fűződik, akiknek 1890-ben jelent meg a "The Right To Privacy" (A magánszférához való jog) című tanulánya a Harvard Law Review kiadványban.⁷⁰ 1948. december 10-én került elfogadásra ENSZ Közgyűlése által az Emberi Jogok Egyetemes Nyilatkozata, mely a világszervezet emberi jogokkal kapcsolatos álláspontját tartalmazza.

A nyilatkozat 30 cikkben fogalmazza meg az emberi jogokat, melyek fajra, színre, nemre, nyelvre, vallásra és politikai meggyőződésre való tekintet nélkül megilletnek minden embert.⁷¹

A 12. cikk rendelkezik a magánszféra védelmével kapcsolatosan:

Senkinek magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez.

Bár a nyilatkozat az államokra nem kötelező, hatásosan lehet vele diplomáciai és erkölcsi elvárásokat támasztani a kormányokkal szemben. A nyilatkozat alapját képezi két, kötelező erejű ENSZ-egyezménynek, melyeket 1966. december 16-án fogadott el a Közgyűlés (Polgári és Politikai Jogok Nemzetközi Egyezségokmánya; Gazdasági, Szociális és Kulturális Jogok Nemzetközi Egyezségokmánya).

Közgyűlés egy későbbi döntése december 10-ét az emberi jogok napjának nyilvánította, továbbá az Emberi Jogok Egyetemes Nyilatkozata jelenleg a legtöbb nyelvre és nyelvjárásra lefordított dokumentum, mely egyetemességét és a benne megfogalmazott jogok fontosságát

⁶⁸ California Law Review, Vol. 48, No. 3, 1960 augusztus

⁶⁹ Pollard vs. Photographic Co.: 40 Ch. Div. 345

⁷⁰ Warren and Brandeis, 1890, 5.

⁷¹ A Nyilatkozat magyar nyelvű fordítása az ENSZ honlapján, az alábbi címen érhető el (2014. 07. 16.):
http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/hng.pdf

jelzi.⁷² Az emberi jogok egyetemességének koncepciója és az erre vonatkozó nemzetközi egyezmények állami szintű végrehajtása közötti viszonyban jelenik meg az egyetemesség és az egyedi állami szuverenitás közti feszültség. A legfontosabb nemzetközi normák végrehajtása is szuverén államok akaratán múlik⁷³.

1949-ben jelent meg George Orwelltől az 1984 (eredeti címén Nineteen Eighty-Four), mely egy disztópiában (negatív utópia) játszódó satirikus politikai regény. A történet egy totalitárius állam keretei között mutatja be a főszereplők és az állampolgárok életét, akik magánszférával egyáltalán nem rendelkeznek. A mindent látó, állampolgárok privát szféráját semmibe vevő, személyes adatait korlátlanul kezelő államokat rendszeresen illetik „Orwelli” jelzővel napjainkig.

Az Európa Tanács 1950. november 4-én, Rómában fogadta el az **Emberi Jogok Európai Egyezményét**⁷⁴, mely nem rendelkezik a személyes adatok védelméről, azonban a magánszféra védelmével kapcsolatos cikke az 50-es években különös jelentőséggel bírt.⁷⁵

8. Cikk

Magán- és családi élet tiszteletben tartásához való jog

1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák.

2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

1952-ben alapította meg Truman elnök a **National Security Agencyt** (NSA), mely később az internet legnagyobb kormányzat által működtetett adatfeldolgozójává vált (nem hivatalos információk alapján) nemzetbiztonsági feladatok ellátása céljából: adatokat gyűjt, dekódol és

⁷² A new world record: Universal Declaration in 370 languages, 2010. 04. 20.

<http://www.ohchr.org/EN/NewsEvents/Pages/AnewworldrecordUDHR.aspx>

⁷³ Paczolay Péter: Az emberi jogok egyetemessége, in: Ünnepi Kötet Lábady Tamás 70. születésnapja alkalmából, szerk.: Csehi Zoltán – Koltay András – Landi Balázs – Pogácsás Anett, Pázmány Press, Budapest, 2014, 500.

⁷⁴ Hivatalosan kihirdetett magyar elnevezése: "Az emberi jogok és alapvető szabadságok védelméről szóló Egyezmény". (angolul Convention for the Protection of Human Rights and Fundamental Freedoms, vagy röviden European Convention of Human Rights). A hivatalos magyar fordítás az Európa Tanács alábbi oldalán érhető el: http://www.echr.coe.int/Documents/Convention_HUN.pdf

Az egyezmény végrehajtására hozták létre az Emberi Jogok Európai Bíróságát (European Court of Human Rights, rövidítve: ECoHR).

⁷⁵ Az Egyezmény Magyarországon 1992. november 5-től hatályos. Az egyezményt – és több kiegészítő jegyzőkönyvét – az 1993. évi XXXI. törvény hirdette ki.

rendszerét globálisan, továbbá védi az Egyesült Államok hírközlési rendszereit és adatbázisait a kiberterrorizmus ellen és az amerikai vállalatokat az ipari kémkedőktől.⁷⁶

A szervezet neve 2013-ban lett ismert a világ számára, amikor Edward Snowden titkos dokumentumokat szivárogtatott ki az NSA titkos hírszerző és kémkedő tevékenységéről, mely során a világ bármely részén bármilyen eszközt meghekkelték, amennyiben azt szükségesnek találták⁷⁷.

Az 1970-es években az adatvédelem fogalmában és használatában is jelentős változás következett be, amikor a védelem az adatok és az adatalanyok széles körére került kiterjesztésre: az addig csak érzékeny adatokat megillető jogszabályi korlátozás és védelem az egyén minden hozzá köthető információjára kezdett kiterjedni, továbbá az egyes szakmák titoktartással és bizalommal kapcsolatos szabályai (pl.: orvosok, papok) egyre több szervezetre és egyénre alkalmazandóak lettek az életviszonyok széles terét lefedve.

1977-ben a **Polgári Törvénykönyv novellája** kibővítette a személyiségi jogvédelem kereteit, számos új személyiségi jog szabályozására, mások részletesebb kifejtésére került sor. Különösen a képmás védelmére vonatkozó szabályozással és a számítógépes adatfeldolgozásra vonatkozó rendelkezésével (*"A számítógéppel történő adatfeldolgozás nem sértheti a személyhez fűződő jogokat."*) a Ptk. novella adatvédelmi szempontból fontos lépésnek tekintendő.⁷⁸

Az első kifejezetten adatvédelem tárgyában megszületett nagy nemzetközi dokumentum a **Nemzetközi Gazdasági és Együttműködési Szervezet (OECD) Irányelvei** voltak.

A nemzetközi adatáramlások az 1970-es évek végére szerves részeivé váltak a nemzetközi gazdasági életnek. Félő volt, hogy a – még kezdetleges - nemzeti adatvédelmi szabályozások ennek gátjai lehetnek.

Az OECD⁷⁹ az adatvédelem globalizációjára tekintettel 1980-ban fogalmazta meg az adatvédelmi irányelveit⁸⁰, melyek elsődleges célja a nemzetközi gazdasági életben az adatok szabad áramlásának és azok védelmének biztosítása volt, hogy a kereskedelmi akadályokat megszüntethessék.

Az alábbi alapelvek kerültek megfogalmazásra, melyek napjainkig aktuálisak.

⁷⁶ National Security Agency, <http://www.nsa.gov/> (2014. 08.06.)

⁷⁷ What we know about NSA leaker Edward Snowden, in: The Guardian, 2013. 06. 10.

<http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>

⁷⁸ Magyar Közlöny, 2002/15/II. szám, 29.

⁷⁹ Magyarország 1996. május 7-én csatlakozott a szervezethez

⁸⁰ OECD irányelvek a magánélet védelméről és a személyes adatok határokon átvitelő áramlásáról, magyar nyelvű áttekintés: <http://www.oecd.org/sti/ieconomy/15590228.pdf>

A korlátozott adatgyűjtés alapelve: korlátozni kell a személyes adatok gyűjtését, valamint bármilyen ilyen jellegű adatot törvényes és tisztességes eszközökkel kell beszerezni, és, megfelelő esetben, az alany tudtával és beleegyezésével.

Adatminőség alapelve: a személyes adatok legyenek relevánsak azokra a célokra nézve, amelyekre azokat felhasználják, és amennyire ezen célokhoz szükséges, legyenek pontosak, teljesek és állandóan aktualizáltak.

Szándékmegjelölés alapelve: a személyes adatok gyűjtésének szándékát legkésőbb az adatgyűjtéskor meg kell határozni és azok későbbi felhasználását csak e célokra, vagy azokkal nem összeegyeztethetetlen célokra kell korlátozni és amint ezek minden egyes szándékváltozás során meghatározásra kerülnek.

Felhasználási korlátozás alapelve: a személyes adatokat nem szabad nyilvánosságra hozni, rendelkezésre bocsátani vagy bármilyen más módon felhasználni az eredeti célokon kívül, kivéve, ha ahhoz az adatalany hozzájárul, vagy a törvény engedélyezi.

Biztonsági garancia alapelve: a személyes adatokat ésszerű biztonsági garanciákkal kell ellátni olyan kockázatokkal szemben, mint az adatok elvesztése, elpusztítása, felhasználása, megváltoztatása, nyilvánosságra hozatala vagy azokhoz engedély nélkül való hozzáférés.

Nyitottság alapelve: általános nyitottsági politikát kell folytatni a személyes adatok kezelésével kapcsolatosan, hogy az adatok léte, természete, az adatfelhasználás célja, az adatkezelő személye és tartózkodási helye megállapítható legyen.

Egyéni részvétel alapelve: az adatalanyoknak biztosítani kell, hogy az adatkezelőtől vagy mástól megtudhassa, hogy kezel-e vele kapcsolatos személyes adatot, amennyiben igen, azokat az adatokat megismerhesse (elvárható időn belül, nem aránytalanul magas díjért, értelmezhető módon). Jogában áll az adatalanyoknak továbbá, hogy tájékoztatási kérelmének elutasítása esetén és az adatkezeléssel szemben jogorvoslattal élhessen. Kérheti továbbá, hogy az adatait töröljék, helyesbítsék, módosítsák vagy kiegészítsék.

Felelősségre vonhatóság alapelve: az adatellenőrző legyen felelősségre vonható, amennyiben a meghatározott alapelveket nem tartja be.

Bár az OECD Irányelvek nem kötelezőek, annak alapelvei komoly hatással voltak az adatvédelem szabályozására nemzetközi és nemzeti szinteken: az Európa Tanács adatvédelmi egyezményen keresztül az EU adatvédelmi jogának kidolgozására, így közvetetten a magyar szabályozásra is hatással volt.

Kiemelendő, hogy az Egyesült Államok is tagja az OECD-nek, ezért az irányelvek mintegy közös nevezőnek tekinthetők Európa és az USA között, továbbá számos irányelv – az ET-

egyezményen keresztül – az EU adatvédelmi jogának kidolgozására, így közvetetten a magyar szabályozásra is hatással volt.

Különösen jelentős európai jogi dokumentum az **Európa Tanács Adatvédelmi Egyezménye** a személyes adatok gépi feldolgozásának a tárgyában⁸¹, mivel benne szerepel a magánélet védelméből levezetett - és attól önállósítva - a személyes adatok védelméhez való jog.⁸²

Az egyezmény 1981-ben került elfogadásra és hatálya kiterjed „a személyes adatok automatizált állományaira” és a „személyes adatok gépi feldolgozására” mind a köz-, mind a magánszféra területén. A tagállamoknak lehetősége van nyilatkozatot tenni arról, hogy az egyezményt „a személyes adatok nem gépi eszközökkel feldolgozott adatállományaira” is alkalmazzák – ilyen nyilatkozatot tett a Magyarország is.⁸³

Az egyezmény által meghatározott adatkezelési alapelvek az OECD irányelvekkel hasonlóan, az alábbiak szerint szabályozzák annak folyamatát.

A személyes adatokra vonatkozó követelmények a gépi feldolgozás során:

- a) az adatokat csak tisztességesen és törvényesen szabad megszerezni és feldolgozni,
- b) az adatokat csak meghatározott és törvényes célra szabad tárolni, és attól eltérő módon nem szabad felhasználni,
- c) az adatoknak tárolásuk céljával arányban kell állniuk, és meg kell felelniük e célnak, azon nem terjeszkedhetnek túl,
- d) az adatoknak pontosaknak, és ha szükséges, időszerűeknek kell lenniük,
- e) az adatok tárolási módjának olyannak kell lennie, amely az adatalany azonosítását csak a tárolás céljához szükséges ideig teszi lehetővé.

Az egyezmény 1998-ban vált a magyar jogrendszer részévé.⁸⁴

Német Alkotmánybíróság határozata 1983-ban az adatvédelmi jog új generációjának megszületését jelentette.

A Német Alkotmánybíróság elé került ügy tárgya az 1983-as német népszámlálástörvény volt, mely népszámlálást rendelt el, s az kiterjedt az azonosító adatokon túl a foglalkoztatással kapcsolatos adatokra is, továbbá a népszámláláshoz kapcsolódott a nem mezőgazdasági vállalkozások, munkahelyek összeírása, valamint a lakóingatlanokkal kapcsolatos épület- és lakásstatisztikai felmérése is. A népszámlálástörvény lehetővé tette a felvett adatok

⁸¹ Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során

⁸² Péterfalvi Attila: Adatvédelem és információszabadság a mindennapokban, HVG-ORAC Lap- Könyvkiadó Kft., Budapest, 2012, 39.

⁸³ Jóri, 2009, 30.

⁸⁴ Kihirdette a 1998. évi VI. törvény

összekapcsolását a lakcímnnyilvántartással az adattartalom pontosítása céljából és adattovábbításra is lehetőséget adott közigazgatási szervek számára (anonim módon).

Az információs önrendelkezési jogot az általános személyiségi jogból vezette le a német alkotmánybíróság⁸⁵, melynek tartalmát és védelmi eszközeit nem statikusnak, hanem nyitottnak és folyamatosan bővülőnek tartották az életviszonyok változásaival, különös tekintettel számítástechnika fejlődésére.

Az elektronikusan, részben vagy egészben automatizált módon megvalósuló adatkezelés az alkotmánybíróság szerint jelentősen megváltoztatja az ilyen műveleteknek az állampolgár magánszférájára gyakorolt hatását: míg korábban aktákhoz kellett visszanyúlni, mely jelentős emberi és szervezeti erőforrásokat emésztett fel, természetes gátat szabva az adatokkal végrehajtható műveletek körének, addig a technológia fejlődésének következtében akadálytalanul lehet a személyes adatokat összekapcsolni és kombinálni.

A technika által kinyitott kapuk így lehetővé teszik, hogy az adatokat távolság és időkorlát nélkül, akár másodpercek alatt előhívják, azokat akár „személyiségképpé” formálják anélkül, hogy az érintett arról tudna, vagy annak helyességét ellenőrizhetné, mely által előállhat az a helyzet, hogy az állampolgár nincsen tisztában a róla nyilvántartott adatokról.

Az alkotmánybíróság határozatában napjainkig ható meghatározást tett, amikor kimondta, hogy *a személyiségi jog magában foglalja „az egyénnek az önrendelkezés eszméjéből következő illetékességét arra, hogy alapvetően mikor és milyen mértékben fedi fel személyes életének tényállásait”*⁸⁶. Példaként hozta fel, hogy az állampolgár, ha bizonytalan abban, hogy feljegyeznek-e információkat róla bizonyos élethelyzetekben, akkor tartózkodhat az olyan kockázatosnak tekinthető magatartásoktól, mint egy gyűlésen vagy tüntetésen való részvétel.

Az Alkotmánybíróság kiemelte ugyanakkor, hogy az információs önrendelkezés joga sem korlátlan. Közérdekből és az arányosság elvét figyelembe véve lehetséges annak korlátozása, feltéve, hogy a szabályozás meghatározza az adatkezelés célját és az adatok körét, melyek szükségesek a cél elérésére, és csak addig kerülnek felhasználásra, amíg az elengedhetetlen.

A korlátozáshoz szükségesnek tartotta továbbá az Alkotmánybíróság a megfelelő tájékozhatást és az átláthatóságot, hogy az állampolgár a teljes adatkezelés során követhesse az adatai útját.

Az Alkotmánybíróság határozatában alkotmányellenesnek nyilvánította a törvény azon szakaszait, melyek a népszámlálásból származó adatok egyéb célú felhasználását tették

⁸⁵ Németországi Szövetségi Köztársaság Alaptörvénye, 1. cikk (1) Az emberi méltóság elidegeníthetetlen. Ennek tisztelete és védelme minden állami szerv kötelezettsége.

2. cikk (1) Mindenkinek joga van személyisége szabad kibontakoztatásához, amennyiben mások jogait nem sérti és az alkotmányos rend és az erkölcsi törvény ellen nem vét.

⁸⁶ Jóri, 2009, 26.

lehetővé a közigazgatás részére, mivel a statisztika és a közigazgatási cél összekapcsolása áttekinthetetlen helyzetet eredményez a polgár számára.

Az **ENSZ Adatvédelmi Irányelvével** saját szervezetére vonatkozóan jogi előírásokat határozott meg, és a tagállamai számára nem kötelező erejű ajánlásokat adott.⁸⁷

Az 1960-as évek óta vizsgálja az ENSZ az elektronikus adatfeldolgozásnak az emberi jogokra gyakorolt hatásait. Az Emberi Jogi Bizottsága és a Főtitkárság több jelentéssel is vizsgálta a kérdéskört, majd 1990-re készült el az irányelv tervezete személyes adatokat tartalmazó akták számítógépes feldolgozása vonatkozásában⁸⁸, mely a magán és a közjog körébe tartozó adatkezelőkre, továbbá az automatizált és a manuális adatfeldolgozásra szintén alkalmazandó volt. Az irányelv négy alapvető elemet határozott meg: az adatok minőségének biztosítását, a célhoz kötöttség alkalmazását, az érintettek betekintési jogának biztosítását, illetve az adatbiztonsághoz szükséges intézkedések megtételét. Az irányelv új alapelvként határozta meg a hátrányos megkülönböztetés tilalmát, mely a szenzitív adatok körében bírt különös jelentőséggel.

Az ENSZ ajánlásában kiemeli, hogy a szükséges hatáskörrel és illetékességgel felruházott felügyelő hatóságokat kell létrehozni az adatvédelem követelményeinek betartatása és a jogérvényesítés érdekében, továbbá a határon átnyúló adatforgalom vonatkozásában mind a küldő, mind a fogadó oldalán azonos mértékű védelmet kell biztosítani.

Az 1989. október 23-án kihirdetett alkotmánymódosítással⁸⁹ létrejött a **köztársasági alkotmány**, mely a személyes adatok védelmét és az információszabadságot alkotmányos szintre emelte.

59. § (1) A Magyar Köztársaságban mindenkit megillet a jóhírnévhez, a magánlakás sérthetetlenségéhez, valamint a magántitok és a személyes adatok védelméhez való jog.

(2) A személyes adatok védelméről szóló törvény elfogadásához a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges

A német és a magyar adatvédelmi jogfelfogás közel áll egymáshoz, mely leginkább a két ország alkotmánybíróságának adatvédelmi gyakorlatára vezethető vissza. Magyarország adatvédelmi

⁸⁷ Mező István: Személyes adatok védelme az Európai Unió jogában és Magyarországon, Miskolc, 2007, 42.

⁸⁸ Guidelines for the Regulation of Computerized Personal Data Files, elfogadva 1990. december 14-én az ENSZ Közgyűlése által

<http://www.refworld.org/docid/3ddcafaac.html>

⁸⁹ 1949. évi XX. törvény, a Magyar Köztársaság Alkotmánya, XII. fejezet, 59. §

jogának egyik alapkövének számító 15/1991. (IV. 13.) AB határozat több elemében épít a német adatvédelem dogmatikáját kidolgozó 1983-as szövetségi alkotmánybíróági határozatra.⁹⁰

Az **Alkotmánybíróság** 1991. április 13-án hozta meg határozatát⁹¹ a **személyi szám használatáról**, mellyel Magyarország népesség-nyilvántartásának teljes jogi rendszerét - az adatvédelmi törvény hiányából eredő aktivizmussal - hatályon kívül helyezve a személyes adatok védelmével kapcsolatos jogintézmények sorát vitte be a jogrendszerbe (pl.: célhoz kötöttség, információs önrendelkezési jog).

Az Alkotmánybíróság megállapította, hogy a személyes adatok meghatározott cél nélküli, tetszőleges jövőbeni felhasználásra való gyűjtése és feldolgozása, továbbá a korlátlanul használható, általános és egységes személyazonosító jel (személyi szám) alkotmányellenes.

Az indítványozó az állami népességnylvántartásról szóló 1986. évi X. számú törvényerejű rendelet, valamint az annak végrehajtására hozott törvényerejű rendeletek⁹² alkotmányellenességének megállapítását kérte, mivel azok szerint nem feleltek meg az alapvető jogok és kötelességek szabályozására vonatkozó alkotmányos kötelezettségeknek, továbbá a jogalkotásról szóló törvénnyel⁹³ sem találta összeegyeztethetőnek.

A vizsgálat alá vont törvényerejű rendelet egy olyan állami népességnylvántartási rendszer működését szabályozta a hozzá kapcsolódó végrehajtási rendeletekkel együtt, mely egy integrált személyi adatbankként tartalmazta volna a teljes népesség adatait a lehető legszélesebb körben, az egészségügyi adatoktól kezdve a vagyoni adatokon át a hivatali ügyekig.

Az Alkotmánybíróság - a 20/1990. (X. 4.) AB határozat⁹⁴ szerinti gyakorlatát folytatva - a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezte, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként:

„Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról.”

Indoklásában kiemelte az Alkotmánybíróság, hogy kivételesen törvény korlátozhatja az érintett információs önrendelkezési jogát, ha megfelel a garanciális feltételeknek⁹⁵, mely által az

⁹⁰ BVerfG 65, 1, („Volkszählungsurteil”)

⁹¹ 15/1991. (IV. 13.) AB határozat

⁹² A Minisztertanács 25/1986. (VII. 8.) és 102/1990. (VII. 3.) MT számú rendelete

⁹³ 1987. évi XI. törvény a jogalkotásról

⁹⁴ 20/1990. (X. 4.) AB határozat a közpénzzel rendelkezők vagyonnyilatkozat tételének kötelezettségére vonatkozó közérdek és az egyén magánszférája közötti összhang mérlegelésével kapcsolatosan húzza meg a határt.

⁹⁵ 1949. évi XX. törvény, 8. § (2) A Magyar Köztársaságban az alapvető jogokra és kötelességekre vonatkozó szabályokat törvény állapítja meg, alapvető jog lényeges tartalmát azonban nem korlátozhatja.

érintett képes követni a személyes adatainak útját azok feldolgozása során a megfelelő tájékoztatásnak köszönhetően, továbbá a jogait is érvényesíteni tudja.

Az indoklás rámutatott, hogy az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája a célhoz kötöttség, mely célnak konkrétan és előre meghatározottnak kell lennie.

A megtámadott törvényerejű rendelet viszont olyan homályosan és nyitottan fogalmazta meg az adatkezelés célját, hogy abba bármilyen adatkezelési művelet belefért volna akármilyen személyes adattal, melynek következtében semmilyen korlátot és információt nem biztosított a műveletekre⁹⁶, így a „semmitmondó” szöveg alkalmatlan arra, hogy az adatfeldolgozásnak bármiféle irányt vagy határt szabjon, azaz hogy célhoz kötöttségről egyáltalán beszélni lehessen”.

Aggályos volt a nyilvántartható adatok körének meghatározása is, mely szintén nyitottan volt megfogalmazva úgy, hogy a Minisztertanács egyoldalú döntésével bármikor bővíthette volna tetszőlegesen.⁹⁷

A rendelkezés nem csupán az Alkotmány alapvető jogokkal és kötelezettségekkel kapcsolatos rendelkezéseibe ütközött, hanem a jogalkotási törvénnyel is, mely a törvényhozási tárgyak között sorolta fel a személyi nyilvántartást.⁹⁸

A tvr. teljességéből hiányzott a cél folytonossága vagy a cél megváltoztatásának legitimitása is. A tvr. avval próbálta a hiányzó biztosítékokat pótolni, hogy a nyilvántartó rendszerből csak azokat az adatokat engedte volna továbbítani volna az egyes hivataloknak, melyek a feladatkörük (céljuk) ellátásához szükségesek (pl.: egészségbiztosításnak csak az egészségügyi adatokat). *A „második adatkezelés” szabályossá tétele az Alkotmánybíróság szerint sem orvosolhatja az teljes folyamatot, mivel „a célhoz kötöttségből következik, hogy a meghatározott cél nélküli, készletre, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés- és tárolás alkotmányellenes”, és „ez teljesen kiszolgáltatja az adatalanyokat, átvilágíthatóvá teszi magánszférájukat is, továbbá egyenlőtlen kommunikációs helyzetet eredményez, amelyben az érintett nincsen tisztában avval, hogy az adatfeldolgozó mit tudhat róla.*

⁹⁶ A tvr.-ben írt célmeghatározás (1. § (1) bekezdés: „az állampolgár jogai érvényesítésének és kötelezettségei teljesítésének előmozdítása, az állami szervek, a gazdálkodó és társadalmi szervezetek, egyesületek, valamint magánszemélyek társulásai (a továbbiakban együtt: szervezetek) munkájának segítése”)

⁹⁷ 1986. évi X. számú törvényerejű rendelet, 4. § Az állami népességnylvántartás az állampolgár személyi számát, alapvető személyazonosító és lakcím adatait tartalmazza. A nyilvántartott adatok körét a Minisztertanács határozza meg.

⁹⁸ 1987. évi XI. törvény a jogalkotásról, 5. § Az állampolgárok alapvető jogai és kötelezségei körében törvényben kell szabályozni különösen
1) a személyi nyilvántartást.

Nem konstruálható meg tehát alkotmányosan olyan megoldás, hogy egy meghatározott cél nélküli, központi integrált adatbankra nézve az adatvédelemhez való alkotmányos jog egyik konstitutív elemét, a célhoz kötöttséget csakis a lekérdezőkre tartsa érvényesnek. Az ún. törvényes adatminőségnek ugyanis a feldolgozás minden szakaszában fenn kell állnia. Nem elégséges ugyanis, ha a garanciák csak egyes feldolgozási szakaszokban érvényesülnek, az nem orvosolja más fázisok alkotmányellenességét, így nem kielégítő a tvr. előírása⁹⁹, amely szerint az adatkérő a népességnyilvántartásból kapott adatot csak az adatkérés indokaként megjelölt célra használhatja.

A támadott tvr. alkotmányellenes, mert „nem határozza meg az adatfeldolgozás célját, ezzel összefüggésben nem határozza meg pontosan a feldolgozott adatok körét, lehetővé teszi a népességnyilvántartás szolgáltatásaihoz más, meg nem határozott nyilvántartások igénybe vételét, továbbá az érintett jogait nem biztosítja a megkívánt mértékben, különösen nem tartalmaz kielégítő garanciákat az érintett védelmére az adattovábbítás feltételeit illetően.”

Az Alkotmánybíróság kiemelte továbbá, hogy az ilyen adatfeldolgozás az emberi méltóságot is sérti, mivel az adatokból összeálló ún. „személyiségprofil” - melynek elkerülése az egyes adatfeldolgozások jogszerűségének megítélésénél alapvető szempont – a széles, de határozatlan gyűjtőkörű adatfeldolgozások velejárója.

A hasonlóan integrált, központosított állami nyilvántartások terveit el kellett ejteni a társadalmi ellenállás miatt a hatvanas évek közepén az Egyesült Államokban, a hetvenes években pedig Franciaországban és a Német Szövetségi Köztársaságban is. A központi adatbankok által felszínre hozott problémák gerjesztői lettek az adatvédelmi törvényhozásnak.

Az Alkotmánybíróság határozatának fontos üzenete, hogy az *„államigazgatás hatékonysága” nem lehet olyan érdek, mely az információs önrendelkezési jog sérelmével járó adatfeldolgozást igazolná.*¹⁰⁰

⁹⁹ 25/1986. (VII. 8.) MT. rendelet 5. §(2)

¹⁰⁰ Az Alkotmánybíróság határozatában tett megállapításai és elvárásai a tisztességes és törvényes adatkezeléssel kapcsolatban visszaköszönnek a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvényben:

1. § (3) E törvény biztosítja a természetes személy (a továbbiakban: polgár) személyes adataival való önrendelkezési jogának, valamint az egyéb alkotmányos jogok érvényesítéséhez és a közigazgatás hatékonyságának biztosításához szükséges személyazonosító, lakcím és értesítési cím adatok használatához fűződő közérdek összhangját.

(4) E törvény a nyilvántartás törvényességét annak célhoz kötöttségével, az adatkezelés feltételeinek és a személyes adatok körének pontos meghatározásával, az adatkezelési jogosultságoknak a nyilvántartás szervei közötti megosztásával, továbbá az adatkezelés időbeni korlátozásával biztosítja.

(5) E törvény garanciális szabályokat állapít meg a nyilvántartásban kezelt adatok védelmére, valamint előírja az adatkezelés és a szolgáltatás ellenőrzésének kötelezettségét.

(6) A személyazonosító jel csak az e törvényben meghatározott korlátozott körben és szabályozott feltételek mellett, valamint az ebben megállapított határidőig használható.

A **magyar adatvédelmi törvény** tervezetének első változatát a Központi Statisztikai Hivatal megbízásából Sólyom László készítette el 1988-ban. A magyar kormány a 3022/1989. számú határozatával 1989 januárjában jóváhagyta a személyes adatok kezeléséről és a közérdekű adatok nyilvánosságáról szóló törvény szabályozásának alapjait, és felkérte az igazságügyi minisztert, hogy a törvény tervezetét 1990. december 31-ig az Országgyűlés elé terjessze be.

Az egyeztetések és a szakmai viták következtében adatvédelmi törvény nem került betervezésre a megadott határidőig, arra még két évet várnia kellett a magyar törvényhozásnak. 1992. október 17-én került végül kihirdetésre az első magyar adatvédelmi törvény¹⁰¹, melynek rendelkezései máig hatással vannak a magyar adatvédelmi szabályozás rendszerére.

Ha összehasonlítjuk a hatályos információs önrendelkezési jogról és az információszabadságról szóló törvény szövegével¹⁰², a hasonlóság szembeötlő. A törvény elfogadásakor európai mércével is jelentős volt: 1992-ben még az adatvédelmi irányelv is csak a szövegezés szakaszában volt, mely 1995-ben került elfogadásra, 3 évet adva a transzformációra. Az Európa Tanács 1981-es Egyezményén túl tehát nem létezett olyan európai mérce, mely a jogalkotó számára alapul szolgálhatott volna.

Az adatvédelem és a közérdekű adatok nyilvánosságának egy törvényben való magas szintű szabályozása mindenféle külső nyomás nélkül történt meg, a magyar jogalkotói akarat jelentős sikerét felmutatva.

A törvény az adatkezelés olyan alapelveit tartalmazta, mint az érintett tájékoztatásának kötelezettsége, a célhoz kötöttség elve, szükségesség elve, az adatminimalizálás elve, a törvényes és tisztességes adatkezelés elve, a kezelt adatok minőségének és az adatbiztonság elve.

A jogszabály negyedik fejezete tartalmazta az adatvédelmi biztos és az adatvédelmi nyilvántartás intézményét. Magyarország első adatvédelmi biztosát 1993. október 1-ig kellett volna megválasztani az állampolgári jogok országgyűlési biztosáról szóló törvény¹⁰³ alapján, végül 1995. június 30-án választotta meg az Országgyűlés¹⁰⁴ Magyarország első adatvédelmi ombudsmanját Majtényi László személyében.

¹⁰¹ 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

¹⁰² 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

¹⁰³ 1993. évi LIX. törvény az állampolgári jogok országgyűlési biztosáról

¹⁰⁴ 84/1995. (VII. 6.) OGY határozattal

Az adatvédelmi törvény első jelentős módosításait 1995-ben az államtitokról és a szolgálati titokról szóló törvény¹⁰⁵ és a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló törvény¹⁰⁶ iktatta be.

A Titoktörvény avval egészítette ki a biztos jogosítványait, hogy kezdeményezhette az államtitokkörben, valamint a szolgálati titokkörben meghatározott adatfajták szűkítését vagy bővítését, továbbá, ha az adatvédelmi biztos eljárása során az adat minősítését indokolatlannak tartotta, a minősítőt annak megváltoztatására vagy a minősítés megszüntetésére szólíthatta fel.¹⁰⁷

1995-ben került elfogadásra hosszas előkészítő munka után az **Európai Parlament és a Tanács 95/46/EK irányelve** (adatvédelmi irányelv), mely a személyes adatok védelmét és szabad áramlását tűzte ki célul az Európai Unión belül. Az irányelv szükségességét adta, hogy a tagállamokban jelentős különbségek voltak az adatvédelmi szabályozásokban, és a csatlakozást követően a tagállamok között felgyorsult az adatok áramlása, mely megkívánta a vonatkozó jogszabályok harmonizálását. Az irányelv magasra helyezte a védelem szintjét, több tagállam (különösen az Egyesült Királyság) erősen lobbizott az elfogadása ellen, mert számukra komoly módosításokat tett szükségessé a jogrendszerükben.¹⁰⁸

Az Európai Unióhoz való csatlakozáshoz szükséges jogharmonizációs feladatok körébe tartozott az adatvédelmet szabályozó törvény és a vonatkozó EU irányelv összhangjának a megteremtése. A törvényi szabályozás módosításának szükségességét a 2002-ben készült Országjelentés is hangsúlyozta, mint elvárt és teljesítendő feladatot. Fontos szempont volt, hogy az irányelv alapján az uniós tagállamokon belül egységes elvek mentén lehet csak személyes adatot kezelni, illetve továbbítani a tagállamok között és harmadik államokba.

A jogalkotásnak reagálnia kellett technika felgyorsult fejlődésére, illetve a nemzetközi szabályozás alakulására az adatvédelmi törvény felülvizsgálatával. A jogszabály. hatálybalépése óta ugyanis az informatika és az információtechnológia fejlődése lehetővé tette, hogy az adatkezeléssel kapcsolatos döntések meghozatala és azok technikai végrehajtása szervezeti és technikailag is elkülönüljön egymástól, mely magával vonta a felelősségi

¹⁰⁵ 1995. évi LXV. törvény az államtitokról és a szolgálati titokról

¹⁰⁶ 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

¹⁰⁷ Az adatvédelem története, Adatvédelmi biztos már megszűnt honlapjának legutolsó mentett változata, 2011. 12. 31.

¹⁰⁸ Az irányelv elfogadásának körülményeiről és történetéről a tanulmányom EU Bíróságának joggyakorlatával kapcsolatos fejezetében írok részletesen.

viszonyok átalakulását is. A technikai fejlődése és a nemzetközi kötelezettségek így szükségessé tették az adatfeldolgozó fogalmának és felelősségének önálló meghatározását¹⁰⁹.

Az Európai Unió Tanácsának 95/46/EK Irányelve egyértelmű fogalmi meghatározást adott az adatkezelő és az adatfeldolgozó elhatárolására, valamint külön rendelkezéseket fogalmazott meg az adatfeldolgozó felelősségével kapcsolatban.

Az fent meghatározott technikai és nemzetközi jogi kötelezettségek miatt született meg az adatvédelmi törvény novellája, melyet 2003. június 23-án fogadott el az Országgyűlés¹¹⁰. A törvény fogalomrendszerét is ki kellett egészíteni az Irányelv végrehajtásához szükséges mértékben (pl. hozzájárulás fogalma, bűnügyi személyes adat). Olyan előremutató kiegészítések kerültek a törvénybe, mint a személyes adat (beleértve a különleges adatokat is) feldolgozásának az érintett "létfontosságú érdekeinek" védelméhez szükségessége, vagy az adatalany fizikai vagy jogi cselekvőképességének hiánya miatt a hozzájárulás hiányában végzett adatkezelés. Lényeges változtatás volt továbbá, hogy az adatfeldolgozó érdemi döntést nem hozhat, saját célú adatfeldolgozást nem végezhet.

Szintén új elemként került bevezetésre a magyar adatvédelmi jogba az automatizált egyedi döntés és az érintettet megillető tiltakozási jog. A novella bevezette továbbá a belső adatvédelmi felelős intézményét, valamint az adatkezelők széles körénél kötelezővé tette az adatvédelmi és adatbiztonsági szabályzat alkalmazását.

A módosításnak köszönhetően honosodott meg az adatkezelések előzetes ellenőrzése, mely alapján a kockázatosabb adatkezeléseket a polgárok jogainak védelme érdekében már megkezdésük előtt megvizsgálhatta az adatvédelmi biztos. A novella egyik legjelentősebb változásaként egészült ki az adatvédelmi biztos hatásköre hatósági jellegű jogosítványokkal, így az adatvédelmi biztosnak lehetősége nyílt arra, hogy elrendelje a jogellenes adatkezelések zárolását, törlését vagy megsemmisítését, megtiltsa a jogosulatlan adatkezeléseket és feldolgozásokat, továbbá felfüggeszthette az adatok külföldre továbbítását.

Az Európai Unió Alapjogi Chartája tartalmazza azokat az alapvető jogokat, melyeket az Európai Uniónak és a tagállamoknak az uniós jogszabályok végrehajtása során tiszteletben kell tartaniuk. Kidolgozói a nemzeti kormányok, az Európai Bizottság egy-egy tagja és az Európai Parlament tagjai voltak.

¹⁰⁹ 1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról, I. Fejezet, 1. § (1) b)

¹¹⁰ A 2003. évi XLVIII. törvénnyel kerültek be a törvénybe annak a személyi, tárgyi és területi hatályát meghatározó rendelkezések

A Charta jogilag kötelező erejű dokumentum, amelyet azért hoztak létre, hogy elismerjék és hangsúlyozzák az alapvető jogoknak az Unió jogrendjében betöltött szerepét. Hét fejezetben, 54 cikkelyen keresztül határozza meg az Európai Unió alapvető értékeit, melyet 2000-ben, Nizzában hirdettet ki ünnepélyesen a Parlament, a Tanács és a Bizottság.¹¹¹

Az ünnepélyes kihirdetés azonban nem tette jogilag kötelező erejűvé a Chartát, mellyel a 2004-ben aláírt európai alkotmánytervezet elfogadása ruházta volna fel. A ratifikációs folyamat bukása miatt a Charta a Lisszaboni Szerződés elfogadásáig csupán az alapvető jogokról szóló nyilatkozat maradt.¹¹²

A Charta 2009. december 1-én vált jogilag kötelező erejűvé¹¹³, így az EU elsődleges joganyagának részévé vált, mely által a másodlagos uniós joganyag és a nemzeti intézkedések megfelelési vizsgálatának egyik szempontjává vált.

A benne foglalt polgári, politikai, gazdasági és szociális jogokat az Európai Unió Alapjogi Ügynöksége védelmezi, mely 2007. március 1-től működik Bécsben.¹¹⁴

A Chartában külön cikk foglalkozik a személyes adatok védelmével, mely az EU elkötelezettségét mutatja a magánszféra és a személyes adatok védelmével kapcsolatosan.¹¹⁵

8. cikk, A személyes adatok védelme

(1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

(2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.

(3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie.

Az információs önrendelkezési jogról és az információszabadságról szóló törvény¹¹⁶ az 1992-es adatvédelmi törvény helyét vette át, annak jelentős részét és magas védelmi szintjét

¹¹¹ Módosításokat követően 2007-ben újra kihirdették.

¹¹² Az Európai Parlament weblapja, <http://www.europarl.europa.eu/aboutparliament/hu/0003fbc4e5/Az-Eur%C3%B3pai-Uni%C3%B3-Alapjogi-Chart%C3%A1ja.html>

¹¹³ Az Európai Unióról szóló szerződés 6. cikkének (1) bekezdése kijelenti, hogy „az Unió elismeri az Európai Unió Alapjogi Chartájának [...] szövegében foglalt jogokat, szabadságokat és elveket; e Charta ugyanolyan jogi kötőerővel bír, mint a Szerződések”.

¹¹⁴ A korábbi, Rasszizmus és Idegengyűlölet Európai Megfigyelőközpont nevű intézmény feladatait veszi át, de tevékenységét más területekre is kiterjeszti.

¹¹⁵ hivatalos magyar nyelvű fordítás:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:hu:PDF>

¹¹⁶ 2011. évi CXII. törvény

megtartva, az EU Irányelv által megkövetelt szükséges módosítások beemelésével a hazai jogrendszerbe.

A „régí” törvénynek az alapfogalmakra, alapelvekre és az adatnyilvántartásra vonatkozó szabályai csak kisebb változáson estek át. Az Irányelvvel összhangban az adatkezelés jogalapjai változtak meg a „klasszikus” hozzájárulás vagy törvény párost megújítva, továbbá az úgynevezett harmadik pilléres kerethatározat, a bünygyi együttműködésre vonatkozó uniós szabályok is bekerültek az új jogszabályba. Az Infotv. legnagyobb változtatása az intézményi oldalon, hogy megszüntette az ombudsmani rendszert¹¹⁷, létrehozva a Nemzeti Adatvédelmi és Információszabadság Hatóságot¹¹⁸

A törvény hatályát tekintve lényegi változás nem történt a korábbi szabályozáshoz képest.

Az „új” Polgári Törvénykönyv¹¹⁹ a „személyiségi jogok” elnevezést használja a magánszféra védelmét biztosítani hivatott jogok megjelölésére a „személyhez fűződő jogok” helyett.

A Ptk. a generálklauzula mellett külön rendelkezéseket tartalmaz a jogalkalmazói gyakorlatban már kikristályosodott személyiségi jogok védelméről, melyek többsége –segítséget nyújtva a bírói jogalkalmazásnak - besorolható a nevesített esetek valamelyikébe.

A Ptk. új szabályként mondja ki a személyiségi jogok körében a magánélet (magánszféra) védelmét.

2:42. § [A személyiségi jogok általános védelme]

(1) Mindenkinek joga van ahhoz, hogy törvény és mások jogainak korlátai között személyiségét szabadon érvényesíthesse, és hogy abban őt senki ne gátolja.

(2) Az emberi méltóságot és az abból fakadó személyiségi jogokat mindenki köteles tiszteletben tartani. A személyiségi jogok e törvény védelme alatt állnak.

(3) Nem sért személyiségi jogot az a magatartás, amelyhez az érintett hozzájárult.

2:43. § [Nevesített személyiségi jogok]

A személyiségi jogok sérelmét jelenti különösen

e) a magántitokhoz és a személyes adatok védelméhez való jog megsértése;

g) a képmáshoz és a hangfelvételhez való jog megsértése.

2:46. § [A magántitokhoz való jog]

¹¹⁷ Az 1992. évi LXIII. törvény szerint a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való alkotmányos jog védelme érdekében az Országgyűlés adatvédelmi biztost választott azok közül az egyetemi végzettségű, büntetlen előéletű, kiemelkedő tudású elméleti vagy legalább 10 évi szakmai gyakorlattal rendelkező magyar állampolgárok közül, akik az adatvédelmet érintő eljárások lefolytatásában, felügyeletében vagy tudományos elméletében jelentős tapasztalatokkal rendelkeznek és köztisztvisletnek örvendenek. Az adatvédelmi biztosok: Majtényi László (1995–2001), Péterfalvi Attila (2001–2007), Jóri András (2008–2011)

¹¹⁸ A hivatal elnökét a miniszterelnök javaslatára a köztársasági elnök nevezi ki. 2012-től Péterfalvi Attila korábbi adatvédelmi biztos tölti be ezt a tisztséget.

¹¹⁹ 2013. évi V. törvény a Polgári Törvénykönyvről

(1) A magántitok védelme kiterjed különösen a levéltitok, a hivatásbeli titok és az üzleti titok oltalmára.

(2) A magántitok megsértését jelenti különösen a magántitok jogosulatlan megszerzése és felhasználása, nyilvánosságra hozatala vagy illetéktelen személlyel való közlése.

A „új” Ptk. megszüntette a – elméleti viták és jogalkalmazási nehézségek által terhelt - nem vagyoni kártérítés intézményét és helyette bevezette a sérelemdíjat, mint a személyhez fűződő jogok megsértésének közvetett kompenzációját, illetve annak pénzbeli elégtételt jelentő magánjogi büntetését.¹²⁰

A nem vagyoni kártérítés problémája onnan ered, hogy a magánjogban a kár pénzben kifejezhető és rendszerint összegszerűen kimutatható vagyoni hátrányt jelent, míg a nem vagyoni sérelem viszont vagyoniilag nem kifejezhető, ugyanakkor ellensúlyozása pénzben történik.

A Ptk. az elellentmondás kiküszöbölése céljából a személyiségi jogsértések nem vagyoni következményeinek pénzbeli elégtétellel szankcionálását jórészt a kártérítés szabályaitól elválasztva oldja meg, biztosítva a személyiségi jogok megsértése esetén az okozott sérelem pénzbeli kompenzációját a személyiségi jogok sajátosságaihoz igazítva.

A Ptk. a „sérelemdíj intézményének bevezetésével betetőzi a közel fél évszázados fejlődési folyamatot, amelynek során a személyiségi jogok magánjogi sérelme fokozatosan kivált a tulajdonost megillető dologi jogi oltalom burkából”.

A sérelemdíj kettős funkcióval rendelkezik: a személyiségi jogsérelem esetén a kompenzáálás eszköze, továbbá „magánjogi büntetésnek” is tekinthető a jogsértések megelőzése céljából.¹²¹

A kompenzációra és elégtételre való törekvés a jogvédelemre szoruló sértettnek, míg a büntetés a jogsértőnek szól (visszatartási cél). E kettős funkció szélesebb körben ad lehetőséget a sérelemdíj összegének meghatározása során a különböző körülmények mérlegelésére.

A sérelemdíj egyszeri reparációját jelenti a nem vagyoni sérelemnek, melyet a korábbi bírói gyakorlat is kialakított a járadék és az egyösszegű nem vagyoni kártérítés kizárásával.¹²²

A leglényegesebb változás az új szabályozásban, hogy a sérelemdíj megfizetésének nem feltétele, hogy a sértett az őt ért hátrányt bizonyítsa¹²³, tehát a jogsértés ténye önmagában

¹²¹ BDT2002. 692.: a nem vagyoni kártérítésben a büntetési jelleg is benne szerepelhet, amennyiben a károsult sérelmére a károkozó bűncselekményt követett el, akkor is, ha az a bűncselekmény az előkészületi stádiumban megrekedt.

¹²² BH2011. 248.: a nem vagyoni kártérítés egy összegben és járadék formában egyszerre nem alkalmazható.

¹²³ Az Alkotmánybíróság 34/1992 (VI. 1.) határozatában fejtette ki véleményét a joghátrány megkövetelésével kapcsolatosan: „Felelősségi szabályként nem alkotmányellenes tehát az a konstrukció, amely - a jogintézmény

sérelemdíjjal szankcionálható¹²⁴ (a szabályozás ugyanakkor nem zárja ki, hogy a sértettet ért hátrány és annak mértéke figyelembe legyen véve a sérelemdíj összegének megállapításánál).¹²⁵

A jogsértés ténye önmagában, bizonyított hátrány nélkül is azzal a jogkövetkezménnyel jár, hogy a személyiségi jogában megsértett személy sérelemdíjat követelhet. Az új Ptk. szerint tehát az eszmei hátrány bizonyítása nem szükséges.

A személyiségi jogok megsértése esetén alkalmazandó jogkövetkezmények más pontokon is eltérnek a korábbi szabályozástól. Megszűnt a közérdekű bírság intézménye, mely nehezen volt összeegyeztethető a magánjog rendszerével a korábbi törvénykönyvben és a bírói gyakorlat is ritkán élt vele.

Az új Ptk. indokolásából kitűnik, hogy a vagyoni elégtétel tágabb kategória, mint a kompenzáció, hiszen magában foglalja a sérelemmel okozott hátrány kiküszöbölése mellett a sérelmet szenvedett félben a jogsértő magatartás miatt keletkezett szubjektív hiányérzet, veszteségérzés megszüntetését, de legalábbis csökkentését. Az elégtétel magában foglalja a jogsértés társadalmi elítélését és az okozott sérelem kompenzálásához fűződő igény elismerését is; célja, hogy a személyiségi jogsérelmet szenvedett személynél a megbomlott testi és lelki egyensúly helyreálljon. A sérelemdíj összegének meghatározásánál e szempontokra is figyelemmel kell lenni.¹²⁶

Az új szabályozás az objektív szankciók körében biztosít lehetőséget a sértett számára a jogsértőnél a jogsértéssel előállt vagyoni előny megszerzésére a jogalap nélküli gazdagodás szabályai szerint, mivel a személyiségi jogok megsértése vagyoni előnyhöz is juttathatja a jogsértőt. Adatvédelmi szempontból jogalapot adhat ilyen követelésre, ha az adatkezelő jogosulatlanul szerzi meg és kezeli az érintett személyes adatait, melyet értékesít, vagy reklámbevétel szerzésére használ fel. Példaként említhető, amikor egy újság engedély nélkül készített fényképpel és a magánszféra megsértésével szerzett információkkal növeli a lap eladási számát.

szerkezeti ellentmondásaira is figyelemmel - a károsultnál jelentkező következményeket írja elő a nem vagyoni kártérítés feltételül.”

¹²⁴ A korábbi gyakorlat több esetben evvel ellentétesen foglalt állást, megkövetelve a hátrány bizonyítását. Lásd: BH1996. 304.

¹²⁵ A változás miatt a bíróságoknak új megoldásokat kell találniuk a bagatell-ügyek kiszűréséhez.

¹²⁶ A Fővárosi Ítélőtábla Polgári Kollégiuma 1/2013. (VI. 17.) számú határozatával elfogadott kollégiumi véleménye a nem vagyoni kártérítés/sérelemdíj megtérítése iránti követelések elbírálásának a polgári perben felmerülő egyes kérdéseiről.

Igényérvényesítés a hatályos jogszabályok alapján

Az Infotv. alapján az érintett számára a jogérvényesítés több szempontból is kedvezőbb, mint a személyhez fűződő jogainak megsértése miatt kezdeményezett peres eljárásban.

Infotv. ¹²⁷ alapján indított per	Ptk. alapján indított per
<i>eljárás időtartama</i>	
A bíróság soron kívül jár el,	rendes eljárás, jóval hosszabb
<i>bizonyítási teher</i>	
az adatkezelőn	az érintetten (amennyiben ő indította a pert)
<i>eljáró bíróság</i>	
érintett lakóhelye szerinti illetékes bíróság	az alperes (adatkezelő) lakóhelye, székhelye szerinti illetékes bíróság

Kártérítés

Infotv.	Ptk.
<i>felelősség</i>	
objektív az adatkezelő mindig felel, kivéve, ha a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.	vétkességi csak akkor felel az adatkezelő, ha a károkozó magatartása felróható
<i>kártérítés</i>	

¹²⁷ 2011. évi CXII. törvény 22. § (1) Az érintett a jogainak megsértése esetén, valamint a 21. §-ban meghatározott esetekben az adatátvevő az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el.
(2) Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani. A 21. § (5) és (6) bekezdése szerinti esetben a részére történő adattovábbítás jogszerűségét az adatátvevő köteles bizonyítani.
(3) A per elbírálása a törvényszék hatáskörébe tartozik. A per - az érintett választása szerint - az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindítható.
(4) A perben fél lehet az is, akinek egyébként nincs perbeli jogképessége. A perbe a Hatóság az érintett pernyertessége érdekében beavatkozhat.

kártérítés és sérelemdíj	kártérítés és sérelemdíj ¹²⁸
--------------------------	---

Következtetések

A „privacy” szó jelentése a történelem során gyökeresen megváltozott és országonként eltérően fejlődött. Az ókori Európában az egyén politikai jogaitól kezdődően az Egyesült Államokban megvalósuló „én házam az én váram” megközelítésig folyamatosan formálódott.

A privacy fogalmának kibontása és védelme főként az Egyesült Államok jogfejlődéséhez és jogtudásaihoz köthető, azonban napjainkra az USA-ban használt privacy kiüresedett, mivel az amerikai kormány nem tiszteli azt megfelelően, amelyre legszemléletesebb példa az NSA adatgyűjtése, amely ellen az állampolgárok részéről nem volt tapasztalható jelentős ellenállás. Az amerikai vállalatok az ügyfelek személyes adatait jóval kevesebb korlát között kezelhetik, mint az európai vetélytársaik, amelynek ellenére nincsen jelentősebb retorzió az ügyfelek részéről.

Az információs önrendelkezési jog és az adatvédelem gyakorlati érvényesülésén, továbbá történeti fejlődésén keresztül cáfoltam, hogy teljes mértékig fednék egymást.

Az önrendelkezési jog alapján megilleti az egyént az a jog, hogy döntsön a rá vonatkozó információk nyilvánosságra hozataláról, míg az adatvédelmi jog elsősorban az adatkezelőnek állít korlátokat az adatok kezelésével kapcsolatosan.

Az egyént egyre kevésbé illeti meg a választás lehetősége a tekintetben, hogy részt vesz-e a digitális életben (pl. munkahelyi és baráti csoportok a Facebookon, dokumentumok közös használata a Google rendszerén munka- és osztálytársakkal, ETR, Neptun stb.), amely az információs önrendelkezési jog sorvadásához vezetett. A munka, tanulás és magánélet során komoly hátrányokkal jár, ha az egyén nem vesz részt az említett kommunikációs csatornák használatában. Az információs önrendelkezési jog gyengülésével párhuzamosan így az

¹²⁸ 2013. évi V. törvény 2:52. § [Sérelemdíj]

(1) Akit személyiségi jogában megsértenek, sérelemdíjat követelhet az őt ért nem vagyoni sérelemért.

(2) A sérelemdíj fizetésére kötelezés feltételeire - különösen a sérelemdíjra köteles személy meghatározására és a kimentés módjára - a kártérítési felelősség szabályait kell alkalmazni, azzal, hogy a sérelemdíjra való jogosultsághoz a jogsértés tényén kívül további hátrány bekövetkeztének bizonyítása nem szükséges.

(3) A sérelemdíj mértékét a bíróság az eset körülményeire - különösen a jogsértés súlyára, ismétlődő jellegére, a felróhatóság mértékére, a jogsértésnek a sértettre és környezetére gyakorolt hatására - tekintettel, egy összegben határozza meg.

2:53. § [Kártérítési felelősség]

Aki személyiségi jogainak megsértéséből eredően kárt szenved, a jogellenesen okozott károkért való felelősség szabályai szerint követelheti a jogsértőtől kárának megtérítését.

adatvédelmi jog erősödésére és „elkőzjogiasodására” mutatható ki, mivel az egyén védelemre szorul az egyre nagyobb és monopolhelyzetben lévő adatkezelőkkel szemben. A megfelelő védelmhez szükséges, hogy az „érintett-kőzpontú” szabályozás elmozduljon az „adatkezelő-kőzpontú” szabályozás felé¹²⁹.

¹²⁹ Szőke Gergely László: Az európai adatvédelmi jog megújítása, tendenciák és lehetőségek az őnsabályozás területén, doktori értekezés, Pécs, 2014. 164.

3. A személyes adatok védelméhez való jog ütközése alapvető jogokkal az Európai Unió Bíróságának joggyakorlatában

Az Európai Unió adatvédelmi irányelve jelenti az EU adatvédelmi szabályozásának keretét és egyben alapjait, mely az első ilyen szinten elfogadott jogszabály volt adatvédelem tárgyában.

Az Európai Parlament háromszor kérte fel a Bizottságot (1976-ban, 1979-ben és 1982-ben), hogy alkosson irányelvet a tagországok adatvédelmi szabályozásának harmonizálására.

1990-ig kellett várni, hogy a Bizottság az első tervezetét bemutassa, melynek alapjait az akkor hatályos német és francia szabályozások alkották, melyben jelentős szerepe volt, hogy a tervezetet előkészítő bizottság elnöki tisztségét Spiros Simitis töltötte be, aki egyben Németország Hessen tartományának adatvédelmi biztosa is volt.

Az elfogadásig eltelt 5 év alatt komoly viták folytak mind az EU szervei és tagállamai, mind a tudományos és gazdasági élet szereplői között, melynek központjában az alapjogok és az EU négy szabadágának (személyek, áruk, szolgáltatások és a tőke szabad áramlása) konfliktusa állt.

Az EU Parlament az alapvető jogok védelmét képviselte elsősorban, míg az EU Tanácsa és a Bizottság az adatok szabad áramlását tekintette elsődlegesnek a gazdasági szempontok miatt.

A Bizottság 1992 októberében egy módosított tervezettel állt elő az érdekek közelítése céljából: bár az álláspontok közeledtek, továbbra sem volt egyetértés a tagállamok között a védelem mértékéről. Az Egyesült Királyság ellenezte legjobban a tervezet elfogadását, mivel az adatvédelmi szabályozás szintje náluk jelentős mértékben elmaradt a többi európai országtól, így az rájuk róta a legtöbb kötelezettséget.

A hosszas előkészítő munka után végül 1995 októberében elfogadásra került az adatvédelmi irányelv, melynek transzformálására 3 évet kaptak a tagállamok.

Az irányelv kettős, látszólag egymásnak ellentmondó célt hivatott megvalósítani: a személyes adatok szabad áramlását az Európai Unión belül, továbbá a magánszféra és a személyes adatok védelmét.¹³⁰

Az irányelv céljai közötti prioritás eldöntésénél segítségünkre lehet az irányelv jogalapja¹³¹:

¹³⁰ Az Európai Parlament és a Tanács 95/46/EK irányelve, 1 cikk, Az irányelv célja

(1) A tagállamok ezen irányelvnek megfelelően védik a természetes személyek alapvető jogait és szabadságait, különösen a magánélet tiszteletben tartásához való jogukat a személyes adatok feldolgozása tekintetében.

(2) A tagállamok nem korlátozhatják és nem tilthatják a személyes adatok tagállamok közötti szabad áramlását az (1) bekezdés értelmében biztosított védelemmel kapcsolatos indokok miatt.

¹³¹ Az Európai Unió Működéséről szóló szerződés 114. cikke

(1) Ha a Szerződések másként nem rendelkeznek, a 26. cikkben meghatározott célkitűzések megvalósítására a következő rendelkezéseket kell alkalmazni. Az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében és a Gazdasági és Szociális Bizottsággal folytatott konzultációt követően elfogadja azokat a tagállamok törvényi, rendeleti és közigazgatási rendelkezéseinek közelítésére vonatkozó intézkedéseket, amelyek tárgya a belső piac megteremtése és működése.

A két cél közötti határvonal meghúzása a nemzeti jogalkotásoknak is komoly feladat volt, ám a jogalkalmazásnak a mai napig is kihívást jelent a prioritás meghatározása.

A jogalapot tekintve kijelenthetjük, hogy az Irányelv megalkotásakor a belső piac megteremtése és az alapvető szabadságok biztosítása játszhatták a főszerepet, ám ha a megalkotás körülményeit vizsgáljuk (a normát szövegezők jogvédő gyakorlata, a Parlament szándéka), már nem ennyire egyértelmű a helyzet.

A személyes adatok áramlása több okból is szükséges az indoklások szerint: az EU elsődleges jogforrásai által meghatározott alapvető szabadságok között, a belső piac határainak megszüntetése miatt és az intézmények együttműködésének feltételeként, továbbá az információáramlás tudományos célokból is elengedhetetlen.

Az adatok szabad áramlásának engedélyezése célonként nehezen megvalósítható lett volna, ezért került a választás az irányelvre, mely fokozatosan, a nemzeti jogalkotások közelítésével tette lehetővé a korlátok megszüntetését.¹³²

3.1 Az EU Bíróságának viszonya az alapvető szabadságokhoz és az alapjogokhoz

Az Európai Unió elsődleges jogforrásaiban kitűzött egyik legfontosabb cél, a közös piac létrehozása - finomhangolásoktól eltekintve - megvalósult, mely az EU Bíróságának feladatkörére is hatással volt: egyre kevésbé fajsúlyos az alapvető szabadságok hangsúlyozása,

¹³² Orla Lynskey: From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection 's identity Crisis, in: European Data Protection: Coming of Age, Springer Science+Business Media Dordrecht, Brussels, 2013, 75.

míg az alapjogok védelme előtérbe került, melyek között egyre nagyobb jelentőséggel bírnak az információs társadalommal kapcsolatos jogok.¹³³

Az alapjogok védelmével új kihívások és feladatok is hárultak az EU Bíróságára. Legfontosabb az Európai Unió Alapjogi Chartájának értelmezése, mely komoly nehézségekkel állítja szembe a testületet a különböző hagyományokkal és értékrendszerrel rendelkező tagállamok tekintetében, melynek során elengedhetetlen, hogy rendezze a viszonyát az Emberi Jogok Európai Bíróságával.¹³⁴

Az emberi jogok közösségi védelmének vonatkozásában az EU Bíróságára hárul a védelem határvonalának meghúzása a joggyakorlatban, a közösségi kompetenciák tekintetében.¹³⁵

3.1.1 Az adatvédelmi irányelv érvényesülése az EU Bíróságának joggyakorlatában

Az Európai Unió Bírósága több ügyben is döntött az irányelv alkalmazásáról, hatályáról, továbbá kifejtette véleményét joggyakorlata során a két különböző jogalapon és ellentétes elérendő céllal rendelkező jogszabályokkal kapcsolatban, mely szerint, ha a jogszabály jogalapjai és céljai között az egyik domináns, a másik csupán mellékes (járulékos), akkor a jogszabályt úgy kell tekinteni, mintha a domináns cél elérésére hozták volna létre.¹³⁶

Felmerül a kérdés, hogy ezek után az irányelv melyik célja tekinthető dominánsnak, elsődlegesen elérendőnek.

Figyelembe véve az irányelv jogalapját, megalkotóinak és elfogadóinak személyeit, nem jelenthető ki, hogy kizárólag az alapvető szabadságok lettek volna a középpontban.¹³⁷ A Bíróság véleménye szerint az adatvédelmi irányelv két, egymástól elválaszthatatlan céllal rendelkezik, melyek között nincsen domináns és járulékos, mely kivételes az EU Bíróságának joggyakorlatában.

¹³³ Sionaidh Douglas Scott: A tale of two courts: Luxemburg, Strasbourg and the growing European human rights acquis. *Common Market Law Review*, 2006/43, 661.

¹³⁴ Gyenei Laura: Újabb kihívások az uniós emberi jogi bíraskodás területén, *Iustum Aequum Salutare* II. 2006/3–4, 85–99.

¹³⁵ Takis Trimidas: The ECJ and the Draft Constitution: A Supreme Court for the Union? *Federal Trust Constitutional Online Paper* 05/04, <www.fedtrust.co.uk/uploads/constitution/05_04.pdf>

¹³⁶ C-491/01 *Queen v. Secretary of State for Health*, ex parte *British American Tobacco (Inv) Ltd & Imperial Tobacco Ltd*, 2002. 12. 10.

¹³⁷ Barbara Brandtner - Allan Rosas: Human Rights and the External Relations of the European Community: An Analysis of Doctrine and Practice, in: *European Journal of International Law*, 14 April 2014, 475. <http://ejil.oxfordjournals.org/>

Az "Österreichischer Rundfunk" ügyben előzetes döntéshozatali eljárás során kérelmezték, hogy a Bíróság döntsön azon kérdésben, hogy az adatvédelmi irányelvet lehet-e és kell-e alkalmazni az Ausztriai Számvevőszék tevékenységére, mely során munkavállalók fizetéséről kért adatközlést: a Számvevőszék felkérte a cégeket, hogy automatikusan jelentsék be számára, ha valamely munkavállalójuk elér egy meghatározott jövedelemszintet. A fizetési adatokat később a Számvevőszék publikálta volna, a munkavállalók egyéb személyes adataival együtt. A Bíróság elutasította az érvelést, mely szerint az irányelv kizárólag a "négy szabadság" esetén lenne hatályos és úgy rendelkezett, hogy az irányelv rendelkezéseit alkalmazni kell a Számvevőszék adatgyűjtésére, „mert a tagállamok között bármely személyes adat áramolhat, ám az Irányelv megköveteli az ilyen adatok védelmére vonatkozó szabályok betartását az adatok feldolgozása folyamán is, ahogyan azt az irányelv 3. cikke előírja”¹³⁸

Az Európai Parlament és a Tanács 95/46/EK irányelve

3. cikk , Hatály

(1) Ezen irányelvet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon való feldolgozására, valamint azoknak a személyes adatoknak a nem automatizált módon való feldolgozására, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

(2) Az irányelv nem alkalmazandó az alábbi személyesadat-feldolgozásokra:

- a közösségi jog hatályán kívül eső tevékenységek, mint például az Európai Unióról szóló szerződés V. és VI. címeiben megállapítottak, valamint a közbiztonsággal, a védelemmel, a nemzetbiztonsággal (beleértve az ország gazdasági jólétét is, ha a feldolgozási művelet nemzetbiztonsági ügyre vonatkozik), továbbá a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek,*
- a természetes személy által kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett adatfeldolgozás.*

Az irányelv hatályának kérdéséről és személyes adatok interneten való publikálásáról döntött a Bíróság a Lindqvist ügyben¹³⁹, melynek tényállása, hogy Lindqvist asszony egy egyházközségben dolgozott, melynek keretében honlapot hozott létre hívőtársaival kapcsolatosan, melyen több személyes adatot is közzétett. A Bíróságnak arról kellett döntenie,

¹³⁸ Joined Cases C-465/00, C-138/01 & C-139/01, Österreichischer Rundfunk, 2003. 05. 20.

¹³⁹ Case C-101/01 Bodil Lindqvist, 2003. 11. 06.

hogy az irányelv hatályos-e erre a tevékenységre, mivel semmilyen üzleti célja nem volt a hölgynek a honlappal kapcsolatosan, azt társadalmi, vallási célból készítette.

Az főtanácsnok (Advocate General) az EU Bíróságon az irányelv alkalmazása ellen érvelt, mivel szerinte az elsősorban az adatok szabad áramlására lett létrehozva, gazdasági tevékenységekkel kapcsolatban, nem pedig alapjogvédelem céljából. A Bíróság azonban másként vélekedett: „az alapvető jogok különösen fontosak, amint azt a tárgyalt eset is igazolta, melyben lényegében Lindqvist asszony munkájában az emberek úrvacsorára való előkészítése és a szabadságát képező, vallásos életet szolgáló tevékenysége során gyakorolt szólásszabadságát kellett egyensúlyba hozni azon egyének magánéletének védelmével, akiknek személyes adatait Lindqvist asszony feltöltötte saját internetes oldalára”, tehát a Bíróság amellet foglalt állást, hogy az irányelvet alkalmazni kell a személyes adatok interneten végzett feldolgozása tekintetében is.

Lidqvist asszony tevékenységi körére (mely nem volt kizárólag személyes célból és a háztartása körében végzett) így nem alkalmazható az irányelv 3. cikkének (2) bekezdése, mivel azt kiterjesztően értelmezni nem lehet, az irányelvben meghatározott kivételek taxatívak a Bíróság döntése alapján.

Az ügy felvetett egy jelentős kérdést: a személyes adatok honlapon való elhelyezése tekinthető-e az adatok harmadik országba való továbbításnak (mivel azt bárhol bárki elérheti a világon). A Bíróság döntése alapján az információ elhelyezése az Interneten “személyes adatok részben vagy egészben automatizált módon való feldolgozásának” minősül. Mindazonáltal a Bíróság úgy találta, hogy személyes adatok feltöltése egy internetes oldalra nem tekinthető a 95/46 irányelv 25. cikkében szabályozott harmadik országba irányuló továbbításnak.

Az irányelv hatályának értelmezésnél a személyes adatok védelméhez való jog más alapvető jogokkal is összeütközésbe kerül. A sajtószabadság rendszeresen problémát jelent az irányelv értelmezése során. Az EU Bírósága “Tietosuojavaluutettu v Satakunnan Markkinapörssi”¹⁴⁰ ügyben fejtette ki álláspontját a személyes adatok védelme és a sajtószabadság kapcsolatáról. Az ügy rövid tényállása, hogy a Finnországban az adóhatóság publikálta, hogy az egyes állampolgárok mennyi adót fizettek be az adott évben. A publikált adatokból egy magáncég (Satakunnan Markkinapörssi) összeállítást készített régiók és adózók alapján csoportosítva, melyet egy helyi lapban meg is jelentetett.

Az Európai Parlament és a Tanács 95/46/EK irányelve 9. cikk,

¹⁴⁰ Case C-73/07 Satakunnan Markkinapörssi and Satamedia, 2008. 12. 16.

A személyes adatok feldolgozása és a szólásszabadság

A tagállamok e fejezet, a IV. és a VI. fejezet rendelkezései alóli felmentésről, illetve eltérésről kizárólag a személyes adatoknak újságírás, vagy irodalmi, illetve művészi kifejezés céljából történő feldolgozása esetén rendelkezhetnek, amennyiben azok a magánélet tiszteletben tartásához való jognak a szólásszabadságra vonatkozó szabályokkal való összeegyeztetéséhez szükségesek.

A Bíróság kiemelte, hogy bár a sajtószabadság számos esetben kivételt képez az irányelv alkalmazása tekintetében, az általános kivételként való kezelése kikaput jelenthetne, mivel elég lenne minden esetben a személyes adatok tagállam általi publikálása a kibúváshoz a rendelet hatálya alól.

Az ítéletében az EU Bírósága úgy rendelkezett, hogy a cég publikációs tevékenysége személyes adatok feldolgozásának minősül, és az irányelv hatálya alá esik, még akkor is, ha előtte a személyes adatok már nyilvánosan publikálásra kerültek egy állami szerv által.

A két alapvető jog összhangba hozásához a tagállamoknak rendelkezniük kell a kivételekről és a korlátozásokról az adatvédelmi szabályozásuk tekintetében, hogy a sajtószabadság is érvényre juthasson.

3.1.2 A közérdekű adatok nyilvánosságának és a személyes adatok védelméhez való jognak az ütközése az EU Bíróságának joggyakorlatában

Bavarian Lager v. Commission¹⁴¹ ügyben az EU Bíróságára hárult a feladat, hogy mérlegeljen két alapvető jog között a közérdekű és egyben személyes adatokat is tartalmazó EU dokumentumokhoz való hozzáféréssel kapcsolatos jogvita során.

A Bavarian Lager egy 1992-ben alapított vállalat, mely német söröket importált az Egyesült Királyságba. A hatályos jogszabályok¹⁴² az Egyesült Királyságban hátrányos helyzetbe hozták a hazai sörfőzdékkel és kereskedőkkel szemben, így a Bavarian Lager kezdeményezte a probléma megoldását a Bizottságnál, mely meg is tette a szükséges intézkedéseket az Egyesült Királyság felé, mivel a kifogásolt jogszabály nem teljesítette az alapvető szabadságokkal kapcsolatos kötelezettségeket (árak és szolgáltatások szabad áramlása). Az Egyesült Királyság

¹⁴¹ C-28/08 P Commission v Bavarian Lager, 2010. 06. 29.

¹⁴² Guest Beer Provision, Supply of Beer (Tied Estate) Order 1989 SI 1989/2390

a Bizottság döntse alapján késedelem nélkül módosította a szükséges jogszabályokat, betartva az uniós joggal kapcsolatos kötelezettségeit.

A Bavarian Lager kérvényezte a Bizottságtól, hogy adja ki számára az üggyel kapcsolatos megbeszélésen (1996. október 11-én) készült jegyzőkönyveket, melyen a Bizottság, az Egyesült Királyság és a Confédération des Brasseurs du Marché Commun¹⁴³ képviselői voltak jelen¹⁴⁴.

A Bizottság tovább is küldte a kért dokumentumot a Bavarian Lagernek, azonban abból kihúzta a neveket és más személyes adatokat, a jelenlévő személyek magánszférájának védelmére hivatkozva az 1049/2001/EK rendelet alapján.¹⁴⁵

Az 5 személy neve azért lett kihúzva, mert ketten kifejezetten megtagadták hozzájárulásukat személyes adataik publikálásához, hárman pedig nem nyilatkoztak.

A Bavarian Lager ezt követően kezdeményezett eljárást az EU Bíróságánál, mely a Bizottság titkosítással kapcsolatos határozatát hatályon kívül helyezte, mivel a nevek nyilvánosságra hozatala nem teremti meg a 1049/2001 rendeletben meghatározott „magánszféra és a magánszemély becsületének” sérülését.

A Bizottság ezután fellebbezett a döntés ellen, melynek hatására a Bíróság megváltoztatta korábbi döntését: mégis hatályos a rendelet az adott esetre és a személyes adatok védelme elsőbbségben részesült, így az iratok személyes adatok nélkül kerültek továbbításra.

A Bíróság arra jutott továbbá, hogy a Bizottságnak joga volt felülvizsgálni a jegyzőkönyvek kiadását, mely során cenzúrázta az 5 nevet, mivel a Bavarian Lager nem tudta alátámasztani, hogy számára fontos lett volna az 5 név megismerése, vagy az jogi helyzetére bármilyen hatással lett volna.

3.1.3 Személyes adatok védelméhez való jog és a szerzői jogok

¹⁴³ Confederation of Common Market Brewers

¹⁴⁴ Az Európai Unió Alapjogi Chartája, 42. cikk, A dokumentumokhoz való hozzáférés joga

Bármely uniós polgár, valamint valamely tagállamban lakóhellyel, illetve létesítő okirat szerinti székhellyel rendelkező természetes vagy jogi személy jogosult hozzáférni az Unió intézményeinek, szerveinek és hivatalainak dokumentumaihoz, függetlenül azok megjelenési formájától.

¹⁴⁵ Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. 05. 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről, 4. cikk 1) Az intézmények megtagadják a dokumentumokhoz való hozzáférést, ha a közzététel kedvezőtlenül befolyásolná a következők védelmét: b) a magánszféra és a magánszemély becsületének védelme, különösen a személyi adatok védelmére vonatkozó közösségi joganyagnak megfelelően.

A Promusicae vs Telefónica ügy: a Promusicae egy szerzőket (producerek, zene és audiovizuális szerzők) képviselő non-profit szervezet Spanyolországban, mely a Telefónica internetszolgáltató ellen indított keresetet, követelve, hogy a szolgáltató adja ki azon internethasználók adatait, akik illegális zeneletöltést végeztek egy speciális programmal (KaZaA).¹⁴⁶

Promusicae a zeneletöltő felhasználók ellen a szerzői jogok megsértése miatt indított volna keresetet kártérítés, a jogsértő magatartástól való eltiltás és a többi illegálisan letöltő felhasználó elrettentése céljából.

A Madridi Kereskedelmi Bíróság az Európai Bíróság véleményét kérte ki avval kapcsolatosan, hogy mely uniós jogszabályt alkalmazzák az adott kérdésben: az Elektronikus kereskedelemről szóló irányelvet¹⁴⁷, a szerzői és szomszédos jogok védelméről szóló irányelvet¹⁴⁸, vagy az irányelvet a szellemi tulajdonjogok érvényesítéséről.¹⁴⁹

Kérdés volt továbbá, hogy a spanyol szabályozás ütközik-e az uniós joggal, mely alapján az internetszolgáltatók 1 évig voltak kötelesek megőrizni az felhasználók adatait, melyek kizárólag nemzetbiztonsági és bűnüldözési célból voltak felhasználhatóak.

Az Unió elektronikus hírközlési adatvédelmi irányelve¹⁵⁰ úgy rendelkezik, hogy a tagállamok kötelesek biztosítani a kommunikáció bizalmasságát a publikus kommunikációs csatornákon és a társadalom számára elérhető elektronikus hírközlési szolgáltatások során, továbbá eltérő rendelkezések hiányában tilos adataik tárolása és továbbítása.

5. cikk, A közlések titkossága

(1) A tagállamok nemzeti jogszabályok révén biztosítják a nyilvános hírközlő hálózatok és a nyilvánosan elérhető elektronikus hírközlési szolgáltatások segítségével történő közlések és az azokra vonatkozó forgalmi adatok titkosságát. Különösen megtiltják a közlések és az azokra vonatkozó forgalmi adatok felhasználókon kívüli személyek által történő, az érintett felhasználó hozzájárulása nélküli meghallgatását, lehallgatását, tárolását vagy más módon történő

¹⁴⁶ KaZaA egy zeneletöltő program, mely a "torrent"-hez hasonló "peer to peer" fájlmegosztó rendszert használt az adatok megosztására és cseréjére.

¹⁴⁷ Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól ("Elektronikus kereskedelemről szóló irányelv")

¹⁴⁸ Az Európai Parlament és a Tanács 2001/29/EK irányelve (2001. május 22.) az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolásáról

¹⁴⁹ Az Európai Parlament és a Tanács 2004/48/EK irányelve (2004. április 29.) a szellemi tulajdonjogok érvényesítéséről

¹⁵⁰ 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)

elfogását vagy megfigyelését, kivéve, ha az ilyen személy a 15. cikk (1) bekezdésével összhangban jogszerűen jár el.

6. cikk, Forgalmi adatok

(1) E cikk (2), (3) és (5) bekezdésének, valamint a 15. cikk (1) bekezdésének sérelme nélkül, az előfizetőkre és felhasználókra vonatkozó, a nyilvános hírközlő hálózat vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatás nyújtója által feldolgozott és tárolt forgalmi adatokat törölni kell, vagy anonimmé kell tenni, ha a közlés továbbításához ezek már nem szükségesek.

Az irányelv alapján bizalmasság elve alól kivételt jelentenek a nemzetbiztonsági ügyek, a bűnüldözés, és az elektronikus hírközlési szolgáltatások jogosulatlan használata, azonban a polgári peres eljárások nem szerepelnek a kivételek között.

Azonban az irányelv szerint lehetséges az elektronikus hírközlési szolgáltatás bizalmasságának a korlátozása, amennyiben az mások alapvető jogainak védelméhez szükséges.

Ezáltal fennáll az elvi lehetősége annak, hogy a tagállamok olyan jogszabályt alkossanak, mely lehetővé teszi a személyes adatok kiadását polgári peres eljárások esetében is, amennyiben az mások alapvető jogainak védelméhez szükséges és ez a védelem arányban áll a személyes adatok védelméhez való jog korlátozásával.

Mivel az EU másodlagos jogforrásai nem adtak egyértelmű választ a kérdésre (csupán a kiadás elvi lehetősége állt fenn), ezért a Bíróság az elsődleges jogforrásokat vette vizsgálat alá a jogeset eldöntése céljából: az elsődleges jogforrások elemzése során kiemelte a Bíróság, hogy a tulajdonhoz való jognak részét képezi a szerző szellemi alkotásának védelméhez való joga, továbbá a hatékony jogorvoslathoz való jog is megilleti a tulajdonost. Ezen jogok alapelvei a közösségi jognak, melyet összhangba kell hozni a személyes adatok védelmével és a magánszféra védelméhez való joggal.

Egyik oldalról kijelenthetjük, hogy a felhasználók, szolgáltatók és a szerzői jogtulajdonosok közös érdeke, hogy a felhasználók személyes adatai és digitális nyomai biztonságban legyenek, felfedés nélkül, mivel ez növeli bizalmukat az elektronikus szolgáltatások (pl.: legális fizetős internetes zeneletöltés iTunes-on, filmnézés NetFix-en) iránt, mely a jövőben több hasznot hajthat a jogtulajdonosoknak.

Másik oldalról szemlélve a kérdést, jelenlegi helyzetben a lemezeladásokra komoly hatással van az illegális letöltések elterjedése, mely mind a jogtulajdonosok bevételeit, mind a szerzők megélhetését és ösztönzését veszélyezteti.

A Bíróság megállapítása különösen jelentős volt, mivel ekkor jelentette ki először ítélezésében, hogy a magánszférához és a személyes adatok védelméhez való jogok is alapvető jognak minősülnek a közösségi jogban. Ugyanakkor ítéletében valamelyest összemosta a magánszférához való jogot és a személyes adatok védelméhez való jogot:

“Azonban fontos megjegyezni, hogy abban a vitatott helyzetben, amelyben a kérdést előterjesztő bíróság felteszi ezt a kérdést, a fent említett két alapjog mellett más alapjog is érvényesül, mégpedig a személyes adatok védelméhez, és így a magánélet tiszteletben tartásához való jog.”¹⁵¹

A Bíróság ítéletében nyitva hagyta a kérdést, hogy mely jognak kell az adott esetben elsőbbséget élveznie. Az alapvető jogok fontosságát hangsúlyozva kiemelte, hogy a tagállamok a kérdéses irányelvek alapján nem kötelesek olyan jogszabályokat alkotni, melyek köteleznék a szolgáltatókat az adatok kiadására, ugyanakkor a tagállamoknak úgy kell az irányelveket beültetniük, hogy azok más alapvető jogokkal is megférjenek és azokkal minél kisebb mértékben ütközzenek, így védeni kell a szerzői jogok tulajdonosait is.

A Bíróság gyakorlatilag visszaadta a kérdés eldöntését a nemzeti bíróságokhoz, mely a jogalkotók és jogalkalmazók szerint is könnyen “forum shopping”-ot eredményezhet.

3.2 Az EU Bíróság és a személyes adatok védelméhez való jog Lisszabon után

A Bíróság a „Volker und Markus Schecke” ügy¹⁵² eldöntése során a személyes adatok védelme és az arányosság elve alapján hatályon kívül helyezte az EU agrártámogatásokról szóló rendeleteinek egyes részeit.

Az EU agrártámogatásokról és azok elosztásáról szóló rendeletei¹⁵³ előírták, hogy az agrártámogatásokban részesülő nyertes pályázók neveit és az elnyert összeget publikálni kell évente az illetékes szervek honlapján.

A nyertes pályázók egy csoportja nem értett egyet az eljárás jogosságával Németországban, ahol szövetségi szinten az agrárminisztérium publikálta az adataikat, mivel szerintük a

¹⁵¹ “However, the situation in respect of which the national court puts that question involves, in addition to those two rights, a further fundamental right, namely the right that guarantees protection of personal data and hence of private life.”

¹⁵² C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, judgment, 2010. 11. 09.

¹⁵³ Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy and its implementing Commission Regulation (EC) No 259/2008

személyes adataik nyilvánosságra hozatala megsértette a magánszférához való jogukat, mely az Európai Unió Alapjogi Kartájának védelme alatt áll.

A Bíróság leszögezte, hogy különösen fontos az átláthatóság a közpénzek elosztásánál, mely általános érdek, ugyanakkor ennek a biztosítása jogi személyek és természetes személyek esetében eltérő lehet.

A Bíróság kiemelte, hogy a személyes adatok védelme kizárólag a természetes személyeket illeti meg, és ezen ügy során a nyertes farmerok, mint magánszemélyek szerepeltek a publikált listán, mely harmadik személyek számára is elérhető volt a Világ bármely részéről.

A személyes adatok nyilvánosságra hozatala az érintettek beleegyezésével történhetett volna meg, azonban a publikáló szerv avval nem rendelkezett.

Jelen estben a Bíróság szerint a személyes adatok védelméhez való jogot csak annyira lett volna szabad korlátozni, amennyiben az feltétlenül szükséges, és az átláthatóság követelménye nem élvez elsőbbséget a személyes adatok védelmével szemben.

Több alternatív módszer is felmerülhetett volna publikáláskor az érintettek védelmével kapcsolatban és az arányosság biztosítására, mint például a csak meghatározott összeghatár feletti, vagy csak bizonyos gyakorisággal nyertesek személyes adatainak a publikálása.

Ítéletében a Bíróság az indoklásával következetesen a 1290/2005 rendelet egyes részeit, valamint a 259/2008 rendeletet teljes egészét érvénytelenné nyilvánította.

3.2.1 Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos, Mario Costeja González

Mario Costeja González, spanyol állampolgár 2010-ben tett panaszt a Spanyol Adatvédelmi Hatósághoz a La Vanguardia Ediciones SL újság (egy spanyol napilap, mely nagy példányszámban került kiadásra) és a Google Spain ellen, mivel ha a Google keresőjébe beütötték az ő nevét, akkor La Vanguardia újság két cikke is megtalálható volt a keresési eredmények között, melyek számára negatív tartalmúak voltak.

A cikkek a társadalombiztosítás felé fennálló tartozásai miatt árverezés alá került házáról és az eljárásáról szóltak, melyek Mr. González szerint már megoldódtak és így nem aktuálisak.

Az eljárás legfőbb kérdése, hogy egy internetes kereső oldal üzemeltetője felelős-e tőle független harmadik oldalak tartalmáért, amelyek megjelennek a találatok között.

Az EU Bírósága megállapította, hogy a Google adatkezelőnek minősül, továbbá a társadalom aktuális és pontos információhoz jutásának joga és az érintettek magánszférájához való joga közül az érintettek jogát tekintette végül elsődlegesnek, melyet annyival kiegészített, hogy a két jog közötti egyensúlyt esetenként kell megvizsgálni, mivel a prioritást meghatározza az információ típusa (mennyire különleges adat), az információnak az érintett magánéletére gyakorolt hatása, továbbá a közérdek az adat nyilvánosságával kapcsolatosan (közérdekű adatok, politikusok és más közszereplők tevékenységei).

A Bíróság arra a kérdésre, hogy az érintett kérvényezheti-e a kereső üzemeltetőjétől az egyes találatok eltávolítását a listáról, a választ attól tette függővé, hogy a kérdéses találatokban megjelenő tartalom megfelel-e az irányelv rendelkezéseinek: amennyiben kérés pillanatában avval nincsenek összhangban, akkor törölni kell őket.

A Bíróság döntését részletesen elemzem dolgozatomban az internetes keresők és a felejtés jogának vizsgálatánál.

3.2.2 Az Európai Unió Bíróságának Safe Harbort megszüntető ítélete

(Maximilian Schrems v Data Protection Commissioner)

A Facebook európai felhasználóinak adatai Írországból (ahol a cég európai székhelye van) továbbküldésre kerültek az Egyesült Államokba, ahol a cég szerverein tárolásuk, kezelésük történt.

Az EU Adatvédelmi Irányelve alapján személyes adat főszabályként csak olyan országba küldhető, melyben biztosított az adatok megfelelő szintű védelme.

Mivel az USA és az EU adatvédelmi szabályozásai, elvárásai jelentősen különböznek egymástól, ezért a két rendszer áthidalására és az USA-ba történő adattovábbítás megkönnyítése céljából jött létre a „Safe Harbor – Biztonságos Kikötő” rendszer. A Safe Harbor jogszabályi alapját a Bizottság 2000. július 26-i 2000/520/EK határozata 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 szóló dokumentumok adták.

Amennyiben egy USA-ban székhellyel rendelkező vállalat teljesítette az Európai Unió által is elfogadott adatvédelmi elveket és regisztrált a Safe Harbor programra, úgy e vállalat tekintetében az adatvédelem megfelelő szintje biztonságosnak volt tekinthető.

Maximilian Schrems, egy osztrák állampolgár (jogász, 2008 óta a Facebook felhasználója) 2013-ban panaszt nyújtott be az Ír Adatvédelmi Hatósághoz, miután Edward Snowden¹⁵⁴ által nyilvánosságra kerültek az Egyesült Államokban folyó, NSA (National Security Agency) és az amerikai kormány egyéb titkosszolgálati szervei által végzett szinte korlátlan adatgyűjtések¹⁵⁵. Panaszában leírta, hogy az Egyesült Államokba küldött személyes adatok nem részesülnek megfelelő védelemben. A Safe Harbor (és az egyéb adatküldési módszereik is) csupán az

¹⁵⁴ Edward Joseph Snowden amerikai számítógépes szakember, a Booz Allen Hamilton tanácsadó cég volt munkatársa, az amerikai Nemzetbiztonsági Ügynökség (NSA) volt vezető tanácsadója (vállalati fedésben), a Központi Hírszerző Ügynökség (CIA) volt műveleti tisztviselője (vállalati fedésben) és az Egyesült Államok Védelmi Hírszerzési Ügynökségének (DIA) volt oktatója (vállalati fedésben), aki azzal vált közismertté, hogy nyilvánosságra hozott szigorúan titkos dokumentumokat, amelyekből kiderül, hogy az amerikai titkosszolgálatok széles körben figyelik az emberek mobiltelefon-hívásait és internetes tevékenységét az Egyesült Államokban és világszerte.

¹⁵⁵ Nyilvánosságra került, hogy az NSA világszerte több mint egy milliárd ember telefonos és internetes kommunikációját követi figyelemmel és nem csak a terrorizmusról, hanem külpolitikai, gazdasági, konkrét kereskedelmi témákról is adatokat gyűjt. Az NSA kiterjedt kémtevékenységet folytatott az Európai Unió, az Egyesült Nemzetek Szervezete és számos olyan kormányzat ellen is, amelyek egyébként az Egyesült Államok szoros szövetségesei, így például Angela Merkel német kancellár telefonját is lehallgatták. A kiszivárgott dokumentumok szerint az NSA-nak hozzáférése van a Google, a Microsoft, a Facebook, a Yahoo, a YouTube, az AOL, a Skype, az Apple és a Paltalk rendszeréhez.

adatokat kezelő cégekkel szemben védi a személyes adatokat, az Egyesült Államok titkosszolgálati szervei ellen azonban nem nyújt védelmet.

Az Ír Adatvédelmi Hatóság elutasította Maximilian Schrems keresetét arra hivatkozva, hogy a Bizottság 'Safe Harbor' határozata megfelelő védelmet nyújt a személyes adatoknak, továbbá nem járhat el a Bizottság határozatával kapcsolatosan.

A Hatóság döntését a panaszos megtámadta bíróságon (the High Court of Ireland), mely előzetes döntéshozatali eljárást kezdeményezett az EU Bíróságán.

Az EU Bírósága határozatában egyértelművé tette, hogy az olyan szabályozást, amely lehetővé teszi a hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, úgy kell tekintetni, hogy az a magánélet tiszteletben tartásához való jog lényegét sérti.

Az EU állampolgárainak nem volt lehetősége arra, hogy tudomást szerezzenek a róluk folyó adatkezelésről, abba betekinthessenek, helyesbítést kérjenek, vagy bármilyen jogorvoslattal éljenek, így alapvető jogaik sérültek.

Továbbá, a Bíróság megerősítette, hogy a tagállamok adatvédelmi hatóságai még a 95/46/EK irányelv 25. cikkének (6) bekezdése szerinti megfelelőségi határozat megléte esetén is hatáskörrel rendelkeznek arra vonatkozóan, és kötelesek teljes függetlenséggel eljárva megvizsgálni, hogy a harmadik ország felé irányuló adattovábbítás megfelel-e a 95/46/EK irányelvben megállapított – az Alapjogi Charta 7., 8. és 47. cikkének fényében értelmezett – követelményeknek. Ugyanakkor a Bíróság azt is kijelentette, hogy csak a Bíróság állapíthatja meg az uniós jogi aktusok, így a Bizottság megfelelőségi határozatának érvénytelenségét.¹⁵⁶

A Bíróság érvénytelennek nyilvánította az „Safe Harbor” határozatot¹⁵⁷ és kötelezte az Ír Adatvédelmi Hatóságot, hogy megfelelő alapossggal vizsgálja meg Maximilian Schrems panaszát¹⁵⁸.

¹⁵⁶ A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a 95/46/EK irányelv alapján, az Európai Bíróság C-362/14. sz. (Schrems-) ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról, Brüsszel, 2015.11.6.

¹⁵⁷ A Bíróság ítélete „A védett adatkikötő működése az uniós polgárok és az EU-ban letelepedett vállalatok szempontjából” című, 2013-as bizottsági közleményre épül, amelyben a Bizottság számos hiányosságot azonosított, és 13 ajánlást tett. Ezen ajánlások alapján a Bizottság 2014 januárja óta folytat tárgyalásokat az USA hatóságaival azzal a céllal, hogy megújult és erőteljesebb megállapodást vezessenek be a transzatlanti adatcseréhez.

¹⁵⁸ Court of Justice of the European Union, Judgment in Case C-362/14, Maximilian Schrems v Data Protection Commissioner, Luxembourg, 6 October 2015

A határozat arra ösztönözte a 29. cikk alapján létrehozott munkacsoportot – a tagállamok összes adatvédelmi hatóságának képviselőiből és az európai adatvédelmi biztosból álló független tanácsadó szervet –, hogy nyilatkozatot bocsásson ki az ítéletből levont első következtetésekről. Egyebek mellett a fenti nyilatkozat az adattovábbítással kapcsolatos alábbi iránymutatást tartalmazta.

Az ítéletről kiadott hivatalos sajtóközlemény szerint a Bíróság úgy ítéli meg, hogy az Európai Bizottság azon határozatának létezése, amely megállapítja, hogy valamely harmadik ország megfelelő védelmi szintet biztosít a személyes adatok védelme terén, nem korlátozhatja a tagállami adatvédelmi hatóságok számára az Európai Alapjogi Chartában biztosított jogköröket.

A tagállami hatóságok, így a magyar adatvédelmi hatóság is jogosult arra, hogy teljes függetlenséggel megvizsgálja a harmadik országba irányuló adattovábbítások kapcsán az adatvédelmi garanciák meglétét. Ez a jogosultság akkor is megilleti a hatóságot, ha az Európai Bizottság a tárgyban határozatot fogadott el.¹⁵⁹

Az Európai Parlament Állampolgári Jogok, Bel- és Igazságügyi Bizottsága (LIBE) jelentést bocsátott ki 2014-ben az USA kormánya által végzett adatgyűjtésekről és a Safe Harbor érvényesüléséről, amelyben megállapításra került, hogy az nem képes megfelelő biztosítékokat nyújtani a személyes adatok kezeléséhez.

A Safe Harbor programban résztvevő társaságoknak évente kellett jelentést benyújtania arról, hogy megfeleltek-e a programban megfogalmazott 7 adatvédelmi irányelvnek. Christopher Connolly (a LIBE Bizottság tagja) bírálta a Safe Harbort, és vizsgálatai alapján hétből egy Safe Harbor kérelem valótlan volt, továbbá a társaságok 30 százaléka nem kínált megfelelő tájékoztatást a vitarendezési lehetőségekről¹⁶⁰.

Kérdés, hogy valóban az Európai Bíróság feladata arra rávilágítani, hogy a közjogi kivétel, amelyet az Egyesült Államok kormánya használ a korlátlan adatgyűjtéshez, sérti az európai jogot, és a nyilvánvaló helyzet ellenére miért nem tudtak az EU szervei időben megfelelő lépéseket tenni, amellyel megelőzhetők volna az olyan bizonytalan helyzeteket, amely a Safe Harbor és a Privacy Shield között keletkezett.

Az ítélet felveti továbbá annak kérdését is, hogy az európai kormányok és titkosszolgálatok adatkezeléseire, az állampolgárok adataihoz való hozzáférésre vonatkozó –az amerikaihoz

¹⁵⁹ A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye az Európai Unió Bíróságának a Safe Harbor ügyben hozott ítéletéről (C-362/14.), 2015. 10. 06.

¹⁶⁰ EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance, Chris Connolly, Galexia, Strasbourg, October 7. 2013.

nagyon is hasonló – szabályai mennyiben felelnek meg az adatvédelem és az alapjogi korlátozás alkotmányos követelményeinek¹⁶¹.

Meg kell jegyezni ugyanakkor azt is, hogy az Európai Bíróság az egyik legjelentősebb kifogása a Safe Harbour rendszerrel szemben az volt, hogy nem garantálta az USA hatóságaival szembeni jogvédelmet az érintett európai polgárok számára. Ez azonban a megmaradó adatküldési lehetőségek esetében sem biztosított.

3.3 Következtetések összegzése az EU Bíróságának joggyakorlatáról

Az Európai Unió Bírósága a bemutatott jogesetek jelentős részében nem adott konkrét választ az esetek eldöntésére, vagy nyitva hagyott több kérdést is, melyet a tagállami törvényhozásoknak és jogalkalmazóknak kell megválaszolniuk.

A nemzeti törvényhozások és bíróságok bármilyen rendelkezést és döntést hoznak a jogesetekre, azok teljesen egységesek biztosan nem lesznek, mely könnyen oda vezethet, hogy a nagy vállalatok a kisebb ellenállás felé haladva a kevésbé szigorú szabályozást alkalmazó országokba helyezik át tevékenységüket és székhelyüket, probléma felmerülése esetén pedig forum shopping lehet a különbségek következménye.

A jogesetek közül kiemelendő a Google jogvitája az adataik eltávolításáért küzdő felhasználókkal, mivel a mindennapi életünkre az ügy következményei komoly hatással lehetnek: kérhetjük a velünk kapcsolatos információk törlését a Google-től, továbbá lehetséges, hogy ugyanarra a keresésre más eredményeket kapunk majd Európában, mint a világ más részein.

Az internetre bármilyen adat, ha egyszer felkerült, nagyon sokáig ott marad, és ezt az elvet az Európai Bíróság döntése nem is érinti: nem az információ eredeti közlőjét, és nem is a tárhelyszolgáltatót kötelezi a tartalom eltávolítására, hanem a keresőt, amivel a tartalmat meg lehet találni.

Google és a keresők nélkül az internet olyan, mint egy több milliárd kötetes könyvtár könyvtárosok nélkül: azt találjuk meg, amiben segítenek, és amit fontosnak tartanak, mely

¹⁶¹ Domokos Márton, Polefkó Patrik: Egy bírósági döntés következményei - avagy az Európai Bíróság ún. Schrems döntésének hatásai, a Safe Harbor sorsa és a felmerülő kérdések az adatvédelem területén, Infokommunikáció és Jog, 2015. 4. szám

hatalmat jelent, melyet nem szabad sem korlátozás nélkül gyakorolni, sem komoly cenzúrának alávetni¹⁶².

¹⁶² Dan Sisson: Google Secrets – How To Get the Top 10 Ranking on the Most important Search Engine in the World, Blue Moose Webworks, 2003, 9-12.

4. A felejtés joga és az internetes közvetítő szolgáltatók

4.1 Az adatkezelő és adatfeldolgozó meghatározásának szempontjai napjaink összetett adatkezelései során

Az Európai Unió adatvédelmi irányelvének alapvető célja, hogy minden adatkezelésnek legyen – legalább egy – felelőse, aki a közösségi és nemzeti adatvédelmi jogszabályok érvényesüléséről gondoskodik. Így került megalkotásra az adatkezelő intézménye, aki az adatkezelés célját és módját ténylegesen meghatározza¹⁶³.

Az informatika fejlődése megkönnyítette a távmunkát és kiszervezések („outsourcing”) megvalósítását, melynek következtében az adatfeldolgozások jelentősen megváltoztak. Az olyan műveletek, melyeket korábban egy szervezetben belül végeztek el, napjainkban harmadik felek hajtják végre: saját jogi osztály helyett ügyvédi irodákat bíznak meg a cégek, a rendszergazdai teendőket és a honlap üzemeltetését is külsős informatikai cégek látják el.

Az interneten a tartalmegosztó oldalak megjelenése egy új folyamatot indított el: egyre több szolgáltatás üzemeltetője próbálja meg magát adatfeldolgozóként feltüntetni és a felelősséget áthárítani.

Az adatfeldolgozások több szereplő általi megvalósítása miatt különösen fontos az adatkezelő és az adatfeldolgozó személyének elhatárolása, személyük pontos meghatározása, mivel az adatvédelmi jogszabályokból eredő köteleességekért elsősorban az adatkezelő felel.

4.1.1 Adatkezelő

Az adatvédelmi szabályozás központi eleme az adatkezelő személyének kérdése. A technológia által megváltozott élethelyzetekben is a legelső és legfontosabb adatvédelmi feladat az adatkezelő személyének pontos meghatározása, mivel az adatkezeléssel kapcsolatos

¹⁶³ Az Európai Parlament és a Tanács 95/46/EK irányelve, 2. cikk

d) "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;

kötelezettségek teljesítéséhez¹⁶⁴ és az érintett jogainak gyakorlásához¹⁶⁵ rajta keresztül vezet az út, továbbá ő vonható felelősségre¹⁶⁶ azok megszegéséért vagy nem teljesítéséért.

Az adatkezelő személye kulcsfontosságú az alkalmazandó jogszabályok eldöntésénél is: az irányelv és a nemzeti törvényhozások az adatkezelő személyéből kiindulva határozzák meg hatályukat.¹⁶⁷ Így minden adatkezelésnél a legfontosabb feladat annak tisztázása, hogy ki az adatkezelő: akit a jogszabály kijelöl, aki formálisan a szerződésben adatkezelőként van meghatározva, aki a tényleges döntést meghozza az adatok sorsáról, vagy aki az adatkezelési műveleteket végrehajtja, vagy végrehajtatja.

Ahhoz, hogy a több szereplős adatkezeléseknél is meg tudjuk állapítani, hogy ki a folyamatért felelős adatkezelő, szükséges az adatkezelő törvényi meghatározásának fogalmi elemeit megvizsgálni.

„az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv”: adatkezelő az érintettel szemben – aki csak élő természetes személy lehet - bármilyen entitás lehet.

Tagállamonként – az irányelv határai között – lehetnek eltérő adatvédelemmel kapcsolatos rendelkezések, továbbá a polgári jogi és büntetőjogi szankciók is, de ahhoz, hogy ki tudjuk választani az alkalmazandó jogrendszert, az adatkezelésért felelős személy megállapításának szabályai egységesek kell, hogy legyenek.

Az adatkezelői minőség megállapítása során más jogintézmények átfedőnek és avval ütközőnek tűnhetnek. Ilyen például a szerzői jog tulajdonosa, aki egyben adatkezelői minőségben is részt vehet a jogviszonyokban (a két szerep nem zárja ki egymást). Más jogágakban lefektetett felelősségi viszonyok ugyanakkor segíthetnek megtalálni a felelős személyét: a magánjog és közjog területén kikristályosodott megoldások irányt mutathatnak az adatkezelő személye felé. Amennyiben az adatkezelő egy szervezet, az adatkezelési műveleteket természetes személyek végzik: az adatkezelést ők a szervezet képviselőjében, érdekében végzik munka-, megbízási,

¹⁶⁴ Az adatvédelmi irányelv 6. cikk (1) bekezdése tartalmazza az az adatkezelés alapelveit (pl. tisztességes és törvényes cél, célhoz kötöttség), majd a (2) szakasz úgy rendelkezik, hogy az adatkezelő feladata gondoskodni arról, hogy az (1) bekezdés rendelkezései teljesüljenek.

¹⁶⁵ Az adatvédelmi irányelvben az érintett számára biztosított jogok, mint például a tájékoztatáshoz, helyesbítéshez, tiltakozáshoz való jog (10-12. cikk, 14. cikk) gyakorlása az adatkezelőn keresztül lehetséges.

¹⁶⁶ Adatvédelmi irányelv, 23. cikk, (1) A tagállamoknak rendelkezniük kell arról, hogy mindenki, aki jogellenes adatfeldolgozási művelet vagy az ezen irányelv értelmében elfogadott nemzeti rendelkezésekkel összeegyeztethetetlen intézkedés eredményeképpen kárt szenvedett, az adatkezelőtől kártérítésre jogosult az elszenvedett károkért.

¹⁶⁷ 4. cikk (1) A személyes adatok feldolgozására minden tagállam az ezen irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza, amennyiben:

a) az adatfeldolgozást a tagállam területén az adatkezelő egy szervezete tevékenységeinek keretében végzik; amennyiben ugyanaz az adatkezelő több tagállam területén is letelepedett, meg kell tennie a szükséges intézkedéseket annak biztosítása érdekében, hogy szervezeteinek mindegyike megfeleljen az alkalmazandó nemzeti jog által megállapított kötelezettségeknek.

vagy egyéb jogviszony keretében, így magatartásuk a szervezetnek tudható be, tehát a felelős adatkezelő a szervezet.

A nagy szervezetek általában kijelölnek egy személyt, aki az adatkezelésekért felel: az adatok felvétele és kezelése során az általános adatvédelmi és speciális ágazati jogszabályok betartatása a feladatuk. Az ilyen személyek is csupán a szervezet képviselőjében járnak el, a felelős továbbra is a szervezet marad, így téves az a megközelítés, mely szerint az adatkezelő szervezetnél az adatfeldolgozási műveleteket végző természetes személyek minden esetben adatkezelők lennének és egyenként felelősek. Az ilyen megoldás az érintett érdekeivel is ellentétes lenne: a szervezet – általában – tökeerősebb, és az adatkezelés megsértése esetén okozott károkat könnyebben lehet jogi úton érvényesíteni vele szemben és rajta keresztül, mint egyenként a műveleteket végzőkkel¹⁶⁸.

A szervezet keretében dolgozó természetes személy kizárólag az adatkezelés megsértése esetén válik adatkezelővé¹⁶⁹, mely esetben az érintett szintén a szervezettel szemben érvényesítheti az igényét, majd az adatkezelő szervezet a kárát külön polgári jogi eljárás keretében érvényesítheti az alkalmazottjával szemben.

Büntetőjogi szempontból az alkalmazott önállóan felel, mely megerősíti, hogy jogsértés esetén ő is adatkezelőnek minősül, mivel a büntetőjogi felelősségre vonás feltétele, hogy az elkövető felelősséggel tartozzon az adatvédelmi jogszabályok megtartásáért.

A személyes adattal való visszaélés tényállásának a minősített esetében a minősítő körülményből következik, hogy az elkövető valamely állami vagy önkormányzati szervezetben is részt vehet az elkövetés megvalósítása során¹⁷⁰ (melyért természetesen a büntetőjogi felelőssége önálló), így téves a megközelítés, mely az adatkezelő szervezetében az adatkezelést megsértő természetes személyt az adatkezelésből kiváló harmadik félnek tekinti, mivel az

¹⁶⁸ Természetesen jogszabály nem zárja ki, hogy magánszemély és egy szervezet közösen, ketten legyenek adatkezelők egy adatkezelésben, amennyiben egymástól függetlenek, és együtt határozták meg az adatkezelés célját és módját (pl. partnerek).

¹⁶⁹ Adatvédelmi irányelv, 2. cikk f) "harmadik személy" az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely nem azonos az érintettel, az adatkezelővel, a feldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy a feldolgozó közvetlen felügyelete alatt felhatalmazást kaptak az adatok feldolgozására;

¹⁷⁰ 219. § (1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy

b) az adatok biztonságát szolgáló intézkedést elmulasztja, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

(4) A büntetés büntett miatt három évig terjedő szabadságvesztés, ha személyes adattal visszaélést hivatalos személyként vagy közmegbízatus felhasználásával követik el.

fogalmilag kizárt: harmadik személyeknek nincsen és nem is lehetett felhatalmazásuk műveleteket végezni az adatokon.¹⁷¹

Attól függetlenül, hogy a szervezetnél dolgozó adatkezelést megsértő személy önálló adatkezelővé minősül át (addig csupán a szervezet képviselőjeként végezte az adatkezelést), az adatkezelés megsértéséért a szervezet is felelősséggel tartozik. A kártérítési igényt vele szemben is lehet érvényesíteni, mivel minden szervezetet kötelezettség terheli arra nézve, hogy biztosítsa a személyes adatok biztonságának technikai és szervezési intézkedéseit¹⁷², így illetéktelenek a szervezeten belül sem férhetnének hozzá adatokhoz.

A szervezetet terheli továbbá a felelősség a megfelelő és megbízható emberek kiválasztására, akik abban az esetben sem sértik meg a személyes adatok kezelését, ha ahhoz jogosultságuk van hozzáférni, továbbá a nagy vállalatok, melyek – akár dollárban is – milliós kárt okozhatnak az adatok nem megfelelő kezelésével, nem háríthatják át a felelősséget egy magánszemélyre, akin gyakorlatilag lehetetlen behajtani a követelést.

„amely önállóan vagy másokkal együtt”

Az első magyar adatvédelmi törvény alkalmazása során jelent meg az a – téves – megközelítés, hogy egy adatkezeléshez csupán egy adatkezelő¹⁷³ kapcsolható.¹⁷⁴ Az elgondolás alapját az adatvédelmi nyilvántartás adta, melynek alkalmazása során az adatkezelésnél egy adatkezelőt lett volna a legpraktikusabb megnevezni a felelősség egyszerűsítése céljából.

Az adatvédelmi irányelv és az élet is meghaladta ezt az elképzelést: mindennaposak az olyan adatbázisok, melyekhez több szerv, cég vagy személy fér hozzá adatkezelési jogosultsággal.

Elég csak arra gondolnunk, hogy egy beteg adatait a kórház és a társadalombiztosítás is módosíthatja a kezeléseik függvényében, vagy egy google dokumentumot egy időben többen is szerkeszthetnek.

Az adatok közös kezelése és feldolgozása nagyon sokféleképpen valósulhat meg a mindennapi életben: nem csupán egy műveleten dolgozhatnak többen (pl. több adatkezelő közösen veszi fel

¹⁷¹ Adatvédelmi irányelv, 2. cikk f) "harmadik személy" az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely nem azonos az érintettel, az adatkezelővel, a feldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy a feldolgozó közvetlen felügyelete alatt felhatalmazást kaptak az adatok feldolgozására;

¹⁷² Adatvédelmi irányelv, 17. cikk (1) 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.

¹⁷³ ABI 1999, 109

¹⁷⁴ Jóri, 2009, 122.

az adatokat), hanem könnyen lehet, hogy több adatkezelő több különböző műveletet vagy műveletsorozatot hajt végre (pl. egyik adatkezelő a tárolásért, másik a felvételért, harmadik a továbbküldésért felelős), továbbá az sem biztos, hogy egyenlő mértékben vesznek részt valamely feladatban.

A komplex, többszereplős adatfeldolgozásoknál annak eldöntéséhez, hogy közös adatkezelésről, vagy csupán adatkezelő és adatfeldolgozó viszonyról van-e szó, meg kell vizsgálni a szerződés szövegén túl a valódi szerepeket is: az adatfeldolgozás céljának és módjának meghatározásában ki vesz részt ténylegesen.

Pusztán az a tény, hogy többen működnek közre az adatkezelés megvalósításában, vagy, hogy adatokat továbbítanak és osztanak meg egymással, még nem vonja magával a közös adatkezelés tényállását.

Például ha egy budapesti egyetemi kar felkér egy vidéki kart képzés lebonyolítására és átküldi a hallgatók személyes adatait, abban az esetben két külön adatkezelőről beszélhetünk.

Abban az esetben beszélhetünk közös adatkezelésről, ha a cél vagy mód meghatározásában több szereplő vesz részt.

Az előbbi példánál maradva, ha a két egyetemi kar közösen hoz létre és működtet egy adminisztrációs felületet a hallgatók jelentkezésére és tanulmányi ügyeinek lebonyolítására (pl. Neptun, ETR), akkor az adatkezelés módját közösen határozzák meg, így közös adatkezelőnek minősülnek.

A közös adatkezelés megvalósulásához nem szükséges, hogy egyik fél csak a célt, másik csak a módot határozza meg: akár közösen is meghatározhatják mindkettőt, de az is lehetséges, hogy az egyik fél csak a mód vagy cél egy részét határozza meg.

Amikor egy munkaerőt igénylő cég kapcsolatba lép egy diákszövetkezettel, hogy számára meghatározott létszámban szaktudással rendelkező (pl. angolul beszélő) diákokat közvetítsen ki munkavégzésre, abban az esetben a cég adatkezelőként jár el, mert ő határozta meg az adatfeldolgozás célját és módját (munkavégzési célból az iskolaszövetkezettel kötött megállapodás keretében). Ugyanakkor a diákszövetkezet, mely nyilvántartotta a diákok adatait – akik egyben tagsági jogviszonyban is álltak a szövetkezettel – szintén adatkezelőnek tekinthető, mivel kiválasztásban és az adminisztrációban (adatkezelés módja) meghatározó szerepe van, tehát a cég és a diákszövetkezet közös adatkezelőnek minősülnek ebben az adatkezelésben.

Az adatvédelmi irányelv szövegezése során merült fel az a – téves – megközelítés, mely alapján ha egy adatbázishoz egy személy, vagy szervezet hozzáfér, abban az esetben adatkezelőnek kellene tekinteni. A rendelkezés végül nem került bele az elfogadott szövegbe, melyet később

a gyakorlat is igazolt: attól, hogy valaki személyes adatokhoz hozzáfér, még nem tekinthető adatkezelőnek, sőt, a személyes adatokhoz való közvetlen hozzáférés sem feltétele az adatkezelői minőség megállapításának.

Ha az adatkezelési műveleteket mikro szinten vizsgáljuk, több esetben úgy tűnhet, hogy elkülönült adatkezelőkkel állunk szemben, ha azonban makro szinten figyeljük meg az adatkezelési műveleteket, rámutathat arra, hogy nem adatkezelési műveletek láncolatával van dolgunk (elkülönült célokkal és módokkal), hanem „műveletek összességével”¹⁷⁵, melyeknek a célja közös.

Ha például számlát nyitunk egy pénzügyintézetnél, mely azt vezeti és ellátja az adminisztrációs feladatokat, majd az adóhatóság megkeresi a bankot, hogy szolgáltatson ki felé az információkat, abban az esetben két elkülönült adatkezelőről beszélünk, mert nem avval a – közös - céllal vette fel a bank az adatokat, hogy az adóhatóságnak átadja.

Abban az esetben viszont, ha a bankot megbízzuk, hogy utaljon pénzt egy külföldi bankszámlára (SWIFT rendszeren keresztül), akkor az csak a kettő szolgáltató (bank és a SWIFT) közös magatartásával valósulhat meg, így azok közös adatkezelőnek tekinthetők.

A több személy által végzett adatkezelésnél felmerül kérdés, hogy a felelősségük egyetemleges-e. Az irányelv – és az Infotv. - erre vonatkozólag konkrét rendelkezést nem tartalmaz, azonban a joggyakorlat és az adatkezelő felelősségénél használt egyes szám¹⁷⁶ arra utal, hogy az adatkezelők felelőssége egyetemleges. Az egyetemleges felelősség mellett szól az érintettek érdeke is: különösen a nagyszámú adatkezelő részvételével megvalósuló adatkezelések esetében jelenthetne nehézséget az érintett számára, hogy melyik adatkezelőt keresheti meg igényének érvényesítése céljából.

Fontos kiemelni, hogy nem zárja ki az adatkezelőként való minősítést, ha az adatkezelő nem tudja minden törvény által előírt kötelezettségét ellátni: a tájékoztatáshoz, vagy helyesbítéshez való jogot adatfeldolgozóval, vagy közös adatkezelés esetén másik adatkezelővel is elláttathatja, különösen, ha az érintett jogainak érvényesítését egyszerűbbé teszi (pl. érintett

¹⁷⁵ Adatvédelmi irányelv, 2. cikk b) "személyes adatok feldolgozása" ("feldolgozás") 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, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés;

¹⁷⁶ Adatvédelmi irányelv. 23. cikk (1) A tagállamoknak rendelkezniük kell arról, hogy mindenki, aki jogellenes adatfeldolgozási művelet vagy az ezen irányelv értelmében elfogadott nemzeti rendelkezésekkel összeegyeztethetetlen intézkedés eredményeképpen kárt szenvedett, az adatkezelőtől kártérítésre jogosult az elszenvedett károkért.

(2) Az adatkezelő részben vagy egészben mentesül e felelősség alól, ha bizonyítja, hogy a kárt okozó eseményért nem felelős.

lakóhelyén lévő képviselőt bíz meg a kötelezettségek ellátásával). A delegálás azonban nem változtat a tényen, hogy a felelősség az adatkezelőt terheli.

Az ilyen többszereplős, komplex feldolgozások esetén különösen fontos, hogy a szerepek és felelősség ki legyenek osztva a felek között úgy, hogy az adatvédelmi jogszabályok rendelkezései úgy érvényesülhessenek, mintha egy adatkezelő személy vagy szervezet végezné az összes műveletet.

„meghatározza a személyes adatok feldolgozásának céljait és módját;

A fogalmi elemek közül hangsúly a „meghatározza” kifejezésen van, mely nem jelenti ugyanazt, mint az - irányelv első tervezeteiben szereplő - „eldönti”. Az Infotv. az irányelvnél szűkebben határozza meg az adatkezelő fogalmát, mivel abban benne szerepel a „döntés meghozatala”, továbbá a „végrehajtása, vagy végrehajtatása” is.¹⁷⁷

További probléma az Infotv. meghatározásában, hogy az megbízási jellegű jogviszonyra utal az adatkezelő és adatfeldolgozó relációjában, pedig az adatfeldolgozás tipikusan meghatározott feladat, mely során az adatfeldolgozó valamilyen eredmény elérésére vállalkozik¹⁷⁸ (pl. adatok archiválása)¹⁷⁹.

Léteznek olyan adatokon végzett műveletek is, melyek – gondossági kötelezettségük alapján – inkább a megbízási jogviszonyhoz állnak közelebb (pl. tárhely biztosítása adatoknak), ám a mindennapi életben nem ez a jellemző, különösen a célhoz kötöttség miatt: az adatokat csak a cél megvalósítására lehet felhasználni, és a szükséges ideig tárolni (kivétel a történelmi, statisztikai és tudományos adatkezelés, megfelelő garanciákkal)¹⁸⁰.

Az adatkezelés céljának és módjának „meghatározása” és az avval kapcsolatos „döntés” megkülönböztetése azért is különösen fontos, mert álláspontom szerint az adatfeldolgozó is hozhat döntést adatfeldolgozással kapcsolatosan (pl. milyen fajta számítógépet és programot használjon azok tárolására, mely módszerrel semmisítse meg az adatokat), melyek nem

¹⁷⁷ Infotv. 3. § Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.”

¹⁷⁸ Péterfalvi 2012, 71.

¹⁷⁹ A 1992-es adatvédelmi törvényben az adatfeldolgozó fogalma megbízási jellegű jogviszonyra utalt, mely nem lett átemelve az Infotv. meghatározásába.

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, 2. § adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából - beleértve a jogszabály rendelkezése alapján történő megbízást is - személyes adatok feldolgozását végzi.

¹⁸⁰ Adatvédelmi irányelv, 6. cikk, (1) b) A személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat.

lehetnek akkora olyan jelentőségűek, hogy az adatkezelés irányát meghatározzák, csupán technikai és szervezési szintűek lehetnek.¹⁸¹

A „meghatározás” magában foglalja az adatkezeléssel kapcsolatos minden alapvető kérdést, mint például az érintettek személye, feldolgozás ideje, továbbküldése és megsemmisítése.

Az adatkezelő személyének meghatározásához több elmélet is született.¹⁸²

1. Kifejezett jogszabályi felhatalmazáson alapuló hatáskör: ebben az esetben közösségi, vagy tagállami jogszabály rendeli el az adatkezelést és jelöli ki a felelős adatkezelő személyét. Gyakori azonban, hogy a jogszabály meghatároz egy végrehajtandó feladatot, és kijelöli annak felelősét (pl. önkormányzatot egy szociális alapú segély szétosztására), azonban az adatkezelőt külön nem nevezi meg, de a feladatból egyenesen következik annak a személye. Ide sorolhatjuk azt az esetkört is, amikor valamely jogszabály kötelez egy szervezetet, hogy az állam részére adatokat szolgáltatson (pl. adóval kapcsolatos ellenőrzések) ki, vagy, hogy azokat tárolja tovább (pl. telefontársaságok nemzetbiztonsági okokból őrizzék meg a forgalmi adatokat).

2. Beleértett hatáskör esetén nem nevezi meg konkrétan a jogszabály az adatkezelőt, viszont a jogintézmény jellegéből és a joggyakorlatból meghatározható az adatkezelésért felelős fél. A polgári jog, munkajog és más jogágak területén is a felelősségi viszonyokból, a jogokból és kötelezettségekből könnyen megállapítható az adatkezelő személye (pl. egy gépjármű bérleti szerződésnél a bérbeadó, munkajogviszony esetén a munkáltató, banki szerződések esetén a bank).

Az adatvédelmi jog erősödésének köszönhetően a modern kódexek már – kellő részletességgel - rendelkeznek a szabályozott jogviszonyban fennálló adatvédelmi jogokról és kötelezettségekről (pl. Munka Törvénykönyve¹⁸³, hitelintézeteket szabályozó törvények), így a beleértett hatáskör jelentősége folyamatosan csökken.

¹⁸¹ Adatvédelmi irányelv, 17. cikk

(2) A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő – amennyiben az adatfeldolgozás az ő nevében történik – köteles olyan adatfeldolgozót választani, aki a technikai biztonsági intézkedések és az elvégzendő adatfeldolgozásra vonatkozó szervezési intézkedések tekintetében megfelelő garanciákat nyújt, továbbá köteles biztosítani az említett intézkedések teljesítését.

¹⁸² Article 29 Data Protection Working Party: Opinion 1/2010 on the concepts of "controller" and "processor" 10-13.

¹⁸³ 2012. évi I. törvény a munka törvénykönyvéről, 10. § (2) A munkáltató köteles a munkavállalót tájékoztatni személyes adatainak kezeléséről. A munkáltató a munkavállalóra vonatkozó tény, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet.

(3) A munkaviszonyból származó kötelezettségek teljesítése céljából a munkáltató a munkavállaló személyes adatait - az adatszolgáltatás céljának megjelölésével, törvényben meghatározottak szerint - adatfeldolgozó számára átadhatja. Erről a munkavállalót előzetesen tájékoztatni kell.

3. **A tényleges befolyáson alapuló hatáskör:** ebben az esetben az összes körülmény vizsgálata során állapítható meg, hogy a jogviszonyban melyik fél határozza meg ténylegesen az adatkezelés célját és módját.

Legelső lépésként a felek között létrejött szerződés rendelkezéseit szükséges megvizsgálni: amennyiben megnevezi az adatkezelő személyét, már támpontként szolgálhat. Ha nincs konkrétan megnevezve az adatkezelő, akkor a szerződésben szereplő jogok és kötelezettségek segíthetnek megállapítani az adatkezelés felelőjét.

Amennyiben nincs ok kételkedni a szerződés szövegében, abban az esetben sem mindig könnyű megállapítani a feldolgozó és adatkezelő személyét annak a szövegből: sok esetben annyira összetett jogviszonyokról van szó, hogy a szerződések szövegén túl vizsgálni kell az adatkezelést ténylegesen meghatározók személyét is.

Egyre gyakrabban merül fel a szigorodó adatvédelmi szabályok miatt, hogy a szerződés a felelősség áthárítása céljából más személyt jelöl meg adatkezelőnek, mint aki ténylegesen döntési jogosultsággal rendelkezik az adatok felett: különösen az internet világában, ahol a szolgáltatások esetén összemosódnak a szerepek, gyakran lépnek fel az oldal üzemeltetői adatfeldolgozóként, áthárítva a felhasználóra az adatkezelés felelősségét.

Ilyen esetekben az összes körülmény vizsgálata alapján lehet meghatározni azt a felet, amelyik az adatkezelés célját és módját ténylegesen meghatározza.

Még egy adatkezelő és adatfeloldozó között létrejött tiszta jogviszonyban is jogsértés esetén az adatfeldolgozó adatkezelővé válhat (pl. az adatok tárolásáért felelős adatfeldolgozó továbbküldi az adatokat harmadik félnek az adatkezelő engedélye nélkül, vagy marketing célokra használja fel). A kérdés, hogy az adatfeldolgozó az eredeti adatkezelés tekintetében vált-e adatkezelővé, vagy egy új adatkezelést hozott létre a jogsértő magatartásával.

A kérdés különösen aktuális, mivel a legnépszerűbb internetes oldalak és szolgáltatások üzemeltetőiről többször derült már ki, hogy a személyes adatokat nem az adatvédelmi szabályzatnak és célnak megfelelően használták fel.

A különösen nagy horderejű SWIFT jogeset is egy ilyen problémát vetett fel: az adatfeldolgozó túllépte az adatkezelőtől kapott hatáskörét, és a kért adatkezelési műveleteken túl olyanokat is végzett, melyekre nem lett volna jogosultsága.¹⁸⁴

A SWIFT (Society for Worldwide Interbank Financial Telecommunication) egy belga vállalat, mely a bankok közötti pénzügyi műveletekhez biztosít technikai háttérrel nemzetközi szinten.

¹⁸⁴ Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 2006. November 23. 2-6.

A SWIFT minden pénzügyi műveletnek adatait 124 napig tárolja az Európai Unióban és az Egyesült Államokban (ugyanazokat az adatokat tükrözve mindkét helyen): az utalással kapcsolatos adatok olyan személyes adatokat tartalmaznak, mint az utaló és a címzett fél neve, számlaszáma, közlemény, az utalt összegek nagysága, valutája és gyakorisága.

Az Egyesült Államok a szeptember 11-ei terrortámadások után indított egy programot a terroristák pénzmozgásainak követése és megakadályozása céljából¹⁸⁵, melyhez szüksége volt a SWIFT adatbázisára: az USA Kincstára felkérte a SWIFT amerikai leányvállalatát, hogy számára adja ki a pénzügyi mozgások adatait, melyet a SWIFT bizonyos korlátozásokkal teljesített, viszont erről az Európai Uniót és a bankokat – kevés kivétellel - nem tájékoztatta.¹⁸⁶ A SWIFT és a pénzügyi intézetek által megkötött szerződések semmilyen felhatalmazást nem adtak arra vonatkozóan, hogy a tranzakciók lebonyolításán és az avval kapcsolatos törvényi kötelezettségeken túl bármilyen adatkezelést valósítson meg a SWIFT.

Bár a SWIFT adatfeldolgozóként szerepelt formálisan a jogviszonyban, az adatok továbbküldésével adatkezelővé minősült át, annak minden felelősségét magával vonva.

Az ügy rámutat arra a problémára, hogy a szerződések szövegén túl az adatkezelések valódi felelőseit csak a tények és gyakorlatuk alapján lehet meghatározni: a tény önmagában, hogy valaki a személyes adatok kezelésének céljával vagy módjával kapcsolatosan döntést hoz, magával vonja az adatkezelői minőséget, tekintet nélkül a szerződésben vagy jogszabályban szereplő rendelkezésekre.

Az adatkezelő fogalmi eleme az adatkezelés *céljának*¹⁸⁷ és *módjának*¹⁸⁸ a meghatározása. A két kifejezés pontos fogalmának tisztázása alapvető jelentőséggel bír: a cél megmutatja, hogy pontosan mit kell valamelyik félnek meghatároznia ahhoz, hogy adatkezelőnek tekinthessük. A magyar és angol értelmező szótárak a célt egy megvalósítandó, elvárt eredménynek tekintik, míg a módot az annak eléréséhez szükséges magatartásként.

A célt és a módot úgy is megközelíthetjük, hogy a cél a „miért” a mód a „hogyan” kérdésre adja meg a választ az adatkezelés tekintetében.

A cél és a mód meghatározásának mértékét is figyelembe kell venni az adatkezelő személyének meghatározásánál: különösen az összetettebb, többszereplős jogviszonyokban fontos tisztázni,

¹⁸⁵ Terrorist Finance Tracking Program (TFTP)

¹⁸⁶ 2006-ban szivárgott ki SWIFT ügy a New York Timesban: Eric Lichtbau and James Risen: Bank Data Is Sifted by U.S. in Secret to Block Terror, New York Times, 2006. 06. 23.
http://www.nytimes.com/2006/06/23/washington/23intel.html?hp&ex=1151121600&en=18f9ed2cf37511d5&ei=5094&partner=homepage&_r=0

¹⁸⁷ wikiszótár: „Megvalósítandó eredmény, amely egy kívánatos állapot, vagy elért hely.”

Magyar Értelmező Kéziszótár:

¹⁸⁸ Magyar Értelmező Kéziszótár

hogy melyik fél milyen mértékben, mekkora ráhatással képes a mód és a cél meghatározásában részt venni. A meghatározásban való részvétel nagysága lehet az elválasztó vonal az adatkezelő és adatfeldolgozó között sok esetben.

Amikor az adatkezelés folyamatában résztvevő félről szükséges megállapítani (pl. kiszervezés, „outsourcing”) esetén, hogy adatkezelő vagy adatfeldolgozóként vesz-e részt az adott jogviszonyban, fel kell tenni a kérdést, hogy abban az esetben, ha őt nem kérik fel, végezné-e egyáltalán az adatkezelést. Amennyiben csak felkérték, akkor a cél meghatározásában nem vett részt.¹⁸⁹

A „mód” meghatározása esetén történeti értelmezés hívható segítségül: az adatvédelmi irányelv tervezetében az adatkezelő fogalmában 4 elem szerepelt (cél, személyes adat és műveletek meghatározása, továbbá harmadik fél hozzáférése az adatokhoz), melyek helyett csupán a cél és a mód került be az irányelv végleges szövegébe. Feltételezve, hogy az adatkezelő fogalmát nem szerették volna szűkíteni (az irányelvben végig megmaradt a cél, hogy a személyes adat és az adatkezelésért felelős fél minél tágabban legyen értelmezve), az adatkezelés módja magában foglalja annak meghatározását, hogy mely személyes adatokat dolgozzák fel a cél eléréséhez, milyen adatkezelési műveleteket hajtsanak végig rajta, és hogy mely adatfeldolgozókat bízzák meg azok feldolgozásával.

4.1.2 Adatfeldolgozó

Az adatfeldolgozó személye¹⁹⁰ fontos szerepet játszik az adatfeldolgozás bizalmasságának és biztonságának a megvalósításában, mivel csak olyan személy lehet adatfeldolgozó, aki az adatkezelő utasításai szerint jár el, mely által az adatkezelés nem térhet el az eredeti céltől.

¹⁸⁹ Adatvédelmi irányelv, 16. cikk

Bármely, az adatkezelő vagy az adatfeldolgozó meghatalmazásával eljáró személy, beleértve magát az adatfeldolgozót is, aki a személyes adatokhoz hozzáféréssel rendelkezik, kizárólag az adatkezelő utasítása alapján dolgozhatja fel ezeket az adatokat, kivéve, ha erre őt jogszabály kötelezi.

¹⁹⁰ Adatvédelmi irányelv, 2. cikk

e) "feldolgozó" az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely személyes adatokat dolgoz fel az adatkezelő nevében.

Infotv. 3. cikk 18.

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi.

Az adatkezelő és adatfeldolgozó megkülönböztetésének alapja, hogy az adatokon műveleteket végzők közül egyértelműen meg kell határozni, hogy ki felel a teljes folyamatért és melyik fél látja el a „végrehajtó” szerepét.

Az adatfeldolgozó személye releváns az alkalmazandó jog megállapításánál is: az adatbiztonsággal kapcsolatos technikai és szervezési intézkedések esetén annak a tagállamnak kerülnek az adatvédelmi jogszabályai alkalmazásra, melynek területén az adatfeldolgozó letelepedett.¹⁹¹

A mindennapi gazdasági életben egyre gyakoribb, hogy a rugalmasság növelése, a pénzügyi és egyéb kockázatok csökkentése céljából a vállalatok kiszervezéseket hajtanak végre: a könyvelés, jogi képviselő és garanciális ügyintézők harmadik felekkel való megoldása mindennapossá vált.

Az alvállalkozók és a külső szolgáltatást nyújtó harmadik felek alkalmazása együtt jár avval, hogy az ügyfelek, alkalmazottak és további érintettek személyes adatai egyre több szervezethez jutnak el egy szolgáltatás megvalósítása során.

Az információs és kommunikációs technológia fejlődése megkönnyítette harmadik felek bevonását, az egymástól távol lévő szervezetek közötti kapcsolattartást és a szervezeti differenciálás megvalósítását.

Tovább bonyolítja a kérdést, hogy az internet terjedésével egyre több globálisan nyújtott szolgáltatást veszünk igénybe (pl. felhő alapú szolgáltatások), melyek üzemeltetői több ország területéről valósítják meg az adatfeldolgozást (pl. a székhely egy országban van, de adatközpont minden kontinensen, a reklámozásért felelős leányvállalatok pedig országonként megtalálhatóak).

Az adatkezelő döntésén múlik, hogy a saját szervezetén belül oldja-e meg az adatok feldolgozását, vagy azok – akár egy részük - elvégzésével adatfeldolgozót bíz meg.

Az adatfeldolgozó két legfontosabb fogalmi eleme, hogy az adatkezelő személyétől teljesen el van különülve, és hogy az ő nevében és utasításai alapján végzi az adatfeldolgozást.

Az adatfeldolgozó személyének kérdése mindig egy konkrét jogviszonyban vizsgálendő: az a tény, hogy egy szervezet tipikusan adatfeldolgozási tevékenységet végez (pl. könyveléssel,

¹⁹¹ Adatvédelmi irányelv 17. cikk (1)

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.

(3) az (1) bekezdésben megállapított kötelezettségek annak a tagállamnak a jogszabályai szerint kerülnek meghatározásra, amelyben a feldolgozó letelepedett, és azok a feldolgozóra is vonatkoznak.

informatikai karbantartással foglalkozó vállalkozások), még nem következik egyenesen, hogy adatfeldolgozóval állunk szemben. Ugyanaz a személy végtelen számú jogviszonyban lehet jelen, melyeket egyenként megvizsgálva lehet csak megállapítani, hogy adatkezelőként, vagy feldolgozóként végzi-e a tevékenységét.

Ha az érintett munkáltatója egy könyvelőirodával köt szerződést bérszámfejtés céljából, a könyvelőiroda adatfeldolgozóként fog eljárni. Abban az esetben, ha a munkavállaló felkeresi az irodát, hogy az segítsen neki az egyéni vállalkozásával kapcsolatos ügyintézésben is, már adatkezelőként jár el a könyvelőiroda.

Az irányelv alapján az adatkezelőnek és az adatfeldolgozónak a jogi helyzet tisztázása érdekében szerződést kell kötnie¹⁹², melyben rendelkezniük kell többek között arról, hogy az adatfeldolgozó csak az adatkezelő utasításai szerint járhat el.

Fontos kiemelni, hogy a szerződés nem konstitutív hatályú, így az adatfeldolgozás – bár nem szabályosan – anélkül is megvalósulhat, melynek következtében szükséges minden adatkezelés esetén megvizsgálni, hogy ténylegesen ki végzi az adatfeldolgozást, mely sok esetben eltérhet a szerződésben leírtaktól (ha egyáltalán van szerződés). Az ilyen adatfeldolgozás természetesen jogszabályba ütközik és az adatvédelmi hatóságok eljárását és szankciókat vonhata maga után. A mindennapi gazdasági életben a tipikusan adatfeldolgozással foglalkozó szervezetek és személyek (pl. adattárolást biztosító vállalat) mintaszerződésekkel rendelkeznek, melyeket az ügyfelek (az adatkezelők) jelentős része változtatás nélkül ír alá. Az adatkezelő meghatározásában fogalmi elem, hogy „meghatározza az adatkezelés célját és módját”, ám ebben az esetben az adatfeldolgozó által előre megírt mintaszerződést használják az adatkezelők. Amennyiben a szerződés megfelel az adatvédelmi jogszabályoknak, mely által magában foglalja az adatkezelő utasítás jogkörét és az érintettek jogait, a szerződés érvényes és hatályos a felek között, függetlenül a megszövegezésének folyamatától.

Attól, hogy az adatkezelő nincsen alkupozícióban a nála jóval nagyobb adatfeldolgozó vállalattal (pl. Apple felhő tárhelyének használata, Google levelezőrendszerén adatok küldése),

¹⁹² Adatvédelmi irányelv, 17. cikk (3) Adatfeldolgozón keresztül történő adatfeldolgozásra olyan szerződésnek vagy jogi aktusnak kell vonatkoznia, amely az adatfeldolgozót az adatkezelővel szemben köti, és amely különösen a következőket tartalmazza:

- az adatfeldolgozó kizárólag az adatkezelő utasítása alapján járhat el,
- az (1) bekezdésben megállapított kötelezettségek annak a tagállamnak a jogszabályai szerint kerülnek meghatározásra, amelyben a feldolgozó letelepedett, és azok a feldolgozóra is vonatkoznak.

(4) A bizonyítékok megőrzése céljából az adatvédelemre és az (1) bekezdésben említett intézkedésekkel kapcsolatos előírásokra vonatkozó szerződés vagy jogi aktus részeit írásba vagy egyéb, azzal egyenértékű formába kell foglalni.

ugyanúgy felelős azért, hogy olyan szerződési feltételeket fogadjon el, melyek megfelelnek az adatvédelmi jogszályoknak.¹⁹³

A felhő alapú szolgáltatók esetében sokszor keverednek az szerepkörök és az adatfeldolgozók bizonyos adatok tekintetében adatkezelőnek minősülhetnek, amely a saját célú adatfeldolgozás tilalmának megsértését is eredményezheti.

Az al- és további felhasználás tilalmának enyhítése az adatfeldolgozó számára megoldást jelenthetne a fennálló helyzetre. Az adatkezelő és adatfeldolgozó külön jogalanyiségének szükségességét is többen megkérdőjelezik, azonban az a felelősség elhatárolásánál jelenthet gyakorlati nehézségeket.

A felhőszolgáltatók által végzett adatkezelés veszélyeinek és a jogi kérdések bizonytalanságának csökkentését a szabályozás módosításával, nemzetközi egységesítésével, az érintettel kötendő adatvédelmi megállapodások kötelező tartalmának megállapításával, a szolgáltatók önszabályozásával, és technológiai védelmi és szervezési intézkedések bevezetésével lehetne kezelni¹⁹⁴.

Az adatkezelési döntések meghozatala és azok végrehajtása sok esetben gép által meghozott döntés is lehet. Tovább bonyolítja a helyzetet az egyre fejlettebb mesterséges intelligencia (MI) problémája. Kijelenthető, hogy napjainkra az eszközök kiléptek az adatfeldolgozás, azaz a technikai feladatellátás szerepköréből.

Az MI által meghozott döntésekért ki a felelős: a felhasználó, vagy az MI megalkotója? A károkozás esetén milyen felelősségi kategória alkalmazandó? Eszteri Dániel cikkében részletesen kielemez a kérdést, amely során arra a konklúzióra jut, hogy a szerződéses viszonyokban a felelősséget több jogalany is viselheti. Annak eldöntéséhez, hogy mely jogalany a felelős, mindig a probléma természetéből kell kiindulni, és, hogy az melyikük mulasztásával van okozati összefüggésben, így például rendeltetésszerűen működő szoftver esetén a felhasználó a felelős, hibásan működő szoftver esetén a felhasználó a fejlesztőtől kártérítést követelhet hibás teljesítés alapján¹⁹⁵.

Összegzésként megállapítható, hogy a cél meghatározása fenn van tartva az adatkezelőnek: az adatfeldolgozó és más személyek nem vehetnek részt semmilyen szinten és mértékben a cél

¹⁹³ Article 29 Data Protection Working Party: Opinion 1/2010 on the concepts of "controller" and "processor" 24-29.

¹⁹⁴ Bocskó Viktor, Boldizs Péter, Loós Csaba, Major Tamás: A dolgok internete – technológiai háttér, információbiztonsági és adatvédelmi aspektusok, Infokommunikáció és Jog, 2015. 2-3. 58.

¹⁹⁵ Eszteri Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései, Infokommunikáció és Jog, 2015. 2-3. 48-51.

meghatározásában. A cél meghatározásában való legkisebb mértékű részvétel is az adatkezelői minőséget vonja maga után. A mód meghatározásában való részvétel már nem ennyire egyértelmű: olyan technikai és szervezési jellegű döntéseket meghozhat az adatfeldolgozó, melyek az érintett jogaira és az adatokra nincsenek jelentős hatással. Az adatfeldolgozó az adatkezelőtől és a jogszabályoktól kapott szűk mozgástérben meghatározhatja például, hogy milyen fajta számítógépen, mely programokkal és biztonsági intézkedésekkel tárolja és dolgozza fel az adatokat, továbbá szintén megszabhatja, hogy milyen szervezet és személyi kör végezheti a műveleteket az adatokon. Amennyiben az adatfeldolgozó az adatkezelőtől kapott és a jogszabály által megengedett határokat átlépi, adatkezelővé minősül át, annak minden kötelezettségét és felelősségét magával vonva.

4.1.3 Az internetes közvetítő szolgáltatók

Az internettel együtt az internetes közvetítő szolgáltatók szerepe is folyamatosan növekedett: a keresőszolgáltatások, szociális hálózatok, aukciós oldalak, tárhelyet és megosztást biztosító szolgáltatások nélkül az internet másmilyen lenne, mint napjainkban. Az internetes keresők nélkül a web ismeretlen része láthatatlan lenne számunkra, a közösségi szolgáltatások és a szociális hálózatok nélkül a kapcsolattartás nem működhetne a megszokott gördülékenységgel, a tárhelyet és megosztást biztosító oldalak nélkül nem helyezhetnék a felhasználók folyamatosan a felhőbe a munkájukat és a privát tartalmaikat, az online aukciós és adásvételt közvetítő oldalak pedig egyre nagyobb részét jelentik a kereskedelemnek.

Az internetes közvetítő szolgáltatók¹⁹⁶ harmadik felek között segítik elő a tranzakciókat és a kommunikációt, mely során hozzáférést biztosítanak, tárolnak, továbbítanak, indexelnek és keresést nyújtanak a harmadik felek által biztosított adatokhoz¹⁹⁷.

¹⁹⁶ 2001. évi CVIII. törvény 2. §

l) Közvetítő szolgáltató: az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely la) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);

lb) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);

lc) az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);

ld) információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);

¹⁹⁷ OECD definition of internet intermediaries: Internet intermediaries 'bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties (Source: OECD).

A közvetítőket gazdasági szempontból nézve olyan szolgáltatóknak is tekinthetjük, melyek összekötik a felhasználókat és harmadik fél szolgáltatókat a piaci igény kielégítésével, ugyanakkor értéket és piacokat is teremthetnek.

Az összekötő szerepük úgy valósul meg, hogy infrastruktúrájuk segítségével összegyűjtik, értékelik és osztályozzák a szétszórt információkat. A közvetítő szolgáltatások gyakran bizalmi szerepet is betöltenek: a felek közötti kommunikációt regisztrációhoz és személyazonosság felfedéséhez kötik, a tranzakciókat pedig nyomon követhetővé teszik a későbbi bizonyítás megkönnyítéséhez.

Különösen a kétoldalú piacokon virágzanak a közvetítő szolgáltatások online és offline: a kereskedelemben az eladó és vevő között, a marketingben a hirdető és a fogyasztó, a tartalomszolgáltatás területén a tartalomszolgáltató- és fogyasztó között. Minél többen használják a közvetítő szolgáltatásokat, azok annál nagyobb bevétellel, így infrastrukturális háttérrel és tárgyalóerővel is rendelkeznek, melyet „hálózati effektusnak” is nevezhetünk¹⁹⁸.

Egy aukciós kereskedelmi oldal (Vatera, Ebay) annál értékesebb, minél több eladó és vevő van jelen, egy közösségi hálózat (Facebook) akkor használható, ha a felhasználók ismerősei szintén tagok és meg tudják találni egymást.

Minél többen használják, annál nagyobb értékkel és használhatósággal rendelkezik a szolgáltatás, ezért a közvetítő szolgáltatók arra törekednek, hogy népes felhasználó tábort építsenek, melynek napjainkban elsősorban a fejlődő országok biztosítják a táptalajt.

Az ilyen szolgáltatások tipikusan olyan termékek, melyeket az emberek használata nem fogyaszt, nem csökkent, nem teszi nehezebben elérhetővé (non-rivalry product), így a felhasználói tábor növekedése előtt nincsen akadály. A felhasználói létszám növelése nem csak a használhatóság miatt, hanem üzleti érdekből is különösen fontos számukra, mivel a felhasználói adatbázis nagysága és részletessége váltható haszonra a hirdetési piacokon.

Az Internet egyik alapvető tulajdonsága, hogy nyitott és decentralizált, mely lehetővé teszi, hogy elméletileg bárhol a világon engedély nélkül rákapcsolódjanak¹⁹⁹. A internet fejlődésére (a kezdeti katonai fejlesztést leszámítva) jellemző, hogy az alulról felfelé építkező technológiával valósult meg, szemben a telekommunikációs szektorral, mely kormányok és vállalatok szabályozásával és támogatásával fejlődött a jelenlegi szintre. Az internet legtöbb

¹⁹⁸ Hálózati effektus alatt azt értjük, ha egy áru vagy szolgáltatás annál értékesebb, minél többen használják. Legklasszikusabb példa erre a telefon: ha 1 embernek van csak, akkor értéktelen, ha mindenkinek, akkor nagyon értékes.

¹⁹⁹ Az egyes országok törvényhozásai előírhatnak azonban feltételeket a csatlakozáshoz. Ilyen lehet például a személyes adatok megadásának szükségessége bármilyen (vezeték nélküli) hálózathoz való csatlakozás esetén.

szabványa nyitott és szabadon felhasználható²⁰⁰, mely a nyitottsággal és decentralizáltsággal megkönnyíti a közvetítő szolgáltatók színre lépését és hatékony működését.

A társadalmi és gazdasági hasznosságukat hangsúlyozó tanulmányok²⁰¹ és beszámolók az általuk közvetlenül és közvetetten teremtett munkahelyekből indulnak ki: növekvő bevételeik folytán egyre több munkavállalót alkalmaznak az internetes közvetítéssel foglalkozó cégek és sok más szektort is fellendítenek, így az online reklámpiar és a tartalomszolgáltatás különösen nagy haszonélvezője a működésüknek. Az adásvétel és az egyedi termékek értékesítése az aukciós és árfigyelő oldalaknak (pl. Vatera, Ebay, árgép.hu) köszönhetően megváltozott, mely lehetőséget nyújt a fogyasztóknak, hogy olcsóbban jussanak termékekhez és szolgáltatásokhoz, ugyanakkor az eladóknak is különösen nagy lehetőséget jelent, hogy egyedi termékeiket minél nagyobb vásárlóközönséghez juttathassák el.

Fontos megjegyezni, hogy a közvetítő szolgáltatók többféle szerepet látnak el és sokféle szolgáltatást nyújtanak, így gyakori, hogy a közvetítés mellett tartalomszolgáltató funkciójuk is van. Ilyen például, amikor az internetszolgáltató maga is kínál szerkesztett tartalmakat, az aukciós oldalak árulnak saját árut, vagy az internetes kereső saját hírszolgáltatást kínál (pl. www.msn.com, Google News). Abban az esetben, ha saját szolgáltatást közvetítenek, általában nem vonatkoznak rájuk a jogszabályi kivételek és mentességek a tartalomért való felelősség tekintetében.²⁰²

A közvetítő szolgáltatók szerepei között sok esetben komoly ellentét tapasztalható: a magánszféra és a felhasználók bizalmának védelme és a személyre szabott szolgáltatások és célzott marketing nehezen férnek meg egymás mellett.

Dolgozatomban különösen a közösségi hálózatok és az internetes keresők szempontjából közelítem meg a kérdést.

A közvetítő szolgáltatók osztályozása

Az Interneten jelenlévő szolgáltatások sokfélesége miatt többféle osztályozás is született velük kapcsolatosan, azonban kizárólag közvetítő szolgáltatásokra koncentrálva az alábbi osztályozást, mivel az uniós jogszabályok is a kivételeket e mentén állapítják meg.

²⁰⁰ pl. TCP (Transmission Control Protocol) A TCP két különböző számítógépen futó programok között az adatfolyam megbízható, sorrendhelyes átvitelét hivatott biztosítani.

²⁰¹ The Economic and Social Role of Internet Intermediaries, OECD, 2010. 04. 6.

²⁰² 2000/31/EK irányelv 12 – 14. §

A céljaikat tekintve a legjelentősebb közvetítő szolgáltatók lehetnek Internetes szolgáltatást nyújtók (Internet Service Providers), web hosting szolgáltatók, internetes keresők, online kereskedelmi és aukciós oldalak, fizetési rendszerek, közösségi hálózatok.

Az internetes szolgáltatást nyújtók (Internet service providers) olyan szolgáltatókat érthetünk, melyek infrastruktúrájuk segítségével vezetékes vagy vezeték nélküli Internet hozzáférést biztosítanak előfizetőik számára. Amennyiben egyéb szolgáltatásokat is biztosítanak (pl. GPS, tartalomszolgáltatás), azok eltérő szabályozás alá esnek.

Web hosting szolgáltatásokat web tárhely szolgáltatásnak fordíthatjuk, mely alatt olyan szolgáltatást érthetünk, mely során az igénybe vevő egy szerverből kap a használatra egy eszmei hányadot, melyen saját weblapot, levelezőrendszert és egyéb web alapú szolgáltatást működtethet²⁰³. A szerver az adott honlapot egy IP cím alatt tárolja, melyre a domain név (pl. www.sony.hu) irányít el. Leggyakrabban egy számítógép (szerver) több weboldalnak biztosít helyet, azonban nagyobb oldalak esetén (pl. Google, Facebook) akár több ezer szerver is szükséges lehet egy oldal kiszolgálásához.

A web tárhely szolgáltatója tehát az elérhetőséget biztosítja a tartalomhoz, melynek szerkesztője általában eltérő személy.

Az internetes keresők feltérképezik, majd indexelik és a felhasználó számára kereshetővé teszik a más szolgáltatók által készített tartalmakat.

Az online kereskedelmi és aukciós oldalak harmadik felek által értékesítésre felkínált termékeknek az eladásra kínálásához nyújtanak segítséget. Alapesetben a termékeket nem ők gyártják, nem ők értékesítik (pl. Ebay). A legnagyobb kereskedelmi oldalak azonban a kialakult piaci helyzetükből adódóan saját maguk is eladóvá válnak, mivel a helyzetüket előnyösebbé tudják tenni azáltal, hogy a saját termékeiket előbbre sorolják a találatok között (pl. Amazon).

Az internetes fizetési rendszerek (Visa, PayPal) is közvetítő szerepet töltenek be a bankok, az ügyfelek és a fizetés címzettjei között.

A közösségi hálózatok a felhasználók számára lehetővé teszik kapcsolatok építését és tartalom megosztását (pl. Facebook, Myspace).

²⁰³ <http://www.techterms.com/definition/webhost>

4.1.4 Az internetes kereső fogalma és működése

„Az emberiség legelőször az alexandriai könyvtárban igyekezett egy időben és helyen összegyűjteni minden fellelhető emberi tudást. A legutóbbi próbálkozás? A Google”

Brewster Kahle, az Internet Archive alapítója

Az internetes keresők működését leegyszerűsítve 3 fázisra bonthatjuk. Az első szakaszban keresőrobotok (crawl) – melyek az internet végigbongészésére használt programok – végigpásztázzák az internetet oldalról oldalra, majd az összegyűjtött információkat összegyűjtik egy adatbázisba (index), mely a második fázist jelenti annak tartalmával. A harmadik fázis az adatbázis elérése az internetes kereső felületén keresztül (runtime system).

Az internetes keresők által nyújtott szolgáltatás az Európai Unióban információs társadalommal összefüggő szolgáltatásnak²⁰⁴ tekinthető, mely *„általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás.”*

A fogalmi elemek közül az *„általában térítés ellenében”* alapján lehet ingyenes és ellenszolgáltatás fejében nyújtott a szolgáltatás. Az *„általában”* szóval azért tette a jogalkotó gyakorlatilag elhagyhatóvá a fogalmi elemet, mert a gazdasági modellek közül leginkább az a megoldás került előtérbe az interneten, hogy az ingyenes szolgáltatásért a szolgáltató a reklámokból szerez bevételt, melyet a felhasználó személyes adataival növel meg.

A *„távolról”* azt jelenti, hogy a szolgáltatást a felek egyidejű jelenléte nélkül nyújtják, így nem minősül *„távolról”* nyújtott szolgáltatásnak, amelyet a szolgáltató és a szolgáltatást igénybe vevő fizikai jelenlétében nyújtanak, még ha ehhez elektronikus eszközt is vesznek igénybe. Ilyen például a repülőjegy foglalása az utazási irodában, melyet hiába végeznek online, ha az ügyfél személyesen jelen van az irodában.

„Elektronikus úton” azt értjük, hogy a szolgáltatás kezdőpontjától való elküldése és célállomásán való fogadása és tárolására elektronikus berendezés útján történik, valamint annak elküldése, továbbítása és vétele teljes egészében vezetéken, rádión, optikai vagy egyéb elektromágneses eszköz útján zajlik le.

Nem *„elektronikus úton”* nyújtott szolgáltatások az anyagi tartalommal bíró szolgáltatások, még ha elektronikus eszközök útján nyújtják is őket, így a készpénz- vagy jegykiadó automatákkal (bankjegyek, vasúti jegyek) végrehajtott tranzakciók nem minősülnek annak. Az olyan szolgáltatások sem tartoznak bele ebbe a körbe, amelyeket nem elektronikus

²⁰⁴ 98/48/EK irányelv által módosított 98/34/EK irányelv 1. cikkének (2) bekezdése szerinti szolgáltatások

feldolgozó/nyilvántartó rendszerek útján nyújtanak (pl. távbeszélő szolgáltatások, telefax/telex szolgáltatások).

A "szolgáltatást igénybe vevő egyéni kérelmére" azt jelenti, hogy az adatok továbbításával nyújtott szolgáltatás egyéni kérelemre történik, így az egyéni kérelem nélkül, adatátvitel útján, korlátlan számú egyéni igénybevevő részére egyidejűleg nyújtott szolgáltatások (egy pontról több pontra történő átvitel) nem minősülnek annak. Ilyennek tekinthető például a rádiós műsorszórás.²⁰⁵

Fontos kiemelni, hogy az információs társadalommal összefüggő szolgáltatások nem korlátozódnak csupán azokra a szolgáltatásokra, amelyek on-line szerződéskötést eredményeznek, hanem olyan szolgáltatásokat is magukban foglalnak, amelyekért az igénybe vevők nem fizetnek. Ilyen szolgáltatások tipikusan az internetes információs szolgáltatás és kereskedelmi tájékoztatás, vagy az adatok kereséséhez és az azokhoz való hozzáféréshez vagy azok visszakereséséhez eszközt nyújtó szolgáltatások²⁰⁶. Az információs társadalommal összefüggő szolgáltatások olyan szolgáltatásokat is magukban foglalnak, amelyek adatok hírközlő hálózaton keresztüli továbbításából, vagy egy hírközlő hálózathoz való hozzáférés biztosításából, vagy a szolgáltatás igénybe vevője által rendelkezésre bocsátott adat számára tárhely szolgáltatásából állnak.²⁰⁷

Az információs társadalommal összefüggő szolgáltatások szabad mozgása sok esetben egy általánosabb elv egyedi megnyilvánulása lehet a közösségi jogban, nevezetesen a véleménynyilvánítás szabadságáé, amelyről a minden tagállam által ratifikált, az Emberi jogok és alapvető szabadságok védelméről szóló egyezmény 10. cikkének (1) bekezdése rendelkezik.

Internetes keresők és az adatvédelmi jog kapcsolata az Európai Unióban

Az internetes keresőszolgáltatások biztosíthatóak az EU területén kívülről, és az EU területén belülről egy, vagy több tagállam területéről.

²⁰⁵ 98/48/EK irányelv által módosított 98/34/EK irányelv V. melléklet

²⁰⁶ 2000/31/EK irányelv (18)

²⁰⁷ A 89/552/EGK irányelv szerinti televízióműsor-terjesztés és a rádióműsor-terjesztés nem minősül az információs társadalommal összefüggő szolgáltatásnak, mivel nem egyedi kérelemre nyújtják; ezekkel ellentétben információs társadalommal összefüggő szolgáltatások a ponttól pontig történő adatátvitel révén megvalósuló szolgáltatások, mint például a megrendelt videoszolgáltatás vagy a kereskedelmi tájékoztatás elektronikus levélben történő küldése.

Amennyiben egy – vagy több - tagállam területén letelepedett²⁰⁸ szolgáltató biztosítja a kereső szolgáltatást, abban az esetben egyértelműen az adatvédelmi irányelv alapján megalkotott nemzeti adatvédelmi törvények alkalmazandóak²⁰⁹. A letelepedés fogalma tágan értelmezendő: bármilyen jogi formában – helyi iroda, leányvállalat, képviselő ügynökség – lehetséges. Ha a szolgáltató az EU területén kívülről nyújtja a szolgáltatást, abban az esetben akkor alkalmazható a tagállam adatvédelmi törvénye, ha a területén található berendezéssel történik az adatok feldolgozása.

Az adatvédelmi irányelv hivatalos magyar fordítása nem fogalmaz pontosan, mivel nem tartalmazza az angol nyelvű szövegben²¹⁰ szereplő „tagállam területén letelepedett szolgáltató” (establishment of the controller on the territory of the Member State) kifejezést, helyette „tagállam területén az adatkezelő egy szervezete tevékenységeinek keretében végzik” fordítást használja, mely nem egyértelmű.

Szintén magyarázatra szorul „az adatfeldolgozást a tagállam területén az adatkezelő egy szervezete tevékenységeinek *keretében* végzik” megfogalmazás, melynek magyar fordítása pontatlan (the processing is carried out *in the context* of the activities of an establishment of the controller on the territory of the Member State). Az „in the context” a „keretében” szónak van fordítva, mely azt szükségtelenül szűkíti, az „összefüggésben”, vagy „avval kapcsolatosan” szerencsésebb lenne.

²⁰⁸ 2000/31/EK Irányelv (19) A szolgáltató letelepedésének helyét a Bíróság esetjogával összhangban kell meghatározni, amely szerint a letelepedés fogalma állandó telephelyen, határozatlan ideig ténylegesen végzett gazdasági tevékenységet foglal magában; ez a követelmény abban az esetben is teljesül, ha egy vállalkozást határozott időre hoznak létre; a szolgáltatásait egy internetes weboldalon keresztül nyújtó vállalkozás telephelye nem az a hely, ahol a weboldalát támogató technológia található, és nem az a hely, ahol weboldala hozzáférhető, hanem az a hely, ahol gazdasági tevékenységét végzi; ha egy szolgáltatónak több telephelye van, fontos annak meghatározása, hogy az adott szolgáltatást mely telephelyről nyújtja; ha nehéz meghatározni, hogy a több telephely közül melyikről nyújtanak egy adott szolgáltatást, azt a helyet kell a szolgáltatásnyújtás helyének tekinteni, ahol a szolgáltató adott szolgáltatással kapcsolatos tevékenységeinek a központja van.

(57) A Bíróság következetes ítélkezési gyakorlata szerint a tagállam fenntarthatja magának a jogot, hogy intézkedéseket tegyen olyan szolgáltató ellen, aki, illetve amely másik tagállamban telepedett le, de tevékenysége teljes egészében vagy nagy részben az előbbi tagállam területére irányul, ha a letelepedés helyét azzal a céllal választotta, hogy kikerülje azokat a jogszabályokat, amelyek akkor vonatkoztak volna rá, ha az előbbi tagállam területén telepedett volna le.

²⁰⁹ Adatvédelmi Irányelv 4. cikk (1) A személyes adatok feldolgozására minden tagállam az ezen irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza, amennyiben:

a) az adatfeldolgozást a tagállam területén az adatkezelő egy szervezete tevékenységeinek keretében végzik; amennyiben ugyanaz az adatkezelő több tagállam területén is letelepedett, meg kell tennie a szükséges intézkedéseket annak biztosítása érdekében, hogy szervezeteinek mindegyike megfeleljen az alkalmazandó nemzeti jog által megállapított kötelezettségeknek;

²¹⁰ Data protection Directive, Article 4. (1) Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

Az eredeti szövegben a hangsúly azon van, hogy az adatfeldolgozás és a letelepedett szervezet tevékenysége között valamilyen *kapcsolat, összefüggés* („in the context”) létezik, melyet szintén tágan kell értelmezni. Így annak minősül, ha a letelepedett szervezet a szolgáltató és a felhasználók közötti kapcsolattartást valósítja meg (pl. ügyfélszolgálat), vagy a reklámozással kapcsolatban teljesíti a kéréseket és fogadja a kifizetéseket (pl. célzott reklámozás megvalósítása Google esetében ügynökségen keresztül), vagy a tagállami bíróságok és egyéb hatóságok határozataival kapcsolatos kéréseket és kötelezettségeket teljesíti (pl. adatok kiszolgáltatása bírósági végzések, vagy titkosszolgálati megkeresések esetén).

A másik lehetőség az uniós adatvédelmi normák alkalmazására, ha a keresőszolgáltató bár nincsen letelepedve egyik tagállamban sem, de ott használ fel berendezést a személyes adatok feldolgozására.²¹¹

A fordítás szintén pontatlan, mivel az irányelv magyar fordításban „személyes adatok feldolgozása céljából gépi vagy más olyan *„eszközt alkalmaz”* szerepel, mely azt sugallja, hogy a szolgáltató a saját tulajdonú berendezést alkalmaz, vagy valamilyen szerződés alapján használati jogosultsággal rendelkezik a berendezés felett (pl. szerverfarmot bérel).

Az eredeti szövegben azonban úgy szerepel, hogy „berendezést felhasznál” („*makes use of equipment*”²¹²), amely tágabb kategóriát jelent, melyet a joggyakorlat és a 29. cikk szerinti Adatvédelmi Munkacsoport által kiadott iránymutatások is alátámasztanak.²¹³

Berendezés felhasználásába a szerverpark felhasználásán túl olyan tevékenység is beleillik, mely során a szolgáltató a felhasználó berendezését (pl. számítógép, tablet, okostelefon) használja fel adatok feldolgozására, így berendezés felhasználásának minősül, ha olyan cookiet alkalmaz a felhasználó eszközén, mely adatokat gyűjt, dolgoz fel, és/vagy továbbít, melynek következtében szinte az összes keresőszolgáltatóra alkalmazhatóak az EU adatvédelmi normái. Az adatvédelmi rendelet a jogelkerülést és a felhasználók jogainak védelmét szem előtt tartva a hatályát kiterjeszti minden olyan adatfeldolgozásra, mely során az Európai Unióban lakóhellyel rendelkező érintett személyes adatait dolgozzák fel, továbbá a műveletek termékek

²¹¹ Adatvédelmi Irányelv 4. cikk (1) A személyes adatok feldolgozására minden tagállam az ezen irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza, amennyiben:

c) az adatkezelő nem telepedett le a Közösség területén, és a személyes adatok feldolgozása céljából gépi vagy más olyan eszközt alkalmaz, amely a fenti tagállam területén található, kivéve, ha ezt az eszközt kizárólag a Közösség területén átmenő adatforgalom céljára használják.

²¹² Data protection Directive, Article 4. (1) Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

²¹³ Article 29 Data Protection Working Party: opinion 1/2008 on data protection issues related to search engines, 2008. 04. 04.

vagy szolgáltatások nyújtásával, vagy az érintett viselkedésének nyomon követésével kapcsolatosak.²¹⁴

A keresőszolgáltatók programjai feltérképezik és végigkutatják az internetet, majd a gyorsítótárba (cache) lementik az adatokat. A lementett adatok között személyes adatok is találhatóak. Az adatvédelmi irányelv nem tartalmaz speciális rendelkezéseket az olyan információs társadalommal összefüggő szolgáltatásokra, melyek közvetítőként vesznek részt az adatok továbbításában.

Az adatvédelmi irányelv rendelkezései az adatkezelőkre alkalmazandóak, így az a kérdés, hogy a keresőszolgáltatók annak minősülnek-e, és amennyiben igen, az eredeti tartalomszolgáltatóval (melynek a tartalmát begyűjtötték a gyorsítótárba) közös kezelőnek minősülnek-e. A 29-es Munkacsoport szerint a keresőszolgáltatók az arányosság elve alapján nem tekinthetők elsődleges adatkezelőknek abban az esetben, ha csupán közvetítőként összegyűjtik és keresésre bocsátják az adatokat.²¹⁵

A keresőszolgáltatók kontrollja az adatok felett elsősorban arra terjed ki, hogy a találatok közül eltávolítsák vagy blokkolják a személyes adatokat, melyek adatkezelői jogosultságoknak is tekinthetők, azonban az eltávolításra való kötelezettségeik tagállamonként különbözhetnek.

A keresőszolgáltatók sok esetben nem tekinthetők csak közvetítőnek: a Google például a web egy részét szerverein lementve tárolja (melyeket sokszor gyorsabban ér el a hálózat, mint a valódi oldalt).

Az weblapoknak – melyeken a tartalom eredetileg publikálásra kerül – van lehetőségük megakadályozni, hogy a keresőszolgáltatók információkat gyűjtsenek: használhatnak olyan parancsokat, melyek megtiltják a keresőrobotok működését.

Ugyanakkor a keresőszolgáltató is hatékony eszközökkel rendelkezik, hogy a személyes adatok gyűjtését korlátozza vagy megakadályozza: a nevek, címek (földrajzi és elektronikus levél cím), személyi számok, telefonszámok jellegzetes formátumuk miatt könnyedén automatikusan kiszűrhetők. A technológia fejlődése lehetővé teszi személyes adatok pontosabb válogatását, melyre példa az arcfelismerő technológia a képek feldolgozása során, így hamarosan elérhetővé válhat valamely személy kiszűrése a képtalálatok közül is.

²¹⁴ Adatvédelmi rendelet, 3. cikk Területi hatály

(2) E rendeletet kell alkalmazni a nem az Unióban letelepedett adatkezelő által végzett, az Unióban lakóhellyel rendelkező érintettek személyes adatainak feldolgozására, ha a feldolgozási tevékenységek

a) termékek vagy szolgáltatások ilyen érintettek számára történő nyújtásához kapcsolódnak; vagy

b) viselkedésük nyomon követéséhez kapcsolódnak.

²¹⁵ Article 29 Data Protection Working Party: opinion 1/2008 on data protection issues related to search engines, 2008. 04. 04., 14.

Az adatvédelmi irányelv és az internetes keresők

Az adatvédelmi irányelv alapján megszületett nemzeti szabályozások alapelveként várják el az adatkezelőktől, hogy az adatkezelés jogos céllal rendelkezzen, így az adatok gyűjtése kizárólag valamely meghatározott és törvényes célból valósulhat meg.

Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, továbbá a szükségesség elve alapján csak olyan személyes adat kezelhető, mely a cél megvalósulásához elengedhetetlen. A tárolás idejével kapcsolatban alapvető szabály, hogy a személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.²¹⁶

A legnagyobb keresőszolgáltatók használhatóak regisztrált felhasználóként és névtelenül is. A regisztráció során a felhasználó elfogadja a felhasználási feltételeket, mely során hozzájárul a személyes adatai kezeléséhez az abban meghatározott célokra és időtartamra. A névtelenül – regisztráció nélkül - szolgáltatást igénybe vevő felhasználók adatait azonban a szolgáltató nem tárolhatja és használhatja fel az aktuális keresés célján túl.²¹⁷

A keresőszolgáltatók olyan célokat adnak meg a feldolgozás alapjának, mint például a szolgáltatás minőségének, vagy biztonságának növelése. A Google esetében²¹⁸ például a találatok nem lehetnének ennyire pontosak, ha nem ismernék a felhasználó korábbi keresési szokásait. A kevés rákeresett szóból és információból nem tudná a kereső kitalálni a felhasználó kívánságát és érdeklődését.

²¹⁶ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 4. § (1) – (4)

²¹⁷ Adatvédelmi irányelv, 7. cikk

A tagállamok rendelkeznek arról, hogy a személyes adatok csak abban az esetben dolgozhatók fel, ha:

a) az érintett ahhoz egyértelmű hozzájárulását adta; vagy
b) 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
f) 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 az 1. cikk (1) bekezdése értelmében védelmet élvező érdekei az alapvető jogok és szabadságok tekintetében.

²¹⁸ Google adatvédelmi irányelve (2014. 11. 12.): Adatvédelmi Szolgáltatásainkat több, különféle módon használhatja – információk keresésére és megosztására, a másokkal való kommunikációra vagy új tartalom létrehozására. Azáltal, hogy Ön információkat oszt meg velünk, például egy Google Fiók létrehozásakor, mi még hatékonyabbá tudjuk tenni szolgáltatásainkat, ezáltal Önnek még pontosabb keresési eredményeket és hirdetéseket tudunk bemutatni, fel tudjuk gyorsítani és meg tudjuk könnyíteni a másokkal való kapcsolatfelvételt és a másokkal történő megosztását

A Majestic Research által készített felmérés alapján a felhasználók fele csupán 2-3 szót gépel be a keresőbe, míg 20%-uk csak 1 szót, és 5%-uk használhatna több szót vagy részletes keresést.²¹⁹

A Munkacsoport állásfoglalása ugyanakkor kiemeli, hogy a felhasználó személyének azonosítása nem szükséges a szolgáltatás színvonalának növeléséhez, mivel névtelenül is lehetséges egy felhasználó keresési szokásainak nyilvántartása és azokat csupán egy anonimizált azonosító kódhoz kötni, tehát a rendszernek elég tudnia, hogy az érintett személy mire keresett rá eddig, de a nevét és egyéb személyes adatait nem szükséges tárolnia.

Evvel a véleménnyel a szolgáltatók nem értenek egyet, mivel a felhasználó nemzetiségének, nemének és korának ismerete szignifikánsan növeli az érdeklődési kör feltérképezését és a találatok hatékonyságát.

Érdekesen hangzik a személyes adatok védelmének biztosítása még több személyes adat gyűjtésével. Minél több azonosító adat áll a szolgáltatást nyújtó rendelkezésére, annál bonyolultabb és egyben biztonságosabb, megerősítéssel rendelkező beléptetési és hitelesítési rendszer hozható létre.

A hirdetési piacon elkövetett csalás elleni védelem is alapot szolgáltat az adatok megőrzésére.

Az internetes hirdetési modellek mellett több módszer is elterjedt, hogy azokból csalogók illegális haszonra tegyenek szert. Ilyen módszer például a klikkelési csalás: a hirdetésre való klikkelés után fizet a hirdető a szolgáltatónak, azonban a rendszert könnyen lehet manipulálni, amennyiben egy programmal folyamatosan kattintatnak a megjelenő hirdetésre, így a hirdető valós megtekintések nélkül fizet a klikkelések után a szolgáltatónak. Ebből a módszerből elsősorban a közvetítő reklámügynökségek juthatnak haszonhoz. Ezt a fajta csalást könnyen ki lehet szűrni például a cookie-k és IP címek tárolásával: a szolgáltató nyomon tudja követni, hogy egy eszközről hányszor kattintottak valamely hirdetésre, kiszűrve a gyanús sokat kattintókat. Véleményem szerint ebben az esetben is szükséges lenne csak a minimális mennyiségű adatok felhasználása a csalások megelőzése érdekében, vagy egyéb biztonsági módszerek kidolgozása a felhasználó monitorozása helyett.

A könyvelésre is gyakran hivatkoznak internetes cégek a személyes adatok megőrzése esetén, azonban a Munkacsoport állásfoglalása rámutatott, hogy ahhoz - még ha szükséges is a felhasználók száma - azonosíthatóságuk nem releváns.

²¹⁹ Battelle, 2006, 29.

A jogi okokból is szükség lehet az adatok megadására. Az interneten megvalósuló bűncselekmények visszaszorítása csak úgy lehetséges, ha a felhasználókról olyan személyes adatok állnak rendelkezésre, amely alapján tevékenységük nyomon követhető.

A bűnüldöző hatóságok is rendszeresen megkeresik a szolgáltatókat, továbbá bírósági végzésekből is kötelezni próbálják őket felhasználói adatok kiadására. Az eljárások és a kormányokkal való együttműködések országonként változhatnak, azonban a felhasználók adatainak hosszabb tárolására jogalapot nem adhat a bűnüldözés, mivel minél nagyobb és hosszabb ideig tárolt egy adatbázis, annál nagyobb kisértést adhat a hatóságoknak és másoknak, hogy céljaikra és érdekeikre felhasználják.

A Munkacsoport véleménye szerint az adatkezelés jogalapjai nincsenek eléggé kimerítően és részletesen kidolgozva. A „felhasználói élmény javítása” és a „biztonság növelése” annyira tág meghatározások, hogy nehezen biztosítják a határozottság követelményét.

Fontos követelmény továbbá, hogy a személyes adatok kezelése általában akkor lehetséges, ha ahhoz az érintett hozzájárult, vagy azt jogszabály engedélyezi.²²⁰

A felhasználók személyes adatainak a feldolgozásához jogalapot adhat továbbá, ha azokat szerződés teljesítése céljából szükséges kezelni. Így például, amikor egy online turisztikai oldalon foglalnak a felhasználók repülőjegyet, akkor a szerződés teljesítése céljából tovább kell küldenie a szolgáltatónak az adatokat harmadik feleknek (pl. légitársaság, bevándorlási hivatalok). A keresőszolgáltatóknál azonban csak korlátok között alkalmazható ez a kivétel.

A Google az általános szerződési feltételekben rendelkezik arról, hogy a személyes adatokat és a felhasználó által feltöltött tartalmakat egyéb célokra is felhasználja. A célok között szerepel a felhasználó által igényelt szolgáltatás megfelelő szintű biztosítása, amely alatt érthetjük a szerződés teljesítéséhez szükséges adatkezelést is, mivel olyan tágan fogalmaz, hogy a megfelelő információ birtokában hozott konkrét hozzájárulásról nehezen beszélhetünk²²¹.

Jogalként szolgálhat az adatkezelésre továbbá az adatkezelő jogos érdeke, amelyet szűken kellene értelmezni.²²² A Google esetében a bűncselekmények megelőzése körében

²²⁰ 2011. évi CXII. törvény 5. § (1) Személyes adat akkor kezelhető, ha

a) ahhoz az érintett hozzájárult, vagy

b) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).

²²¹ Google ÁSZF (2014. 11. 12.): Automatizált rendszereink elemzik az Ön tartalmait (beleértve az e-maileket is), hogy személyre szabott termékfunkciókat kaphasson, például egyéni keresési eredményeket, testreszabott hirdetéseket, illetve a spamek és rosszindulatú programok észlelését. Ez az elemzés a tartalom elküldésekor, fogadásakor és tárolása során történik.

²²² EC study on implementation of data protection directive (Study Contract ETD/2001/B5-3001/A/49) comparative summary of national laws by Douwe Korff (consultant to the European Commission), Human Rights Centre, University of Essex, Cambridge, 2002. 09, 80.

alkalmazható a lényeges jogos érdek, amely során a feltöltött adatok kerülnek vizsgálat alá és szükség esetén eltávolításra.

Elméletileg tehát a keresőszolgáltatók nem tárolhatnák tovább a felhasználók adatait a cél eléréséhez szükséges időnél, azonban a mindennapi gyakorlat felülírta ezt az alapelvet: a hatékonyabb találatok és nagyobb nyereség elérése érdekében a szolgáltatók a felhasználók hozzájárulásával akár hosszabb távon is tárolhatják a személyes adatokat.

Az elektronikus kereskedelmi irányelv

Az adatvédelmi irányelv és a keresőszolgáltatók kapcsolatánál már említésre került, hogy a cookie-k használata maga után vonja az irányelv hatályát.

Hasonló a helyzet az elektronikus kereskedelmi irányelv esetében is, mivel az ilyen eszközök, például az azonosításra szolgáló kódsorozatok – a cookie-k - törvényes és hasznos eszközök lehetnek a honlap tervezés és a hirdetések hatékonyságának elemzése terén, valamint az on-line ügyletekben résztvevő felhasználók azonosításakor.

Amennyiben az ilyen eszközöket, a szolgáltatások nyújtásának megkönnyítésére szánják, használatuk azzal a feltétellel engedélyezhető, hogy a szolgáltatók az adatvédelmi irányelvnek megfelelően a cookie, illetve hasonló eszközök céljáról egyértelmű és pontos tájékoztatást adnak a felhasználóknak annak érdekében, hogy a tudomásuk legyen az általuk használt végberendezésen elhelyezett adatokról.

Az ilyen esetekben a felhasználók részére lehetőséget kell biztosítani arra, hogy megtagadhassák a cookie-k vagy hasonló eszközök végberendezésükön történő tárolását, mely különösen fontos, ha más felhasználók is hozzáférhetnek a felhasználó végberendezéséhez, és ezáltal bármely, azon tárolt magánjellegű adathoz is. A felhasználó végberendezésére telepítendő különféle eszközök használatára vonatkozó tájékoztatás és a megtagadás joga egy csatlakozás alkalmával egyszer ajánlható fel, mely kiterjedhet az ilyen eszközök későbbi csatlakozások során történő használatára is.²²³ Egyes honlap tartalmakhoz való hozzáférést

²²³ 2002/58/EK irányelv 5. cikk (3) A tagállamok gondoskodnak arról, hogy az elektronikus hírközlő hálózatoknak egy előfizető vagy felhasználó végberendezésében történő adattárolásra való felhasználása, illetve az ott tárolt adatokhoz való hozzáférésre való felhasználása csak azzal a feltétellel legyen megengedett, ha az érintett előfizetőt vagy felhasználót a 95/46/EK irányelvvel összhangban egyértelműen és teljes körűen tájékoztatják - többek között - az adatkezelés céljairól, valamint ha az érintett előfizetőnek vagy felhasználónak joga van visszautasítani az adatkezelő által végzett ilyen adatkezelést. Ez a rendelkezés nem akadályozza az olyan műszaki tárolást, illetve műszaki hozzáférést, amelynek kizárólagos célja az elektronikus hírközlő hálózaton keresztül történő közléstovábbítás vagy annak megkönnyítése, vagy amely az előfizető vagy felhasználó által kifejezetten kért, információs társadalommal összefüggő szolgáltatás nyújtásához feltétlenül szükséges.

valamely cookie-nak vagy hasonló eszköznek a helyzet teljes ismeretében kinyilvánított elfogadásához lehet kötni, amennyiben az ilyen eszközt törvényes célból használják.²²⁴

A keresőszolgáltatásokra relevánsak még az irányelv kéréstlen kereskedelmi tájékoztatással kapcsolatos rendelkezései, melyek alapján az elektronikus levelek közvetlen üzletszerzési célból történő használata kizárólag az ahhoz előzetesen hozzájáruló előfizetők vonatkozásában lehetséges. Annyi enyhítést tesz a szolgáltatók felé az irányelv, hogy amennyiben az adatkezelő elektronikus levelezés céljából szerzi meg az ügyfeleitől az elektronikus elérhetőségi adataikat egy termék vagy szolgáltatás értékesítése során, ugyanaz a természetes vagy jogi személy ezeket az elektronikus elérhetőségi adatokat felhasználhatja saját hasonló termékeivel vagy szolgáltatásaival kapcsolatos közvetlen üzletszerzési célra, abban az esetben, ha az ügyfelek számára - az adatok gyűjtésekor és minden egyes üzenet küldésekor, amennyiben az ügyfél az ilyen felhasználást első alkalommal nem tagadta meg - lehetőséget biztosít arra, hogy az elektronikus elérhetőségi adatok ilyen célú felhasználása ellen díjmentes és egyszerű módon kifogással élhessenek.

Általánosságban kijelenthető volt az EU Bíróságának „Google Spain” ítéletéig, hogy a keresőszolgáltatás nem esik az adatmegőrzési irányelv hatálya²²⁵ alá, mivel a keresett szavak tartalomnak tekinthetők, nem pedig forgalmi adatnak.

A keresőszolgáltatók és az elektronikus hírközlési szolgáltatások kapcsolata

A keresőszolgáltatókról általánosságban ki lehet jelenteni, hogy nem esnek az elektronikus hírközlési irányelv hatálya alá.²²⁶

Az elektronikus hírközlési szolgáltatás lényege jelek átvitelében, továbbításában fogható meg. Az elektronikus hírközlési szolgáltatók jelként továbbítják a fogadó fél részére telefon esetén a hangot, televízió esetén a képet és a hangot, valamint az internet vonatkozásában az adattömeget, miközben a jelek előállításában nem vesznek részt.²²⁷

²²⁴ 2002/58/EK irányelv (25)

²²⁵ 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről
5. cikk (2) Ezen irányelv alapján a közlés tartalmát felfedő adat nem őrizhető meg.

²²⁶ 2002/58/EK irányelv ("Elektronikus hírközlési adatvédelmi irányelv")

(12) Ez az irányelv nem keletkeztet a tagállamok számára kötelezettséget arra vonatkozóan, hogy kiterjesszék a 95/46/EK irányelv alkalmazását a jogi személyek jogos érdekeinek védelmére, amely a hatályos közösségi és nemzeti jogszabályok keretén belül biztosított.

²²⁷ Nemzeti Fogyasztóvédelmi hatóság, Elektronikus hírközlési szolgáltatások köre, 2012.01.31.

http://www.nfh.hu/magyar/hasznos/szolg/hirkozles/hirkozles_2

Az elektronikus hírközlési szolgáltatásokat általánosságban három nagy területre lehet felosztani: telefonszolgáltatás, rádió- és televízió-műsorelosztás, valamint internet hozzáférési szolgáltatás.

Az irányelv is kiemeli, hogy nem minősül elektronikus hírközlési szolgáltatásnak a tartalomszolgáltatás, vagy ilyen tartalom felett bármilyen szerkesztési jogot biztosító szolgáltatás, így például műsor készítése vagy internetes újság szerkesztése.²²⁸ Nem alkalmazható az irányelv továbbá a tárhelyszolgáltatókra és az egyéb internetes szolgáltatásokat nyújtó vállalkozásokra (pl. webáruházak).

A keresőszolgáltató azonban biztosíthat a felhasználók számára olyan szolgáltatást, mely a hírközlési és az adatmegőrzési irányelv hatálya alá esik. Ilyen szolgáltatás lehet egy elektronikus levelező szolgáltatás, mellyel a legnagyobb internetes keresőszolgáltatók rendelkeznek: Googlenak a Gmail, Microsoftnak a Hotmail, Yahoónak a Yahoo mail.

Az elektronikus levelezéssel kapcsolatban fontos tisztázni, hogy milyen mértékben tekinthető információs társadalommal összefüggő szolgáltatásnak, mely magával vonja az avval kapcsolatos kötelezettségeket. Az elektronikus kereskedelemről szóló irányelv bevezetése szerint nem információs társadalommal összefüggő szolgáltatás az elektronikus levelezés vagy azzal egyenértékű egyéni kommunikációs eszköz használata, ha azt kereskedelmi, üzleti vagy szakmai tevékenységükön kívül eljáró természetes személyek veszik igénybe, ideértve az ilyen személyek közötti szerződéskötés céljából történő használatot is. Kiemeli az irányelv továbbá, hogy a munkavállaló és munkáltatója közötti szerződéses jogviszony nem információs társadalommal összefüggő szolgáltatás.²²⁹

A közvetítő szolgáltatók felelőssége

Az online tartalmakért való felelősség kérdése több jogterületen is komoly kérdéseket vet fel: az ipari titkok, szellemi alkotások, személyes adatok védelme és a jogsértések felelőseinek megnevezése és megítélése nem egységes a világ országaiban.

²²⁸ 2002/21/EK, 2. cikk c) „elektronikus hírközlési szolgáltatás”: olyan, általában díjazás ellenében nyújtott szolgáltatás, amely teljes egészében vagy nagyrészt elektronikus hírközlő hálózaton történő jelátvitelből áll, beleértve a műsorterjesztő hálózatokon nyújtott távközlési szolgáltatásokat és átviteli szolgáltatásokat, de nem foglalja magában az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások segítségével történő tartalomszolgáltatást, illetve az ilyen tartalom felett szerkesztői ellenőrzést biztosító szolgáltatásokat; nem foglalja magában a 98/34/EK irányelv 1. cikkében meghatározott olyan, információs társadalommal összefüggő szolgáltatásokat, amelyek teljes egészében vagy nagyrészt nem elektronikus hírközlő hálózaton történő jelátvitelből állnak;

²²⁹ 2000/31/EK irányelv (18)

Kérdés, hogy felelősnek tekinthetőek-e a csupán közvetítő szolgáltatók: a másolt DVD adásvételét lehetővé tevő internetes kereskedő portál (pl. Vatera, Ebay), a jogsértő tartalmak keresésében nélkülözhetetlen internetes kereső (pl. Google) és személyiségi jogokat megsértő fényképek közzétételét lehetővé tevő közösségi oldalak (Facebook, Myspace), melyek a tartalmak szállítását nem kezdeményezik, annak tartalmát nem határozzák meg, a címzettet nem választják ki, milyen jogalapon és milyen mértékben tekinthetőek felelősnek²³⁰.

A közvetítő szolgáltatók felelősségével kapcsolatosan 3 féle modellt különböztethetünk meg: a szigorú (objektív) felelősséget, a „safe harbor”-t és a teljes immunitást határolhatjuk el egymástól, melyek között természetesen léteznek átmeneti rendszerek.

A szigorú – mondhatjuk objektív – felelősségi modell leginkább olyan országokban található, ahol az állam kontrollálja a sajtót és a szólásszabadság sem alapvető érték (pl. Kína). Ebben az esetben a közvetítő szolgáltató közvetlenül felelős a tartalomért, függetlenül attól, hogy tudott-e annak jogsértő jellegéről, így az ilyen modell mellett a közvetítő szolgáltatónak folyamatosan ellenőriznie – cenzúráznia – kell a rajta átfolyó tartalmakat. A jogsértésnek komoly büntető- és polgári jogi következményei is lehetnek.

Vertikális szinten nézve a jogrendszer nem a szolgáltatók között tesz különbséget, hanem az általuk közvetített tartalomban határolja el jogsértést megvalósítót a többitől. Ilyen például az Egyesült Államokban a Digital Copyright Millennium Act 1998 (DMCA), mely a közvetítő szolgáltatók szellemi alkotásokkal kapcsolatos felelősségét szabályozza.

Horizontálisan szemlélve a felelősséget különböző szinteken más felelősséggel rendelkeznek a közvetítő szolgáltatók, melyre tipikus modell az Európai Unió elektronikus kereskedelemről szóló irányelve²³¹, mely mentességet biztosít a felelősség alól a kizárólag jeltovábbítással foglalkozó szolgáltatóknak (telekommunikációs- és internet szolgáltatók).

A korlátozott felelősségű modell esetén a kormányok gyakran elvárják, vagy kötelezik a szolgáltatókat, hogy rendszereikbe építsenek be automatikusan működő szűrőket a jogsértő tartalmak kimutatására és dolgozzanak ki etikai kódexeket a személyes adatok és a felhasználók jogainak védelme érdekében.

Végül a teljes immunitás modellje esetén a közvetítő szolgáltatók nem felelősek a rajtuk átfolyó harmadik felek tartalmaiért semmilyen mértékben. Csak kisebb államokban fordul elő, gyakorlatban igen ritka (pl. Szingapúr²³²).

²³⁰ Janet Lowe: *Secrets of the World's Greatest Billionaire Entrepreneurs*, Sergey Brin and Larry Page, John Wiley & Sons, Inc., 2009, 250-270.

²³¹ 2000/31/EK irányelv

²³² Singapore Electronic Transactions Act 2010

4.2 A felejtés joga

A felejtés jogának megszületése a bűnügyi nyilvántartások²³³ megjelenéséhez kapcsolható, melynek előzményei a XIX. században létrehozott rendőrségi adatbázisok, melyek még manuális nyilvántartások voltak, és csak helyi szinten voltak elérhetőek. A XX. században kerültek bevezetésre a központi, országos nyilvántartási rendszerek, melyek a század végén a számítástechnika fejlődésének köszönhetően az elektronikus adatbázissá alakultak²³⁴, így jellemzőjük lett a könnyű kereshetőség, az adatok összekapcsolhatósága és az „örök emlékezet”. A XXI században a következő lépés volt az adatbázisok nemzetközi szintű összekapcsolása.²³⁵

A büntetés nem csupán a bűncselekmény jogkövetkezménye, hanem az általános és speciális prevenciót megvalósító jogintézmény. Az általános prevenció célja annak megelőzése, hogy a társadalom tagjai bűncselekményt kövessenek el, melynek - többek között – egyik eszköze a büntetéstől való félelem. Amikor egy bűncselekmény esetén a nyilvánosság tájékoztatásával folyik le az eljárás, majd az ítélelhirdetés, annak – az eljárásjogi garanciák mellett – az egyik fontos szerepe, hogy a társadalom tagjai tájékozódjanak, és tisztában legyenek avval, hogy ha ők is hasonlóan cselekednek, rájuk is ugyanolyan negatív jogkövetkezmények vonatkoznak tetteikért. Az információhoz való jog szerepe ebben az esetben előnyhöz jut, hogy más jogok érvényesülését előremozdítsa (pl. lopás esetén a tulajdonhoz való jogot, vagy testi sértés esetén a testi épséghez való jogot).

A speciális (egyéni) prevenció célja, hogy az egyén ne kövessen el újabb bűncselekményt, mely csak úgy valósulhat meg, ha az elítélt visszailleszkedik a társadalomba, melynek céljából a büntetés kiszabását illetve végrehajtását követően gondoskodni kell az elítélt rehabilitációjáról,

²³³ Bíró Gyula: Kriminalisztika, Debreceni Egyetem ÁJK. Lícium-ART Könyvkiadó Kft., Debrecen, 2010, 73.: A bűnügyi nyilvántartás a törvényben meghatározott adatokat tartalmazó, közhitelű hatósági nyilvántartás, amelynek feladata az e törvényben meghatározott adatok gyűjtése, kezelése, azokról okiratok kiadása, törvényben meghatározott jogosultaknak adatok szolgáltatása. Alapvető jelentősége abban a funkciójában fedezhető fel, hogy az általuk rendszerbe foglalt adatok, illetve azoknak az értékelése lehetőséget biztosít a bűncselekmény tettesre, elkövetésének körülményeire vonatkozó következtetések levonására. Közvetett módon pedig a bűnüldözési cél eléréséhez is segítséget nyújt, hiszen a korábban felderített bűncselekményekkel összefüggő elemzett és értékelt adatok is a részét képezik.”

²³⁴ Finszter Géza: A bűnügyi nyilvántartások helyzete és fejlesztési lehetőségei. In: Kriminológiai tanulmányok, 2006. 43. köt. 39-41.

²³⁵ Európai Bűnügyi Nyilvántartási Információs Rendszer 2012 áprilisában kezdte meg működését.

mely biztosítja a büntetett előélethez fűződő hátrányok alóli mentesülést. A társadalomba való visszailleszkedés – és a speciális prevenció – egyik alapja a megbélyegzettség hiánya, melyről a mentesítés gondoskodik.²³⁶

A felejtés joga folyamatosan ütközésben van az információhoz való joggal, és a mérleget az idő billenti el közöttük: egy információ, mely aktuális, közérdekű, és a társadalom joggal tarthat igényt arra, ott az információhoz való jog kerül előtérbe. Az idő múlásával azonban a kérdés már aktualitását vesztheti, az igények elévülhetnek és az egyének a joga kerülhet előtérbe.

Amikor egy társadalmat megrázó bűncselekmény elkövetője ellen zajlik az eljárás, és (nyilvánosan) ítéletet hirdetnek, a közérdek megkívánja a megfelelő tájékoztatást és információt (mely alól kivételt jelenthet a sértett jogainak védelme).

Az társadalom – érhetően – tart a bűncselekmények elkövetőitől, így ha a büntetését letöltő szabadult megpróbál munkát, barátokat, társat keresni, komoly hátrányba kerülhet, ha a múltjáról tudomást szereznek. A társadalomnak is az érdeke, hogy visszailleszkedjen, és ne kövessen el újabb bűncselekményt, melyhez elengedhetetlen a felejtés joga, így az idő múlása felülírhatja az információhoz való jogot.

Azonban történelmi érdekből, vagy valamely közszereplő által elkövetett, közérdeket érintő cselekménynél továbbra is előtérben maradhat az információhoz való jog.

Az társadalom – érhetően – tart a bűncselekmények elkövetőitől, így ha a büntetését letöltő szabadult megpróbál munkát, barátokat, társat keresni, komoly hátrányba kerülhet, ha a múltjáról tudomást szereznek.

4.2.1 A technikai akadályok elhárítása

Az elektronikus adatfeldolgozás, az internet és a keresők megváltoztatták a felejtés jogát: az informatika elterjedése előtt is jelentek meg újságcikkek és televíziós közvetítések a bírósági ítéletekről és az elítéltekről, melyek bárki által megtekinthetők, megvásárolhatóak, archiválhatóak és gyűjthetők voltak. Az ilyen anyagok elméletileg bármikor előkereshetők, a könyvtárakban és az archívumokban elérhetőek, gyakorlatban azonban mégsem egyszerű a helyzet az érdeklődő számára: komoly kutatómunkával, idő és pénz ráfordításával (pl. könyvtári tagság, kiadónak fizetni az archívumból való előkeresésért és másolásért) lehet fellelni a kívánt cikkeket, dokumentumokat.

²³⁶ Nagy Ferenc: Anyagi büntetőjog, általános rész II, Szeged, 2014. 231-232.

A helyzetet jól mutatja az Egyesült Államok Legfelsőbb Bíróságának egy 1989-ben született ítélete²³⁷. Az ügy tényállása, hogy egy újságíró kérvényezett az FBI-tól egy régen lezárt ügygel kapcsolatban dokumentumokat, melyek azonban 4 ember bűnügyi lajstromát (criminal records) is tartalmazták, így az FBI az iratok kiadását megtagadta, az egyikük személyiségi jogaira hivatkozva (a 4-ből már csak egy élt). Az újságíró ezután fordult bírósághoz, majd az ügy eljutott a Legfelsőbb Bíróság szintjére, mely egyhangúan az alábbi megállapítást tette:

„A kérdés, hogy az egyébként nehezen megszerezhető adatok összegyűjtése (és az igénylő részére átadása) hatással van-e az érintett érdekeire a magánszférájával kapcsolatban.

Hatalmas különbség áll fenn a között, hogy a kérdéses adatokat a bírósági, megyei nyilvántartásokban, és a helyi rendőrség adatbázisaiban, országon átívelő hosszú keresőmunka után lehet elérni, vagy összesítve egy központi számítógépes nyilvántartásból.”

A Legfelsőbb Bíróság megállapítása több, mint 20 éve született meg, azonban napjaink helyzetét is jól tükrözi: az internet világa felborította az állampolgár magánszférájának részét képező felejtéshez való jog működését. Az információ, mely eddig adatmorzsákból volt összeállítható hosszas keresőmunka árán, ma már elérhető bárhol, bármikor, gyorsan és ingyen, akár inkognitóban is.

Az interneten elérhető adatok korlátozására a világ több részén születtek olyan megoldások, melyek a bírói ítéleteket anonim módon helyezik el az interneten, vagy a mentesítés időpontjában teszik azokat névtelenné. Azonban az internet egyik tulajdonsága, hogy az érdeklődésre számot tartó információk növekvő gyorsasággal (exponenciálisan) terjednek rajta: egy sorozatban illő ügy ítélethirdetéséről készült cikkek, megrázó beszámolók percek alatt körbeutazhatják a Földet, és a legtöbb nyelvére lefordításra kerülnek.

Az információ terjedésére jellemző, hogy az nem ismer földrajzi és nyelvi határokat, továbbá tárolása meghatározhatatlan számú számítógépen valósul meg. A Spanyolországban kihirdetett ítéletet, ha átveszi a New York Times, onnantól minden ország valamely online médiumában lesz rá legalább hivatkozás, vagy –amennyiben nagy érdeklődésre és reklámbevételre tarthat számot – saját nyelvre lefordított cikk. Az információ eltávolítása az internetről ilyenkor már lehetetlen, az elérését megakadályozni nem lehet, csupán nehezíteni: a keresőszolgáltatások nélkül nehéz az előbányászásuk.

A fennálló helyzet így ütközést eredményezhet az egyén személyes jogai (magánszférához való jog, felejtéshez, személye kifejlődéséhez és az újrakezdéshez való jog) és a sajtószabadság

²³⁷ Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

között. Nem lehet általánosságban kijelenteni, hogy az egyén felejtéshez való joga élvezne elsőbbséget, azt konkrét esetben arányossági tesztnek eleget téve lehetséges csak megállapítani. Az internet tele van olyan jogsértő tartalmakat tároló és megosztó helyekkel, amelyek ellen még nemzetközi egyezményekkel és hatósági együttműködéssel sem tudnak mit tenni az illetékes hatóságok.²³⁸

Egykor köznapiak, múltónak gondolt tevékenységeinket és szokásainkat – mint például mit vásároltunk, olvastunk, kivel kommunikáltunk – megőrzi a digitális technológia és az internet az örökkévalóságnak.²³⁹

A problémára már az üzleti életben is felfigyeltek, így több magáncég is foglalkozik az online reputáció figyelésével és helyreállításával, melyet több módszerrel próbálnak meg elérni: a negatív tartalmat szolgáltató oldalak felkeresése, pozitív információkat tartalmazó oldal kreálása és a keresőkben magas rangsorolásra helyezése.

Ha az adatkezelő az érintett kérésére törli is a rá vonatkozó adatokat, azok még elérhetőek maradnak az internetes keresők átmeneti tárolóiban („cache”)²⁴⁰.

A sajtó legfőbb érdeke és működésének alapja, hogy a megjelenő információk hírértékkel rendelkeznek: a cél az olvasó figyelmének és érdeklődésének a felkeltése, mely legtöbb esetben a profit alapja is. A közmédia esetében a profitot leszámítva a hírérték szintén alapvető igényként jelenik meg.

A felejtés jogát és érvényesülését vizsgálva az egyik legfőbb probléma az újságok (különösen az internetes újságok) archívumai: ebben az esetben hírértékről már nem beszélhetünk, továbbá már az adott médiumnak sem termelnek reklámbevételt, és az információ közérdekűségéről sem lehet általában már olyan mértékben beszélni, mivel az adott személy cselekménye által felmerült társadalmi probléma lehetséges, hogy már megoldódott (pl. ártatlanságára fény derült, vagy büntetését kitöltötte).

Az információk nyilvánossága felé billentheti a mérleget, ha közérdekű információkról van szó, vagy ha történelmi, statisztikai²⁴¹ célokból szükséges az adatok nyilvánosságra hozatala és archívumban való megőrzése.

²³⁸ Brian Leiter: *Cleaning Cyber-Cesspools: Google and Free Speech*, Harvard University Press, 2010, 155.

²³⁹ John Battelle: *Keress*, HVG Kiadó Zrt, Budapest, 2006, 17.

²⁴⁰ A gyorsítótár működése (<https://support.google.com/websearch/answer/1687222?hl=hu&p=cached>):

A Tárolt változat link: a Google feltérképezi az internetet, és pillanatképeket készít minden oldalról. A pillanatképek biztonsági mentésként szolgálnak arra az esetre, ha az oldal nem lenne elérhető. Ezek az oldalak aztán a Google „gyorsítótárába” kerülnek. Amikor rákattint a Tárolt változat feliratú linkre, megjelenik a webhely legutóbb mentett verziója.

²⁴¹ Statisztikai célok esetén a kérdésre megoldást jelenthet az adatok anonim módon való tárolása.

Ha egy sikkasztó állami vezető ellen folyó eljárás során a sajtó közvetít, az hírértékkel rendelkezik és közérdekű, mert a társadalomnak joga van tudni az elsikkasztott javakról és annak következményeiről. Azonban, ha másod-, vagy harmadfokon folyik az eljárás, azt az információt is hozzá kellene fűzni az archívumokban az erről szóló cikkekhez, a megbélyegzés elkerülése céljából, továbbá, ha az eljárás lezárult – és az elkövető esetleg mentesítve is lett – az ő személyes érdeke meghaladja az adott újságét, mivel az archívumban róla szóló cikkek hírértékkel már nem rendelkeznek - így profitot sem termelnek -, továbbá a közérdekűségről sem lehet olyan szinten beszélni, mint a nyilvánosságra kerülés idején.

Az Emberi Jogok Európai Bírósága a felejtés jogának és a sajtószabadságnak a viszonyára tért ki egyik ítéletében, mely során a szólásszabadság és sajtószabadság volt az elsődleges kérdés.²⁴²

Az ügy tényállása, hogy a Times Newspaper papíralapon és internetes lapján is két cikket publikált egy – állítólag maffia vezető - orosz állampolgárról, aki több pénzmosási akcióban vett részt céghálók közvetítésén keresztül. Az orosz férfi neve szerepelt a cikkekben, így azonosítható volt, mely miatt keresetet indított az újság ellen sajtó útján elkövetett rágalmozás miatt. Az eljárás alatt az újság nem távolította el az internetes oldaláról – az archívumból - a kifogásolt cikkeket, csupán hozzájuk fűzte, hogy a cikkbeli állítások bírósági eljárás alatt vannak, melynek következtében a férfi beadott még egy keresetet, mert az archívumban korlátlanul elérhetőek az ő jó hírnevét sértő cikkek, melyek valóságtartalmának eldöntése folyamatban van. Az újság kifogásolta, hogy második keresetet a férfi az arra fennálló határidőn túl nyújtotta be, azonban a bíróság kimondta, hogy a határidő minden egyes internetes hozzáférésnél újratekintődik. A bíróság döntése azt jelentette, hogy amíg az archívumban a cikk megtalálható, addig a keresetindítási jognak nincsen akadálya. Az újság fellebbezett a döntés ellen, mivel szerinte a sajtószabadságot sérti, hogy az archívumban szereplő cikkek miatt az újság bármikor felelősségre vonható a személyiségi jogaiban sértett által, mely szerinte „szüntelen felelősséget” jelent a sajtó számára.

A Bíróság kiemelte, hogy egyetért az újság azon megállapításával, hogy az internetes archívumok fontos szerepet töltenek be az információk összegyűjtésében és tárolásában, melyek történelmi, oktatási és kutatási szempontból is értékesek, mivel a társadalom bármely tagja által közvetlenül és ingyenesen elérhetőek. A Bíróság az archívumok szerepének elismerése mellett kifejtette azok másodlagos helyét a sajtó feladatában: a Bíróság szerint a sajtó elsődleges feladata a társadalom tájékoztatása, mely egy demokratikus társadalomban a

²⁴² Times Newspapers Limited v. the United Kingdom, no. 3002/03 and no. 23676/03, ECHR, 2009. 05. 10.

vezetés kontrollját is jelenti²⁴³, ezért a sajtószabadság különösen fontos jogként jelenik meg. Az archívumok esetében azonban olyan adatokról van szó, melyek a nyilvánosság tájékoztatásával kapcsolatos feladatukat betöltötték, így az államoknak nagyobb mozgástere van az egyén jogait érvényesíteni az archívumok üzemeltetőivel szemben.

Az Emberi Jogok Európai Bíróságának ítéletéből az a megközelítés körvonalazódik, mely alapján a sajtószabadság a komoly hírértéknél – melyről elsősorban friss hír esetén beszélhetünk – jobban érvényesülhet az egyén személyes jogaival szemben, míg az idő múlásával - és a hír archívumba kerülésével – a hírérték csökken, az egyén jogait előtérbe helyezve.

Az Emberi Jogok Európai Bírósága hasonlóan vélekedett a Rotaru ügyben, mely során egy állampolgárról kerültek egy bírósági eljárás során nyilvánosságra olyan információk, melyeket a titkosszolgálat gyűjtött róla évtizedekkel az eljárás előtt. A Bíróság kiemelte, hogy így meg lett sértve az állampolgár magán- és családi élet tiszteletben tartásához való joga (Emberi Jogok Európai Egyezménye (8. §), mivel az ilyen adatok tárolását felül kell vizsgálni, és nyilvánosságra hozataluk különösen sérelmes. Bár a Bíróság nevesítve nem mondta ki, de a felejtéshez való jogot is sérti az adatok eljárás során való kezelése, melyek - még ha igazak is lennének – az érintett személyes jogait sértik.²⁴⁴

Az idők kezdetek óta az emberek számára a felejtés volt a természetes és normális, míg a részletes emlékezés kivételes és különleges, különösen az analfabetizmus megszűnéséig. Napjainkban a technikának köszönhetően a helyzet megfordulni látszik: az emlékezés vált alapvetővé a digitális nyomaink miatt.

Andrew Feldmar, egy kanadai fizioterapeuta gyakran járt át Kanadából az Egyesült Államokba a munkája miatt is, azonban egy napon nem úgy alakult az átmenetel, mint az addig megszokta: a határőr rákeresett az interneten Feldmar nevére, és a kereső kidobott egy általa írt tudományos cikket, melyben leírja, hogy az 1960-as években ő is kipróbálta az LSD-t.

Feldmart ezután órákig ott tartották, majd újlennyomatot vettek tőle, és aláíratnak vele egy nyilatkozatot, melyben elismerte, hogy már próbált ki kábítószer. Végül nem engedték át a határon, annak ellenére, hogy több évtizeddel ezelőtt drogozott, melynek büntetőjogi következményei már rég elévültek, azonban bevándorlás és vízum szempontjából relevánsnak bizonyult.²⁴⁵

²⁴³ A Bíróság ítéletében a „public watchdog” kifejezést használja, mely alatt képletesen a köz (demokrácia) házőrzőjét érthetjük.

²⁴⁴ Rotaru v. Romania, no. 28341/95, ECHR, 2010. 05. 04.

²⁴⁵ Viktor Mayer-Schönberger: Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, Princeton and Oxford, 2009, 13-17.

Feldmar nem tudhatta, hogy ilyen következményei lesznek a cikkének, amikor azt megírta, hiszen a digitális technológia nem volt akkor még olyan a szinten, hogy egy határőr akármikor előkeresse azt másodpercek alatt.²⁴⁶

Így felléphet az a helyzet, hogy bármikor szankcionálhatókká válnak a megőrzött információk, ha az erősebb fél érdekeit szolgálja²⁴⁷.

A kirívó esetektől eltekintve megszámlálhatatlan alkalommal van hatással az emberek életére az interneten róluk található információ, úgy hogy nem is tudnak róla. Az ilyen esetekre leggyakoribb példa az álláskereső: a Microsoft által készített felmérés alapján a munkaközvetítő cégek és a HR-esek a jelentkezők 75%-ánál megtekintik a weben róluk található információkat közösségi oldalakon, keresőkön, blog oldalakon, online játék oldalakon. Az munkaközvetítők 70% úgy nyilatkozott, hogy utasítottak el már jelentkezőt az interneten róla található információk miatt.²⁴⁸

Az internet miatt kénytelenek az emberek tudatosan cselekedni, mivel az megmerevíti a jelent és bármikor visszaköszönhet az életükben, melyre az emberi agy és társadalom nincsen felkészülve.²⁴⁹

A felejtésnek komoly központi szerepe van az ember döntéshozó mechanizmusában: a segítségével lehet döntést hozni a jelenben a múlt – nagy hatással lévő, ezért nehezen felejtethető - tanulságainak ismeretével, de akadályoztatása nélkül.

A felejtés nem csupán az egyén döntésében, hanem társadalmi szinten is megmutatkozik: a társadalom, a körülöttünk lévők felejtésére is szükség van, hogy az ember tovább tudjon lépni. Az új kapcsolatok létesítéséhez, vagy az üzleti életben a csőd után új vállalkozás indításához tiszta lappal elengedhetetlen a társadalom részéről a felejtés, és hátrány nélküli megítélés.

A felejtés intézményével a társadalom elismerheti és esélyt adhat arra, hogy az egyén képes fejlődni, és nagyobb tapasztalattal új – helyesebb – döntéseket hozni.

A kifejezetten nevesített „feledésbe merüléshez” való jog francia eredetű (le droit à l’oubli), elsőként – úttörő jelleggel – a francia adatvédelmi biztos Alex Türk vetette fel egy javaslatában, mely szerint egy nemzetközi bizottságot kellene felállítani, amely a beérkező kérelmek alapján esetről esetre mérlegelhetné, hogy egy adott információ, adat megjelenése sérti-e az illető emberi méltóságát vagy

²⁴⁷ Székely Iván: A felejtés joga az információs társadalomban, Információs Társadalom 10. évf. 3-4. sz. 2010.

²⁴⁸ The New York Times: The Web Means the End of Forgetting
http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all&_r=1&

²⁴⁹ Mayer, 26.

egyéb személyiségi jogait, s az eltávolítandó-e. A javaslat részletei azonban kidolgozatlanok maradtak.²⁵⁰

Talán az első alkalom a felejtés jogának angol jogirodalomban való említésére egy 1974-ből cikkből származik²⁵¹, amelyben gondnokság alá helyezett személy egyetlen megmaradt jogaként írja le a szerző. A felejtés joga azonban mást jelentett az említett kontextusban, mint a napjainkban: a cikkben leírt felejtés joga a Warren is Brandeis által is kifejtett „egyedülélthez való joggal” (right to be let alone”) hozható összefüggésbe²⁵².

A felejtés jogának egyik legfontosabb alapja az idő múlása, amely az adatkezelő és a társadalom érdekeit háttérbe helyezheti az egyén magánszférához való jogaival szemben az esetek döntő többségében²⁵³.

2. ábra: Az idő múlásának hatása az adatkezelésre²⁵⁴

folyamatos vonal: a megtörtént adatkezelés hatása

szaggatott vonal: a meg nem történt adatkezelés esete

²⁵⁰ Navratyil Zoltán: Internet és szólásszabadság: a „felejtés” joga és a „feledésbe merüléshez” való jog, Iustum Aequum Salutare, XI. 2015. 2. 86.

²⁵¹ Ross E. Campbell: Comment, Progress in Involuntary Commitment, 49 WASH. L. REV. 617, 640 (1974).

²⁵² W. Gregory Voss, Céline Castets-Renard: Proposal for an International Taxonomy on the Various Forms of the 'Right to Be Forgotten': A Study on the Convergence of Norms, 14 Colorado Technology Law Journal 281 (2016) (Issue 14.2), 2016. 284.

²⁵³

²⁵⁴ Paulan Korenhof, Jef Ausloos, Ivan Szekely, Meg Ambrose, Giovanni Sartor, Ronald Leenes: Timing the Right to Be Forgotten, A study into “time” as a factor in deciding about retention or erasure of data, Computers, Privacy and Data Protection Conference 2014. 21.

Alapvetően három személyi kört lehet határolni egymástól, akik a felejtéshez való jog szempontjából relevanciával bírnak:

1. az érintett személy, akire az információ vonatkozik, aki az alapján beazonosítható,
2. az adott weboldal üzemeltetője, ahol a személyes adat megtalálható (pl. sajtótermék online kiadása),
3. harmadik fél weboldalainak a működtetői, akik a más által feltöltött tartalmakat a saját felületükön linkelik, átveszik vagy mutatják be.

Érdekes javaslat született Mayer-Schönberger Viktor részéről a felejtés egyensúlyának visszaállentésére: az automatikus törlés bevezetése a felhasználó által megadott idő elteltével. A könyvében a megoldást úgy írja le, hogy amikor a felhasználó valamilyen tartalmat készít (pl. fénykép, dokumentum) a mentés alkalmával a fájl neve mellett beállítható lenne a megőrzés ideje (pl. 5 év, 15 év) amelynek elteltével automatikusan törlésre kerülne az adat. A törlési idő akár módosítható is lehetne és a szerző tovább árnyalja a megoldást a törlés előtti figyelmeztetés lehetőségével, így még a felhasználó értesülhetne törlés előtt, és dönthetne arról, ha meg szeretné hosszabbítani a tárolást.

Technikailag könnyen megvalósítható lenne a javaslat, mivel egy fájl esetében a törlés időpontja csupán egy tulajdonság lenne a sok közül: a név, keletkezés ideje, fotó GPS koordinátáihoz hasonlóan ez megoldás nem növelné a fájl méretét, és az automatikus törlődés is a jelenlegi operációs rendszerekben könnyen megvalósítható lenne²⁵⁵.

A megoldást lehetne alkalmazni akár az interneten használt szolgáltatások esetében is. A Google keresései során megadható lenne a keresés megőrzésének ideje a keresett szó után. Így ha csak egyszeri alkalommal keres rá a felhasználó egy tárgyra, például egy fürdőruhára, akkor bejelölhetné a keresés tárolási idejét nullára. Evvel szemben, amikor az érintett valamilyen témában hosszabb távon tervez kutatni, mint például egy orvos valamilyen betegség tárgyában, akkor a keresés tárolását hosszabb időtartamban adná meg.

A megoldás természetesen a nagy adatkezelők érdekeivel ellentétes, amelyek minél több adatot szeretnének feldolgozni, azonban nekik is lehetne hasznuk belőle, mivel a nagy mennyiségű rendelkezésre álló adat közül nehéz eldönteniük a komoly erőforrás igénybevételével és algoritmusokkal is, hogy melyek a relevánsak. Így történhet meg, hogy egy férfinak sminkelésről szóló könyvet ajánl az Amazon, mivel csupán egyszer keresett a Google segítségével sminkkészletet a felesége születésnapjára.

²⁵⁵ Viktor Mayer-Schönberger: Delete: The Virtue of Forgetting in the Digital Age, Princeton: Princeton University Press, 2009. 101-103.

Mayer-Schönberger is megfogalmaz a kritikát és fenntartásokat a megoldással kapcsolatban, amelyek között központi helyet foglal el a tárolás időpontjának jogalkotó általi meghatározása, valamint a felhasználók tudatosságának és felfogásának a változtatása²⁵⁶.

Véleményem szerint a törlés helyett egy kevésbé radikális módszerrel is tudósítható lenne a felhasználókban a felejtés fontossága és az adatok biztonsága: törlési idő helyett „archiválási idő” lehetne megadható az adatokon, amelynek elteltével az adat áthelyezésre kerülne egy tömörített és jelszóval védett mappába, ahova csak a mentést végző felhasználónak lenne hozzáférési joga, másnak nem. Az áthelyezett fájlok törlésre kerülnének az eredeti helyükről, és csak a biztonságos mappába csak a felhasználó által kerülhetnének biztonsági lépések után elérhetőek.

4.2.2 A felejtés joga az adatvédelmi irányelvben

A felejtés joga az adatvédelmi irányelv keretei között is – az érintett kérelme nélkül – automatikusan érvényesül: a célhoz kötöttség elve alapján az adatkezelő az adatokat csak addig tárolhatja az érintetthez köthetően, amíg az a célok eléréséhez szükséges. A cél elérése után a tagállamok által meghatározott módon lehet csak tárolni az adatokat, amely általában anonim tárolást jelent.²⁵⁷

Az irányelv biztosítja a felejtés jogának gyakorlását az érintett kérelmére is: bármikor kérheti az adatkezelőtől, hogy tájékoztassa a róla folyó adatkezelésekről (azok céljáról is), majd kérheti az adatok törlését is, amennyiben azok kezelése nem felel meg az irányelv rendelkezéseinek, amely magában foglalja az esetkört, amikor az adatkezelés a célhoz kötöttsége nem érvényesül.²⁵⁸

Az adatkezelés sikeres kifogásolása azonban nem minden esetben vezet automatikusan az adatok törléséhez, sok esetben csak szüneteltetik az adatkezelést (pl. az érintett felkerül egy

²⁵⁶ Viktor Mayer-Schönberger 110-113.

²⁵⁷ Adatvédelmi irányelv, 6. cikk (1) A tagállamok rendelkeznek arról, hogy a személyes adatok:

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges ideig teszi lehetővé. A tagállamok állapítják meg a személyes adatok történelmi, statisztikai vagy tudományos célból, hosszabb ideig történő tárolásának megfelelő garanciáit.
b) gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további feldolgozása nem végezhető e célokkal összeférhetetlen módon. A személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat

²⁵⁸ Adatvédelmi Irányelv, 12. cikk

b) az esettől függően kérje az olyan adatok helyesbítését, törlését vagy zárolását, amelyek feldolgozása nem felel meg ezen irányelv rendelkezéseinek, különösen az ilyen adatok hiányos vagy hibás volta miatt;

listára, melyen azon előfizetők szerepelnek, akik semmilyen marketing célú levelet és információt nem igényelnek).

Az irányelv megalkotói tisztában voltak avval, hogy a személyes adatokat történelmi, tudományos, vagy statisztikai célból felhasználók az esetek jelentős részében olyan adatokat használnak fel, melyek eredetileg nem ilyen célokból lettek felvéve és kezelve (pl. sportmérkőzéseken jegyzőkönyvezni kell a baleseteket és az orvosi ellátásokat, melyeknek utólag sporttörténelmi jelentőségük is lehet, de később felhasználásra kerülhetnek az adott sportág veszélyességének megállapítására is statisztikákon keresztül).

A tudományos, statisztikai és történelmi célok a társadalmi hasznosságuk miatt tekinthetőek kivételnek, így a tagállami szabályozások a felejtés jogát korlátozhatják az ilyen felhasználások esetén megfelelő garanciák mellett. A garanciák tagállamonként változnak, általában az adatok anonimmé tétele szükséges a további felhasználáshoz és az említett 3 ok valamelyikének igazolása.

Az Európai Unió adatvédelmi rendeletében kiemelt figyelmet kapott a felejtés joga, automatikusan érvényesülővé téve azt. Viviane Reding, a José Manuel Barroso által vezetett Bizottság alelnökének (feladatköre: igazságszolgáltatás, alapvető jogok és uniós polgárság) az EU adatvédelmi rendeletének tervezetével kapcsolatban híressé vált idézete „God forgives and forgets but the Web never does!”, vagyis „Isten megbocsát és felejt, azonban a Web soha” tükrözi a rendelet megalkotásának szemléletét a részéről.²⁵⁹

A világhálón az adatok tárolásának időtartama természetesen nem örök: az érdektelen adatok lehet, hogy sok év után már a biztonsági mentésekből is törölődhetnek, míg az érdeklődésre számot tartó, a világhálón elterjedt adatok (pl. valamely híresség kompromittáló fotói) gyakorlatilag bármikor megtalálhatóak lesznek valamely archívumból.

Az interneten tárolt adatok természete teljesen eltér a fizikailag tárolt adatokétól, melyek tárolása komoly helyigénnyel jár, így az emberi és anyagi erőforrást emészt fel, mely által pénzügyi megfontolásból is célszerűbb és olcsóbb azokat megsemmisíteni, mint hosszú távon tárolni. Az elektronikusan tárolt adatok az adattárolók fejlődésének köszönhetően könnyedén megtarthatóak hosszú ideig, mivel a képeket és videókat leszámítva a cikkek és szöveg alapú információk tárolása csekély tárhely igényvel rendelkezik. A legfontosabb különbség a fizikai és az elektronikus tárolás között, hogy míg a fizikailag tárolt archívumokat pénzügyi megfontolásból megéri törölni, addig az elektronikusan tárolt internetes adatbázisokból egyes adatokat sokszor drágább törölni, mint tárolni hagyni.

²⁵⁹ Az idézet egy konferencián hangzott el Brüsszelben 2010. 11. 30-án, The European Data Protection and Privacy Conference, http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm

A nagy adatbázisok, mint például a Facebook, vagy Google több szerveren tárolja biztonsági mentésben az adatokat, földrajzilag is elkülönítve, így technikailag nem egyszerű minden szerverről és azok „cache” tartományából is kitörölni. A másik ok a törléssel kapcsolatos munka: a nagy tárolókapacitás miatt fölösleges foglalkozni a kisméretű adatokkal, a törlésükre áldozott munkaerő költsége meghaladja az avval elérhető hasznot általában. Annak ellenére, hogy az irányelv biztosítja a felejtés jogát a célhoz kötöttség megszűnésével, a gyakorlati életben az adatok törlése vagy anonimmé változtatása a jogkövető adatkezelőtől függ. Annak a meghatározása azonban sok esetben nem egyértelmű, hogy meddig szükséges az adatok felhasználása a cél eléréséhez, hiszen egy jogviszonyban a főkötelezettség teljesítése után is maradhatnak olyan mellékes kötelezettségek, melyek céljából továbbra is tárolni szükséges az adatokat (pl. bizonyítás vagy garanciális ügyintézés céljából). Az irányelv alapján az ilyen esetekben korlátozni kell a kezelt adatok körét a szűkült célhoz, vagy névtelenné tenni azokat, azonban az adatkezelők inkább a szükséges adatoknál többet tárolnak, hogy a szükséges célt biztosan meg tudják valósítani. A hosszabb tárolásnak több oka is van a törléssel kapcsolatos munkától az adatbázissal elérhető – sokszor anyagi – előnyökig.

Olyan technikai megoldások jelenthetnék a megoldást, melyek az adatkezelés kezdetétől biztosítják a felejtés jogát, a feldolgozó rendszerbe beépítve, alapvető értéként („privacy by default”), melynek egyik módja lehetne, hogy az adatok már a felvételkor lejáratí idót kapnak, és annak leteltével névtelen adattá válnának – megszüntetve az érintettel való kapcsolatba hozhatóságot -, vagy törölődnének.

A „privacy by default” esetén nem csak az érintettnek nem szükséges beavatkoznia, mely különösen fontos az internet világában, ahol sokszor az adatkezelés az érintett tudta nélkül valósul meg. Az adatkezelő szempontjából is releváns az adatok jövőben sorsának rendezése már azok felvételekor, mivel a felelős adatkezelő személye megszűnhet a természetes személy halálával, vagy a jogi személy megszűnésével, az adatokat sorsukra hagyva.

4.2.3 A felejtés joga az adatvédelmi rendeletben

Az EU adatvédelmi rendelete általános hatállyal szabályozza a személyes adatok védelmével és kezelésével összefüggő tevékenységeket. A jogi norma közvetlenül alkalmazandó jellegéből fakadóan tagállami átültetés nélkül eredményez jelentős változásokat Magyarországon is.

Bővül a szabályozás köre, mivel minden olyan esetben alkalmazni kell majd, amikor árut vagy szolgáltatást kínálnak az Unióban lévő személyeknek, vagy az adatkezelés az ő magatartásuk követésére irányul.

Ennek különösen az online adatkezelések körében lesz jelentősége, és az adatok védelme mellett a piaci szereplők egyenlő esélyeinek biztosítását is célozza. Az új rendelet megerősíti a felhasználók „felejtéshez” (a teljes törlésre) és az adatok hordozhatóságához való jogát, utóbbi az online szolgáltatások közötti adatmigrációt segíti majd.

Az adatkezelőket a szabályok megsértéséért bizonyos körben 10 millió euróig, vagy a globális árbevétel két százalékáig terjedő pénzbüntetéssel is sújthatják majd. Más esetekben, mint például személyes adatok harmadik országba történő jogellenes továbbítása esetén a szankció 20 millió euróig, vagy a globális árbevétel 4 százalékáig is terjedhet.

A „felejtés joga” elnevezés megtévesztő lehet, mivel a való életben az interneten teljes mértékig ezen jog nem érvényesülhet a technológiai korlátok és az adattárolás mechanizmusa miatt, így sok esetben a felhasználóban azt a hamis elképzelést idézheti elő, hogy valóban képesek a személyes adataik kontrolljára az interneten. Valójában csak az internetes keresőkön és közösségi hálókön (az internet „könyvtárosain”) keresztül lehet megakadályozni, hogy az eltüntetendő személyes adatokhoz való hozzáférés ne legyen egyszerű, mivel az említett cégeket egyszerűbb a hatóságoknak számon kérni, míg a külföldi oldalakat, fájlmegosztó hálózatokat nehéz, vagy sok esetben lehetetlen a hazai bíróságoknak és hatóságoknak utasítani, vagy felelősségre vonni azok tulajdonosait, vezetőit²⁶⁰.

Bár az adatvédelmi irányelv korábban is biztosította az érintett számára a törléshez való jogot, azonban azt röviden szabályozva olyan esetekre határozta meg, amikor az adatkezelés nem felelt meg irányelv rendelkezéseinek²⁶¹. Az adatvédelmi rendelet evvel szemben a tiltakozáshoz való jogot szélesebb körben engedélyezi az érintettnek²⁶², különösen amennyiben az adatkezelés közvetlen üzletszerzés céljából történik.

²⁶⁰ David Lindsay: The right to be forgotten in European Data Protection Law, in: Emergin Challenges in Privacy Law - Comparative Perspectives, 2014. 300-310.

²⁶¹ Adatvédelmi Irányelv 95/46/EK

12. cikk A tagállamoknak biztosítaniuk kell minden érintett számára a jogot, hogy az adatkezelőtől:

b) az esettől függően kérje az olyan adatok helyesbítését, törlését vagy zárolását, amelyek feldolgozása nem felel meg ezen irányelv rendelkezéseinek, különösen az ilyen adatok hiányos vagy hibás volta miatt;

²⁶² AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016/679 RENDELETE

21. cikk A tiltakozáshoz való jog (1) Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. (2) Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha a törvényben meghatározott indokok valamelyike fennáll.

Az adatvédelmi rendelet alapján a felejtéshez való jog az alábbi esetekben teljesülhet.

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

Ebben az esetben az adatkezelés már elérte a célját, így például az egy áru megrendelésekor az kiszállításra és átvételre került, amelyért a vételárát is megfizették, továbbá a szavatosság ideje is lejárt. Fontos tehát, hogy az adott jogviszonyból eredő jogok és kötelezettségek rendezésre kerüljenek, a jövőben nem szükséges az érintett adatainak a felhasználása.

Sok szolgáltatás esetében azonban nem egyértelmű, mikor teljesült a cél. A Google esetében például egy keresés lefolytatása és a böngésző bezárása után joggal érezheti a felhasználó, hogy a cselekménye lezárult, az a célját elérte. Azonban a keresőszolgáltatók, hogy hosszabb távon pontosabb és az adott személy számára releváns találatokat mutassanak, a felhasználó korábbi kereséseit is figyelembe veszik.

A Facebook esetében a felhasználó posztjai sokszor csupán a pillanatnak szólnak, azonban azok megőrzésre kerülnek, ugyanígy a felhasználó cselekményei is folyamatosan naplózva vannak (pl. kinek az adatlapját tekintette meg, milyen eseményekre kattintott rá).

Véleményem szerint célszerű lenne a posztok esetében időkorlát lehetőségét biztosítani a felhasználók részére, hogy a felejtéshez való jogukat könnyebben tudják érvényesíteni.

b) Az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja.

Amennyiben az adatkezelés alapja kizárólag a felhasználó hozzájárulása, abban az esetben törölni kell a kezelt adatot a felhasználó kérésére. A gyakorlatban azonban sokszor egyéb jogalapja is keletkezik utólag az adatkezelésnek, még ha annak eredetileg a felhasználó hozzájárulása volt az alapja. Így például az áru megrendelésénél a szavatossági idő lejártáig az eladó megőrizheti a vevő adatait, mivel arra jogszabály kötelezi.

A Facebook esetében amennyiben a felhasználó szerepel mások fényképein vagy bejegyzéseiben, utólag nehéz és körülményes lehet azokat eltávolítani, különösen abban az

tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

esetben, ha nincs azokon automatikusan megjelölve, így azokról nem is szerez tudomást. Azonban a felhasználó amennyiben meg van azokon jelölve, az eltávolítás szintén időigényes és nehézkes, amelyre megoldást jelenthetne egy speciális felület vagy opció a Facebook-on²⁶³, például egy gombnyomással való eltávolítás lehetősége a posztokból és fényképekről, amelyekben a felhasználó említésre került, vagy azokon szerepel. A problémakörrel dolgozatomban részletesen foglalkozom a Facebook hozzájárulásával kapcsolatos fejezetben.

c) az érintett a 21. cikk (1) bekezdése alapján tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;

d) a személyes adatokat jogellenesen kezelték;

A személyes adatok kezelésének jogellenessége egyértelmű olyan esetekben, amikor a jogalap hiányzik, például jogellenesen lett megszerelve az érintett megtevéseztésével.

Közösségi hálózatokon számtalan példa található arra, hogy olyan érintettekről is személyes adatok kerülnek megosztásra és feldolgozásra, akik nem felhasználói a közösségi hálózatnak és ahhoz hozzájárulásukat nem adták (pl. fénykép feltöltése, vélemény írása a személyről, posztban megemlítése). Ilyen esetekben különösen fontos lenne annak biztosítása, hogy az érintett regisztrálás nélkül is tiltakozhasson és élhessen a felejtéshez való jogával²⁶⁴.

Kérdés továbbá, hogy olyan esetekben is jogellenes-e az adatok kezelése, amikor például az adatok pontatlanok, vagy a tájékoztatási kötelezettséget az adatkezelő nem teljesítette maradéktalanul. Dolgozatomban a Facebook tájékoztatási kötelezettségének megfelelőségét több ponton aggályosnak találtam.

Különösen jelentős a felejtéshez való jogot kiegészítő új rendelkezés, amely alapján az adatkezelőnek meg kell tennie az ésszerű lépéseket a felejtés jogának érvényre juttatásához abban az esetben is, ha az adatokat már nyilvánosságra hozta²⁶⁵. Kérdéses, hogy az „ésszerű lépések” és az „elérhető technológia” milyen megoldásokat takar.

²⁶³ Cesare Bartolini, Lawrence Siry: The right to be forgotten in the light of the consent of the data subject, Computer Law and Security Review 32. 2016. 223-224.

²⁶⁴ Jordan D. Brougher: The right to be forgotten: applying European privacy law to American electronic health records, Indiana Health Law Review Vol. 13:2, 2016. 523.

²⁶⁵ (2) Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és az (1) bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A felejtés joga nem korlátlan, az adatvédelmi rendelet a véleménynyilvánítás szabadsága, az adatkezelőre háruló jogi kötelezettség, közérdek és jogi igények érvényesítése érdekében csak korlátozottan engedi érvényesülni a felejtéshez való jogot²⁶⁶.

Az adathordozhatósághoz való jog

Az adatvédelmi rendelet alapján, ha a személyes adatok kezelése automatizált módon történik, az érintett számára – az adatai feletti rendelkezés erősítése érdekében – lehetővé kell tenni, hogy általa az adatkezelő rendelkezésére bocsátott, rá vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, és azok egy másik adatkezelő részére továbbításra kerüljenek. Ez a jog abban az esetben gyakorolható, ha az érintett a személyes adatokat a hozzájárulása alapján bocsátotta rendelkezésre, vagy ha az adatkezelés szerződés teljesítéséhez szükséges.²⁶⁷

E jog nem gyakorolható akkor, ha az adatkezelés jogalapja a hozzájárulástól vagy szerződéstől eltérő egyéb jogalap, továbbá nem állhat fenn olyan adatkezelőkkel szemben, amelyek a személyes adatok kezelését közhatalmi feladataik gyakorlása keretében végzik.

Az érintett jogosult továbbá arra, hogy – amennyiben az technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

Az adathordozhatósághoz való jog azonban nem teremthet olyan kötelezettséget az adatkezelők számára, hogy egymással műszakilag kompatibilis adatkezelő rendszereket vezessenek be vagy tartsanak fenn. Ha egy személyes adatállomány egynél több érintettre vonatkozik, a személyes

²⁶⁶ Adatvédelmi rendelet, 17. fejezet (3) Az (1) és (2) bekezdés nem alkalmazandó, amennyiben az adatkezelés szükséges: a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából; b) a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából; c) a 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján; d) a 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az (1) bekezdésben említett jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

²⁶⁷ Adatvédelmi rendelet 20. cikk Az adathordozhatósághoz való jog,

(1) Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

a) az adatkezelés a 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul; és
b) az adatkezelés automatizált módon történik.

adatok megszerzéséhez való jog nem sértheti az adatállományban szereplő egyéb érintettek jogait.

Felmerül a kérdés, hogy ha az adatkezelőknek nem kell kompatibilis rendszereket kialakítaniuk, akkor hogyan lenne lehetséges az adatok hordozhatósága egy komplex szolgáltatás esetében, mint például a közösségi hálózatok vagy az email szolgáltatók. A megoldás azért is lehet nehézkes, mert szellemi- és versenyjoggal kapcsolatos problémákat vet fel.

Fotómegosztó oldalak esetében például könnyű lehet az adatok exportálása és importálása, azonban egy közösségi hálózat esetében az adatok „leveséről” beszélhetünk, amelyek össze vannak keveredve egymással és mások személyes adataival is (pl. egy képen más személyek is szerepelnek és meg vannak jelölve). Ilyen esetben az adatok küldése technikai és jogi akadályokba ütközhet.

4.2.4 A felejtés joga és az internetes keresők

A felejtés jogának legfőbb életre hívói az internetes keresők, a közösségi hálózatok és olyan közvetítő csatornák, melyek lehetővé teszik a tartalom előkeresését és megosztását, akkor is, ha az tengernyi információ között van, akár egy több éves archívum mélyén. A közösségi hálózatokon bárki – személyes preferencia alapján – gyorsan elterjeszthet olyan témákat és régi információkat, melyeket az ismerősei – vagy meghatározhatatlan számú csoport tagjai - már rég elfelejtettek.

A fórumokban található viták és személyes vélemények, melyekben akkor kijelentőik száz százalékgig biztosak voltak, vagy hittek egy eszmében, már könnyen megváltozhatott utána: a 17 éves gimnazista teljesen másképp fogja látni a világot, mint a 22 éves egyetemista, pedig csak öt év eltérésről beszélünk. Az internetes keresők a véleményeiket bármikor elő tudják hozni.

Az adatvédelmi hatóságokhoz növekvő számban érkeznek panaszok az internetes keresőkkel kapcsolatban. Adatvédelmi szempontból az internetes keresők kettős szerepben léphetnek fel: keresőszolgáltatóként (mint közvetítők) és mint tartalomszolgáltatók (a gyorsítótárban eltárolt adatok következtében).

Mint tartalomszolgáltatók, az internetes keresők komoly szerepet töltenek be a publikációk közönség részére való eljuttatásában. Mint kereső szolgáltatást nyújtók, személyes adatok széles skáláját gyűjtik a szolgáltatást igénybe vevőkről: a keresési preferenciáktól egészen az

IP címig és cookie-k által megfigyelt internetezési szokásokig. Ha az érintett regisztrált felhasználóként veszi igénybe a szolgáltatást, a begyűjtött adatok minősége és mennyisége jelentősen megváltozik, a profilkép megalkotását jelentősen megkönnyítve. Tovább árnyalja a helyzetet, hogy az interneten jelen lévő információmorzsákból szintén úgy alkotható személyiségkép, mely a keresőszolgáltatók nélkül lehetetlen volna az adatok szétszórtsága miatt²⁶⁸. Problémát jelent, ha az információk közül valamely téves, vagy idejétmúlt, vagy egyszerűen más ugyanolyan nevű személyhez kötődik, negatívvá változtatva a profilképet anélkül, hogy a felhasználó tehetne arról, és komoly károkat okozhat az érintett életében a már említett módokon.

A múltbéli adattömeg megőrzése, újraelemzése, adattárházak építése és adatbányászati módszerek alkalmazása versenyelőnyt nyújthat az üzleti szférában és hatékonyságnövekedést a kormányzati szektorban, és jól illeszkedik abba a „technooptimista” elképzelésbe, amely szerint a technológia alkalmazásával megoldhatók a társadalmi problémák.

A nem felejtő internet a tudományos és technikai információk terén is okozhat problémákat: az internethasználó elavult, téves, jelenlegi megítélésünk szerint elfelejtendő vagy megváltoztatandó információkhoz juthat, amelyek relevanciája, minősége kérdéses. Az internet mint kimeríthetetlen információforrás és emlékezőgép serkenti az információkeresés illusztratív használatát: „a Google-ban mindenre van példa” (és természetesen mindennek az ellenkezőjére is).²⁶⁹

A legnagyobb keresőszolgáltatók nem csupán keresési lehetőséget, hanem szolgáltatások széles skáláját nyújtják a felhasználók részére, amely az elektronikus levelezőrendszerektől a közösségi szolgáltatásokon keresztül a navigációig bármilyen fajta lehet²⁷⁰.

A különböző szolgáltatásokkal kapcsolatban a legfontosabb adatvédelmi kérdés azok információinak összekapcsolása, mivel a felhasználó által végzett cselekmények a különböző alkalmazásokban könnyen személyiségképpé kapcsolhatók össze.

A Microsoft és a Google esetében az adatvédelmi szabályzatuk magában foglalja az adatforrások összekapcsolását²⁷¹.

²⁶⁸ Christina Burns – Michael P. Sauers: Google Search Secrets, Chicago, 2014, 15-25.

²⁶⁹ Székely Iván, Jog ahhoz, hogy elfelejtsenek és töröljenek, Információs társadalom 13. évf. 3-4. sz. 2013, 3.

²⁷⁰ Google Tips and Tricks, Imagine Publishing Ltd., 2013, 14.

²⁷¹ Microsoft adatvédelmi irányelvek (<http://privacy.microsoft.com/>)

“When you register for certain Microsoft services, we will ask you to provide personal information. The information we collect may be combined with information obtained from other Microsoft services and other companies.”, “We also deliver advertisements and provide website analytics tools on non-Microsoft sites and services, and we may collect information about page views on these third party sites as well.”

A felhasználó a regisztrálásnál (szolgáltatások közül több olyan is van, mely csak regisztrációval lehet használni, mint például a levelező rendszer) megadja a legfontosabb személyes adatait, majd a különböző szolgáltatások szintén adatforrásként szolgálhatnak²⁷². A navigációból könnyen meg lehet tudni, hogy a felhasználó hol él, merre utazik, mi a hobbija, milyen ételt szeret (melyik étterembe jár), milyen vallású (melyik templomba jár)²⁷³.

Az elektronikus levelek is tartalmuknál és címzetteknél fogva sokat elárulnak a küldő személyéről. Bár a szolgáltatók szabályzataikban kiemelik, hogy a levéltitkot tiszteletben tartják, említésre kerül azok tartalmának automatikus, gép általi vizsgálata is (pl. bűnmegelőzési célokból)²⁷⁴.

A Google ellen Kaliforniában indítottak keresetet annak tárgyában, hogy az elektronikus levelek tartalmát olvassa-e.²⁷⁵

A Google képviselői és ügyvédei a bíróságon védekezésüként előadták, hogy minden felhasználónak számolnia kell avval, hogy az elektronikus levelek automatikus feldolgozás alá kerülnek. Érdekes analógiával éltek továbbá: ha valaki egy rendes, papír alapú levelet küld az üzletpartnerének, vagy kollégájának, akkor nem meglepő, hogy a címzett asszisztense (személyi titkárja) azt kibontja. A példával a Google magát a felhasználók személyi asszisztenseként szeretné feltüntetni és a levelek tartalmának megtekintését igazolni.

A Google avval védekezik továbbá a Gmail felhasználók esetében, hogy ők a regisztráláskor elfogadták a felhasználói feltételeket és az adatvédelmi szabályzatot. Azonban a Google nem csak a regisztrált Gmail felhasználók által elküldött leveleket kezeli automatikusan, hanem a Gmail fiókokba beérkező leveleket is, melyeket természetesen olyan személyek is küldhetnek,

Google adatvédelmi irányelvek (<http://www.google.com/intl/en/privacy.html>):

“We may combine personal information collected from you with information from other Google services or third parties to provide a better user experience, including customizing content for you.”

²⁷² Nicholas Carr: *The Big Switch*, W. W. Norton & Company, Inc., New York, 2008, 47-75.

²⁷³ Google adatvédelmi és általános szerződési feltételek (2014. 11. 14.):

Az implicit helyadatok olyan adatok, amelyek alapján nem tudjuk megállapítani, hogy eszköze épp hol van, de következtetni tudunk arra, hogy Ön egy adott hely iránt érdeklődik vagy épp az adott helyen tartózkodik. Az implicit helyadatokra példa egy begépett keresési lekérdezés egy bizonyos helyről. Az implicit helyadatok különböző módokon használjuk fel. Ha például beírja az „Eiffel-torony” kifejezést, abból arra következtetünk, hogy a Párizs közelében lévő helyekről szeretne információkat találni, így ezt később felhasználhatjuk ahhoz, hogy ezekről a környékbeli helyekről javaslatokat mutassunk Önnek.

Bizonyos termékek, például a Google Térkép Mobilhoz részletes navigációja pontosabb helyadatokat használ. Ezeknél a termékeknel rendszerint ki kell választani az eszközalapú helyszolgáltatások bekapcsolását.

²⁷⁴ Chris Ridings - Mike Shishigin: *PageRank Uncovered*, 2002, 5-8.

²⁷⁵ USA District Court Northern District of California San Jose Division, Case No. 5:13-md-02430-LHK

A kereset és a Google védekezése az alábbi címen érhető el:

<https://www.scribd.com/doc/160134104/Google-Motion-to-Dismiss-061313>

akik nem Gmail felhasználók, így olyan levelek tartalmát is elolvashatja, melyeknek küldője semmilyen kapcsolatban nem állnak a Google-val²⁷⁶.

A jogi védekezésben a Google egy régi precedensre hivatkozott, amely alapján a levelet küldő félnek nem lehet elvárása a levéltitok iránt, ha a levelet önként harmadik fél kezébe adta át (akár kézbesítés céljából).²⁷⁷

Mivel a keresőszolgáltatók a reklámból és fizetett találati eredményekből nyerik bevételeik jelentős részét, ezért a személyre szabott reklámozásnál minden adatmorzsa jelentős.

Az felhasználó keresési szokásai jóval többet árulnak el róla, mint azt gondolná. A gyógyszerekre, ismerősökre, hobbiakra, saját nevére keresés bőséges információt szolgáltat, melyre az AOL²⁷⁸ ügy is rámutatott: 2006-ban az AOL nyilvánosságra hozta több, mint fél millió felhasználó keresési előzményeit névtelenül, azonban nagyon sokuk személyazonosságára rá lehetett jönni a keresési kérdések összekombinálásával (anélkül, hogy a saját nevükre rákeresők lettek volna).

4.3 Az Európai Unió Bíróságának döntése a Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos, Mario Costeja González ügyben

Mario Costeja González, spanyol állampolgár 2010-ben tett panaszt a Spanyol Adatvédelmi Hatósághoz a La Vanguardia Ediciones SL újság (egy spanyol napilap, mely nagy példányszámban került kiadásra) és a Google Spain ellen, mivel ha a Google keresőjébe beütötték az ő nevét, akkor La Vanguardia újság két cikke is megtalálható volt a keresési eredmények között, melyek számára negatív tartalmúak voltak.

A cikkek a társadalombiztosítás felé fennálló tartozásai miatt árverezés alá került házáról és az eljárásáról szóltak, melyek Mr. González szerint már megoldódtak és így nem aktuálisak.

Mr. González kérvényezte, hogy a La Vanguardia távolítsa el a róla szóló cikkeket, vagy módosítsa oly módon, hogy a személyes adatokat töröljék belőle, megszüntetve az érintettel való kapcsolatba hozhatóságot. Kérvényezte továbbá a Google-tól, hogy távolítsa el a keresési

²⁷⁶ Kristina Cutura: Advertising on Google: The High, Performance Cookbook, Packt Publishing, Birmingham – Mumbai, 2013, 47-160.

²⁷⁷ Jason Mick: Google: Yes, we "Read" Your Gmail, 2013. 08. 15.

<http://www.dailytech.com/Google+Yes+we+Read+Your+Gmail/article33184.htm#sthash.55NWTmdH.DzspukoP.dpuf>

²⁷⁸ Az America Online, vagy röviden csak AOL egy céges hálózati és internet szolgáltató.

találatok közül a cikkeket, mert azok rá negatív információkat tartalmaznak és már alaptalanok: az adóságát kifizette és az eljárás megszűnt évekkel ezelőtt.

A Spanyol Adatvédelmi Hatóság elutasította a La Vanguardia elleni kérvényt, mivel a Hatóság szerint az újság a cikket és a benne szereplő adatokat jogszerűen szerezte meg és publikálta. Furcsa módon a Hatóság a Google elleni kérvényt jóváhagyta, így arra kötelezte a kereső őriást, hogy tegye meg a szükséges teendőket annak érdekében, hogy a találati eredmények között ne jelenjenek meg a Mr. González számára sértő cikkek.

A döntés ellen a Google bírósághoz fordult, amelyben kérte a Spanyol Adatvédelmi Hatóság döntésének megsemmisítését. A bíróság előzetes döntéshozatali eljárást kezdeményezett az Európai Unió Bíróságánál a kérdés eldöntése céljából.

Az eljárás legfőbb kérdése, hogy egy internetes kereső oldal üzemeltetője felelős-e tőle független harmadik oldalak tartalmáért, amelyek megjelennek a találatok között.

Az EU Bírósága megállapította²⁷⁹, hogy az internetes keresők algoritmusai folyamatosan és szisztematikusan az internet publikus információi között kutatnak (melynek jelentős része személyes adatokat is tartalmaz), így megvalósítják az adatvédelmi irányelv által meghatározott adatkezelés fogalmát, mivel adatokat gyűjt, elemez, tárol és rendszerez, melyeket a megfelelő kérés alapján a felhasználó részére rendelkezésre bocsát a találati eredmények között (még ha az algoritmus nem is tesz különbséget a személyes és az egyéb adat között).

A Bíróság kiemelte továbbá, hogy az algoritmus által végzett műveletek adatkezelésnek minősülnek annak ellenére is, hogy csupán harmadik oldalak tartalmaira mutatnak rá, amelyek már előzőleg publikálva voltak, mivel ha az ilyen eseteket kivételnek tekintenék az adatvédelmi irányelv hatálya alól, az jelentősen csökkentené annak az alkalmazhatóságát és hatékonyságát. A Bíróság szerint a kereső üzemeltetője „adatkezelőnek” minősül, mivel az irányelv alapján ő határozza meg az adatkezelés célját és módját. Annak ellenére, hogy az információkat harmadik független oldalak publikálják, a keresőt működtető adatkezelő jelentős hatással van a magánszférához való alapvető jogra, így a keresőmotor operátora köteles rendelkezésére álló technikai és szervezési lehetőségek keretében mindent megtenni azért, hogy az irányelv rendelkezéseinek az adatkezelés megfeleljen.

Így a Bíróság szerint az érintettnek joga van a kereső üzemeltetőjét közvetlenül megkeresni, ha a keresőmotor által kiadott találatok olyan oldalra mutatnak, mely róla személyes adatokat tartalmaz, és amennyiben az üzemeltető nem teljesíti a kérést, az érintett felkeresheti a kompetens hatóságokat annak érdekében, hogy a találatokat eltávolítsák.

²⁷⁹ C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014. 05. 13.

A Bíróság így visszautasította azon érvelést, hogy az adatok feldolgozása és a keresés lefuttatása a Google külföldi szerverein történik, mely által kibújt volna az irányelv hatálya alól. Az irányelv területi hatályával kapcsolatban megállapításra került, hogy a Google Spain a Google Inc. leányvállalata Spanyolország területén, így az irányelv alkalmazható rá, mivel „letelepedett” vállalkozásnak minősül, mely egy tagállam területén folytat gazdasági tevékenységet: a tagállam állampolgárai által végzett keresésekkel kapcsolatosan promótál és értékesít hirdetési felületeket profitszerzés céljából.

A Bíróság kiemelte, hogy a keresővel egy személlyel kapcsolatos információk összegyűjtve és strukturáltan megjeleníthetők, amelyek összekapcsolásra másképpen nem lenne lehetőség, vagy csupán nehezen lenne megvalósítható.

A kereső, mely mindenkinek a rendelkezésére áll bárhol és bármikor, így alkalmas lehet személyiségek kialakítására, mely a magánszférára különösen jelentős hatással lehet, így annak működése a Bíróság szerint nem csak gazdasági szempontok szerint vizsgálendő. Ennek következtében a kereső üzemeltetőjének felelősségi körébe tartozik meghatározott körülmények között, hogy a találati listából eltávolítsa azokat a linkeket, amelyek egy személy nevére való keresés után olyan harmadik fél által készített weboldalra mutatnak, amelyek az adott személlyel kapcsolatos információkat tartalmaznak.

A Bíróság ítéletében fontosnak tartotta az Internet használóinak azon érdekét, hogy valamely személyről vagy kérdésről aktuális és pontos információkat kereshessenek és találhassanak, melyet összhangba kell hozni az érintett magánszférához való jogával. Érdekes, hogy az ítélet megfogalmazásában a Bíróság elválasztotta egymástól és külön nevesítette a privacy-hez (vagyis a magánszférához), és a személyes adatok védelméhez való jogot (a privacy a jogtudomány és a jogalkalmazás jelenlegi állása szerint magába foglalja a személyes adatok védelméhez való jogot)²⁸⁰.

A Bíróság a társadalom aktuális és pontos információhoz jutásának joga és az érintettek magánszférához való joga közül az érintettek jogát tekintette végül elsődlegesnek, melyet annyival kiegészített, hogy a két jog közötti egyensúlyt esetenként kell megvizsgálni, mivel a prioritást meghatározza az információ típusa (mennyire különleges adat), az információnak az érintett magánéletére gyakorolt hatása, továbbá a közérdek az adat nyilvánosságával kapcsolatosan (közérdekű adatok, politikusok és más közszereplők tevékenységei).

A Bíróság arra a kérdésre, hogy az érintett kérvényezheti-e a kereső üzemeltetőjétől az egyes találatok eltávolítását a listáról, a választ attól tette függővé, hogy a kérdéses találatokban

²⁸⁰ Xavier Tracol: “Invalidator” strikes back: The harbour has never been safe, Computer Law and Security Review Vol. 32. 2016. 356-358.

megjelenő tartalom megfelel-e az irányelv rendelkezéseinek: amennyiben kérés pillanatában avval nincsenek összhangban, akkor törölni kell őket. Ítéletében kiemelte, hogy a kérés pillanatában kell eldönteni, hogy az információk megfelelnek-e az irányelv rendelkezéseinek, mivel az eredetileg jogszerűen publikált adatok is az idő múlásával pontatlanná válhatnak (a publikálás óta új tények kerültek nyilvánosságra, melynek fényében a tényállás megváltozott), tévesnek bizonyulhatnak (a bíróság megállapította a vádlott alkalmasságát), vagy egyszerűen aktualitásukat veszíthetik (az elítélt letöltötte büntetését, az adós kifizette az adóságát és megoldotta a kényes helyzetét). Amennyiben az előző 3 eset valamelyike fenn áll, a kereső üzemeltetőjének el kell távolítania a találati listából az érintettel kapcsolatba hozható linkeket, amennyiben nem áll fenn egyéb körülmény (pl.: közérdek). A Bíróság kimondta, hogy az érintettnek meg kell adni a lehetőséget, hogy közvetlenül kéréssel élhessen a kereső üzemeltetője felé és annak a kérést megfelelően meg kell vizsgálnia. Amennyiben az üzemeltető úgy találja, hogy a kérés nem alapos és nem teljesíti azt, az érintettnek biztosítani kell az illetékes hatósághoz vagy bírósághoz való fordulás jogát, melynek döntését a keresőnek végre kell hajtania.

Az ítélet kihirdetése után a Google illetékese csalódottságának adott hangot, mert a határozat szerinte ellentmond a bíróság főtanácsnokának tavaly kiadott, nem kötelező érvényű állásfoglalásának, amely szerint az érzékeny információk eltávolítása a keresési találatokból sérti a szólásszabadságot, és a bíróság általában elfogadja a főtanácsnok álláspontját.

Viviane Reding, az Európai Bizottság igazságügyi ügyekben illetékes alelnöke szerint a Bíróság ítélete az adatvédelmi szabályok szigorításának brüsszeli törekvéseit igazolja. Az ítéletben nem került meghatározásra az internetes kereső fogalma²⁸¹.

Az ügy érdekessége, hogy Mario Costeja González azt szeretne volna, ha senki nem szerez tudomást a régi adósságairól és problémáiról az idejétmúlt újságcikkeken keresztül, azonban ennek pont az ellenkezőjét érte el: szinte minden országban és nyelven megjelent híradás és cikk a Bíróság döntéséről, melyen keresztül ő is a média kereszttüzébe került.

4.4 A kérelmek elbírálásának problémái és a lehetséges megoldások

²⁸¹ Julia Kerr: What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What It Means for the Future of the Right to be Forgotten, Chicago Journal of International Law, Volume 17, Number 1 Article 7, 2016.

A törlési folyamatra a Google egy űrlapot hozott létre. Az űrlapon a név és az e-mail cím megadása mellett a személyazonosság dokumentummal történő igazolására is szükség van, ehhez az érvényes vezetői engedélyének, nemzeti személyazonosító igazolványának vagy más fényképes személyazonosító igazolvány (pl. útlevél) képét kell feltölteni.²⁸²

A személyes adatok megadása után az eltávolítani kívánt webcímet kell megadni, továbbá indokolni a törlési kérelmet.

A Google figyelmeztet: az eltávolításról való döntés előtt/mellett a kérést az illetékes adatvédelmi szervnek, és az eltávolított tartalom gazdájának is továbbküldhetik, így az adott oldal üzemeltetői tudni fogják, hogy ki és milyen indokkal kérte az oldalra mutató egyes keresési találatok eltávolítását. A Google keresési találatai közötti megjelenés vállalatok és üzletemberek számára aranyat ér²⁸³, azonban a magánszemélyek jelentős részének inkább nehézséget okozhat.

A Bíróság döntése felveti a kérdést, hogy az internetes keresők üzemeltetői hogyan állapíthatják meg az érintettek kéréseinek hitelességét, az adat aktualitását és a közérdekűséget, továbbá egy magánszemély hogyan bizonyíthatná, hogy már nincsenek hitelekkel kapcsolatos problémái és nem jelent veszélyt a hitelezőkre (akiknek jogos érdekük tudni az adós fizetési képességéről és hajlandóságáról).

A kérvényező érintett nem képes alátámasztani, hogy adóságai nincsenek, hiszen erről közhitelű nyilvántartás nem létezik. A rokonok, barátok és más magánszemélyek felé fennálló hitelekről nem vezetnek nyilvántartást. Lehetséges, hogy másik adóssággal pótolta az előzőt, amely az interneten megjelent tartalom alapjául szolgált.

Tegyük fel, hogy mégis valamilyen módon bizonyítani tudja a kérvényező, hogy a kérdéses adóssága megoldódott. Ebben az esetben mennyi idő után tekinthető a hír elavultnak: egy évvel, vagy öt évvel? Mennyi ideig van joga a jövőbeni hitelezőknek informálódni a potenciális adósról? A probléma megoldásában a megfelelő joggyakorlat kialakulásáig a bankszektorban alkalmazott megoldások jelenthetnek az adatkezelők számára segítséget.

A bankok országos és nemzetközi szinten is vezetnek nyilvántartást a nem szerződészerűen teljesítő adósokról. Magyarországon a hatályos szabályozás alapján²⁸⁴ a Központi

²⁸² A Google-hez intézett törlés iránti kérelmet az alábbi oldalon lehet benyújtani:

https://support.google.com/legal/contact/lr_eudpa?product=websearch

²⁸³ Jeff Jarvis: What Would Google Do?: Reverse-Engineering the Fastest Growing Company in the History of the World, 2011, 40-42.

²⁸⁴ 1996. évi CXII. törvény (Hpt.) a hitelintézetekről és a pénzügyi vállalkozásokról, amely meghatározza a Központi Hitelinformációs Rendszer (KHR) üzemeltetésével és felhasználásával kapcsolatos szabályokat. 2001. évi CXX. törvény (Tpt.) a tőkepiacról, amely tartalmazza a KHR-el kapcsolatos adatkezelési szabályokat. 2007. évi CXXXVIII. törvény (Bsz.) a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól.

Hitelinformációs Rendszerben (KHR) aktív státuszban tartják nyilván az adóst, akinek 90 napot meghaladó, minimálbérnél magasabb összegű lejárt tartozása van. Az aktív státusz gyakorlatilag egy feketelistát jelent: a bankok nem, vagy csak nagyon kedvezőtlen feltételekkel adnak hitelt az adósoknak.

Amennyiben az adós helyzete rendeződik (kifizeti a tartozását, a pénzügyi intézet a biztosítékokból kielégíti a követelését, vagy a szerződést átütemezik), passzív státuszba kerül 1 évre (köznyelven „szürke lista”): nagyobb valószínűséggel kaphatnak hitelt, mint az aktív státuszúak, de még mindig kedvezőtlenebb feltételekkel, mintha semmilyen formában nem szerepelnének a nyilvántartásban.

Azok az adósok, akiknek a tartozása behajthatatlanná vált (pl.: a bank már leírta a tartozást), 5 évig maradnak benne a rendszerben.

A pénzügyi szektorban alkalmazott eljárás analógiájára akár 5 évben (az általános elévülési időre tekintettel) is meg lehetne határozni az érintettel kapcsolatos adatkezelés korlátját az internetes keresők üzemeltetőinek.

A Google Spain ítélet megszületése után az egyik legjelentősebb kérdés, hogy milyen módon lehetne megvalósítani a felejtés jogának érvényesítését, és kinek kellene elvégezni a törlésre irányuló kérelmek alaposságának vizsgálatát: az EU szerveinek, a nemzeti bíróságoknak, adatvédelmi hatóságoknak, vagy az internetes keresőknek?

Létrejöhett volna egy olyan megoldás, amely alapján a törlésre irányuló kérelmeket az adatvédelmi hatóságokhoz lehetett volna benyújtani, majd azok a vizsgálat után a keresőket utasítanák a törlés elvégzésére. Azonban ehelyett a Google-ra hárult a felelősség és a hatáskör, hogy törlési kérelmeket bíráljon el, ügyről ügyre kialakítva az bírálati gyakorlatot. Természetesen a Google és a keresők döntései ellen lehet az adatvédelmi hatóságoknál és bíróságoknál fellebbezni, azonban az első szó joga a Google-nál van²⁸⁵.

A helyzet természetesen a Google számára sem kedvező, hiszen evvel a hatáskörrel nem akartak és nem is terveztek rendelkezni, amely számukra felelősséget és anyagi terhet is jelent²⁸⁶.

361/2009 (XII. 30) Kormányrendelet a körütekintő lakossági hitelezés feltételeiről és a hitelképesség vizsgálatáról, amely a hitelező által elért hitelinformációs rendszerből való lekérdezési kötelezettséget írja elő.

²⁸⁵ Shaniqua Singleton, Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD, 44 Ga. J. Int'l & Comp. L. 2015. 187-193.

²⁸⁶ Edward Lee: Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten, UC Davis Law Review, No. 2015-13, 1035-1040.

3. ábra: az érintett törlésre irányuló kérelmének elbírálása a 2016-ban

Mivel az EU tagállamaiban a Google a keresőpiac több, mint 90 százalékát uralja, és az ítélet is vele kapcsolatosan született, így dolgozatomban a Google kérelmezési eljárását vizsgálom elsősorban.

A Google az ügymenetének kialakítása során a jogi csapata több olyan iránymutatást is meghatározott már a kérelmekkel kapcsolatosan, amelyek eredetileg az ítéletben nem szerepeltek²⁸⁷. A kérelmek elbírálásához a Google több jogi csoportot hozott létre, amelyek között az ügyek súlyuk szerint kerülnek elosztásra. A nehezen eldönthető ügyeket a senior jogászok vizsgálják meg.

Amennyiben egy kérelem elutasításra kerül, akkor annak indokát a Google meghatározza (pl. közérdek, vagy publikus beszéd), továbbá tájékoztatják az érintettet az adatvédelmi hatóságokhoz való fellebbezés jogáról.

Jóváhagyás esetén értesítésre kerül az érintett és a weboldal is, amelyről az adat eltávolításra került. Fontos továbbá, hogy amennyiben a jövőben a sikeres kérelmező nevére keresnek, a találati lista alján értesítés jelenik meg az eltávolítás tényéről.

²⁸⁷ Kérelme értékelése során megvizsgáljuk, hogy szerepelnek-e elavult információk Önről az eredmények között, továbbá hogy fűződik-e információkhoz – például mert pénzügyi visszaéléssel, szakmai mulasztással, büntetőítélettel kapcsolatosak, vagy mert kormányzati tisztségviselők publikus megnyilvánulásairól van szó.
(Google Súgó, letöltés ideje: 2016. 11. 15.)

A sikeres eltávolítás esetében csak a Google európai oldalainak találatairól történik meg az eltávolítás, amely jelentősen csökkent a felejtés jogának hatékonyságát, mivel napainkban a társadalom mobilitása és az utazások árának csökkenése miatt a társadalom egyre jelentősebb része használja a Google-t külföldön is. Amennyiben valaki tényleg alaposan keres egy személy után, és látja, hogy a keresett találati lista moderálásra került, abban az esetben könnyen megoldhatja, hogy például az amerikai Google oldalán indítson keresést. A problémára a 29-es Munkacsoport is felhívta a figyelmet²⁸⁸.

2016 november 18-ig a Google több, mint 600 ezer eltávolítás iránti kérelmet kapott, amely 1.78 millió linkre vonatkozott. A Google a kérelmek 42 százalékát hagyta jóvá, amely valós vizsgálatot mutat. Félő volt, hogy a Google az egyszerűbb utat választva, enyhe vizsgálattal legtöbb esetben eltávolítás mellett dönt, energiát és pénzt megspórolva.

A Google az ítélet után létrehozott egy külső tanácsadó testületet, amely független európai szakemberekből (professzorok, jogvédők) állt, hogy megvizsgálják az Európai Unió Bíróságának felejtés jogával kapcsolatos döntését és annak megvalósítására javaslatot tegyenek.

A tanácsadó testület jelentésében²⁸⁹ több szempontot ajánlott a kérelmek elbírálásának figyelembevételére:

1. Az érintett közéleti szerepvállalása
2. A kérelmezett információ természete, beleértve a gépelés során megjelenő automatikus ajánlások
3. Az adat forrása
4. Az eltelt idő, és annak hatása a konkrét esetre

A fentiek alapján kijelenthető, hogy a Google a kérdést a súlyának megfelelően kezelte, megfelelő tudással és háttérrel rendelkező csapatokat és tanácsadó testületeket állított össze feladata ellátásához.

Azonban felmerül a kérdés, hogy ez a hatáskör miért a Google-re hárult és mit csinálhatna jobban, továbbá az elutasított kérelmek milyen okokból nem kerültek fellebbezésre a kérelmezők által.

²⁸⁸ Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131-12, at 3, 9, 14/EN WP 225 (Nov. 26, 2014) [hereinafter Art. 29 Data Prot. Working Party, Guidelines]

²⁸⁹ The Advisory Council to Google on the Right to be Forgotten’ report (2015):

http://docs.dpaq.de/8527-report_of_the_advisory_committee_to_google_on_the_right_to_be_forgotten.pdf

A Google a kialakult helyzet alapján szabályalkotó, döntéshozó és vizsgálati jogkörökkel is rendelkezik alapvető jogok érvényesítésével kapcsolatosan. Az EU Bíróságának döntése után a Google határozta meg a felejtéshez való jog szabályait, a kérelmekről az első döntést szintén ő hozza meg, továbbá a kérelmek alaposságát és a benyújtott dokumentumokat is a Google vizsgálja meg, amelyek különösen jelentős hatáskörök.

A Google első körös vizsgálata melletti érvek közül a legjelentősebb a költséghatékonyság: a nemzeti adatvédelmi hatóságoknak a bírálatok kezeléséhez jelentős személyi és eszközállomány bővítése lenne szükséges. Minden tagállam adatvédelmi hatóságának külön elkészíteni egy online panaszkezelési felületet nem lenne gazdaságos, és a működésük, színvonaluk között is eltérések lennének.

Az EU hatáskörének hallgatólagos delegálása a Google-ra több szempontból is problémás lehet. A Google alkalmazottai nem köztisztviselők/közalkalmazottak, hanem egy profitorientált vállalat dolgozói, amelynek elsődleges célja a saját és részvényesei érdekeinek a képviselete. Egy közalkalmazott/köztisztviselő másképpen vonható felelősségre és munkavégzésére egyéb etikai szabályok is vonatkozhatnak, míg a Google esetében a kérelmező még azt sem tudhatja, hogy ki bírálja el a kérelmét, továbbá, hogy a bíráló tagoknak milyen képesítése van, mennyire vannak felkészítve a kérelmek kezelésére.

Egy közigazgatási eljárás során van lehetőség személyes ügyintézésre és meghallgatásra, a Google esetében ez nem áll fenn, amely nem csak a technológiában kevésbé jártas érintetteknek jelentethet komoly hátrányt.

A Google érdeke elsősorban, hogy minél több keresést futtassanak le rajta, amelyhez elengedhetetlen a releváns és minél teljesebb találati lista. A Google-nak ugyanakkor jelentős gyakorlata van már a kérelmek kezelésében: az USA-ban a Digital Millennium Copyright Act folytán már évtizedes tapasztalattal és több millió elbírált kérelemmel a háta mögött rutinosan tudta megkezdeni a kérelmek kezelését, még ha eltérő jogi problémával kapcsolatban is kellett megtennie.

Megjelentek továbbá olyan online szolgáltatások, amelyek ellenszolgáltatásért cserében segítenek az érintetteknek a kérelmeik benyújtásában a keresőszolgáltatók részére. Az ilyen szolgáltatásokkal kapcsolatban problémaként merül fel, hogy akkor is elkérhetik a pénzüsszeget, amennyiben az eltávolítási kérelem sikertelen, és már a kérelem benyújtásakor is valószínűsíthető volt az elutasító határozat²⁹⁰.

²⁹⁰ Sebastian Schweda: Right to Be Forgotten Also Applies to Online News Archive, Supreme Court Rules, European Data Protection Law Review Volume 1, Issue 4. 2015. 301.

Kérdésként merül fel továbbá, hogy a kisebb online keresők, amelyek nem rendelkeznek megfelelő anyagi háttérrel a kérelmek elbírálásához, hogyan lennének képesek felejtés jogának érvényre juttatására. Bár a piaci részesedésük a Google, Bing és Yahoo mellett elenyésző, ha valaki teljesen el szeretné távolítani a rá vonatkozó találatokat a többi, kisebb internetes keresőnél is, az valószínűleg nem lenne megvalósítható²⁹¹.

A döntési gyakorlat kialakítása egy új területen hosszabb időbe telhet és a kezdeti hibák elkerülhetetlenek. A kísérleti nyúl szerepét és felelősségét a Google kapta meg: az uniós és a nemzeti hatóságok másodfokú szinten vannak, a Bing és Yahoo alacsony részesedéssel bírnak a keresőpiacon Európában.

A megoldást egy egységes uniós online kezelőfelület jelenthetné, amelyen a felhasználók benyújthatnák a kérelmüket, továbbá a személyes kapcsolatfelvétel és benyújtással kapcsolatos segítségnyújtás a nemzeti adatvédelmi hatóságoknál történhetne.

Az egységes kezelőfelület egyik előnye, hogy az ott benyújtott kérelmek automatikusan alkalmazhatóak lennének a Bing-re, Yahoo-ra és egyéb keresőkre is, így az érintettnek nem kellene az egyes szolgáltatók felületein külön beadványt szerkesztenie és dokumentumokat feltöltenie, így jóval egyszerűbb és felhasználóbarátabb megoldás lenne.

4. ábra: az érintett kérelmének elbírálása hibrid bizottságok által

²⁹¹ Bunny Sandefur: The best practice of forgetting, Emory International Law Review, Vol. 30 Issue 1, 2015. 90-114.

Az egységes kezelőfelület után továbbra is a keresőszolgáltatóknál maradna a döntés lehetősége első körben, amely jelentős terhet venne le a nemzeti adatvédelmi hatóságokról.

A felhasználó érdekeit azonban egy beépített mechanizmus védené: amennyiben a keresőszolgáltatók közül az egyik jóváhagyná a kérelmet, míg valamelyik elutasítaná, abban az esetben a kérelem automatikus felülvizsgálatra kerülne egy hibrid bizottság által²⁹².

A felülvizsgálatot hibrid nemzeti bizottságok végezhetheték a nemzeti adatvédelmi hatóságok koordinálása alatt: a bizottságok a hatóságok szakembereiből, továbbá a keresőszolgáltatók és civil jogvédő szervezetek delegáltjaiból állhatnának, amely biztosítaná az érdekelt felek képviselését, társadalmi kontrollt, a szakmai háttérrel és nem utolsósorban terhet venne le a hatóságokról is.

Így például egy 5 fős nemzeti bizottság állhatna 3 hatósági szakemberből, 1 keresőszolgáltató és 1 jogvédő szervezet általi delegáltból. Tagállamonként akár több bizottság is lehetne, az ügyteher függvényében.

A módszer előnye lenne, hogy több keresőszolgáltató véleménye kerülhetne összehasonlításra, továbbá ütközésük esetén a hibrid bizottság lehetne a mérleg nyelve. Az eljárással kapcsolatos költségek is összességében csökkennének, a több párhuzamos eljárás megszüntetésével, mivel a kérelmek egységesen kerülnének elbírálásra²⁹³.

A vázolt eljárás alól kivételt képezhetnének az érintett számára különösen fontos és súlyos esetek, mint például a bűncselekmények áldozatai, akikkel kapcsolatban a kereseti találatok eltávolítását egyből követelhetné az adatvédelmi hatóság oly módon, hogy az eltávolítás

1. A Google összes országban lévő találati listájából történne,
2. Az eltávolítás tényéről a találati lista alján nem jelenne meg információ,
3. Az oldal, amelyen az információ publikálásra került, nem kapna értesítést.

A megoldás a Google számára is előnyös lenne, mivel a hibrid bizottságokban a Yahoo és a Bing delegáltjai is jelen lehetnének, így nem csak a Google-t érnék a vádak és a döntés terhe a felejtés jogával kapcsolatban a keresőszolgáltatók közül.

²⁹² Lee, 1038.

²⁹³ Emmanouil Bougiakiotis: The enforcement of the Google Spain ruling, *International Journal of Law and Information Technology*, 2016, Vol. 24, 326-335.

A hibrid bizottságok döntése ellen továbbra is lehetséges lenne fellebbezni a nemzeti adatvédelmi hatóságokhoz, azonban véleményem szerint jóval kevesebben élnének ezzel a lehetőséggel, mivel a hibrid bizottságok döntése és az elsőkörös vizsgálat mechanizmusa komolyan alátámasztaná a döntést, továbbá az adatvédelmi hatóságoknak is könnyebb és gyorsabb lenne eldönteni a fellebbezett kérelmeket a hibrid bizottság által vizsgált és kidolgozott anyagok birtokában.

Az adatvédelmi hatóságok döntése ellen pedig lehetséges lenne bírósági úton megoldást keresni.

A felejtés jogának igazi érvényesülése lenne, ha az eltávolítás a Google összes országban elérhető oldaláról megtörténne, azonban az nehezen lenne megvalósítható, mivel egyes országokban másképp mérlegelik az alkotmányos alapjogok egymáshoz való viszonyát, így például az Egyesült Államokban a szólás- és sajtószabadság különösen erős az első alkotmánymódosítás alapján²⁹⁴.

Az keresési találatokból eltávolított oldalak értesítése azért is jelenthet problémát, mivel már több olyan oldal alakult, ahol listázzák az eltávolított oldalakat és kérelmeket, amelyek gáncsolják a felejtés jogának érvényesülését olyan esetekben, amikor a Google, vagy a fellebbezés folytán a hatóságok a kérelmet jogosnak találták²⁹⁵.

²⁹⁴ Az AOL találati listáján megjelenített tartalmakkal kapcsolatos eltávolítási kérelem elutasítása is rámutat a szólás- és sajtó szabadság különböző megközelítésére, *Zeran v. America Online*, 129 F.3d 327, 331 (4th Cir. 1997);

²⁹⁵ Julia Powles: *The Case That Won't Be Forgotten* Loyola University of Chicago Law Journal 583, 2015. 609.

4.5 Következtetések

A dolgozat jelen fejezetében áttekintettem a felejtés jogának kialakulását, érvényesülésének feltételeit és módjait, továbbá lehetséges megoldásokat vettem fel az offline és online megvalósításának erősítéséhez.

A felejtés jogának érvényesítéséhez legelső lépcső az adatkezelő személyének meghatározása, amely az online adatkezelések során a közvetítő szolgáltatók miatt egyre nehezebbé vált, továbbá a felejtés és a törlés nem feltétlenül fedik egymást: hiába létezik egy információ az internet tengerében, ha azt nem lehet megtalálni a közvetítő szolgáltatók segítségével.

Mivel sok esetben az információ eltávolítása az internetről nem lehetséges, így a felejtéshez való jog sok esetben az „elrejtéshez való jog” felé vezet, amelyet jól illusztrál, hogy a probléma kezelése a legnagyobb internetes keresőszolgáltatóval kapcsolatban csúcsosodott ki.

Bár a fejezetben az adatkezelő és adatfeldolgozó elhatárolása hangsúlyos szerepet kapott, a felejtés jogának gyakorlati megvalósításának vizsgálata során realizálódott számomra, hogy a hagyományos különbségtétel a kezelő és feldolgozó között az online környezetben - ahol az érintett különösen védelemre szorul - meghaladtá vált, hiszen a tartalomfogyasztás és terjesztés egyre inkább áttételesen történik, amelyet a Facebook hírportál funkciója is jól mutat.

A felejtés jogának természetessé tételére Viktor Mayer-Schönberger javaslata – az adatok automatikus törlési idővel való ellátása – merőben új megközelítést jelent, amely az érintettek számára tudatosítaná, hogy az adatok jobb, ha nem az örökkévalóságnak szólnak.

Véleményem szerint a törlés helyett egy kevésbé radikális módszerrel is tudósítható lenne a felhasználókban a felejtés fontossága és az adatok biztonsága: törlési idő helyett „archiválási idő” lehetne megadható az adatokon, amelynek elteltével az adat áthelyezésre kerülne egy tömörített és jelszóval védett mappába, ahova csak a mentést végző felhasználónak lenne hozzáférési joga, másnak nem. Az áthelyezett fájlok törlésre kerülnének az eredeti helyükről, és csak a biztonságos mappába csak a felhasználó által kerülhetnének biztonsági lépések után elérhetőek.

Hasonló megoldást lehetne alkalmazni akár az interneten használt szolgáltatások esetében is. A Google keresései során megadható lenne a keresés megőrzésének ideje a keresett szó után. Így ha csak egyszeri alkalommal tervez a felhasználó egy tárgyra keresni, például egy esküvői gyűrűre, akkor bejelölhetné a keresés tárolási idejét nullára. Evvel szemben, amikor az érintett

valamilyen témában hosszabb távon tervez kutatni, mint például egy PhD hallgató a dolgozata tárgyában, akkor a keresés tárolását hosszabb időtartamban adná meg.

A felejtés jogának érvényesüléséhez az EU Bíróságának határozata mérföldkőnek számított, és egy olyan folyamatot indított el, amely az érintettek érdekeit védi a legnagyobb online adatkezelőkkel szemben.

A Google kénytelen volt magára vállalni a törlésre irányuló kérelmek elbírálására vonatkozó szabályok és eljárások kialakítását, amelyet sok éves szerzői jogi kérelmekkel kapcsolatos gyakorlatával gyorsan és szakszerűen teljesített a saját költségére és felelősségére, azonban a helyzet távol áll a tökéletestől.

Az eljárással kapcsolatban kiemelttem a személyes ügyintézésrel és a közfeladatok Google-ra delegálásával kapcsolatos problémákat, alternatív megoldási javaslatokat kidolgozva oly módon, hogy a nemzeti hatóságokra se háruljon különösen nagy ügyteher, továbbá más internetes keresők és civilek is részt vehessenek a folyamatban.

Az megoldást egységes uniós online kezelőfelület jelenthetné, amelyen a felhasználók benyújthatnák a kérelmüket, továbbá a személyes kapcsolatfelvétel és benyújtással kapcsolatos segítségnyújtás a nemzeti adatvédelmi hatóságoknál történhetne.

Az egységes kezelőfelület után továbbra is a keresőszolgáltatóknál maradna a döntés lehetősége első körben, amely jelentős terhet venne le a nemzeti adatvédelmi hatóságokról.

A felhasználó érdekeit azonban egy beépített mechanizmus védené: amennyiben a keresőszolgáltatók közül az egyik jóváhagyná a kérelmet, míg valamelyik elutasítaná, abban az esetben a kérelem automatikus felülvizsgálatra kerülne egy hibrid bizottság által, amely hatóságok szakembereiből, továbbá a keresőszolgáltatók és civil jogvédő szervezetek delegáltjaiból állhatnának, biztosítva az érdekelt felek képviselését, társadalmi kontrollt, a szakmai háttérrel és nem utolsósorban terhet venne le a hatóságokról is.

A módszer előnye lenne, hogy több keresőszolgáltató véleménye kerülhetne összehasonlításra, továbbá ütközésük esetén a hibrid bizottság lehetne a mérleg nyelve. Az eljárással kapcsolatos költségek is összességében csökkennének, a több párhuzamos eljárás megszüntetésével, mivel a kérelmek egységesen kerülnének elbírálásra.

A felejtés jogának érvényesítéséhez rámutattam továbbá az egyes kérelmek elbírálása során felmerülő nehézségekre, mint például a tények valóság tartalmának az eldöntése hivatalos határozatok, bírósági ítéletek hiányában, lehetséges megoldást keresve az egyes szektorokban kialakított elévülési idők alkalmazásával, így például egy személy fennálló adósságával

kapcsolatban a bankok által üzemeltetett „fekete” és „szürke” listák során alkalmazott elévülési időkkal.

Az eljárások és a bírálati szempontok tökéletese, továbbá a felhasználói tudatosság növelése jelentik a kulcsot a felejtés jogának az érvényesítéséhez, továbbá az alapjoggal való ütközésének a feloldásához, amely különösen fontos az érintettek jogainak védelméhez, továbbá a véleménynyilvánítás és a sajtószabadság biztosításához.

5. Adatvédelem a közösségi hálózatokon, különös tekintettel a Facebookon

Több, mint egy milliárd felhasználójával a Facebook a világ egyik legnagyobb - nem állami - adatkezelője. Súlyát nem csupán a regisztrált felhasználók száma, hanem az általuk szolgáltatott adatok mennyisége és minősége adja: az alapvető személyes adatoktól (pl. név, születési hely és idő) a különleges adatokig (pl. vallás, politikai nézetek) olyan információk tudhatóak meg a felhasználókról, amelyeket önként adnak meg, növelve annak hitelességét. A felhasználók ismerősein keresztül olyan kapcsolati háló is kirajzolható, melyről másképpen – még titkosszolgálati eszközökkel sem - lehetne tudomást szerezni.

A Facebook személyes adatbázisának egyediségét és különlegességét mutatja, hogy a világ minden országában, ahol a szolgáltatása jelen van, az állami titkosszolgálatok rendszeresen megkeresik és együttműködését kérik (vagy megkövetelik).

A felhasználók számának növekedését csak úgy tudja a vállalat fenntartani, ha egyre több országban nyitja meg a lehetőséget a felhasználók regisztrálására. Egy új ország azonban nem csak felhasználói táborát és hirdetőket hoz magával, hanem egy új jogrendszert is, melynek meg kell felelnie.

Olyan szolgáltatást nyújtani nagyon nehéz, mely egységesen minden országban működőképes és minden jogrendszernek megfelel: a „modern” adatvédelmi jogszabályok egyre több országban jelennek meg és – főként az Európai Unió adatvédelmi elvárásai és standardjai miatt²⁹⁶ - folyamatosan szigorodnak.

Facebookal kapcsolatos adatvédelmi kérdések, problémák és perek voltak, vannak és – a felhasználók számának növekedése miatt - egyre sűrűbb lesz az előfordulásuk. Alig van olyan adatvédelmi joggal foglalkozó jogtudós, aki ne vizsgálná a „Facebook jelenséget”: azon túl, hogy egy maga nemében egyedi adatbázisról van szó, a szolgáltatás alkalmas arra, hogy teljesen új gondolatok terjedjenek el rajta, hatással legyen a titkosszolgálatok működésére, megváltoztassa a reklámozási piacot, és akár forradalmak szerveződjenek rajta (pl. Egyiptom)²⁹⁷.

²⁹⁶ Multinacionális vállalatoknál, melyek nemzetközi szolgáltatásokat nyújtanak, általában az adatvédelmi szabályzataikat és mechanizmusait az Európai Unió által megkövetelt szintre szövegezik meg, mivel ha annak megfelelnek, akkor valószínűleg más országokban sem lesz problémájuk adatvédelem szempontjából.

²⁹⁷ Carol Huang: Facebook and Twitter key to Arab Spring uprisings: report, TheNational, 2011. 06. 06. <http://www.thenational.ae/news/uae-news/facebook-and-twitter-key-to-arab-spring-uprisings-report#ixzz3AB7jvokd>

5.1 A Facebook megalapítása és működése

Mark Zuckerberg alapította meg a Facebookot 23 évesen a Harvard egyetem pszichológus hallgatójaként. Az oldal eredeti neve „The facebook” volt, mely egy papír alapú kiadványból eredt, amely az elsőéves hallgatóknak mutatta be a hallgatótársaikat és az egyetem személyzetét.

2004-ben nyitotta meg Zuckerberg az oldalt, melyhez 24 órán belül 1200 hallgató csatlakozott, egy hónapon belül pedig a hallgatók fele az oldal regisztrálói között szerepelt. Az oldal folyamatosan nyitotta meg kapuit az oktatásban részt vevő potenciális felhasználók előtt: először az amerikai egyetemek hallgatói csatlakozhattak, majd később a középiskolások is.

2005-ben az oldal neve rövidebb „Facebook” lett, a „www.facebook.com” domain cím megvásárlásával.

2006. szeptember 26-án nyílt meg a Facebook mindenki számára, aki elérte a 13 éves korhatárt és érvényes e-mail címmel rendelkezett.²⁹⁸ A társaság 2009 óta termel profitot.

2010 júliusában már 500 millió felhasználója volt, majd 2012 szeptemberében lépte át a felhasználók száma az egy milliárdot, mellyel egyben a Világtörténelem egyik leggyorsabban fejlődő vállalkozásává vált.²⁹⁹

A felhasználók száma folyamatosan növekszik (lassuló ütemben): 2014 januárjában már 1 milliárd 300 millióan használták a Facebook-ot havi rendszerességgel.³⁰⁰ További fontos adat a felhasználói aktivitásról, hogy 2011 júniusában egy billiószor látogatták meg a Facebook oldalát, mellyel az internet leglátogatottabb oldalává vált.³⁰¹

A Quantcast, Comscore és a legjelentősebb forgalommérők rangsoraiban rendszeresen a top 3 oldalban szerepel a Facebook a világ leglátogatottabb oldalai között.

A Facebook a legnépszerűbb szociális hálózat az angol anyanyelvű országokban és a nyugati államok többségében is: az Egyesült Államokban, Kanadában, Angliában, Ausztráliában és Új-Zélandon még csak meg sem közelítik a helyi oldalak (USA-ban a MySpace is komoly hátrányba került). Keleten már más a helyzet: vagy a helyi szociális hálózatokat kedveli a lakosság, vagy le van tiltva a Facebook.

²⁹⁸ Carolyn Abram: Welcome to Facebook, everyone, The Facebook Blog, 2006. 09. 26.

²⁹⁹ The Wall Street Journal, 2012. 11.04.

³⁰⁰ Aktív felhasználó: az a természetes személy, aki havonta legalább egyszer bejelentkezik a fiókjába.

³⁰¹ John Paul: "Facebook Hits 1 Trillion Pageviews", ReadWriteWeb, 2011. 08. 24.

http://web.archive.org/web/20110911044951/https://www.readwriteweb.com/archives/facebook_hits_1_trillion_pageviews.php

Több, mint 2,5 milliárd internetező él a Világon, akiket el szeretne érni a Facebook. Nyugaton már egyre nehezebb az aktív felhasználók számát növelni, ezért a vállalat mindent megtesz a keleti bővítés érdekében, hogy a részvényesek által megkívánt növekedést fenntarthassa (a lassulást csökkentse). Mark Zuckerberg többször látogatott Kínába és Oroszországba. Kína több, mint fél milliárd internet felhasználóval rendelkezik, mely hatalmas piacot jelentene, viszont a számukra nem engedélyezett a Facebook használata (kivéve a diplomatákat és a szabadkereskedelmi övezetet³⁰²).

Az aktív felhasználók számának növeléséhez elengedhetetlen az internettel rendelkezők gyarapodása. A Facebook tagja a Megfizethető Internetért Szövetségnek (The Alliance for Affordable Internet).³⁰³

A felhasználók számával kapcsolatosan fontos kiemelni, hogy 8-9 százalékuk nem valódi felhasználó. Egy 2012-es jelentésében a Facebook tért ki erre a kérdésre, melyben megállapításra került, hogy a felhasználói fiókok 4.8 százaléka olyan felhasználóké, akik más néven már rendelkeznek felhasználói fiókkal („duplicate account”), további 2.4 százalékuk olyan felhasználó, melyek nem természetes személyek (pl.: jogi személyek, háziállatok), valamint 1,5 százaléka a felhasználóknak jogtalan regisztráló (pl.: 13 éven aluli, vagy spammelés céljára regisztrált).

Egy 2011-ben a GoodMobilePhones által készített felmérés alapján egy átlagos Facebook felhasználó az ismerősei ötödét nem ismeri.³⁰⁴

A természetes személyek harmada tartozik a nagyon aktív kategóriába, mely többszöri bejelentkezést jelent naponta a szolgáltatások rendszeres használatával. A jövő tendenciája a mobil eszközök használata: az elektronikai és szoftvercégek jelentős része már az okostelefonok és a táblagépek piaca felé terjeszkedik, a hagyományos asztali gépek célközönségének csökkenése miatt.³⁰⁵ A Facebook is mindent megtesz a trend követése

³⁰² Heather Timmons: China will unblock Facebook, Twitter and The New York Times to boost its new free trade zone, Quartz, 2013. 09. 24.

³⁰³ A Szövetség az állami és a privátszféra szereplőinek együttműködéséből jött létre, olyan tagokkal, mint a Google és a Microsoft. Célja, hogy az internetelérést lehetővé tegyék olyan helyeken, ahol az infrastrukturális okokból vagy a társadalom gazdasági helyzete miatt nem vagy csak nagy nehézségek árán lenne lehetséges (elsősorban a fejlődő országokban). Az „elérhetőség” és „megfizethetőség” alatt értik az Egyesült Nemzetek Broadband (szélessávú internet) Bizottsága által meghatározott összeget, mely a havi jövedelem maximum 5%-át jelenti.

³⁰⁴ A feltevés bizonyítására a New Jersey-ben lévő Millburn Gimnáziumban csináltak a hallgatók egy hamis felhasználót „Lauren” néven, akinek a nevében ismerősnek jelöltek 200 felhasználót a gimnázium hallgatói közül. A 200 ember közül csupán kettő küldött üzenetet, melyben kérdőre vonták Laurent, 60%-uk visszajelölt ismerősnek, és csupán 40%-uj utasította őt el. Külön érdekesség, hogy a felmérésben nem is szereplő 55 ismeretlen ember ismerősnek jelölte hamis felhasználót.

³⁰⁵ 2012-ben az világ összes okostelefon használója meghaladta az egymilliárdot, majd 2014-ben elérte a 1,75 milliárdot.

érdekében: 2014-ben a Facebook mobil alkalmazást használó felhasználók száma elérte az egymilliárdot, a cég profitjának jelentős része pedig a mobil szegmensen realizálódott.³⁰⁶

A mobil felhasználók számának növekedésével előtérbe kerülnek a földrajzi helyzet meghatározásán alapuló szolgáltatások: egy felhasználó földrajzi helyzetének meghatározásával olyan személyre szabott reklámok juttathatóak el az érintett részére, mint a közelében lévő étterem aktuális menü ajánlata, vagy a legközelebbi taxi elérhetősége.

Adatvédelmi szempontból több kérdést és aggályt is felvetnek az ilyen szolgáltatások: egy ember útvonaláról és tartózkodási helyeiről olyan érzékeny információk szűrhetőek le, mint a vallása (mely templomban járt), politikai nézetei (részvétel egy politikai gyűlésen), betegsége (tartózkodás egy orvosi rendelőben).

A keresőszolgáltatók és a közösségi hálózatok terjedésében fontos szerepet játszik az oktatás átalakulása is: az ismeretek megszerzésére és terjesztésére a Google és a Facebook is egyre gyakrabban használt platform³⁰⁷.

Bár a helymeghatározást ki lehet kapcsolni, avval sok felhasználó nincsen tisztában, és az érintőképernyős eszközökön egy figyelmetlen mozdulattal könnyen aktívvá tehetjük a szolgáltatást³⁰⁸.

A közösségi háló fogalma

Nehéz pontosan meghatározni a közösségi oldalak fogalmát, mivel eltérést találhatunk közöttük a célcsoport, szolgáltatások, alkalmazások, a begyűjtött adatok minősége és mennyisége, továbbá azok felhasználása terén³⁰⁹.

A közösségi hálózatok olyan kommunikációs platformok, amelyek lehetőséget nyújtanak a felhasználók számára, hogy a személyes adataikból, képeikből adatlapot (profil) hozzanak létre, mely azonosításukra szolgál, továbbá kapcsolatot létesítsenek felhasználókkal és képesek legyenek saját – és sok esetben ismerőseik – kapcsolatrendszerét megtekinteni.

További fontos tulajdonsága a közösségi hálózatoknak, hogy elsősorban nem kapcsolatépítésre, hanem kapcsolattartásra jöttek létre: a hálózatok természetesen alkalmasak arra, hogy a tagok

³⁰⁶ Ben Popper: Facebook now has more than a billion mobile users every month, The company is making nearly twice as much per user as it did one year ago, 2014. 04. 23.

<http://www.theverge.com/2014/4/23/5644740/facebook-q1-2014-earnings>

³⁰⁷ Tara Brabazon: The University of Google: Education in the (Post) Information Age, Ashgate Publishing Limited, 2007, 24-26.

³⁰⁸ Tom Taulli: How To Create The Next Facebook, Apress, 2012, 19-40.

³⁰⁹ Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (1. rész), Infokommunikáció és Jog, 38. szám, 110-112.

idegenekkel is megismerkedhessenek, azonban a kapcsolati rendszer létrejötte a korábbi ismeretségtől függ, mivel a személyes adatok (név, lakhely, munkahely) segíthetnek az ismerősök megtalálásában.

Jogi szemszögből nézve a közösségi hálózatok információs társadalommal összefüggő szolgáltatásnak tekinthetők.

A személyre szabott internet

Napjainkban az internet egyre személyre szabottabbá, kezelhetőbbé válik, mert a weboldalak egyre többet tudnak a felhasználóikról: a keresőkben számukra releváns eredmények születnek, a Facebook híroldalán a felhasználók számára a legérdekesebb, legaktuálisabb hírek jelennek meg, az érdeklődési körüknek megfelelő reklámokkal árasztják el őket.³¹⁰

Az algoritmusok, melyek a felhasználó korábbi tevékenységei és körülményei figyelembe vételével próbálják meghatározni a számukra releváns tartalmakat, hasznosságuk ellenére korlátot is jelentenek: csökkentik az esélyét, hogy új, a megszokott érdeklődési területükön kívüli információt kaphassanak a felhasználók, vagy, hogy olyan emberekről láthassanak híreket, akikkel már rég nem tartják az aktív kapcsolatot. Az általános iskolai osztálytárs állapota és eseményei kisebb eséllyel láthatóak a hírfolyamban, mint a kollégáké, akikkel a felhasználó napi rendszerességgel vált üzenetet³¹¹.

2011-ben a Facebook átnevezte a „Privacy Policy-t” (a magyar fordítás nehézkes: az „adatvédelmi szabályzat” egyértelműen kevesebbet jelent), és az új neve „Data Use Policy” lett (Adatfelhasználási Szabályzat) lett, mely több privacy szkeptikus szerint arra utalhat, hogy a Facebook elsősorban az adatok gyűjtésére, tárolására és felhasználására koncentrál, mivel a profitja ebből származik.³¹²

A közösségi hálózatok arra bátorítják a felhasználókat, hogy minél több személyes adatot osszanak meg, mert azokat majd számítógépes algoritmusokkal kiszűrjük, és a felhasználói közösség számára hasznossá tesszük, még személyre szabottabbá téve a felhasználói élményt.

³¹⁰ Executive Office of the President. (March 29, 2012). Big Data Across the Federal Government. The White House. http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_fact_sheet_final_1.pdf

³¹¹ Brad and Debra Schepp: How find a job on LinkedIn, Facebook, MySpace, Twitter and other social networks, New York, 2012, 149-169.

³¹² Segall, Laurie (March 23, 2012). Facebook strips 'privacy' from new 'data use' policy explainer. CNN Money. <http://money.cnn.com/2012/03/22/technology/facebook-privacy-changes/index.htm>

Állandó kérdés, hogy a Facebook hogyan szűri ki a felhasználók számára releváns információkat és reklámokat. Az adatokat feldolgozó algoritmusok pontos technikai paraméterei az üzleti titok körébe tartoznak, melyek nagyon sok pénzbe és energiába kerülnek minden felhasználói adatbázist feldolgozó vállalatnak, így érthető, hogy azokat nem hozzák nyilvánosságra.

A Facebook részéről Bret Taylor CTO (Chief Technology Officer, Technikai Igazgató) úgy nyilatkozott, hogy „A Facebook programozói készítettek egy matematikai algoritmust, mely megvizsgálja a felhasználó személyes adatait és a nyilvánosságra hozott információkat ..., mely alapján az oldal megpróbálja megjósolni, hogy mi iránt érdeklődik, a korábbi preferenciáit megvizsgálva. A megoldás ahhoz hasonló, amikor a rendszer meghatározza, hogy a hírfolyamra olyan ismerőseink hírei kerüljenek rá vagy kerüljenek előre³¹³, akikkel gyakrabban tartunk kapcsolatot.”³¹⁴

A Facebook algoritmusát, mely a felhasználókról begyűjtött óriási adathalmazt feldolgozza és hasznosíthatóvá teszi a hírfolyam működésében, „EdgeRanknak” hívták 2011-ig, amíg a Facebook meg nem változtatta „News Feed Ranking Algorithma” (hírfolyam rangsorolásáért felelős algoritmus), mely több, mint százezer körülményt vesz figyelembe a hírek rangsorolásánál.

Összetettsége ellenére a működésének alapjai egyáltalán nem bonyolultak, melyek programozói tudás nélkül is megérthetőek.

A legfontosabb fogalom az „Edge”, mely alatt „minden felhasználói tevékenységet” értünk (például személyes adat felöltése, kommentelés, likolás, kép feltöltése, ismeretség létrejötte).

Az algoritmus működése: az „Edge-ek” összessége, melyek súlyozva vannak a „rokonság”, „fontosság” és „aktualitás” alapján.

$$\sum u_e w_e d_e$$

rokonság (ismertség) + fontosság + aktualitás

U_e : a rokonság (ismertség) foka (affinity).

A felhasználó és a hírt létrehozó közötti rokonság foka. Annál nagyobb, minél közelebb áll az adott személyhez.

1. szűk család (szülők, testvér, gyermek)

³¹³ "Facebook programmers have created a mathematical algorithm that will examine the types of posts a person has chosen to give prominent placement to on his or her profile.... Whether food, movies or exercises logged into Facebook, the site will try to predict what you're most passionate about based on past choices, similar to how the system determines its news feed based partly on the people you contact most often"

³¹⁴ Mark Milian (January 19, 2012). 60 apps launch with Facebook auto-share. CNN. <http://www.cnn.com/2012/01/18/tech/social-media/facebook-actions-apps/index.html>

2. távolabbi rokonok (unokatestvér)

3. közeli barát

4. ismerős

Azt, hogy egy adott személy mennyire áll közel a másik felhasználóhoz, az algoritmus abból tudja meghatározni, hogy milyen gyakran és milyen módon létesít kapcsolatot az adott személlyel a Facebookon:

1. rendszeres üzenetváltás,

2. ritka üzenetváltás,

3. ismerős állapotának kommentelése.

4. ismerős valamely posztjának like-olása.

We: fontosság foka

Azt, hogy egy tevékenység mennyire fontos, általában az arra szánt idő hosszából állapítható meg:

1. a kommenteléshez szükséges a legtöbb idő és energia, ezért fontos eseménynek minősül,

2. egy like-hoz csak egy kattintás és egy másodperc kell, így az nem számít fontos eseménynek.

de: aktualitás foka

Egy hír, like vagy komment aktualitását leginkább az mutatja, hogy mennyire friss. Ahogy egy tevékenység öregszik, úgy veszít az értékéből.

A bemutatott három alapvető tényezőn túl a Facebook algoritmusa figyelembe vesz sok más szempontot is, mely közül a legfontosabb a felhasználó érdeklődési köre, mely egyben a személyre szabott hirdetések célba juttatására is szolgál.

Felhasználó: érintett vagy adatkezelő?

Az életviszonyok jelentős részében könnyen meghatározható, hogy ki az adatkezelő és az érintett: egy mobilszolgáltatóval kötött szerződés, egy közvélemény kutatás, vagy bármilyen állami adatkezelés esetén egyértelműek a szerepek.

Az interneten lévő közösségi oldalak (pl. Facebook, Twitter, MySpace) és tartalommegosztó szolgáltatások (Youtube) esetében már elmosódik a határvonal és nem egyértelmű, hogy a felhasználó csupán érintett, vagy adatkezelő is: a közösségi és más tartalommegosztáson alapuló oldalakon tulajdonképpen a felhasználók töltik fel az adatokat, amelyek jelentős része személyes adat, és az oldal a technikai hátteret biztosítja erre.

Az online tartalomfogyasztás világában egyre nehezebb elhatárolni egymástól az hírközlő, közvetítő, adatszolgáltató és kereső fogalmát. A Facebook igyekszik a felsorolt szerepeket egyedül betölteni a jövőben³¹⁵, azonban a felelősség minimális szintre való csökkentésével.

A nem egyértelmű helyzetet az oldalak üzemeltetői igyekeznek kihasználni: hajlamosak magukat csupán adatfeldolgozóként feltüntetni és próbálják az adatvédelemmel kapcsolatos felelősséget a felhasználóra áthárítani.

A közösségi hálózat szolgáltatója adatkezelőnek minősül, mivel meghatározza a személyes adatok feldolgozásának módját és céljait: a szolgáltató határozza meg, hogy milyen fajta adatokat adhatnak meg magukról a felhasználók, milyen formátumban és számban tölthetnek fel képeket magukról és milyen beállításokkal oszthatják meg azokat (mód).

Az adatkezelés céljának meghatározása az adatkezelői státuszt mindig magával vonja: a Facebook részletesen meghatározza, hogy milyen tevékenységek céljából lehet regisztrálni, továbbá az adatkezelés céljai között szerepel a Facebook reklámtévékenységeihez való felhasználás is.³¹⁶

Az adatkezelés módjának és céljának meghatározása egyértelműen az adatvédelmi irányelv és a nemzeti adatvédelmi törvények hatálya alá helyezi a Facebookot.

A közösségi hálózat külső alkalmazásainak (pl. Facebook játékok) üzemeltetői szintén adatkezelőnek minősülnek, mivel a felhasználóktól megkapják a személyes adataikat, melyeket a Facebook felülete és szabályzata keretében³¹⁷, de attól elkülönülve kezelnek.

³¹⁵ Frank Pasquale: Asterisk Revisited: Debating a Right of Reply on Search Results, Journal of Business and Technology Law, Volume 3, Issue 1, Article 5. 2008. 85.

³¹⁶ Facebook adatfelhasználási szabályzat

„A rólad kapott információkat felhasználjuk ahhoz, hogy az általunk kifejlesztett szolgáltatások és funkciók használatát lehetővé tegyük számodra és más felhasználók számára, mint például az ismerőseid, a partnereink, a hirdető, akik a webhelyen hirdetnek, és a fejlesztők, akik az általad használt játékokat, alkalmazásokat és weboldalakat készítik. Például az emberek segítése és az általad végzett vagy megosztott dolgok megkeresése mellett a rólad kapott információkat a következő célokra használhatjuk fel:

-a Facebook termékek, szolgáltatások és az integráció biztonságának megőrzése érdekében tett erőfeszítéseink során;

-a Facebook és mások jogainak és tulajdonának megvédésére;

-hogy tájékoztassunk a helyszíni jellegzetességekről és szolgáltatásokról, például tudassuk veled és ismerőseiddel, ha a közelben valamilyen esemény történik;

-a megtekintett hirdetések hatékonyságának mérése és megértése során, ideértve a számodra érdekes hirdetések küldését;

-hogy javaslatokat tegyünk neked és más Facebook-felhasználóknak, például: javasoljuk ismerősödnek a kapcsolatimportáló használatát, hiszen neked is segítségére volt ismerősök keresésében; hogy egy másik felhasználó vegyen fel téged az ismerősei közé, mivel ugyanazt az e-mail címet importálta, mint te; vagy hogy egyik ismerősöd jelöljön meg téged egy olyan képen, amelyen szerepelsz; valamint

-belső műveletekhez, például hibakereséshez, adatelemzéshez, teszteléshez, kutatáshoz és a szolgáltatások javításához.”

³¹⁷ Facebook API

A felhasználók esetében már több szempontot kell figyelembe venni adatkezelő vagy érintett minőségük megállapításához.

Főszabályként kijelenthető, hogy a felhasználó érintettnek minősül, mivel az adatvédelmi irányelv kivételt tesz az esetükben: ha a természetes személy kizárólag személyes célra végez adatfeldolgozást, abban az esetben nem vonatkoznak rá az adatkezelői kötelezettségek³¹⁸ („háztartási kivétel”). A kivétel olyan hétköznapi használatot ölel fel, amely során a felhasználó saját magáról tölt fel képeket és más személyes adatokat (akár különleges adatokat is, mint például vallása vagy politikai nézetei, melyeket szintén lehetőség van megadni a Facebook adatlapján).

A közösségi hálózatok keretei között azonban lehetősége van a felhasználónak olyan magatartásokat is kifejeznie, melyek már nem illeszkednek a „háztartási kivétel” keretébe, így érintettekből – tudtukon kívül - könnyen adatkezelőkké minősülhetnek át.³¹⁹ A felhasználók a közösségi hálózatokat egyre több esetben használják olyan célokra, melyek már túllépik a „személyes használat és cél” kereteit: szervezetek és egyesületek tagjainak toborzására, összefogására és népszerűsítésére használják az oldalt, amely már kilép a személyes felhasználás medréből.

Amennyiben a felhasználó egy szervezet, vagy egyesület képviselőjében jár el (pl. egy állami szerv, gazdasági társaság, vagy non-profit szervezet) és fejti ki a tevékenységét (pl. tagok toborzása, szervezet népszerűsítése vagy reklámozása, termék promotálása) akkor már nem a saját, hanem a szervezet céljainak megvalósítása érdekében fejti ki a tevékenységet. A „háztartási kivétel” ebben az esetben nem vonatkozhat a felhasználóra, mivel nem, mint természetes személy jár el, hanem a szervezet – egy adatkezelő – képviselőjében.

A közösségi hálózatokat könnyen lehet „adatbányászatra” is használni: a felhasználók összegyűjtik ismerőseik adatait (pl. e-mail, telefonszám), hogy azokat személyes vagy üzleti célra használják. Amennyiben az adatokat az „adatbányász” felhasználó csupán saját személyes célra használja fel (pl. osztálytalálkozó szervezése), és azokat összesítve – mint adatbázist - nem adja át harmadik személynek, még érintettnek tekinthető (a kivétel hatálya alá esik). Abban az esetben, ha a felhasználó az ismerősei adatait üzleti célból gyűjtötte össze és használta fel (pl. Multi Level Marketing, termékek értékesítése), már nem alkalmazható a

³¹⁸ Az Európai Parlament és a Tanács 95/46/EK irányelve 3. cikk (2) Az irányelv nem alkalmazandó az alábbi személyesadat-feldolgozásokra:

- a természetes személy által kizárólag személyes célra, vagy háztartási tevékenysége keretében végzett adatfeldolgozás.

³¹⁹ Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 2009. 06. 12.

kivétel, így az adatkezelő felelősségi szabályaival tartozik, mely alapján jogalappal kell rendelkeznie a személyes adatok kezelésére vonatkozóan.

Adatvédelmi szempontból releváns, amikor a felhasználó úgy állítja be a profilján a róla feltöltött - összes vagy egyes - adatok megtekinthetőségét, hogy azok nyilvánosak – bárki által elérhetőek – legyenek.

Az ilyen nyilvános profilok és személyes adatok a közösségi hálózaton kívülről is elérhetőek és az internetes keresőmotorok által is megtalálhatóak, így egyenértékű avval, mintha a felhasználó nyilvánosságra hozná a személyes adatait egy tetszőleges weblapon.³²⁰

A személyes adatok nyilvánosságra hozatala már kétséges, hogy a „háztartási kivétel” alá tartozik-e: az Európai Unió Bíróságának joggyakorlata szerint nem, mivel „háztartási kivétel” kizárólag a privát és családi környezetben történő adatkezelés keretei között értelmezhető³²¹.

A leírtakból kirajzolódik, hogy amennyiben egy magánszemély gazdasági célra használja fel a közösségi hálózatot (termék értékesítése, marketing), abban az esetben egyértelműen adatkezelésről beszélhetünk.

Az adatkezelő és érintett elhatárolása azonban nehezebb, amikor egy személy valamilyen társadalmi célból végez cselekményeket: ha egy közszereplő (pl. politikus) oszt meg politikai véleményt, vagy kampányol, abban az esetben adatkezelőként tekinthetünk rá, azonban a határvonal kezd elmosódni, amikor csupán magánszemélyként hozza nyilvánosságra a véleményét (pl. a környezetvédelemről) a saját profiljával. Hasonló a helyzet az újságíróknál is, akiknél a publicisztika és a magánvélemény elhatárolása különösen nehéz lehet.

Az elhatároláshoz segítség lehet az ismerősök száma és a megosztott vélemény tartalma: egy 10.000 ismerőssel rendelkező személy már egyértelműen túllép a szűk ismerősi körén és a nyilvánosság számára közvetít információt, a tartalom esetében valamilyen célra felhívás (pl. adománygyűjtés), mások érdekeinek bármilyen képviselése jelentheti az elhatárolás alapját³²².

³²⁰ Facebook adatfelhasználási szabályzat (2014. 08. 24.): „Az adataid nyilvánossá tétele pontosan azt jelenti, ahogyan hangzik: bárki láthatja, beleértve a Facebookon kívüli személyeket is. Az adataid nyilvánossá tétele egyben azt is jelenti, hogy az adott adat:

- a Facebookon kívül is társítható hozzád (vagyis a nevedhez, profilképeidhez, borítóképeidhez, idővonaladhoz, felhasználói azonosítódhoz, felhasználónevedhez stb.);
- megjelenhet, amikor valaki keresést indít a Facebookon vagy egy nyilvános keresőmotorral;
- elérhető lesz az általad és az ismerőseid által használt, a Facebookba integrált játékok, alkalmazások és webhelyek számára; valamint
- bárki számára hozzáférhető lesz, aki API felületeinket, például a Graph API felületet használja.”

³²¹ Case C-73/07 Satakunnan Markkinapörssi and Satamedia, 2008. 12. 16.

³²² Polefko Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (4. rész), Infokommunikáció és Jog, 42. szám, 109-110.

Az adatvédelmi rendelet is szabályozza a háztartási kivételt³²³, továbbá a preambulumban annak alkalmazását a közösségi hálózatokkal kapcsolatban is meghatározza³²⁴, amely alapján a rendelet nem alkalmazandó a személyes adatoknak a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett kezelésére, amely így semmilyen szakmai vagy üzleti tevékenységgel nem hozható összefüggésbe. Személyes vagy otthoni tevékenységnek minősül például a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek.

A rendeletet alkalmazni kell azonban azokra az adatkezelőkre és adatfeldolgozókra, akik a személyes adatok ilyen személyes vagy otthoni tevékenység keretében végzett kezeléséhez az eszközöket biztosítják.

Az adatvédelmi rendelet tisztázza továbbá, hogy a közösségi hálózatoknak nincsen kibúvó a háztartási kivétel alatt, az kizárólag a felhasználó számára áll fenn lehetőségként.

³²³ Adatvédelmi rendelet 2. cikk (2) E rendelet nem alkalmazandó a személyes adatok kezelésére, ha azt:
c) természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik;

³²⁴ Adatvédelmi rendelet preambulum 18.

5.2 Az érintett hozzájárulásával kapcsolatos problémák

A Facebook adatkezelései jelentős részéhez jogalként az érintett hozzájárulását használja fel, azonban a hozzájárulás alapvető követelményei (önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak és félreérthetetlennek kell lennie) nem érvényesülnek maradéktalanul, így feltételezem, hogy az uniós jogszabályoknak nem felel meg a Facebook által legtöbb esetben alkalmazott jogalap.

A közösségi hálózatok adatkezeléseikhez 3 jogalapot használhatnak fel alapvetően az Európai Unióban:

1. az érintett hozzájárulása,
2. az adatkezelés szerződés teljesítéséhez, vagy
3. az adatkezelő vagy adatfeldolgozó jogszerű érdekének érvényesítéséhez szükséges³²⁵.

A „*szerződés teljesítéséhez szükséges*” jogalappal akkor élhetnek az közösségi hálózatok, ha az adatkezelés a szolgáltatás teljesítéséhez feltétlenül szükséges, így például az adatlap alapvető adatainak (név, nemzetiség) megadása és profilkép feltöltése.

Fontos kiemelni, hogy egyes alapvető szolgáltatások teljesítéséhez feltétlenül szükséges adatkezelések esetén még ez a jogalap sem elég, mert jogszabály a felhasználó hozzájárulását teszi szükségessé, így például az Elektronikus hírközlési adatvédelmi irányelv alapján bármilyen szoftver installálása a felhasználó végberendezésén a felhasználó hozzájárulását teszi szükségessé.

A „*jogszerű érdek érvényesítésével*” csak korlátozott keretek között élhetne a közösségi hálózat, így például a rendszer és a többi felhasználó adatainak biztonsága esetén, továbbá „biztonság és megfelelő színvonalú szolgáltatás nyújtása” indokot is csak a valóban szükséges esetben lennének jogosultak felhasználni.

³²⁵ Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (1995. október 24.), 7. cikk

Véleményem szerint minden egyéb adatkezelés esetén az érintett hozzájárulása lenne szükséges annak legitimálásához, amelyeknél a legfontosabb kérdés lenne, hogy opt-in szükséges, vagy opt-out is elégséges.

A legtöbb Facebook által végzett adatkezelések jogi alapja a *felhasználó hozzájárulása*, amelynek önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak, és félreérthetetlennek kellene lennie. Sajnos azonban több, Facebook által végzett adatkezelés esetében is a 4 feltétel egyike, vagy maga a hozzájárulás is hiányzik, amely így nem tekinthető megfelelő jogalapnak.³²⁶

Az egyik legjelentősebb probléma a Facebook egyes adatkezeléseinél, hogy a felhasználónak nincsen kontrollja felettük, mivel a Facebook „mindent vagy semmit” választási lehetőséget kínál csupán az érintettnek, aki így kénytelen vagy elfogadni azokat, vagy a regisztrációval, felhasználással felhagyni.

A „mindent vagy semmit” választási „lehetőség” az érintett hozzájárulásával kapcsolatban vet fel problémákat, mivel valós alternatívája nincsen a Facebooknak, ha az érintett a különböző földrészekén élő ismerőseivel szeretne kapcsolatot tartani egy közösségi hálózaton.

Az önkéntesség problematikáját veti fel, hogy a Facebook szabályzatának az elfogadása a partnereire is kiterjed, így a felhasználó „kénytelen” azoknak az adatkezeléseikhez is hozzájárulni a közösségi hálózat használatáért cserébe.

Miközben a szabályzatot olvasod, tartsd szem előtt, hogy az a Facebook összes olyan márkájára, termékekre és szolgáltatására érvényes, amelyhez nem tartozik külön adatvédelmi szabályzat, illetve amelyek erre a szabályzatra hivatkoznak – ezekre utalunk „Facebook-szolgáltatások” vagy „szolgáltatások” néven.

Fontos megemlíteni továbbá, hogy a Facebook kiterjeszti a hozzájárulást a partnereinek szolgáltatásaira is, így például a Facebook beépülő modulokra is.

A különböző eszközeidről gyűjtött információkat összekapcsolhatjuk – ez megkönnyíti számunkra azt, hogy egységes szolgáltatást tudjunk nyújtani az összes eszközödön. Néhány példa arra, hogy milyen készülékadatokat gyűjtünk:

Jellemzők – például az operációs rendszer, a hardver verziója, az eszközbeállítások, fájl- és szoftvernevek és -típusok, akkumulátor és jelerősség, valamint készülékazonosítók.

³²⁶ Brendan Van Alsenoy, Valerie Verdoodt, Rob Heyman, Jef Ausloos and Ellen Wauters: From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms, 2015, 9-10.

Az eszközök helye – akár konkrét földrajzi helyadatokkal, például GPS-, Bluetooth- vagy WiFi-jelek alapján.

Az internetkapcsolatra vonatkozó adatok – például mobilszolgáltatód vagy internetszolgáltatód neve, a böngésző típusa, nyelve, az időzóna, a mobiltelefonszám és az IP-cím.

A Facebook szolgáltatásainak nyújtásához (a cél eléréséhez) szintén kérdéses, hogy miért szükséges a készülék azonosítók, akkumulátor erőssége, mobiltelefonszám és az IP-cím elmentése. A Facebook érve valószínűleg a biztonság erősítése lenne, de véleményem szerint a felsorolt adatok nélkül is tökéletesen biztosítható lenne a felhasználó biztonsága, amelyre több százezer mobilalkalmazást említhetnénk meg példaként, amelyek nem gyűjtenek ennyi adatot. A célhoz kötöttség elvének az adatkezelés minden szakaszában érvényesülnie kell az adatvédelmi irányelv alapján, azonban a Facebook esetében az adatgyűjtés és az adatok felhasználása nem felel meg ennek: az adatkezelési szabályzat sok esetben általánosan és homályosan fogalmaz.

Gyűjtünk olyan tartalmakat és információkat is, amelyeket mások osztanak meg szolgáltatásaink használata során, köztük rólad szóló információkat is – például amikor téged ábrázoló fényképet osztanak meg, üzenetet küldenek neked, illetve feltöltik, szinkronizálják vagy importálják az elérhetőségi adataidat.

Rólad és a Facebookon vagy azon kívül folytatott tevékenységeidről adatokat kapunk külső partnerektől – például olyan esetben, amikor egy partnerrel közösen kínálunk szolgáltatásokat, vagy hirdetőktől kaphatunk adatokat arról, milyen élményeid voltak velük, illetve milyen módon léptél érintkezésbe velük.

Hasonló a probléma a Facebook alkalmazások használata során, amelyek olyan adatokat is megkapnak, amelyek a szolgáltatás nyújtásához nem szükségesek, csupán a reklámozás hatékonyabbá tételéhez, így a célhoz kötöttség és a felhasználó informálása sem megfelelő, továbbá az érintett hozzájárulása sem lehet emiatt kellően specifikus.³²⁷

A helymeghatározással kapcsolatos adatkezelések esetén szintén szükséges a felhasználó előzetes (opt-in) hozzájárulásának megszerzése, mivel azok különösen érzékeny információkat szolgáltathatnak az érintettől: kórház vagy templom rendszeres látogatása alapján vallás és

³²⁷ Brendan Van Alsenoy, Valerie Verdoodt, Rob Heyman, Jef Ausloos and Ellen Wauters, 11-16.

betegség könnyen megtudható róla.³²⁸ A 29-es Munkacsoport véleménye alapján még akkor is szükséges a felhasználó előzetes hozzájárulásának megszerzése, ha a telefonjának operációs rendszerén alapbeállításként a helymeghatározási adatok megosztása van megadva. A Munkacsoport véleményéből következően a közösségi hálózatok alkalmazásainak külön engedélyt kellene kérni a helymeghatározáson alapuló adatkezeléshez. Véleményem szerint azonban még ez sem elégséges: a Facebooknak alkalmazáson belül egyes helymeghatározáson alapuló adatkezelésekhez (műveletekhez) külön-külön engedélyt kellene kérnie.

A hozzájárulás akkor tekinthető érvényesnek, ha az érintett megfelelően informálva lett nyilatkozatának megadása előtt. Az informálás akkor tekinthető megfelelőnek, ha az részletes, és a felhasználó számára érthető. A Facebook esetében regisztráció során nemhogy nem kell „végig görgetnie” az érintettnek a szabályzatot a regisztrációhoz, még rákattintani sem szükséges: elég csupán kipipálnia egy négyzetet.

A Facebook által alkalmazott megoldás így a legkevésbé alkalmas arra, hogy az érintett akár minimális tájékoztatáson essen át regisztráció során, mely megoldásra az EU Bírósága is kitér ítéletében³²⁹.

Fontos megemlíteni, hogy a Facebook a „Privacy Basics” alatt egy átlátható és könnyen érthető tájékoztatást biztosít az adatok megosztásáról, és arról, hogy egyes felhasználók milyen adatokat láthatnak egymásról, azonban arról elfelejt említést tenni és beállítást megadni, hogy pontosan milyen adatokat láthatnak és gyűjthetnek a Facebook partnerei.

A hozzájárulás félreérthetlensége alatt azt értjük, hogy a felhasználó cselekménye kétséget kizárólag úgy értelmezhető, hogy hozzájárult az adatkezeléshez.

Amennyiben az alapbeállítás a személyes adatok megosztása, és a felhasználó csupán utólagosan dönthet úgy, hogy nem engedélyezi azok kezelését (opt-out), nem beszélhetünk a hozzájárulás félreérthetlenségéről. A Facebookon végrehajtott cselekmények általában széles tömeg részére kerülnek megosztásra (ismerősök ismerősei, külsős alkalmazások), és általában a felhasználó aktív magatartása szükséges ahhoz, hogy az információ csupán szűkebb kör részére kerüljön megosztásra.

³²⁸ Article 29 Working Party Opinion 13/2011 on Geolocation services on smart mobile devices”, WP185, 16 May 2011, 13-14.

³²⁹ Európai Unió Bírósága, Content Services Ltd vs. Bundesarbeitskammer (Case C-49/11), 2012.

“We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services. Learn more about advertising on our Services and how you can control how information about you is used to personalize the ads you see.”

A viselkedés alapú reklámozás esetén Facebook által alkalmazott opt-out megoldás nem tekinthető megfelelő hozzájárulásnak. További probléma a Facebook viselkedésalapú reklámozásának kikapcsolásával, hogy az nem szünteti meg az adatgyűjtést, csupán a hirdetések „megjelenítését” változtatja meg.

Ha kikapcsolod az online viselkedésalapú hirdetéseket, attól még ugyanannyi hirdetést látsz, de ezek talán kevésbé lesznek az érdeklődésednek megfelelőek. Facebookos tevékenységeid alapján is láthatsz esetleg hirdetéseket.

Online érdeklődésalapú hirdetések megjelenítése: (itt jelenik meg a kikapcsolás lehetősége)

A 29-es Munkacsoport állásfoglalásai alapján³³⁰ a viselkedés alapú reklámozásnál szükséges az érintett aktív hozzájárulásának (opt-in) megszerzése, amelynek a Facebook opt-out beállításai nem felelnek meg³³¹.

Hasonló probléma merül fel a közösségi műveletek megjelenítésénél hirdetések esetében, melyeknél alapbeállítás azok megjelenítése. Így történhet meg például, hogy a felhasználó esküvői gyűrűket árusító oldalt like-ol, melyről barátnője és összes ismerőse tudomást szerez. A Facebookon a felhasználó neve és profilképe alapvetően nyilvános, bárki által megtekinthető, mely szintén opt-in megoldással lenne a legbiztonságosabb, mivel így Facebookon kívüli harmadik felek szintén hozzáférhetnek ahhoz, és erről a legtöbb esetben a felhasználók nem is tudnak, abban a téves hitben maradva, hogy a legalapvetőbb adataikat csak az ismerőseik, vagy ismerőseik ismerősei tekinthetik meg³³².

Facebook által gyűjtött adatok összekapcsolásában és reklámbevétellé való alakításában komoly szerepet játszik, hogy a Facebook partnerei lettek a hirdetési piac legnagyobb adatbrókerei³³³. Így a felhasználói szabályzatban szereplő „Facebook partnerei alatt” különösen jelentős adatfeldolgozási és kombinálási háttér áll, amelyről a közvéleménynek nincsen

³³⁰ Article 29 Working Party Opinion 2/2010 on online behavioral advertising, 22 June 2010, WP 171

³³¹ Article 29 Working Party Opinion 15/2011 on the definition of consent, 13 July 2011, WP187

³³² Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 7.

³³³ Facebook Partners With Shadowy ‘Data Brokers’ To Farm Your Information, Sherbit Blog ,April 16, 2015 <https://www.sherbit.io/facebook-partners-with-shadowy-data-brokers-to-farm-your-information/>

tudomása. Így például az Acxiom, Datalogix és Epsilon vállalatokról az átlagos felhasználó valószínűleg még soha nem hallott, ugyanakkor ők az online hirdetési piac mamutjai, akikkel a Facebook együtt dolgozik, és egymás adatbázisait használják fel korlátozott biztonsági intézkedéseket alkalmazva.

A Facebooknak a céltól eltérő adatkezeléseihez jogalapot biztosítani a jövőben még nehezebb lesz, mivel az Adatvédelmi Rendelet szigorúbb követelményeket támaszt az érintett hozzájárulásával szemben az Irányelvhez képest, mivel a Rendelet a kifejezett hozzájárulást („opt-in”) helyezi előtérbe, megkövetelve az érintett akaratának „egyértelmű” kinyilvánítását, nyilatkozat vagy a megerősített „félreérthetetlenül kifejező” cselekedet útján.

A Rendelet preambulumban ki is tér külön az online adatkezelésekkel kapcsolatos problémára, tisztázva, hogy a hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

A fejezetben kifejtésre került, hogy a Facebook adatkezelései során túlterjeszkedik a felhasználó hozzájárulásán. Az Adatvédelmi Rendelet a preambuluma alapján a személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az eredeti céljával, amelyekre a személyes adatokat eredetileg gyűjtötték³³⁴. Annak megállapításához, hogy a további adatkezelés összeegyeztethető-e, figyelembe kell venni az eredeti és a másodlagos célok között fennálló összefüggéseket.³³⁵

A különleges adatok kezelése csak akkor lehetséges a Rendelet alapján, ha ahhoz az érintett kifejezett hozzájárulását adta a „konkrét célból” történő kezeléséhez („specified purposes”)³³⁶, amely egyértelműen szigorúbb szabályozás, mint az adatvédelmi irányelv, amely nem követelte meg a „konkrét” célt.

³³⁴ Annak megállapításához, hogy a további adatkezelés célja összeegyeztethető-e a személyes adatok gyűjtésének eredeti céljával, az adatkezelő – az eredeti adatkezelés jogszerűségére vonatkozó valamennyi előírás teljesítését követően – figyelembe veszi többek között minden, az említett eredeti célok és a tervezett további adatkezelési célok között fennálló összefüggést, az adatgyűjtés körülményeit, ideértve különösen az érintettnek a további adatfelhasználásra vonatkozó, az adatkezelővel fennálló kapcsolatán alapuló észszerű elvárásait is, továbbá a személyes adatok jellegét, a tervezett további adatkezelés következményeit az érintettek nézve, valamint a megfelelő garanciák meglétét mind az eredeti, mind a tervezett további személyesadat-kezelési műveletek során.

³³⁵ Bird & Bird: guide to the General Data Protection Regulation, 2016.

³³⁶ Adatvédelmi Rendelet 8. cikk

Különleges adatok feldolgozása

(1) A tagállamok megtilthatják az olyan személyes adatok feldolgozását, amelyek a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy vi (2) Az (1) bekezdés nem alkalmazandó abban az esetben, ha: a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy az (1) bekezdésben említett tilalom nem oldható fel az érintett hozzájárulásával; lágnézeti meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkoznak.

Fogyasztóvédelmet érintő jogszabályok megsértése

A fogyasztóvédelmi jogszabályok megsértésére vonatkozó rendelkezések alkalmazhatósága is felmerül a Facebook adatkezelési szabályzatának rendelkezéseivel kapcsolatosan, különösen a felelősségének kizárására vonatkozóan³³⁷. A Facebook érve, hogy ingyen nyújtja a szolgáltatásait, nem akadályozza meg a fogyasztóvédelmi szabályok alkalmazhatóságát. Az Európai Bizottság Cloud Expert Working Group³³⁸ (Felhőalapú Szolgáltatás Munkacsoport) véleménye alapján az EU Fogyasztóvédelmi irányelve³³⁹ attól függetlenül alkalmazandó, hogy az áru vagy szolgáltatás nyújtásáért cserében történt-e bármilyen ellenszolgáltatás.

³³⁷ Facebook felhasználói feltételek, 15. Viták (2016. 04. 27.)

TÖREKSZÜNK A FACEBOOK HIBAMENTES ÉS BIZTONSÁGOS MŰKÖDÉSÉRE, DE ÖN AZT A SAJÁT FELELŐSSÉGÉRE HASZNÁLJA. A FACEBOOKOT ADOTT ÁLLAPOTÁBAN BIZTOSÍTJUK BÁRMILYEN KIFEJEZETT VAGY HALLGATÓLAGOS GARANCIA NÉLKÜL, BELEÉRTVE, DE NEM KIZÁRVA AZ ÉRTÉKESÍTHETŐSÉGRE, ADOTT CÉLRA VALÓ ALKALMASSÁGRA ÉS JOGKÖVETÉSRE VONATKOZÓ HALLGATÓLAGOS GARANCIÁT. NEM GARANTÁLJUK, HOGY A FACEBOOK MINDIG BIZTONSÁGOS VAGY HIBAMENTES LESZ, VAGY HOGY A FACEBOOK MINDIG MEGSZAKÍTÁS, KÉSEDELEM VAGY HIÁNY NÉLKÜL FOG MŰKÖDNI.

³³⁸ European Commission's Expert Group on Cloud Computing Contracts Unfair Contract Terms in Cloud-Computing Service Contracts, 1. (letöltve: 2016. 04. 27.)

http://ec.europa.eu/justice/contract/files/expert_groups/unfair_contract_terms_en.pdf

³³⁹ Az Európai Unió Tanácsának 93/13/EGK irányelve (1993. április 5.) a fogyasztókkal kötött szerződésekben alkalmazott tisztességtelen feltételekről

5.3 Javaslatok a teljes értékű hozzájárulás eléréséhez

Véleményem szerint a Facebook adatkezelései jelentős részéhez felhasznált, érintettek által megadott hozzájárulás jogellenessége orvosolható lenne, ha az érintett megfelelő tájékoztatást és több választási lehetőséget kapna regisztrálás során, továbbá a felhasználó a Facebook használata során a felmerülő adatkezelések esetén folyamatosan felugró ablakokat kapna, amely lehetővé tenné számára, hogy döntsön az adott adatkezelés elfogadásáról vagy visszautasításáról annak megtörténte előtt (opt-in). Így például a „like” gomb első lenyomásakor felugró ablakot kapna avval a tájékoztatással, hogy a „like” cselekménye megjelenhet egyes hirdetésekénél³⁴⁰.

Legalább a különleges adatokkal kapcsolatosan ajánlott lenne a fokozott védelem, és a nyilvánosság előli megosztásának alapbeállításként való kikapcsolása³⁴¹.

Szükségesebb talán továbbá, hogy a felhasználónak legalább egy egyszerűsített adatvédelmi és felhasználási szabályzat kivonatán legyen kötelező „végig görgetnie” a sikeres regisztrációhoz, amelyből természetesen egy kattintással el tudná érni a teljes verziót, amelyben egyértelműen tartózkodni kellene határozatlan és homályos megfogalmazásoktól (pl.: „lehetőségek”, „talán”, „felhasználható”³⁴²).

Fontos lenne továbbá részletesen informálni az érintettet, hogy mely adatokat használ fel a közösségi hálózat a szolgáltatás minőségének javítására, biztonság növelésére, és melyek azok az adatok, amelyek csupán marketing céljából kerülnek kezelésre³⁴³.

A facebook adatkezelésével és adatkezelői tájékoztatásával kapcsolatosan megszámlálhatatlan javaslat érkezett már a jogalkalmazók és jogtudósok részéről, így véleményem szerint szigorúbb megoldás lenne szükséges: a facebooknak egy adott országban elérhető oldalán az adatvédelmi tájékoztatóban egy hivatkozást kellene elhelyeznie, amely az ország adatvédelemért felelős szervének egy facebookkal kapcsolatos informáló oldalához vezetne el. Így például Magyarországon a NAIH oldalára elvezető hivatkozást lehetne elhelyezni, amelyre kattintva a magyar állampolgár értesülhetne az adatkezeléssel kapcsolatos veszélyekről és hátrányokról közérthetően.

³⁴⁰ Rebecca Lipman: Online Privacy and the Invisible Market for Our Data, Penn State Law Review, 2016. 805.

³⁴¹ Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (2. rész), Infokommunikáció és Jog, 40. szám, 174-175.

³⁴² Article 29 Data Protection Working Party, Letter from the Article 29 Working Party to Google on Google Privacy Policy, 23 September 2014, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm#2014.

³⁴³ Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (3. rész), Infokommunikáció és Jog, 41. szám, 209-211.

5.4 Javaslát egy rentábilis, „privacy by default” közösségi hálózat megvalósítására

Véleményem szerint a Facebook adatvédelemmel kapcsolatos problémáinak egy részére és megítélésének javítására megoldást jelenthetne, ha a felhasználók élhetnének avval az *opcióval*, hogy ellenszolgáltatás fejében (pl. havonta vagy évente fizetett összeg, vásárlás a Facebook-on keresztül) hirdetések nélküli, fokozott és részletes adatvédelmi beállításokkal rendelkező Facebook szolgáltatást kapnának.

A díj összege megfizethető lenne a felhasználók jelentős részének: a Facebook átlagos bevétele felhasználónként 2016 legelső negyedében az Egyesült Államokban és Kanadában 11,8; Európában 3,9 és Ázsiában 1,5 USA dollár volt³⁴⁴.

³⁴⁴ <http://www.statista.com/statistics/251328/facebook-average-revenue-per-user-by-region/>

A Facebook felhasználónkénti átlagbevétele 2016 első negyedében (USA dollár)

forrás: <http://investor.fb.com/results.cfm>

Az Európai Unió területén így havi 1,3 dollárból (kb. 350 HUF) lenne lehetséges kiváltani egy felhasználó reklámbevételének a kiesését.

Véleményem szerint Nyugat-Európában ez az összeg – mely egy kávé ára - könnyen megfizethető lenne, és a társadalom által is elfogadottabb, hogy a szellemi alkotásokért és online szolgáltatásokért fizessenek.

Közép- és Kelet-Európában az internet elérés és a közösségi hálózatok használatának szintje eléri a Nyugat-Európaét, azonban az online vásárlóerő attól elmarad.

Internet elérés szempontjából a vízvonalzó a 2007. év volt: ekkorra már az EU-28-ban a háztartások többsége (55%) rendelkezett internet-hozzáféréssel. Ez az arány később tovább nőtt, míg – a 2013-as adatokhoz képest újabb 2 százalékpontos növekedés után – 2014-ben elérte a 81%-ot.

Internet-hozzáférés a háztartásokban az Európai Unióban (az összes háztartás százalékában), 2009 és 2014

Forrás: Eurostat

Az EU-28 területén 2014-ben a közösségi oldalak használata jelentette az egyik leggyakoribb online tevékenységet. A 16–74 éves lakosság közel fele (46%) használta az internetet közösségi hálózatok (például a Facebook vagy a Twitter) böngészésére.

Dániában, Svédországban, Magyarországon, Luxemburgban és az Egyesült Királyságban, valamint Izlandon és Norvégiában tíz emberből hat látogatta a közösségi oldalakat, és Hollandiában is csak kevéssel maradt el ettől az arány (59%). A lista végén négy olyan uniós tagállam (Franciaország, Lengyelország, Olaszország és Románia) áll, ahol tíz emberből kevesebb, mint négy használ közösségi médiát.

Az internetet közösségi oldalakon való részvételre használó magánszemélyek aránya az Európai Unióban, 2014 (a 16–74 éves lakosság százalékában)

forrás: Eurostat

Az EU-28 tagállamaiban 2014-ben 50%-ra nőtt azoknak a 16–74 éves magánszemélyeknek az aránya, akik termékeket vagy szolgáltatásokat rendeltek magáncélú felhasználásra az interneten keresztül: ez 2012-höz képest 6 százalékpontos emelkedést jelent.

Azon magánszemélyek aránya, akik a felmérést megelőző 12 hónap során magánhasználatra árut vagy szolgáltatást rendeltek az interneten, 2012 és 2014 (a 16–74 éves lakosság százalékában)

forrás: Eurostat

Az Eurostat felméréseiből kirajzolódik, hogy Közép- és Kelet-Európában is az uniós átlag szintjén áll rendelkezésre internet, és a lakosság közösségi hálózatok iránti érdeklődése is azonos szinten van, azonban az online szolgáltatásokért való fizetés mértéke a Nyugat-Európai szinttől jelentősen elmarad, így a fizetős megoldás nehezen lenne megvalósítható.³⁴⁵

Véleményem szerint a középút is megtalálható lenne: lehetséges lenne egy olyan megoldás alkalmazása, amellyel a felhasználónkénti bevétel 50%-ban reklámbevételből, 50%-ban a felhasználó által fizetett összegből állna.

A felezett összegű reklámbevételt elérhetné a Facebook viselkedésalapú reklámozás nélkül, a felhasználóról csupán alapvető adatok megszerzésével, amelyeket a felhasználó önként adna meg (pl. nem, kor, lakóhely).

Így létrejöhetne egy olyan helyzet, hogy már a felhasználó regisztrálásakor alapbeállításként lennének tiltva teljes mértékben a helymeghatározáson és viselkedésen alapuló adatgyűjtések, továbbá a felhasználó személyes adatainak kiszolgálása a Facebook partnerei részére, és csupán böngészője oldalsávjában kapna reklámokat szalaghirdetésekből, amelyeket bármilyen weboldalon is látogatóként megkapna anélkül, hogy bármilyen információt megadna magáról.

Példa a reklámmentes közösségi hálózatra

Az „Ello” egy 2014-ben alapított reklámmentes közösségi hálózat, amely jelenleg még béta állapotban van, a felhasználói tábora meghaladja az egymilliót. A felhasználói feltételek között világossá teszik, hogy ők soha nem fognak felhasználói adatokat eladni, reklámokat mutatni és nem kötelező a felhasználóknak a valós adataikat megadni (mivel abból nem céljuk bevételt generálni). Az Ello bevétele befektetők és a felhasználók által fizetett összegekből áll, melyért cserébe extra jogosultságokat kaphatnak az oldalon³⁴⁶.

Az Ello hosszú távú fenntarthatósága jelenleg még kérdéses, mivel a felhasználók 20%-a marad csak aktív 1 héttel a regisztrálás után.

³⁴⁵ Eurostat: Az információs társadalomra vonatkozó statisztika – háztartások és magánszemélyek (letöltés dátuma: 2016. április 25.)

http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/hu

³⁴⁶ <https://www.ello.co> (az oldal letöltése: 2015. április 25.)

Az Ello és a hozzá hasonló kezdeményezések elterjedésének legjelentősebb akadályát véleményem szerint az jelenti, hogy az oldal felülete és szolgáltatásainak minősége jelentősen elmarad a Facebook-tól, amely már dollár milliárdokat költött a rendszer kialakítására.

5.5 A Személyes adatok profitra váltása

A közösségi hálózatok elnevezésben a „községi” megtévesztően hathat, mivel a legnépszerűbb szolgáltatásoknak profitorientált vállalatok a tulajdonosai: az egyetemi hallgatók által létrehozott „startupok” sikerességük esetén befektetőket vonzanak, majd a fejlesztések és befektetések megtérüléséhez egyre több bevétel szükséges számukra, melynek csúcspontja a tőzsdén való megjelenés, mely különösen nagy nyomást helyez rájuk a profit növelése érdekében.

A felhasználók személyes adatait az „internet olajának” is tekinthetjük, mivel megismerésük és birtoklásuk jelentős, profitra váltható értékkel bír: a legjelentősebb internetes szolgáltatások (pl.: Google, Facebook, híroldalak) használata ingyenes, így azok a felhasználók adataiból és az ahhoz kapcsolódó hirdetésekből tartják fenn magukat.

Több kísérlet volt internetes szolgáltatások üzemeltetői - elsősorban az online újságok - részéről a tartalom fizetössé tételére, melyek általában nem lettek sikeresek. A legnagyobb internetes cégek sikerét tekintve kijelenthetjük, hogy a legsikeresebb üzleti modell az ingyenes szolgáltatás nyújtása (legalább az alapvető szolgáltatások terén), majd a személyes adatok felhasználása hirdetések értékesítésére.

A felhasználók internetes szokásairól a lehető legtöbbet kell tudniuk a részükre szolgáltatást nyújtó cégeknek, hogy minél célzottabb hirdetéseket juttathassanak el feléjük. A célzott hirdetés előnye, hogy a reklám nagyobb eséllyel éri el a célját. Az elv egyszerű: kontaktlencsét olyan felhasználónak hirdetnek, aki szemüveges³⁴⁷.

Az internetes cégek a felhasználók elemzése céljából naponta akár több százszor is kaphatnak információt arról, hogy éppen mit csinálnak: milyen információra keresnek rá, mit olvasnak, mennyi ideig, honnan jelentkeztek be és milyen eszközről. Ezek után a cégek könnyebben határozhatják meg, milyen hirdetés éri el a legnagyobb valószínűséggel a felhasználóknál a kívánt hatást, majd drágábban értékesíthetik a hirdetési helyeket a sikeres hirdetési arány miatt.³⁴⁸

³⁴⁷ Imran Naseem: Facebook Cash Manuscript, 2012, 22-25.

³⁴⁸ Minél több időt töltünk el aktívabban az interneten, annál több személyes adatot szolgáltatunk magunkról: 2006 óta megduplázódott a száma az internetes kereséseknek a comScore mérései alapján, így 2014 januárjában 14.6 milliárd keresés realizálódott, mely az arra épülő reklámpar növekedését is prognosztizálja.

2014 első negyedévi eredményeit tekintve a Facebook sikeresen váltotta profitra a felhasználók adatait: 2.5 milliárd dollár bevételből több, mint 1 milliárd dollár volt profit, mely a korábbi negyedévnél háromszor nagyobb hasznot jelentett³⁴⁹.

Az Egyesült Államokban és Kanadában felhasználónként 5.18 dollárt bevételt termelt a Facebook, mely azt jelenti, hogy egy ember személyes adatai 2014-ben 1150 Ft-nak megfelelő összeget értek Észak-Amerikában. Ez az összeg jelentősen kevesebb a déli és keleti országokban, de csak idő kérdése, hogy a reklámbevételek a klasszikus (TV, újság) médiáktól online térre áramoljanak a Világ minden részén.

Bár folyamatosan növekszik a Facebook felhasználónként elért nyeresége, még mindig elmarad a Google által elért szinttől, melynek oka, hogy a Facebookot főként fiatalok használják, akik jobban figyelmen kívül hagyják a megtekintendő reklámokat, mivel a kommunikáció, nem pedig tartalomfogyasztás céljából jelentkeznek be a Facebookra³⁵⁰.

A Facebook új tulajdonossal kapcsolatos rendelkezései a felhasználói feltételek között véleményem szerint több ponton is aggályosak és homályosak: nemhogy az adásvétel tárgya nincsen tisztázva, de még az adásvétel ténye sem szükséges az adatok átadásához.

Új tulajdonos.

Amennyiben szolgáltatásaink vagy a hozzájuk tartozó eszközök tulajdonjoga vagy irányítási joga részben vagy teljes egészében megváltozik, adataidat átadhatjuk az új tulajdonosnak.

A „szolgáltatások tulajdonjoga” világos és érthető, az „eszközök tulajdonjoga” azonban már nehezen értelmezhető a személyes adatok átadására: „eszközök” alatt érthetjük a számítástechnikai háttérrel, például a szervereket, amelyeket folyamatosan selejteznek, tulajdonjuk gyakran és könnyen változhat.

Amennyiben a szolgáltatással együtt értékesítik az eszközöket, abban az esetben érthető személyes adatok átadása, azonban csupán a számítástechnikai eszközök átruházása semmilyen alapot nem ad a felhasználók személyes adatainak átadására.

A megfogalmazásban azonban a „vagy” kötőszó szerepel, mely megadja a lehetőséget csupán az eszközök átruházására szolgáltatások nélkül.

³⁴⁹ 2013 utolsó negyedévében 373 millió dollár profitot realizált a vállalat

³⁵⁰ Jellemző, hogy reklámblokkoló kiegészítőket is telepítenek az internetes böngészőjükben.

Andrew Leonard: The Internet's next victim: Advertising, Salon, 2012. 09. 02.

http://www.salon.com/2013/09/02/the_internets_next_victim_advertising/

Aggodalomra ad okot az irányítási jog teljes vagy részleges megváltozására vonatkozó rendelkezés is, mely alapján a tulajdonjog átruházása sem szükséges a személyes adatok átadásához, csupán az irányítás részleges időleges megszerzésével az lehetséges.

A Facebook által végzett horizontális és vertikális adatgyűjtés folyamatosan növekszik.

Horizontális adatgyűjtés alatt azt értjük, hogy a Facebook egyre több érintett adatait képes megszerezni, melynek egyik módja, hogy cégek felvásárlása esetén a tulajdonjoggal együtt azok felhasználói adatbázisát is megszerzi, így például a WhatsApp és az Instagram esetében, továbbá a nem felhasználó természetes személyekről beépülő modulok („social plugin”, mint például a „like” gomb egyes oldalakon) segítségével is információt szerez meg.

Vertikális adatgyűjtés alatt értjük, hogy a Facebook egyre több információt képes az egyes érintettekről megtudni, főként a rendelkezésre álló adatok kombinációjával, így például a téli sport oldalak és a - helymeghatározási adatokból - hegyes vidékek látogatásából összekapcsolható információ, hogy a felhasználó sífelszerelés potenciális vásárlója.

Az online hirdetési piac berobbanása előtt vált szállóigévé, hogy a hirdetésekre költött összeg fele kidobott pénz, csak nem lehet tudni, hogy melyik fél. Az említett helyzetet változtatta meg gyökerestől az internetes hirdetési piac, amelyen a kattintásokat, vásárlások nyomon lehet követni. A Facebookra is egyre jobban igaz az „online buborék”³⁵¹ kialakítása: a hírfolyamot és a reklámokat egyre fejlettebb algoritmusok alapján szabja a felhasználó igényei szerint.

A személyi buborékból különösen nehéz kikerülni, mivel meglehetősen bonyolult működési elvvel ellátott algoritmusok hozzák létre azt, amelyeket jelentős üzleti érdekek és szabadalmak védenek. A véleményszabadság és az informáltsághoz való jog már nem olyan jogosultságok, amelyekre az állam jelenti a legnagyobb veszélyt³⁵².

A Facebook hírfolyam különleges szerepet tölt be a felhasználó lekötéséhez, amely a buborék hatáson túlnő. Egyes vélemények szerint az amerikai elnökválasztásra is komoly hatással lehetett. A hírfolyam felhasználók viselkedésére és hangulatára gyakorolt hatását tanulmánnyal is vizsgálta már a Facebook, amely szintén kisebb botrányba torkollt: egyes személyek hírfolyamának szisztematikus megváltoztatásának hatását mérték a felhasználó hangulatán és cselekményein³⁵³. A kísérlet etikusságának kérdésén túl további problémaként veti fel a

³⁵¹ Eli Pariser: *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, 2011. 4-11.

³⁵² Tatay Eszter: A szűrőbuborék hatása a tájékozottsághoz való jogra, *Infokommunikáció és Jog*, 2015. 2-3. 84.

³⁵³ Jane R. Bambauer: *All Life Is an Experiment. (Sometimes It Is a Controlled Experiment.)*, *Loyola University Chicago Law Journal* Vol. 47. 2016. 492-500.

felhasználó különleges hozzájárulásának hiányát, mivel a kísérletekhez speciális hozzájárulást írnak elő az azt szabályozó jogszabályok a legtöbb országban³⁵⁴.

A Facebook és az online szolgáltatást nyújtó vállalatok többsége mindent megpróbálnak megtenni annak érdekében, hogy minél több információt gyűjtsenek be a felhasználóikról: azt, hogy egy oldal milyen mennyiségű adatot tud megszerezni, elsősorban a felhasználók által az oldalon töltött időtől, az oldal típusától, továbbá attól függ, hogy a szolgáltatás igénybevételéhez mennyi és milyen fajta információt kell megadnia a felhasználónak magáról. A híroldalak általában nem igényelnek semmilyen regisztrációt, a felhasználók bármikor böngészhetnek rajtuk. Már magában ez is sok információt elárul róluk: honnan, milyen fajta eszközről jelentkeztek be és milyen az érdeklődési körük.

A következő fokozat, amikor a felhasználónak regisztrálnia kell egy oldalon, hogy annak a szolgáltatásait igénybe vegye (pl. egy e-mail szolgáltató), ahol a regisztráció során pontos képet ad magáról: kora, lakóhelye és további személyes adatain túl általában iskolázottságára és érdeklődési körére is rákérdeznek az online kérdőívek, melyek végén az adatvédelmi nyilatkozat elfogadása után rendszerint hírlevélre feliratkozást is felkínálnak lehetőségként (általában választhatnak a hírlevelek fajtái között is).

A Facebook és a közösségi oldalak új szintre emelték a begyűjtött információk körét: az önként megadott alapvető személyes adatokon túl teljes személyképet adnak a felhasználók az iskolájuk és a munkahelyünk pontos megadásával, baráti körük és érdeklődésük részletezésével.

A szociális hálózatok felhasználóit két csoportra lehet osztani a személyes adataik felhasználásával kapcsolatosan: vagy nem tudnak azok felhasználásáról (mivel nem olvassák el a felhasználási feltételeket), vagy tudnak róla, de nem akarnak költeni más szolgáltatásra, vagy nincs is más lehetőségük (Magyarországon az iwiw elszorvada óta nincsen valós alternatívája a Facebooknak)³⁵⁵.

Az internetes cégek vezetői avval védekeznek a privacy skeptikusok érvei ellen, hogy a felhasználókat védik az adatvédelmi szabályzatok, amelyek a felhasználók rendelkezésére

³⁵⁴ Caitlyn Kuhs: Need for Informed Consent in the Age of Ubiquitous Human Testing, Loyola of Los Angeles Law Review Vol. 49. 2016. 254-260.

³⁵⁵ Több jogvédő szervezet tiltakozott az ellen, hogy általában csak a felhasználási feltételek között értesülhetnek a felhasználók az adatgyűjtésről, azon kívül nincsen semmilyen jele (pl.: villogó ábra a képernyőn), hogy éppen információk gyűjtése folyik a felhasználóról.

<http://www.eppgroup.eu/topic/European-civil-rights%3A-defending-privacy-with-modern-data-protection>

állnak a regisztráció időpontjában és utána is, így ha később valamely változás számukra nem megfelelő, abban az esetben törölhetik, vagy felfüggeszthetik a tagságukat az adott oldalon.

További indokként hozzák fel a jelenlegi reklámozási rendszer mellett, hogy a felhasználóknak is hasznos, ha olyan ajánlatokat kapnak, melyek érdekelhetik őket: evvel akár pénzt és időt is spórolhatnak. Gyakran az adatokat anonim módon tárolják: konkrét eszközhöz (laptop, tablet, telefon) kapcsolhatóak, nem pedig egy személyhez.³⁵⁶

A hatalmas adatmennyiség, mellyel a legnagyobb webes cégek rendelkeznek (pl.: Facebook, Google, Yahoo), és amellyel közvetlenül érhetnek el felhasználói csoportokat speciális tulajdonságok alapján (pl.: 20 és 50 év között diplomások), olyan előnyt jelentenek a hagyományos hirdetési felületekkel szemben (pl. TV, rádió, újság, plakát), mely behozhatatlan és teljesen megváltoztatja az eddig kialakult piaci struktúrát: a hirdetésekre költött összegek növekvő ütemben csoportosulnak át az online hirdetési felületek felé.

További tendencia, hogy az adatbázisok a legnagyobb cégek kezében összpontosulnak: a nagy vállalatok, mint a Microsoft, folyamatosan vásárolnak fel kisebb webes cégeket, mellyel együtt a felhasználók összes személyes adatát is megkapják (sokszor csupán az adatbázis az egyetlen indok a felvásárlás mellett).

A személyre szabott hirdetések működése és a beépülő modulokkal kapcsolatos adatvédelmi aggályok

Az online viselkedés alapú reklámozás esetén a szolgáltató megfigyeli a felhasználó internetezési szokásait és - a személyes adataikkal összekapcsolva - érdeklődési csoportokba rendezi őket (pl. utazás, autó vagy ruha iránt érdeklődők), majd a csoportoknak az érdeklődési körüknek megfelelő reklámokat mutat.

A működési elve a viselkedés alapú reklámozásnak, hogy a szolgáltató egy „cookie”-ban letárolja a felhasználó eszközén (számítógép, tablet vagy okostelefon) hogy milyen típusú oldalakat látogatott meg³⁵⁷.

Az információból kiderül, hogy a felhasználónak milyen az érdeklődési köre, ezt követően a szolgáltató csoportokba (melyek akár több milliós méretűek is lehetnek) rendezi a felhasználókat, majd a hirdetők és a weboldalak ennek megfelelően alakítják ki a

³⁵⁶ A magyar és az uniós joggyakorlat is a személyes adatok körét szélesen értelmezi: amíg a kapcsolat az adott személy és az adatok között helyreállítható, addig az adatok továbbra is személyes adatnak minősülnek.

³⁵⁷ John Haydon: Facebook Marketing for Dummies, Published by: John Wiley & Sons, Inc, 2013, 13.

reklámkampányaikat, valamint a bannereket³⁵⁸, hogy a célcsoport számára releváns reklámokat jeleníthessék meg³⁵⁹.

A személyre szabott hirdetések előnye, hogy a felhasználók nem kapnak több reklámot a rendszer miatt, csupán azok tartalma lesz az érdeklődési körüknek megfelelő. A szolgáltatóknak közvetlenül azért előnyös a rendszer használata, mert magasabb profitot nyerhetnek reklámbevételekből, mely nyereség – elméletileg - a felhasználóknál is realizálódik: igényesebb szolgáltatást vehetnek igénybe, akár ingyenesen.

A Németországban lévő Schleswig-Holstein tartomány Adatvédelmi Biztosának Hivatala 2011-ben kiadott egy felhívást a tartományi hivatalok részére, melyben a személyes adatok védelmével kapcsolatban aggályát fejezte ki és felkérte hivatalokat, hogy Facebook oldalait és a beépülő moduljaikat szüntessék meg adatvédelmi aggályok miatt.³⁶⁰

Az Adatvédelmi Biztos szerint a Facebook oldalak és beépülő modulok használata sértik a Német Telekommunikációs Törvényt, a Szövetségi Adatvédelmi Törvényt és a tartományi szabályozást is, mivel alkalmazásuk esetén a Facebook személyes adatokat gyűjt és továbbít az Egyesült Államokba, továbbá a felhasználókról 2 évig profilt készít, mely az EU Adatvédelmi Irányelvvel is ütközik³⁶¹.

A Biztos jelentése kiemelte továbbá, hogy a felhasználók a helyzet ellen nem tudnak mit tenni, továbbá a Facebook felhasználási szabályzata nem tartalmazta az erre vonatkozó szükséges tájékoztatást.³⁶²

Az adatvédelmi biztos felkérte a tartományban lévő összes privát weboldal üzemeltetőjét is, hogy szüntessék meg az adatvédelmi szempontból aggályos Facebook szolgáltatások

³⁵⁸ A banner egy szalagszerű hirdetés, mely általában egy weblap szélén helyezkedik el, rákattintva a felhasználó közvetlenül eljuthat a hirdető honlapjára.

<http://www.webopedia.com/TERM/B/banner.html>

³⁵⁹ A felhasznált adatok köre hirdetési csoportonként eltérő lehet, a hagyományos hirdetési hálózatok az abban részt vevő oldalakon gyűjtik a felhasználók adatait.

³⁶⁰ <https://www.datenschutzzentrum.de/presse/20110819-facebook-en.htm>

³⁶¹ Justin Levy: Facebook Marketing (third edition), Que Publishing, Indianapolis, 2012, 48-60.

³⁶² Thilo Weichert adatvédelmi biztos személyes nyilatkozatában is élesen bírálta az adatgyűjtést és annak módszerét: szerinte a Facebook szolgáltatásai és ajánlatai sértik az európai normákat, mely nem gátolja meg az európai honlapok üzemeltetőit, mivel az említett szolgáltatások telepítése és alkalmazása ingyenes és könnyen végrehajtható, továbbá az üzemeltetők számára előnyöket kínál (pl. látogatottság, kattintások és egyéb mutatók monitorozása, mely a hirdetések és a profit növelésénél hasznos). Bár az üzemeltetők számára elméletileg ingyenes, a valóságban a Facebook szolgáltatásai a felhasználók személyes adataival vannak megfizetve, melyet az adatvédelmi biztos a személyes adatokért való felelősség megszegésének tekint egy olyan cég részéről, melynek még leányvállalata sincsen Németországban.

alkalmazását, mivel azok az Egyesült Államokba küldenek személyes adatokat. Szankcióként a Hivatal bírság kiszabását helyezte kilátásba.³⁶³

5.6 Facebook és a gyermekek adatvédelme

Minden ember egy szociális lény, aki a társadalomban valamilyen módon részt szeretne venni, abban a helyét elfoglalni. Az egyénnek a társadalom többi tagjával létrejött kapcsolata kommunikáció révén valósul meg, melynek formája az elmúlt évtizedekben jelentősen megváltozott.

Az online kommunikációnak nem szabhat határt az írásbeliség: hang- és videó hívások népszerűsége folyamatosan növekszik, valamint a virtuális valóság is elérhető közelségbe került³⁶⁴. A gyermekek közötti kommunikációra különösen érvényes ez a változás, mely jelentősen eltér a szüleik által megszokottól, így a szülők nehezen tudják kezelni a helyzetet, mivel nem tudják, milyen korlátok szükségesek.

A fejlett országokban a gyermekek nagyobb biztonságban vannak napjainkban, mint évtizedekkel ezelőtt: a közbiztonság növekedése miatt a gyermekek ellen elkövetett bűncselekmények száma csökkent, a közegészségügy és az életszínvonal fejlődésének köszönhetően az egészségi állapotuk jelentősen növekedett. A gyermekek életszínvonalának és biztonságának növekedése ellenére a média mégis hajlamos eltúlozni az internet és a közösségi média által a gyermekekre leselkedő veszélyek nagyságát.

A gyermekek számára a nyilvános helyeken (legyen az valós vagy virtuális) való részvétel kockázatokkal jár, melyekre őket fel kell készíteni, és ott ők védelmet igényelnek. A védelem szintjének szükségességéről mind a jogalkotók mind a jogalkalmazók véleménye megoszlik: egyesek szerint a számítógép előtt nem érheti baj a gyermeket, mások szerint legalább olyan veszélyes, mintha egy padon ülne valamelyik köztéren.

A gyermekek közterületeken való védelméről az polgári, büntető és szabálysértési törvényeken túl speciális jogszabályok is rendelkeznek (pl. az iskolakerülést tiltó normák), míg a gyermekek

³⁶³ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Facebook-Fanpages und -Plugins: Das ULD weiß, was es tut, 2011. 07. 10.

³⁶⁴ A Facebook 2014-ben vásárolt meg egy virtuális valósággal foglalkozó vállalatot, az Oculus Virtual Reality-t, mely iparági elemzők szerint a felhasználók közötti virtuális valóság létrehozását célozza. Leo King: Facebook, Oculus, And Businesses' Thirst For Virtual Reality, Forbes, 2014. 03. 30. <http://www.forbes.com/sites/leoking/2014/03/30/facebook-oculus-and-businesses-thirst-for-virtual-reality/>

online téren való részvételét kevesebb norma szabályozza, általában a technika fejlődésétől egy lépéssel lemaradva.

A gyermekek számára az online tér használatában korlátot jelentenek a jogszabályok, a szociális normák és a családi környezet, mely akadályok nagysága és mennyisége sokszor frusztrációt és a családdal való konfliktust szül, mivel egy gyermeket nem érdekel az online életet szabályozó törvények és a felhasználói feltételek tartalma.

Nehézséget jelent továbbá, hogy egy gyermek fizikai szabadságát sokkal egyszerűbb korlátozni, mint a virtuális mozgásterét: még a legkifinomultabb szűrőprogramokat is ki lehet játszani felnőtt tartalmak elérésére bármilyen operációs rendszeren, legyen az számítógép, tablet, vagy okostelefon.

A gyermekek online magánszféráját védő szövetségi szintű törvény³⁶⁵ a 13 éven aluli gyermekek online adatkezelését szabályozza az Egyesült Államokban, mely alapján csak a szülő vagy más törvényes képviselő engedélyével lehetséges a 13 éven aluli gyermekek személyes adatainak kezelése. A törvény több kötelezettséget is ró a gyermekek adatait kezelőkre: a felhasználói és adatvédelmi szabályzatokban meg kell határozni az adatkezelés pontos szabályait, a szülők és más törvényes képviselők nyilatkozatának tartalmát és beszerzésének módját, továbbá a törvény az adatkezelésre is különös szabályokat állapít meg.³⁶⁶

A Children's Online Privacy Protection Act (COPPA) megalkotásának célja a gyermekek fizikai és szellemi védelme volt az agresszív marketing ellen és végső soron olyan bűncselekmények ellen, mint a gyermekrablás. Egy gyermeket könnyű interneten rávenni üzletek megkötésére szülei számlájára anélkül, hogy bármilyen körültekintést végeznének: bankkártya vagy emelt díjas sms használatával egyszerűen nyújthatnak ellenszolgáltatást, továbbá az Apple és a Google alkalmazásboltjából letöltött alkalmazásokon keresztül a szüleik tudta nélkül fizethetnek ki hatalmas összegeket (pl. mobil játékokon belül a következő pályára lépésért) pár kattintással. A törvény megalkotói ugyanakkor fontosnak tartották, hogy a jogszabály az innovációt, a gazdasági fejlődést és a gyermekek online tanulását ne akadályozza. Bár a COPPA csak az Egyesült Államok joghatósága alatt alkalmazandó, a Facebook és a legtöbb oldal gyermekek regisztrációját korlátozó szabályai minden felhasználóra vonatkoznak, függetlenül attól, hogy mely ország állampolgárai.

³⁶⁵ Children's Online Privacy Protection Act of 1998, Pub.L. 105–277

³⁶⁶ Az törvény olyan oldalak üzemeltetőire alkalmazandó, akik profitorientált tevékenységet folytatnak, és 13 éven aluliak részére nyújtják a szolgáltatásaikat, vagy tudomásuk van arról, hogy 13 éven aluli veszi igénybe a szolgáltatásukat, COPPA, section 1302 (2) (B)

A törvény által a weblapok üzemeltetőire rótt többletkötelezettség miatt jelentős részük döntött úgy, hogy egyszerűen megtiltja 13 éven aluli gyermekek regisztrálását, mely alól a Facebook sem kivétel. A tiltást úgy oldják meg, hogy a felhasználói feltételekben nem engedélyezik gyermekkorúak számára a csatlakozást és amennyiben regisztrálni kell a honlap használatára, abban az esetben rákérdeznak a regisztráló korára vagy születési dátumára, mellyel ki tudják szűrni a gyermekeket.

A jogszabály és a Szövetségi Kereskedelmi Bizottság³⁶⁷ fellépése miatt az olyan oldalak jelentős része, melyek gyermekeknek készültek (pl. www.disney.com), a felhasználók körét vagy a felhasználók által elérhető funkciókat korlátozták, ha nem rendelkeztek személyi és dologi háttérrel a szülői nyilatkozatok megfelelőségének ellenőrzésére (gyakran a szülők hitelkártyájának adatait használják fel erre a célra).

A Facebook életkorhatára miatt a gyermekek jelentős része hamis adatot ad meg életkoráról: az Egyesült Államokban 2010-ben a 14 évesek 78 %-a, a 13 évesek 62 %-a, a 12 évesek 46 %-a használta a szociális hálózatot.³⁶⁸

Egy 2011-ben készült tanulmány vizsgálat alá helyezte a gyermekkorúak Facebook használatát az Egyesült Államokban, mely alapján átlagosan 10 éves korukban az amerikai szülők már engedélyezik gyermekeiknek a Facebook használatát, sértve felhasználási feltételeket.³⁶⁹

A tanulmány elkészítése során több, mint 1000 háztartásban végeztek felmérést, mely alapján a megkérdezett szülők 76%-a engedélyezte gyermekeik számára 13 éves kor alatt a Facebook használatát. A megkérdezett szülők csupán 53 %-a volt tisztában a korhatárral: ezen belül a 35%-uk azt gondolta, hogy a 13 éves kor csupán ajánlás és nem kötelező, a 65% abban a meggyőződésben volt, hogy a korhatár 16 vagy 18 év, nem pedig 13. A felmérésre a Facebook sajtónyilatkozattal válaszolt, melyben kifejtésre került többek között, hogy naponta 20000 felhasználót törölnek életkorral kapcsolatos probléma miatt.

A Disney 2006-ban vásárolta meg a Club Penguin 12 millió gyermek adataival, mely a világ legnagyobb gyermekek számára készült közösségi hálójá: az oldal játékok, tanulást fejlesztő

³⁶⁷ A Federal Trade Commission (Szövetségi Kereskedelmi Bizottság, továbbiakban: FTC) lép fel a COPPA betartásáért: jelentős pénzbírságokat szabhat ki azon oldalak üzemeltetőire, akik nem szerzik be a megfelelő szülői engedélyeket, vagy nem teszik meg a szükséges intézkedéseket a törvény rendelkezéseinek és a felhasználói feltételeknek a végrehatására.

³⁶⁸ Amanda Lenhart, Kristen Purcell, Aaron Smith, and Kathryn Zickuhr: "Social media & mobile Internet use among teens and young adults," Pew Internet and American Life Project report, 2010. 02. 03. http://www.pewinternet.org/~media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf,

³⁶⁹ Eszter Hargittai, Jason Schultz, and John Palfrey: Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act, in: First Monday, Volume 16, 2011. 11. 07, 1-8. <http://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075>

feladatok és közösségi szolgáltatások nyújtásával foglalkozik. A Club Penguin után a Disney az Online Playdom oldalt vásárolta meg, melynek 42 millió felhasználója volt a jogügylet időpontjában. 2011-ben az FTC 3 millió dollárral büntette meg gyermekek részére szolgáltatást nyújtó oldalakat, köztük a Playdomot³⁷⁰, mert 13 éven aluliak regisztrálhattak és vehették igénybe az oldalak szolgáltatásait anélkül, hogy bármiféle szülői nyilatkozat rendelkezésre állt volna.³⁷¹

Az Adatvédelmi Rendelet speciális rendelkezéseket tartalmaz a gyermekek hozzájárulásával kapcsolatosan, amely alapján a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén a személyes adatainak kezelése csak akkor jogszerű, ha a hozzájárulást a gyermek felett szülői felügyeletet gyakorló személy adta meg, illetve engedélyezte³⁷².

A rendelet megengedi továbbá a tagállamoknak, hogy a 16 éves kortól lefele eltérjenek 13 éves korig, a védelmet kiterjesztve, amely véleményem szerint nem szerencsés, hiszen a rendeltnek pont az lenne a célja, hogy az adatvédelmi szabályozás egységes legyen az EU területén. Az eltérő szabályozások és korhatárok következtében így az EU teljes területén szolgáltatást nyújtó vállalatok kénytelenek lennének a 16 éves korlátot alkalmazni az adatkezeléseik során, a legbiztonságosabb megoldást választva³⁷³. További probléma a 16 éves korhatárral, hogy az túlzottan magas, az USA-ban 13 éves kor van az online védelemhez meghatározva több okból is, amelyhez célszerű lett volna az európai szabályozást is igazítani, vagy közelíteni.

Az adatkezelőnek – figyelembe véve az elérhető technológiát – ésszerű erőfeszítéseket kell tennie, hogy ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója

³⁷⁰ Az FTC elnöke az ügygel kapcsolatban az alábbi nyilatkozatot tette:

„Legyen világos: akár virtuális világot, szociális hálózatot, vagy akármilyen interaktív oldalt üzemeltetsz gyermekek részére, megfelelő tájékoztatással tartozol a szülők felé, és szükséges az engedélyük beszerzése. ... Ez a törvény, a helyes irány, amit követni kell, és ma mai nap döntése bizonyítja, hogy a COPPA megszegése nem olcsó.”

³⁷¹ Federal Trade Commission: Operators of Online "Virtual Worlds" to Pay \$3 Million to Settle FTC Charges That They Illegally Collected and Disclosed Children's Personal Information, 2011. 05. 12.
<http://www.ftc.gov/news-events/press-releases/2011/05/operators-online-virtual-worlds-pay-3-million-settle-ftc-charges>

³⁷² 8. cikk A gyermek hozzájárulására vonatkozó feltételek az információs társadalommal összefüggő szolgáltatások vonatkozásában (1) Ha a 6. cikk (1) bekezdésének a) pontja alkalmazandó, a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.
A tagállamok e célokból jogszabályban ennél alacsonyabb, de a 13. életévnél nem alacsonyabb életkort is megállapíthatnak.

³⁷³ Linklaters: The General Data Protection Regulation: A survival guide, 2016.
www.linklaters.com

adta meg, illetve engedélyezte, amelyhez több lehetőség is rendelkezésre áll. Az Egyesült Államokban került elfogadásra egy olyan megoldás, amely alapján egy fényképes igazolvány és egy fénykép ("selfie") együttes elküldésével a szülő hozzájárulása elfogadható.

A rendszer úgy működik, hogy a szülő elküldi a fényképes igazolványát, majd egy olyan fényképet, amelyet maga készített (selfie) egy webkamerával, vagy a mobil elején lévő fényképezővel, majd a rendszer arcfelismerő algoritmus összeveti a két képet.

Érdekes az Adatvédelmi Rendelet megfogalmazása, amely alapján azokban az esetekben szükséges a szülői hozzájárulás, amennyiben a szolgáltatást „kifejezetten gyermekek részére” kínálják. Felmerül a kérdés hogy például a Facebook kifejezetten gyermekek részére kínált szolgáltatásnak minősül-e. Egy rajzfilm videó megosztó, vagy játékokat áruló oldal esetében egyértelmű a helyzet, azonban egy közösségi hálózatonál, amely nem csak gyermekek részére nyitott, már nehezen eldönthető.

Az Adatvédelmi Rendelet a felejtés jogával kapcsolatban határoz meg további védelmet a gyermekekkel kapcsolatban, akik jogosultak arra, hogy személyes adataikat töröljék és a továbbiakban ne kezeljék. Ez a jog különösen akkor lényeges, ha az érintett gyermekként adta meg hozzájárulását, amikor még nem volt teljes mértékig tisztában az adatkezelés kockázataival, később pedig el akarja távolítani a szóban forgó személyes adatokat az internetről. Fontos, hogy az érintett e jogát gyakorolhatja akkor is, ha már nem gyermek.

A gyermekek biztonságát és személyes adatait több módon is védhetnék a közösségi hálózatok: célszerű lenne, ha a gyermekektől nem kérnének a közösségi hálózatok különleges adatokat regisztrálás során, mivel többek között a vallással és a politikai hovatartozással kapcsolatos véleményeik még kiforratlanok. Fontos lenne továbbá, hogy a közösségi hálózat megfelelő módon ellenőrizze a felhasználók valódi életkorát, melyre több technikai megoldás is rendelkezésre áll. A közösségi hálózatokon belül csoportok hozhatóak létre, melyeknél célszerű lenne korhatárt is a csoport témájával kapcsolatban: egy párkereső csoportban például a gyermekek személyes adatait nem szabadna korlátlanul rendelkezésre bocsátani.

5.7 Fényképekkel és a felhasználó azonosításával kapcsolatos adatkezelések

A felhasználók által feltöltött személyes adatok közül különösen fontos szerepet töltenek be a különleges adatok³⁷⁴: a felhasználó adatlapjával kapcsolatosan a Facebook már a regisztráláskor rákérdez olyan szenzitív információkra, mint a politikai vagy vallási nézet. A különleges adatok a közösségi hálózatokon kizárólag az érintett kifejezett hozzájárulásával kezelhetők, vagy ha ő maga hozza azokat nyilvánosságra³⁷⁵.

A feltöltött képekkel kapcsolatban a jogi helyzet nem ennyire egyértelmű: képekből is kiderülhetnek olyan különleges adatok az érintettekről, mint vallásuk, politikai nézetük, etnikumuk, vagy akár a betegségük (pl. egy politikai gyűlésen készült fényképfelvétel egyértelműen kifejezheti résztvevők politikai nézeteit). A tagállami jogszabályok és joggyakorlat általában nem tekintik különleges adatnak a fényképeket. A 29. Cikk Munkacsoport főszabály szerint nem tekinti különleges adatnak az ilyen fényképeket, kivéve, ha a fényképet azon célból készítették és használták fel, hogy valamilyen különleges adatot hozzon nyilvánosságra az érintettől.³⁷⁶

A Munkacsoport véleményének egyik oka lehet, hogy a fényképen résztvevőket általában csak az ismerőseik ismerik fel, akik a megosztott fényképeket csak véletlenszerűen láthatják, rákeresni az érintett neve alapján nem tudnak, kivéve, ha a nevek meg vannak jelölve a kép leírásában.

Az arcfelismerő programok fejlődésével a különleges adatokat tartalmazó fényképek jogi helyzete is megváltozhat a jövőben: az érzékeny információt tartalmazó fényképek az érintetthez kapcsolhatóvá válhatnak akár másodpercek alatt.

2011 októberében került bemutatásra egy olyan okostelefon alkalmazás koncepciója, amely képes egy személyről egy fotó elkészítése után kiírni annak nevét, születési dátumát, és más személyes adatait. A magánszférát komolyan veszélyeztető technológiának csupán két korlátja volt: a megfelelő adatbázis hiányzott hozzá, hogy a fényképhez személyes adatokat tudjon párosítani, továbbá a sebessége lassú volt, mivel az Egyesült Államok lakosságának (300 millió

³⁷⁴ Adatvédelmi irányelv, 8. cikk (1) A tagállamok megtilthatják az olyan személyes adatok feldolgozását, amelyek a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkoznak.

Infotv. 3. § 3. különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

³⁷⁵ Tagállami jogszabály ettől eltérhet.

Adatvédelmi Irányelv (2) Az (1) bekezdést nem alkalmazható abban az esetben, ha:

a) az érintett kifejezett hozzájárulását adta az említett adatok feldolgozásához, kivéve, ha a tagállam joga úgy rendelkezik, hogy az (1) bekezdésben említett tilalom alól nem engedhető kivétel az érintett hozzájárulásával sem

³⁷⁶ Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 2009, 8.

ember) vizsgálatához több óra is szükséges, így nem alkalmas arra, hogy élesben késedelem nélkül azonosítsa és kiírja az adatokat. A két korlát a megfelelő kormányzati (állami adatbázisok, titkosszolgálatok) vagy céges (pl.: Facebook vagy Google hatalmas adatbázisai) háttérrel könnyen leküzdhető, így csupán idő kérdése, hogy az arcfelismerés élesben is működjön.

2012-ben a Facebook megszerezte a face.com-ot, mely egy arcfelismeréssel foglalkozó cég, technológiájuk olyan szintű fejlettséggel bír, mely képes az arcok felismerésére rossz fényviszonyok és képminőség esetén: még a szemüveg, smink és a Halloween jelmez sem jelent akadályt neki. A Facebook fotó könyvtárában 2013 szeptemberében 350 milliárd kép volt, mely naponta 350 millióval növekszik. Semmilyen szervezet a Világon nem rendelkezik ekkora adatbázissal: a Flickr 10 milliárd fotóval rendelkezik és 3,5 milliót töltenek fel naponta. A kormányok is csupán az igazolványképekkel és az igazságügyi és titkosszolgálati tevékenységükből eredő képekkel rendelkeznek.

Kijelenthetjük, hogy az arcfelismerő technológia első korlátja (a megfelelő adatbázis hiánya) kiküszöbölésre került a Facebook adatbázisával. A feldolgozás megfelelő sebességének elérése pedig csak idő kérdése a felhő alapú technológiának, az internet és a szerverek feldolgozási sebességének köszönhetően.

A Facebook 2010 decemberében kezdte el a technológia használatát³⁷⁷ („Photo Tag Suggest”), mely javaslatokat tett a feltöltött képeken a megjelölendő személyekre³⁷⁸. Adatvédelmi szempontból a Facebook arcfelismerőjével kapcsolatosan problémát jelent, hogy opt-out elven működik, tehát az alapbeállítás szerint be van kapcsolva, és a felhasználónak kell inaktíválni, ha nem kíván élni vele.³⁷⁹

Az arcfelismerő működésének rövid leírása szerint a szoftver az arc speciális tulajdonságai alapján abból egy mintát generál, benne a legfontosabb koordinátákkal (mint pl.: szemek, orr, száj és fül távolsága egymástól). Az ehhez szükséges információkat a felhasználó profilképeiből szerzi meg és olyan képekből, melyeken a felhasználó meg lett jelölve.³⁸⁰

³⁷⁷ Daniel Ionescu: Facebook Adds Facial Recognition to Make Photo Tagging Easier. PCWorld, 2010. 12. 16. http://www.pcworld.com/article/213894/facebook_adds_facial_recognition_to_make_photo_tagging_easier.html

³⁷⁸ A technológia alapja, hogy a gyorsabb találatok érdekében először az ismerőseink, majd ismerőseink ismerősei között keresett rá a felismerő program segítségével, mellyel jelentősen lecsökkenthető az erőforrásainak igénylése és a találatok időtartama.

³⁷⁹ Graham Cluley, Facebook changes privacy settings for millions of users facial recognition is enabled. Sophos naked security, 2011. 06. 07. <http://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/>

³⁸⁰ Facebook súgó, 2014. szeptember 21. <https://www.facebook.com/help/tag-suggestions>

A Facebook, mint univerzális személyazonosító

A legtöbb személyre szabott internetes szolgáltatás és alkalmazás azonosítóhoz és jelszóhoz kötött, melynek megjegyzése és tárolása sokszor gondokat okozhat a felhasználók számára. Aki az egyszerűbb utat választja, minden oldalhoz ugyanazt a jelszót használja, mely komoly veszélyeket rejt: ha egyszer megszerzi valaki valamilyen módon a felhasználó jelszavát, avval minden fiókjába bejuthat.

A kockázatot ismerve aggályos, hogy egyre több alkalmazás és szolgáltatás szeretne univerzális elérést használni, melyhez a Facebook, Google, vagy más elterjedt szolgáltató bejelentkezési rendszere kerülne alkalmazásra.³⁸¹ A probléma hasonlít ahhoz az élethelyzethez, amikor egy kulccsal nyithatjuk a lakásunkat, garázsunkat, az autónkat és a széfünket: kétségtelenül praktikus és leegyszerűsíti az életünket, azonban jelentős kockázatot is hordoz.

A 2000-es évek elején már volt erre egy próbálkozás a Microsoft részéről is, amikor be szeretnék volna vezetni a Microsoft Passportot, mely egységes bejelentkezési és azonosítási felületként funkcionált volna az interneten, azonban kudarcba fulladt a biztonsági problémák miatt.³⁸²

A Microsofttal ellentétben a Facebooknak sikerül egyre több szolgáltatót meggyőznie a bejelentkezési rendszer előnyeiről és az adataikat féltő felhasználókat megnyugtatni, melynek hatására növekszik a Facebook bejelentkezési rendszerét használók száma. Az NSA botrány sajnos rávilágított, hogy az amerikai titkosszolgálat hozzáfér a Facebookhoz: nem nyilvános adataink, levelezéseink és akár jelszavunk is az USA erre szakosodott hatóságainak a kezébe kerülhet, így feltételezhetjük, hogy akár más internetes szolgáltatásainkhoz is hozzáférhetnek. Az eset óta különösen kétséges a Facebook által biztosított univerzális elérés megbízhatósága. A „ne egy kosárban tartsd az összes tojást” mondás jelen helyzetben is igaz lehet.

A Szövetségi Kereskedelmi Bizottság döntése a Facebook adatvédelmi szabályszegéseivel kapcsolatban

³⁸¹ Robyn Peterson: Who Owns Your Identity on the Social Web? Mashable, 2011. 10. 11.
<http://mashable.com/2011/10/21/web-identity/>

³⁸² Passport failure shows the folly of Microsoft's ways, Zdnet, 2005. 01. 04.
<http://www.zdnet.com/passport-failure-shows-the-folly-of-microsofts-ways-3039183062/>

A Szövetségi Kereskedelmi Bizottság hosszas vizsgálat után úgy találta, hogy a Facebook több ponton is megszegte a saját szabályzatait és a magánszférát védő jogszabályokat³⁸³:

a) A Facebook 2009 decemberében megváltoztatta a weboldal működését és megjelenését, mely által olyan információk lettek publikusak, amelyek addig privátnak számítottak. A változtatás előtt a Facebook nem kérte ki a felhasználók engedélyét és nem is tájékoztatta őket, így arra nem tudtak felkészülni a személyes adataik eltávolításával.

b) A harmadik felek által készített alkalmazásokkal kapcsolatban azt állította a szabályzat, hogy csak a céljuk eléréséhez szükséges személyes információkhoz férhetnek hozzá, azonban ez nem volt igaz: a felhasználók bármely személyes adatához hozzáférhettek az alkalmazások, olyanokhoz is, amelyek a rendeltetésszerű működésükhöz nem voltak szükségesek.

c) A felhasználók meghatározhatták, hogy egyes személyes adataikat csak bizonyos felhasználói körök tekinthettek meg (pl.: egy képet csak az ismerősök, vagy ismerősök ismerősei láthatnak), azonban ez a gyakorlatban nem működött, mivel az alkalmazásokon keresztül mások is láthattak olyan információkat, melyekre egyébként nem lettek volna jogosultak.

d) A Facebooknak volt egy „Megbízható alkalmazások” elismerése, mely alapján a Facebook által jóváhagyott alkalmazásoknak biztonságosnak és az adatvédelmi előírásokat tisztelőnek kellett volna lenniük, azonban ez az elismerés valós védelmet nem jelentett.

e) A Facebook azt állította, hogy a törölt vagy felfüggesztett felhasználói fiókok felhasználóinak a képeihez és egyéb adataihoz nem lehet hozzáférni, azonban a törlés vagy felfüggesztés után még hosszú ideig elérhetőek voltak a tartalmak.

f) A Facebook részt vett a „U.S.- EU Safe Harbor” programban (ami az Európai Unió és az Egyesült Államok közötti személyes adatok áramlását teszi lehetővé), azonban valójában nem tette meg az ehhez szükséges intézkedéseket.³⁸⁴

Jogi csatározás helyett a Facebook és a FTC egyezséget kötöttek melyben a Facebook az alábbiakra kötelezte magát:

³⁸³ Pepitone Julianne: Facebook settles FTC charges over 2009 privacy breaches. CNN, 2011. 11. 29.
http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.html

Jon Leibowitz, a FTC elnöke: „A Facebook köteles betartani a privacyvel kapcsolatos kötelezettségeit és ígéreteit, melyeket a felhasználók százmillióinak tesz.”, "A Facebook innovációjának oltárán nem szükséges a privacyt feláldozni. Az FTC mindent meg fog tenni, hogy ez így is legyen."

³⁸⁴ Complaint against Facebook by the Federal Trade Commission, Commissioners: Jon Leibowitz, Chairman, J. Thomas Rosch, Edith Ramirez, Julie Brill
<http://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>

- a) tartózkodni fog a felhasználók megtévesztésétől a személyes információik kezelésével és biztonságával kapcsolatosan (pl. harmadik alkalmazások hogyan férhetnek adatokhoz hozzá),
- b) a jövőben a felhasználók kifejezett hozzájárulása lesz szükséges a privacy-vel kapcsolatos preferenciáik és beállításaik megváltoztatásához,
- c) megteszi a szükséges technikai és szervezési intézkedéseket ahhoz, hogy azon felhasználók adatai, akik törölték fiókjukat, vagy felfüggesztették azt, ne legyenek elérhetőek 30 nap után,
- d) kialakít és fenntart olyan privacyt védő programokat és eljárásokat, melyek az új és régi termékek és szolgáltatások személyes adatokkal kapcsolatos kockázatait csökkentik, majd azokról folyamatosan tájékoztatják a felhasználókat,³⁸⁵
- e) az egyezségtől számított 180 napon belül és az azt követő 20 évben 2 évente független, külsős privacy szakértővel vizsgálhatja meg az adatvédelmi szabályzatát és eljárásait, melyeknek meg kell felelniük a jogszabályok és az FTC által támasztott mindenkori követelményeknek.

Annak ellenére, hogy Facebook többször is felelőssé lett téve a felhasználók magánszférájának és a személyes adatok védelmének megsértése miatt, ez a felhasználók jelentős részét nem zavarja: ugyanúgy bizalmas információkat - még bűncselekményeket is - vitatnak meg a Facebook üzenetküldő szolgáltatásán és osztanak meg egymással csoportokban, továbbá nem szabályozzák a képeik, kiírásaik és csoportjaik megtekintési jogosultságait.

Az FTC ügy lefolyása alatt készült egy felmérés az amerikai Facebook felhasználók között, mely alapján a felhasználók harmada soha nem állította semmilyen tartalmának a privacy beállításait.³⁸⁶

A felhasználók képviselői által felhozott problémák 4 csoportba sorolhatók: a felhasználói feltételek nem megfelelő prezentálása az érintettek részére, megtévesztő információk, a felhasználók folyamatos „késztetése”, hogy az információikat publikusan osszák meg, a problémákat igyekszik a képviselőkkel peren kívül megoldani, sokszor a problémákat nem valószínű orvosolva³⁸⁷.

³⁸⁵ Federal Trade Commission: Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, 2011. 11. 29.
<http://www.ftc.gov/opa/2011/11/privacysettlement.html>

³⁸⁶ Mary Madden, Aaron Smith: Reputation Management and Social Media.
Pew Internet, 2010. 05. 26.

<http://pewinternet.org/Reports/2010/Reputation-Management/Part-2/Attitudes-and-Actions.aspx>

³⁸⁷ Rotem Medzini: Prometheus Bound: An Historical Content Analysis of Information Regulation in Facebook, University of Jerusalem, Faculty of Social Sciences, School of Public Policy, Students; Haifa Center for Law and Technology, 2016. 86.

Adatkezelés a személyes adatok törlése után

A közösségi hálózatok a felhasználókról a fiókjuk törlése után is tárolnak még személyes adatokat. A további tárolás oka legtöbbször technikai, mint szervezési: ha egy merevlemezről az adatokat törlik, valójában az elérhető marad, amíg felül nem írják. Bár léteznek megoldások arra, hogy egy adatot helyrehozhatatlanul megsemmisítsenek a fizikai adathordozó sérelme nélkül annak működése közben, azonban a nagy felhasználói táborot kiszolgáló szolgáltatások esetén a naplófájlok és a biztonsági mentések miatt késedelem nélkül bonyodalmas lenne megoldani az azonnali törlést, melyre adatvédelmi szabályzatában a Facebook³⁸⁸ is felhívja a figyelmet.

A kitiltott felhasználók adatai szintén tárolásra kerülnek, hogy az újbóli regisztrálásuk esetén kiszűrhetőek legyenek. A Munkacsoport ajánlása alapján a kitiltás esetén is csak a felhasználó személyes adatait lehetne megtartani, a kitiltás okát nem. Az adatok tárolásának maximális ideje 1 év³⁸⁹ lehetne³⁹⁰ az ajánlás alapján, a Facebook is 90 napot ad meg maximális időtartamnak technikai okok miatt.

Az adatok további tárolásával kapcsolatban nem csak ellenérvek fogalmazhatóak meg: a más nevében regisztrálók („identity theft”) ellen lehet védekezni, ha a törölt felhasználó azonosítására alkalmas adatokat őriz meg a közösségi hálózat, továbbá a bűncselekményeket közösségi hálózaton kifejtők ellen (pl. zaklatás) is célszerű hosszabb távon védekezni.

A felhasználók nem csak a fiókjukat, hanem a róluk feltöltött egyes információkat, képeket is bármikor törölhetik, frissíthetik, melyre szintén érvényesek a fiók törlésére megadott határidők³⁹¹.

³⁸⁸ Facebook adatvédelmi szabályzat (2014. 09. 22.):

Amikor törlöd a fiókodat, az véglegesen törlődik a Facebookról. Egy fiók törlése általában kb. egy hónapig tart, de bizonyos adatok akár 90 napig is megmaradnak a biztonsági mentésekben és naplókban.

³⁸⁹ Adatvédelmi irányelv, 6. cikk

(1) A tagállamok rendelkeznek arról, hogy a személyes adatok:

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges ideig teszi lehetővé. A tagállamok állapítják meg a személyes adatok történelmi, statisztikai vagy tudományos célból, hosszabb ideig történő tárolásának megfelelő garanciáit.

³⁹⁰ Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 2009, 10.

³⁹¹ Facebook adatvédelmi szabályzat (2014. 09. 22.): Bizonyos információk egy adott szolgáltatás nyújtásához szükségesek, így ezeket csak a fiókod törlését követően töröljük. Némely Facebook-tevékenységet nem a fiókodban tárol a rendszer: ilyen például a csoportoldalon való közzététel vagy az üzenetküldés (ahol előfordulhat, hogy ismerősöd azután küld neked üzenetet, hogy már törölted a fiókodat). Ezeket az adatokat a fiók törlését követően is megőrizzük.

A törlés utáni adatkezeléseknél különösen fontos, hogy a felhasználót tájékoztassák arról, és biztosítsanak részére lehetőséget, hogy informálódhasson akkor is, ha már nem regisztrált felhasználója a közösségi hálózatnak.

5.8 Következtetések

A fejezetben bemutatásra kerültek a Facebook adatkezeléssel kapcsolatos problémái, amelyeknek eredete a közösségi hálózat azon alapvető érdeke, hogy a felhasználók minél több információt töltsenek fel és osszanak meg magukról a hirdetések hatékonyabbá tételéhez. A megosztás ösztönzésén és annak alapbeállítással történő túl a Facebook olyan forrásokon keresztül is gyűjt személyes adatokat, amelyekről a felhasználóknak sok esetben nincsen tudomása és/vagy kontrollja.

A legtöbb Facebook által végzett adatkezelés jogalapja a felhasználó hozzájárulása, amelynek önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak, és félreérthetetlennek kellene lennie. A fejezetben bizonyításra került, hogy több, Facebook által végzett adatkezelés esetében a 4 feltétel egyike, vagy maga a hozzájárulás is hiányzik.

Az önkéntességet a választási lehetőség hiányával, a határozottság és félreérthetlenség problémáját a felhasználó tudta és hozzájárulása nélkül zajló adatgyűjtésekkel mutattam be, amelyeknek eredete a hiányos és nem áttekinthető tájékoztató, amelynek homályos és megtévesztő részleteire rámutattam.

A Facebook hozzájárulással kapcsolatos hiányosságai különösen problémásak lehetnek majd az Adatvédelmi Rendelet alkalmazása során, amely mind az általános, mind a gyermekek hozzájárulásával kapcsolatban szigorúbb követelményeket támaszt, amelyeket a fejezetben bemutattam.

A Facebook történetének, működésének és bevételének vizsgálatát követően a szolgáltatás fizetősé tételét a személyes adatok fokozott védelméért cserében csak korlátozottan tartom megvalósíthatónak.

A Facebook átlagos felhasználónkénti bevétele az Egyesült Államokban „túl magas” ahhoz, hogy azt könnyűszerrel ki lehessen váltani a felhasználók befizetéseivel, míg Ázsiában és a világ jelentős részén a legminimálisabb felhasználói díj fizetése sem jelenthet alternatívát.

Európában ezzel szemben az 1,3 eurós felhasználónkénti havi átlagbevétel nem jelentene különösebb nehézséget a felhasználók jelentős részének, különösen Nyugat-Európában.

Véleményem szerint a középút is megtalálható lenne: lehetséges lenne egy olyan megoldás alkalmazása, amellyel a felhasználónkénti bevétel 50%-ban reklámbevételből, 50%-ban a felhasználó által fizetett összegből állna össze.

A felezett összegű reklámbevételt elérhetné a Facebook viselkedésalapú reklámozás nélkül, a felhasználóról csupán alapvető adatok megszerzésével, amelyeket a felhasználó önként adna meg (pl. nem, kor, lakóhely).

Így létrejöhetne egy olyan helyzet, hogy már a felhasználó regisztrálásakor alapbeállításként le lennének tiltva teljes mértékben a helymeghatározáson és viselkedésen alapuló adatgyűjtések, továbbá a felhasználó személyes adatainak kiszolgálása a Facebook partnerei részére, és csupán böngészője oldalsávjában kapna reklámokat szalaghirdetésekből, amelyeket bármilyen weboldalon is látogatóként megkapna anélkül, hogy bármilyen érzékeny információt megadna magáról.

A felejtés jogának érvényesítésében a Facebooknak is komoly szerepe lehetne, mivel a felhasználók posztjai és cselekményei az esetek jelentős részében csupán a pillanatnak szólnak, azonban azok mégis megőrzésre kerülnek és folyamatosan naplózva vannak. Célszerű lenne a posztok esetében időkorlát lehetőségét biztosítani a felhasználók részére, hogy a felejtéshez való jogukat könnyebben tudják érvényesíteni, vagy alapértelmezett időkorlát megadását lehetővé tenni, hogy a szolgáltatás „privacy by default” legyen.

A felhasználó beállíthatná továbbá, hogy az időtartam elteltével mi legyen az adatok sorsa: törlődjenek, vagy csupán a nyilvánosságuk szűnne meg, így archiválná, vagy csupán közeli ismerősök számára lenne megtekinthető.

6. Személyes adatok küldése az EU területéről az Egyesült Államokba, különös tekintettel az internetes keresőkre és a közösségi hálózatokra

Az Európai Unió, az Egyesült Államok és az ázsiai országok legfőbb alkotmányos értékei között komoly eltéréseket találhatunk, amely áthatja az adott társadalmak adatvédelemmel kapcsolatos elképzeléseit és elvárásait is. Az ázsiai országok társadalmaiban alapvető értékként jelenik meg a közösséghez tartozás, abba való integrálódás, a rend és a család iránti igény, amelyben az individuumnak nincsen akkora súlya, mint a nyugati társadalmakban. A kollektív szemlélet miatt az adatvédelem több ázsiai országban sokáig nem kapott olyan jelentőséget, mint a nyugati államokban.

Európában alapvető érték az emberi méltóság és az egyén jogainak védelme, különösen a mindenható állammal és a társadalom többi tagjával szemben, amelyek a világháborúból és a „mindent látó” szocialista államok emlékéből erednek.

Az Egyesült Államokban evvel szemben kiinduló pontként az egyéni szabadság jelenik meg, mely az individuum kibontakozását biztosítja az állam háttérbe szorításával.

Jól látható a különbség: a liberális piacgazdaság mellett elkötelezett amerikaiak szerint a szabadságra az állam tevékenysége jelentheti a legnagyobb veszélyt, míg az európaiak igénylik az állam védelmét (különösen Kelet-Európában)³⁹².

Az Egyesült Államok abban a szerencsés helyzetben van, hogy a legnagyobb szoftver és technikai óriásoknak (pl.: Google, Apple, Microsoft) a területén van székhelye, melyek a gazdaság egyik fő motorját jelentik, ugyanakkor a „jövőálló” befektetés.

A gazdasági szempontokon túl – legalább annyira jelentős – jogi és nemzetvédelmi kérdések is felmerülnek: milyen jogalapon és hogyan kezelik a hatalmas IT cégek a világ majdnem összes országából rendelkezésükre álló személyes adatokat, továbbá az Egyesült Államok kormányának van-e ehhez hozzáférése. Mielőtt az adatok vándorlásának jogi hátterét vizsgálnánk meg, fontos egy pillantást vetni az USA adatvédelmi jogi szabályozására.

Az USA alkotmánya nem nevesíti a személyes adatok védelméhez és a magánszférához való jogot, így a személyes adatok védelméhez való jog nem vezethető le közvetlenül az

³⁹² Péterfalvi, 2012, 37.

alkotmányból, mint az EU tagállamaiban, azonban több magánszférát védő alkotmánymódosítás³⁹³ és legfelsőbb bírósági döntés³⁹⁴ létezik.

Az Egyesült Államokban a magánszféra védelme inkább a (rabszolgatartásból eredő) diszkrimináció tilalmára és otthon sérthetlenségére (én házam én várom³⁹⁵) fókuszál.

Az amerikai liberális gazdaságban az állampolgárok személyes adatai szabad prédának minősülnek magánszférában (kivéve a bankkártya és TB számok) és a kormányzati szervek számára is, mely a társadalom jelentős részét szemmel láthatóan jelentősen nem zavarja. A hozzáállásukat jellemzi, hogy a szexuális bűncselekmények elkövetőinek listája nyilvános és fényképekkel ellátott, melyről bárkinek joga van tudomást szerezni. A terrortámadások pedig még különösen az adatvédelem ellen hajtják a kormányzati gépezetet és a közvéleményt: az NSA botrány rámutatott, hogy nemzetbiztonsági érdekekre és egy bírósági ítéletre hivatkozva bárkinek a személyes adataihoz és levelezéséhez hozzáférnek az amerikai titkosszolgálatok.

Szövetségi szinten több jogszabály is védi³⁹⁶ az egyén magánszféráját, azonban mindegyik csak annak egy részét, melyre jó példa a Children's Online Privacy Protection Act (Gyermekek Online Magánszféráját Védő Törvény), mely a 13 éven aluli gyermekek magánszféráját védi az interneten: a jogszabály korlátozza a weblapok adatgyűjtési jogát és a szülők hozzájáruló nyilatkozatához köti több szolgáltatás használatát, mely folytán sok oldal inkább nem is engedélyezi a 13 éven aluliak regisztrációját, hogy elkerülje az adminisztratív terheket és a lehetséges bírságokat.

A törvény védi a 13 éven alúkat, viszont semmilyen más konkrét jogszabály nem védi szövetségi szinten a 13 éven felüliek online jogait és személyes adatait.

Hasonló a helyzet az az 1974-es Magánszféra Törvénnyel (Privacy Act³⁹⁷), mely a közszféra adatkezeléseit szabályozza és ír elő garanciákat, azonban a magánszféra adatkezelésével nem

³⁹³ Ilyen például az első (szólás, sajtó- és vallásszabadság, 1789. 09. 25.), negyedik (megalapozatlan házkutatás elleni védelem, 1789. 09. 25.) és az ötödik alkotmánymódosítás.

³⁹⁴ Pl.: *Kyllo v. United States* (a hőkamerák használata állampolgárok házaiban a negyedik alkotmányban meghatározott házkutatás hatálya alá esik, ezért az csak hatósági engedéllyel tehető meg),

Ferguson v. City of Charleston (kórházban drogtesztet a betegen végrehajtani csak az engedélyével lehet).

³⁹⁵ Blackstone's Commentaries on the Laws of England, Book the Fourth - Chapter the Sixteenth: Of Offenses Against the Habitations of Individuals

³⁹⁶ Fair Credit Reporting Act (1970), Bank Secrecy Act (1970), Privacy Act (1974), Family Educational Rights and Privacy Act (1974), Right to Financial Privacy Act (1978), Foreign Intelligence Surveillance Act (1978), Privacy Protection Act (1980), Cable Communications Policy Act (1984), Electronic Communications Privacy Act (1986), Computer Matching and Privacy Protection Act (1988), Video Privacy Protection Act (1988), Telephone Consumer Protection Act (1991), Driver's Privacy Protection Act (1994), Communications Assistance for Law Enforcement (1994), Personal Responsibility and Work Opportunity Reconciliation Act (1996), Identity Theft and Assumption Deterrence Act (1998), USA-PATRIOT Act (2001), Video Voyeurism Prevention Act (2004).

³⁹⁷ Privacy Act of 1974, <http://www.justice.gov/opcl/overview-privacy-act-1974-2012-edition>

foglalkozik, és olyan alapvető adatvédelmi elvektől tér el, mint a célhoz kötöttség elve (az eredetitől eltérő célra is lehet használni az adatokat, és a TB számot általános azonosító kódként engedi kezelni).

Tagállami szinten 10 tagállami alkotmány nevesíti a privacy, azaz a magánszféra védelmét³⁹⁸, és 2 államban a magánszféra sérelme jogalapot adhat polgári eljárás megindítására.

A legtöbb magánszférát védő jogszabály tagállami szinten található, melyeknek a szövetségi szabályozás engedélyezi, hogy a védelem szintjében meghaladják. A legfontosabb magánszférát védő jogszabály a California Online Privacy Protection Act (Kaliforniai Online Magánszférát Védő Törvény), mely a weblapok üzemeltetői számára ír elő kötelezettségeket a látogatók tájékoztatásával és személyes adataik védelmével kapcsolatosan (pl. milyen adatokat gyűjthetnek, kinek küldhetik tovább). Véleményem szerint a jogszabály példaként szolgálhatna egy szövetségi szintű szabályozás elkészítéséhez.

Az Egyesült Államokban szövetségi és tagállami szinten sem létezik az Európai országokéhoz fogható, elkülönült adatvédelmi hatóság, azonban egyes hatóságok és szervezetek rendelkeznek adatvédelemmel kapcsolatos hatáskörökkel, mint például a Szövetségi Kereskedelmi Bizottság³⁹⁹ (Federal Trade Commission), mely a Gyermekek Online Magánszféráját Védő Törvény, a Privacy Shield irányelvek, spammal kapcsolatos szabályok betartásáért felel. A vállalatok nem rendelkeznek kötelezettséggel arra nézve, hogy adatvédelmi felelőst nevezzenek ki, kivéve egyes egészségügyi szektorban tevékenykedő cégeket⁴⁰⁰.

Az USA tagállamainak a „kereskedelmi klauzula”⁴⁰¹ alapján nincsen lehetőségük korlátozni a személyes adatok áramlását külföldi országokba, és jelenleg szövetségi szinten sincs annak akadálya, ellentétben az Európai Unióban hatályos szabályozással⁴⁰².

A személyes adatok megsértése esetén fennálló értesítési kötelezettség azonban amerikai „találmány”, mely a bank- és hitelkártyára alapuló amerikai mindennapi életben különös

³⁹⁸ Alaska (article I, § 22), Arizona (article II, § 8), California (article I, § 1), Florida (article I, § 23), Hawaii (article I, § 6), Illinois (article I, § 12), Los Angeles (article I, § 12), Montana (article II, § 10), South Carolina (article I, § 10), Washington (article I, § 27).

³⁹⁹ A Federal Trade Commission (FTC) általánosságban a fogyasztókat megtévesztő és versenyjogi szabályokat megszegők ellen jár el (fogyasztóvédelmi és versenyhivatalként lehetne elsősorban meghatározni tevékenysége alapján).

⁴⁰⁰ A Health Insurance Portability and Accountability Act (egészségbiztosítás hordozhatóságával és hozzáféréssel kapcsolatos törvény) hatálya alá tartozó személyeknek és vállalatoknak adatvédelmi biztosítékokat és kötelezettségeket ír elő (pl.: orvosoknak, gyógyszerészeknek, patikáknak, egészségbiztosítóknak és kórházaknak adatvédelmi felelős)

⁴⁰¹ Egyesült Államok Alkotmánya, 1. cikk 8. § A Kongresszus hatáskörrel bír... az idegen nemzetekkel folytatott; az egyes tagállamok közötti és az indián törzsekkel folytatott kereskedelem szabályozására;

⁴⁰² Huw Beverly-Smith – Ansgar Ohly – Agnès Lucas-Schoetter: Privacy, Property and Personality, Cambridge University Press, Cambridge, 2005, 47-93.

jelentőséggel bír. Tipikusan a kártya adatok és TB szám lopása esetén írnak elő azonnali intézkedési kötelezettségeket a szövetségi és tagállami jogszabályok⁴⁰³.

Az online privacy védelem is elég megengedő az Egyesült Államokban: cookie-k és más online aktivitást figyelő technológiák nincsenek egységesen és szigorúan szabályozva. A weblapok üzemeltetőire viszont a csoportos perek (class action lawsuit) jelenthetnek komoly kockázatot, mivel jelentős kártérítést ítélnének meg az amerikai bíróságok. Az iparági önszabályozás és kódexek követése az adatvédelem elsődleges módja az USA-ban, melynek hatékonysága komolyan megkérdőjelezhető. Ilyen megoldásra példa a Digitális Reklámozás Szövetség kódexe⁴⁰⁴ („Digital Advertising Alliance code of conduct”), mely az online reklámozással kapcsolatban ír elő kötelezettségeket és követendő magatartásokat (pl. egy ikon jelzése, mellyel egyszerűen kikapcsolható az online viselkedés követés).

Az Egyesült Államokban a feleknek a bírósági eljárások során több joguk van a tekintetben, hogy saját maguk „fedezzenek fel”, kutassanak bizonyíték után, amelyet a bíróság segítségével bekérhetnek, hogy bizonyítékként kerüljenek felhasználásra⁴⁰⁵.

Az említett jog azonban könnyen konfliktusba kerülhet az EU adatvédelmi jogával. Texas Legfelsőbb Bírósága állapította meg egy ügy során, hogy a Volkswagen vállalat Németországban lévő dokumentumaiba nem lehet betekinteni, azokat felhasználni a bírósági eljárás során⁴⁰⁶.

Fontos megemlíteni továbbá, hogy az Egyesült Államok Legfelsőbb Bírósága több esetben döntött úgy⁴⁰⁷, hogy az érintett lemond a személyes adatai védelméről, amennyiben azokat harmadik félnek szolgáltatta ki, amelyet többen harmadik fél doktrínának⁴⁰⁸ (“third-party doctrine”) neveztek el⁴⁰⁹.

⁴⁰³ DLA Piper: Data Protection Laws of the World, 2013, 359.

⁴⁰⁴ Digital Advertising Alliance, <http://digitaladvertisingalliance.org/content.aspx?page=media&id=Media3>

⁴⁰⁵ Daniel J. Solove, Paul M. Schwartz - Privacy Law Fundamentals, 2015. 278.

⁴⁰⁶ VOLKSWAGEN v. VALDEZ, 909 S.W.2d 900 (Tex. 1995)

⁴⁰⁷ Couch v. United States, 409 U.S. 322 (1973), United States vs. Miller, 425 U.S. 435 (1976)

⁴⁰⁸ Edward P. Sisk: Technical Difficulties: Protecting Privacy Rights in the Digital Age, Criminal and Civil Confinement Vol. 42. 2016. 107-108.

⁴⁰⁹ Daniel J. Solove, Paul M. Schwartz - Privacy Law Fundamentals, 2015. 89.

6.1 Személyes adatok továbbítása harmadik államokba az Európai Unióból

Az EU adatvédelmi jogszabályai a legerősebbek és leghatékonyabbak a világon, melyek a személyes adatok védelme - és a jogszabály megkerülésének megakadályozása - céljából nem engedélyezik személyes adatok küldését olyan harmadik országba, mely nem biztosít megfelelő védelmi szintet.⁴¹⁰ A megfelelő védelem megállapításához vizsgálni kell az adott ország jogrendszerét, joggyakorlatát, és a konkrét adatkezelést. Általános „recept” nem létezik a megfelelő védelem megállapításához, azonban az átfogó jogi szabályozás (az adatkezelések általánosságban és törvényi szinten történő szabályozása), és olyan jogintézmények megléte, mint az adatkezeléseket vizsgáló személy vagy hatóság, továbbá a megfelelő jogorvoslati rendszer, és az adatkezelést megsértő adatkezelők elleni szankciók, elvárásként támaszthatóak. Az Egyesült Államok a fentebb írt elemzés alapján nem rendelkezik az megfelelő védelmi szint megállapításához szükséges jogintézményekkel⁴¹¹: a szektorális szabályozás és az általános adatvédelmi felelős hiánya miatt nem éri el az Európai Unió által támasztott védelmi szintet⁴¹². Magában az a tény, hogy egy ország nem éri el az EU által támasztott követelményeket adatvédelem területén, még nem lenne különleges, mivel ennek a mércének kevés ország felel meg⁴¹³, viszont az USA abban a különleges helyzetben van, hogy - a világpolitikai súlyán túl – a legnagyobb internetes és technikai vállalatok a területén vannak, melyek szolgáltatásait az európaiak is rendszeresen használják (Google, Facebook, Microsoft), és ezen szolgáltatások a személyes adatok megadása és azok felhasználása (az üzleti modelljük miatt is) nélkül nem működnek.

⁴¹⁰ Adatvédelmi irányelv 25. cikk (1) A tagállamoknak rendelkezniük kell arról, hogy a feldolgozásra kerülő vagy továbbítás után feldolgozásra szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha – az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül – az adott harmadik ország megfelelő védelmi szintet tud biztosítani.

⁴¹¹ EU adatvédelmi irányelv 25. cikk (2) A harmadik ország által nyújtott védelem szintjének megfelelő mivoltát az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni; különös figyelmet kell fordítani az adatok jellegére, a tervezett adatfeldolgozási művelet vagy műveletek céljára és időtartamára, a kiindulási és a célországra, az adott harmadik országban hatályos, általános és ágazati jogrendre, valamint az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre.

(6) A Bizottság a 31. cikk (2) bekezdésében említett eljárásnak megfelelően megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít e cikk (2) bekezdése értelmében, az egyének magánéletének, jogainak és szabadságainak védelmére vonatkozó belföldi jog, vagy a vállalt nemzetközi kötelezettségek, különösen az (5) bekezdésben említett tárgyalások végeredménye alapján.

⁴¹² Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 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 Adopted by the Working Party on 1999. 01. 26. 2.

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp15en.pdf>

⁴¹³ A megfelelő védelmi szintet biztosító országok (2015. 01. 20.): Andorra, Argentína, Kanada, Svájc, Feröer, Guernsey, Izrael, Isle of Man, Jersey, Új-Zéland, Egyesült Államok (Safe Harbour), Uruguay

A probléma megoldására hozta létre az EU és az USA a Safe Harbor (Biztonságos Adatkikötő) programot, melyhez az Egyesült Államokbeli adatkezelők csatlakozhattak, garantálva a biztonságos adatkezelést, amelyet a Privacy Shield váltott fel. Az utazások esetén az EU és az USA között az utasok személyes adatainak küldése biztonsági okokból⁴¹⁴ szintén kötelessége az érdekelt feleknek.

Több jogtudós az EU adatvédelmi jogának „expanziójáról” beszél, mivel a globális piacon jelenlévő vállalatok nem tudják megkerülni az EU szabályozását: beszállítói, vásárlói, munkavállalói, partnerei között uniós székhellyel vagy lakóhellyel rendelkező fél biztosan van, akik felé, vagy akiktől személyes adatok áramolnak. Az adatküldés jogi alapjához az sem elegendő, ha a két fél azonos tulajdonban van, vagy anya-leányvállalat kapcsolatban.

Az adatok harmadik, megfelelő védelmi szintet nem biztosító országba való elküldésére ugyanakkor több kivétel áll rendelkezésre a szabály alól⁴¹⁵ (pl.: érintett kifejezett hozzájárulása, létfontosságú érdekeinek védelme, közérdek), mely lehetőséget biztosít az adatkezelők számára a probléma áthidalására. A kivételek létrehozása a nemzetközi adatáramlások miatt szükséges, mivel az információs társadalomban a gazdaság egyik alappillére a nemzetközi kereskedelem és az információcsere. A kivételek alkalmazása azonban a mindennapi életben „általánossá” vált. A Munkacsoport is állásfoglalásában felhívta a figyelmet az irányelv védelme, és a kivételek széles köre közötti kapcsolatra⁴¹⁶.

⁴¹⁴ Az USA törvényei megkövetelik a légitársaságoktól, amelyek az Amerikai Egyesült Államokba, onnan, vagy azon keresztül szállítanak, hogy az Amerikai Egyesült Államok Belbiztonsági Minisztériumának (DHS) szolgáltatassanak az utasokkal kapcsolatos bizonyos adatokat, a biztonságos utazás megkönnyítése és az Egyesült Államok biztonságának biztosítása érdekében.

Agreement between the European Community. and the U.S. on the processing and transfer of PNR data by air carriers to the U.S. Dep't of Homeland Sec., Bureau of Customs and Border Prot. Council Directive 2004 O.J. (L 183) 94 (EC).

⁴¹⁵ EU adatvédelmi irányelv 26. cikk (1) A 25. cikktől eltérően, és amennyiben az adott esetre vonatkozó belföldi jogszabályok másképp nem rendelkeznek, a tagállamok rendelkeznek arról, hogy a személyes adatok olyan harmadik országba irányuló továbbítása vagy továbbítás-sorozata, amely a 25. cikk (2) bekezdése értelmében nem biztosít megfelelő szintű védelmet, csak a következő feltételek mellett történhet:

- a) az érintett egyértelműen hozzájárulását adta a tervezett továbbításhoz; vagy
- b) a továbbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges; vagy
- c) a továbbítás az adatkezelő és valamely harmadik fél közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges; vagy
- d) a továbbítás fontos közérdekből vagy jogi követelések létrejötté, érvényesítése vagy védelme miatt szükséges, illetve azt jogszabály írja elő; vagy
- e) a továbbítás az érintett létfontosságú érdekeinek védelme miatt szükséges; vagy
- f) a továbbítást olyan nyilvántartásból végzik, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll, amennyiben a jogszabályok által a betekintésre megállapított feltételek az adott esetben teljesülnek.

⁴¹⁶ Az 1995. október 24-i 95/46/EK irányelv 26. cikke (1) bekezdésének közös értelmezéséről szóló munkadokumentum, 2005. 11. 25.

„A szigorúan megfogalmazott mentességek elsősorban olyan esetekre vonatkoznak, amelyekben az érintettet kevés kockázat éri vagy amelyekben egyéb érdekek (közérdekek vagy az érintett érdekei) felülírják az érintett

Értelmezésre szorul az irányelv „az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül” rendelkezése, mely tulajdonképpen az érintett magánszférájának a védelmét növeli. Bár a szöveg az „irányelv értelmében” elfogadott nemzeti rendelkezésekre szűkíti az adattovábbítás korlátját, tulajdonképpen bármilyen adatvédelmi tárgyú jogszabályra ezt könnyen rá lehet húzni. Így például egy internetes kereskedelmet szabályozó, vagy online adatmegadást korlátozó jogszabályra is érvényes lehet, mely további követelményeket támaszthat a személyes adatok harmadik országba való továbbításával, vagy annak az adattovábbítás előtti személyes adatok felvételével és kezelésével kapcsolatban. Az idézett rendelkezés így a védelem szintjének növelése felé való eltérést engedélyezi.

A Munkacsoport állásfoglalásában kiemeli, hogy az érintettnek a kivételek alkalmazása esetén is joga van kifogással élni az adatkezelés ellen, abban az esetben is, ha nem különleges adatról van szó, mivel az érintettek szempontjából egyéb adatok is lehetnek érzékenyek (pl. olyan pénzügyi adatok, melyek vállalkozására negatív hatással lehetnek).

Fontos kiemelni, hogy a kivételek alkalmazása sem jelent felmentést az adatkezelő kötelezettségei alól, így például a tisztességes adatkezelés elve alapján az adatkezelő akkor is tájékoztatni köteles az érintettet a továbbításról, amennyiben annak továbbítására akár jogszabály támaszt kivételt, akár megfelelő védelmi szintet biztosító országba történik.

6.1.1 Az érintett hozzájárulása

Az érintett hozzájárulásának önkéntesnek, kifejezettnek és megfelelő tájékoztatáson alapulónak kell lennie.⁴¹⁷

A „kifejezett” alatt egy pozitív magatartást értünk, nem pedig hallgatólagos beleegyezést: amennyiben az érintett tudott is a továbbításról, de nem tiltakozott, az nem tekinthető hozzájárulásnak. Ha egy internetes oldal e-maileket küld a felhasználóinak, melyben tájékoztatja őket, hogy az adataikat továbbküldi harmadik félnek egy külföldi országba és biztosítja az opt out lehetőségét, ebben az esetben nem beszélhetünk kifejezett hozzájárulásról.

magánélethez való jogát. Mivel egy általános elv alól jelentenek mentességet, szigorúan kell kezelni őket. Ezenkívül a tagállamok a nemzeti jogban úgy rendelkezhetnek, hogy a mentességek bizonyos esetekben nem alkalmazandók. Ez történhet például azokban az esetekben, amikor különösen sérülékeny csoportokat – dolgozókat vagy betegeket – kell megvédeni.”

⁴¹⁷ Adatvédelmi irányelv 2. cikk h) "az érintett hozzájárulása" az érintett kívánságának önkéntes, kifejezett és tájékozott kinyilvánítása, amellyel beleegyezését adja az őt érintő személyes adatok feldolgozásához.

Egyértelműen kifejezett magatartás alatt azt értjük, ha az érintett egy aktív cselekedetet hajt végre avval a szándékkal, hogy a személyes adatainak harmadik országba irányuló továbbítását támogassa, jóváhagyja.

Kérdésként merül fel, hogy az internetes oldalakon egy rubrika kipipálása, vagy egy előre kipipált rubrika jóváhagyása megfelelő hozzájárulásnak tekinthető-e. A Munkacsoport állásfoglalásban megfelelőnek minősítette a rubrika felhasználó általi kipipálásával létrejött hozzájárulást. Abban az esetben viszont, ha a rubrika előre ki van pipálva, nem beszélhetünk kifejezett hozzájárulásról, csupán hallgatólagos beleegyezésről, vagy arról sem, mivel lehet, hogy a felhasználó észre sem vette a rubrikát.⁴¹⁸ Az EU adatvédelmi rendeletének tervezete a hozzájárulás fogalmában külön kitér az interneten alkalmazott eljárásra, melyet „megerősítést félreérthetetlenül kifejező cselekedetként” említ.⁴¹⁹

A Munkacsoport állásfoglalásában ide sorolta azt az esetkört, mely során a légitársaságok szolgáltatásainak igénybevételéhez hozzájárulást kértek az utasoktól, hogy adataikat harmadik államokba továbbítsák (kiemelve az USA hatóságait), a beléptetéshez és biztonsági intézkedések ellátásához. A Munkacsoport szerint ebben az esetben az utasok a hozzájárulás megadásának kényszere alatt állnak, mivel ha repülni szeretnének, nincsen más választásuk⁴²⁰. Véleményem szerint szerencsésebb megoldás lenne az utasok adatainak küldését a szerződés teljesítéséhez szükséges kivétel alá sorolni, mivel valódi hozzájárulásról ebben az esetben az állásfoglalással egyetértve nem beszélhetünk, viszont egy (külföldi) utazással kapcsolatos szerződésnél a teljesítés alapvető kritériuma, hogy azt harmadik országba küldje tovább az adatkezelő. Egy utazási iroda is továbbküldi a hotelnek, sí tábor esetén a sípályának a neveket a szállás és a csoportos névre szóló sítérlet megvásárlásához. A Munkacsoport által említett esetben az USA hatóságairól van szó, nem privát szervezetekről, azonban bármely országba történő beutazás esetén jogosultak a határrendészeti (és utána a belső rendvédelmi szervek is) igazoltatni, így véleményem szerint nem éri kivételes helyzetből eredendő hátrány az érintett utasokat. Véleményem szerint az USA hatóságai részére történő továbbításban nincsen semmi meglepetés, hiszen a vízumköteles országokba mindig is szükséges volt először a nagykövetségeknél a vízum igénylése, amely során az alapvető személyes adatokon túl

⁴¹⁸ A Munkacsoport 5/2004 véleménye a nem kívánt, közvetlen üzletszerzésre irányuló tájékoztatásról a 2005/58/EK irányelv 13. cikkéről, WP 90, 2004. 02. 27.

⁴¹⁹ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, 4. cikk 11. „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

⁴²⁰ Az 1995. október 24-i 95/46/EK irányelv 26. cikke (1) bekezdésének közös értelmezéséről szóló munkadokumentum, 2005. november 25.

különleges adatokat is (pl. betegség, büntetett előélet, drogfogyasztás) meg kellett adniuk az érintetteknek, amely nem volt opcionális, ha utazni akartak (még ha az USA jelenleg nem is vízumköteles magyar állampolgárok számára).

A legfőbb hiba az utasok adatainak küldésénél az volt, hogy közérdekre hivatkozva továbbították, ebben az esetben viszont csak az USA közérdeke állt fenn. A közérdekre hivatkozás ebben az esetben azért volt nehezen alkalmazható, mert bármely fogadó ország képes közérdeket „kreálni”, így az EU adatvédelmi szabályozása könnyen kijátszhatóvá válna.⁴²¹ A szeptember 11-én elkövetett terrortámadások azonban komoly változást hoztak: olyan biztonsági intézkedésekre is alappal lehet hivatkozni, amelyek a terrorveszély előtt elfogadhatatlanok lettek volna. A közérdekre való hivatkozást leszűkíti az irányelv, amelyre csak kevés kivételt említ, mint például az adó- és vámügyi együttműködés⁴²².

Az önkéntesség esetén fontos kiemelni, hogy az érintettnek lehetősége legyen, ne pedig kényszerhelyzet, különösen lehetséges hátrányok nélkül.

A munkajog területén el kell határolni a munkaviszonyt megelőző, és a munkaviszony alatt történő adatkezelés jogalapjára vonatkozó kérdéseket. A munkaviszonyt megelőző adatkezelés során az érintett önkéntessége a szakirodalom által általában nem vitatott⁴²³, viszont annak megkezdésével már kérdéses. Egy munkavállalónak, ha a munkáltatója kéri a hozzájárulását személyes adatainak továbbításához, valójában nem beszélhetünk független szabad akaratról, hiszen a karrierje, fizetése, vagy akár a munkája múlhat a felettesével való viszonyán. Egy hierarchikus viszonyban így nem beszélhetünk tisztán önkéntes hozzájárulásról. Ugyanakkor a Munkacsoport egy állásfoglalásában kiemeli, hogy bizonyos helyzetekben a munkavállaló érdeke is lehet a személyes adatok továbbítása (pl. karrier biztosítása harmadik országban nemzetközi cégek esetében)⁴²⁴.

A Munkacsoport ajánlásában a multinacionális vállalatoknak címzetten kiemeli, hogy lehetőség szerint egy jogi keretben belül (pl. kötelező érvényű vállalati szabályok) valósítsák meg a személyes adatok tömeges és rendszeres továbbítását, míg az érintett hozzájárulását abban az esetben alkalmazzák, ha az egységes – és az érintett jogait hatékonyabban védő – jogi keret

⁴²¹ Article 29 Working Party: Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, 2002. 10. 24, 6.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp66_en.pdf

⁴²² Adatvédelmi irányelv preambulum (58) mivel bizonyos körülmények között, amikor az érintett ehhez hozzájárult, vagy a továbbítás valamely szerződés vagy jogi követelés kapcsán szükséges, vagy valamely fontos közérdek védelme ezt megkívánja, például adó- vagy vámigazgatási szervek, vagy a társadalombiztosítási ügyekben illetékes hivatalok közötti nemzetközi adattovábbítások esetében.

⁴²³ Balogh Zsolt György - Polyák Gábor - Rátai Balázs - Szőke Gergely László: Munkahelyi adatvédelem a gyakorlatban, Infokommunikáció és jog, 2012. (9. évf.) 50. sz. 97.

⁴²⁴ A Munkacsoport 8/2001 véleménye a személyes adatok feldolgozásáról a foglalkoztatás kontextusában és összefoglalás, 2001. 09. 13.

nem vehető igénybe, vagy aránytalan erőfeszítéssel járna. Abban az esetben is lehetséges az érintett hozzájárulásának elsődleges alkalmazása, amennyiben a küldés az érintett számára kevés kockázatot jelent.

Legjellemzőbb példa a pénzutalás, mely tömeges és mindennapos, melyhez az érintett hozzájárulása elegendő.

A megfelelő tájékoztatás alapvető feltétele az érvényes hozzájárulásnak, így az érintettnek tudnia kell, hogy az adott esetben a hozzájárulása nélkül nem valósulhatna meg az adattovábbítás. Minden fajta adatkezelésnél a hozzájárulás esetén fontos, hogy az érintett megfelelően legyen tájékoztatva, azonban a harmadik országba irányuló adattovábbítás esetén ez különösen lényeges, mivel a külföldi országokban az adatok sorsa nehezen követhetővé (vagy követhetlenné) válik az érintett számára, a jogérvényesítés pedig nehézkes és költséges lenne számára.

A tájékoztatásnak részletesnek és közérthetőnek kell lennie: az érintettnek tisztában kell lennie avval, hogy hozzájárulást adott-e, mely műveletekhez és pontosan milyen mértékben, továbbá a visszavonás és jogorvoslat lehetőségéről⁴²⁵. A tájékoztatásnak ki kell terjednie arra, hogy az adattovábbítás mely országba történik, az adott ország megfelelő védelmet biztosít-e,

A gazdasági élet azonban hozhat olyan helyzeteket, amikor az érintett nem tud előzetesen hozzájárulni az adatai kezeléséhez (pl. vállalatot eladják egy új tulajdonosnak minden anyagi és szellemi javaival együtt, mely magában foglalja az ügyfelek személyes adatait).

6.1.2 A személyes adatok továbbítását jogszabály vagy tagállami hatóság engedélyezi

⁴²⁵ Adatvédelmi irányelv 10. cikk Tájékoztatás az érintettől való adatgyűjtés esetében

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelőnek vagy képviselőjének legalább az alábbiakról tájékoztatnia kell az érintettet, akitől a rá vonatkozó adatokat gyűjtik, kivéve ha az érintett már rendelkezik ezen információkkal:

- a) az adatkezelő, vagy ha van ilyen, képviselőjének személye;
- b) az adatfeldolgozás célja, amelyre az adatokat szánják;
- c) minden olyan további adat, mint például:
 - az adatok címzettjei, illetve a címzettek kategóriái,
 - hogy a kérdések megválaszolása kötelező vagy önkéntes, továbbá a válaszadás elmulasztásának lehetséges következményei,
 - betekintési jog és az érintettre vonatkozó adatok helyesbítéséhez való jog,

amennyiben e további információk, tekintettel az adatgyűjtés sajátos körülményeire, az érintett vonatkozásában a tisztességes adatfeldolgozás biztosításához szükségesek.

Ritka esetkörnek számít, amikor uniós vagy tagállami jogszabály a személyes adatok küldését kifejezetten előírja, vagy arra konkrét engedélyt ad. Gyakoribb eset, amikor valamilyen nemzetközi kötelezettség teljesítéséhez az automatikusan hozzákapszódik (pl. kereskedelmi megállapodás az országok között, mely az érintett felek alvállalkozóinak adatküldését is magában foglalja).

Problémát jelenthet, hogy több jogszabályt akkor hoztak létre, amikor még nem volt például e-mail, vagy nem volt mindennapos jelenség az internetes adatgyűjtés és küldés, így sok esetben a jogalkalmazóra hárul a felelősség a küldés engedélyezésére, mely a megfelelő gyakorlat kialakulásáig jogbizonytalansághoz vezethet⁴²⁶.

A 108. egyezményhez csatolt jegyzőkönyvben kiemelésre kerül, hogy a feleknek (tagállami adatvédelmi hatóságoknak) diszkréciós jogkörébe tartozik kivételek megállapítása a harmadik országokban való adatküldés alól. A jegyzőkönyv kiemeli azonban uniós jog egyik alapelvét is, mely alapján a kivételeket valóban kivételként kell kezelni és csak a szükséges helyzetben élni velük, nehogy a kivétel általános szabállyá váljon.⁴²⁷ A kivételeknek olyan fontos közérdeket vagy méltányolható magánérdeket kell szolgálniuk, mely az egyén magánszférához való jogával mérlegelésre került.

6.1.3 Szerződés megkötéséhez vagy teljesítéséhez szükséges

Ebben az esetkörben az érintett által megkötni kívánt, vagy megkötött szerződés nem jöhet létre, vagy nem teljesíthető a személyes adatok harmadik országba való küldése nélkül.

A 20. század végén lebontott – fizikai és jogi - korlátoknak köszönhetően a szolgáltatások és a személyek szabad áramlása globális szinten megváltozott: még ha a munkavállalás és letelepedés más kontinensen nem is akadálymentes, a turizmus és a kereskedelem szinte korlátok nélkül működik (kevés kivétellel, mint például Észak-Korea), melyhez szükséges a személyes adatok továbbítása is.

Leggyakoribb példa az utazások esetében a hotel és a légitársaságok számára az utasok adatainak rendelkezésre bocsátása. Az utazási irodával kötött szerződés teljesítéséhez szükséges a személyes adatok továbbítása, hogy az utasok igénybe tudják venni az adott

⁴²⁶ Daniel J. Solove: *Nothing to Hide, The False tradeoff between Privacy and Security*, Yale University Press, New Haven & London, 2011, 164.

⁴²⁷ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows 2. (2) a)

szolgáltatásokat. Bár ehhez kapcsolódik, de külön megállapodás részét képezi az EU és az USA között az utasok személyes adatainak küldése biztonsági okokból.

A multinacionális vállalatok költségmegtakarítás és az átláthatóbb, hatékonyabb vezetés érdekében lehetőség szerint központilag szeretnék kezelni a könyvelést, és a dolgozók szervezését.

Abban az esetben, ha például egy multinacionális vállalatban belül a munkavállalók adatai a fizetés, szabadságolás, prémium kifizetéséhez, adózáshoz vagy a nemzetközi munka megszervezéséhez szükségesek, a kivétel alkalmazható.

Nem ennyire egyértelmű a helyzet, amennyiben a vállalatban belül emberi erőforrás szervezésére használják fel az adatokat (pl.: belső statisztikák, ütemtervek elkészítése, dolgozók képzettségéről felmérés, céges továbbképzés), ha egy anyavállalathoz szeretnék azokat továbbítani.

Árnyalhatja a helyzetet, hogy az adott leányvállalat, vagy a multinacionális vállalat adott országbeli szervezete (pl. képviselet, fióktelep) rendelkezik-e saját munkaügyi osztállyal, bérszámfejtéssel: amennyiben rendelkezik, kisebb szükséglet mutatkozik a személyes adatok továbbküldésére határon kívülre, így a továbbítás nehezebben támasztható alá az említett joggalappal.

Garanciális ügyintézéseknél egyértelműen az érintett érdekét szolgálja a személyes adatok továbbítása, mely a szerződés megfelelő teljesítéséhez szükséges. Egy USA-ban megvásárolt laptop európai garanciális ügyintézéséhez elengedhetetlen, hogy a vásárlók adatbázisa egységesen, nemzetközi szinten legyen kezelve.

Amennyiben az adatküldést nem lehet igazolni a szerződés teljesítésének szükségességével még a dolgozók adatainál sem, szükséges más jogalapot, vagy megoldást keresnie az adatkezelőnek.

Az érintett hozzájárulása nem jöhet szóba, hiszen a munkáltató és munkavállaló között hierarchikus viszony van, így az érintett hozzájárulásánál leírt feltételeknek (önkéntes, saját akaratból) nem felelne meg.

6.1.4 Közérdek, jogi követelések létrejötte, érvényesítése vagy védelme

Az utasok adatainak USA-ba való továbbításánál leírtakat kiegészítve különösen fontos, hogy a közérdek a küldő országnál álljon fenn.

A jogi követelések esetén is fontos a szükségesség feltétele. Ha például a Google leányvállalata vagy képviselte ellen jogi útra terelnek egy vitát Spanyolországban, az anyavállalatnál lévő központi jogi osztálynak és a vezetőségnek tudnia kell az ügy részleteiről, hogy megfelelően védekezhessenek a peres eljárás során, vagy meghozzanak egy egyezséghez szükséges döntést. Egy olyan horderejű ügy során, mint a Google Spain, a szükségesség igazolható. Kis horderejű ügyeknél, mint például egy garanciális problémával kapcsolatos kis értékű per (pl. Google Nexus okostelefon meghibásodása), véleményem szerint nem feltétlen szükséges a személyes adatok küldése, amennyiben a leányvállalat le tudja bonyolítani az eljárást, és nincs kihatással a cégcsoport működésére.

A Munkacsoport is kiemeli a szükségességgel kapcsolatban, hogy ez egy adott konkrét helyzetben értelmezendő, és ellenpéldaként olyan extrém esetet hoz fel, mely során minden alkalmazott személyes adatait továbbküldték az anyavállalatnak, a lehetséges jövőbeni peres ügyek miatt.

6.1.5 Nyilvántartásból történő továbbítás

A kivétel olyan nyilvántartásból való személyes adattovábbítást jelöl meg, mely az adott országban bárki, vagy bármely olyan személy számára elérhető, aki a jogos érdekét igazolni tudja. Ezt a kivételt is csak nagyon szűken lehet értelmezni: egy adott ország nyilvántartásába általában az állampolgárok és az ott tartózkodó, arra jogosult külföldiek tekinthetnek be. A beutazásnak egy uniós országba feltételei vannak (ha nem az EU területéről utazik be a személy), tehát egy szűrőn átesik, mielőtt az ország területére lépne és a betekintési jogával élhetne. Az adatok továbbküldése így még teljesen nyilvános nyilvántartásból sem igazolható véleményem szerint harmadik országokba általánosságban⁴²⁸.

Egyes nyilvántartások esetében azonban igazolható a „globális” nyilvánosság, és harmadik állambeli természetes és jogi személyek érdeke a nyilvántartásba való betekintésre, így például a cégnyilvántartásba a nemzetközi üzleti élet tisztasága érdekében bárki betekinthez.

⁴²⁸ Adatvédelmi irányelv preambulum (58) ... vagy amikor a továbbítás jogszabály által létrehozott olyan nyilvántartásból történik, amelyhez a nyilvánosság, vagy a jogos érdekekkel rendelkező személyek hozzáférhetnek, rendelkezni kell a fenti tilalom alóli mentességről; mivel ebben az esetben a továbbítás nem terjed ki a nyilvántartásban szereplő összes adatra, illetve összes adatkategóriára, és amennyiben a nyilvántartást az olyan személyek által való hozzáférésre szánták, akiknek ehhez jogos érdeke fűződik, a továbbítást csak e személyek kérelmére lehet elvégezni, vagy akkor, ha a címzettek a szóban forgó személyek;

Bár a Munkacsoport állásfoglalásában kiemeli, hogy a teljes nyilvántartás nem továbbítható, véleményem szerint ez azért sem releváns kérdés, mert még az állampolgárok személyesen sem kaphatják meg a teljes adatbázist, és csak meghatározott szűkítő feltételekkel kereshetnek benne. A cégnyilvántartásban is csak egy adott cégre lehet rákeresni, és annak adatait megtekinteni, míg bizonyos személyek üzleti érdekeltségeire nem lehetséges (pl. egy személy nevére rákeresve nem lehet megtudni a tulajdonában álló cégeket).

6.1.6 Kötelező erejű vállalati szabályok

A kötelező erejű vállalati szabályokat (Binding Corporate Rules, „BCR”) jellemzően a nemzetközi vállalatok alakítják ki és alkalmazzák a különböző országokban elhelyezkedő (EU-n kívül is) egységei közötti adatcsere szabályozására.

A BCR meghatározza a cég szervezetét és működését a személyes adatok nemzetközi továbbítása tekintetében egyazon cégcsoporton belül, ahol a különböző országokban székelő szervezeti egységek vonatkozásában az országok nem biztosítanak – az európai mércék szerinti - megfelelő szintű védelmet.

Ezek alapján különösen hasznos az olyan vállalatcsoportok számára, amelyek különböző jogrendszerben működnek, és működésük során a személyes adatok továbbítása mindennapos gyakorlat. A BCR nem szolgáltat alapot ahhoz, a továbbítás csoporton kívülre történjék.

A BCR-eknek tartalmazniuk kell, hogy az érintett személyes adatait külföldre továbbítják, panaszt tehet a nemzeti adatvédelmi hatóságnál és igényét a bíróságon is érvényesítheti, ha személyes adatainak kezelésével kapcsolatban jogsérelem érte. A szabályoknak biztosítaniuk kell, hogy az érintett legalább ugyanolyan jogokkal rendelkezzen a jogsértő adatkezelést végző vállalattal szemben, mint amit az EU adatvédelmi irányelve vagy a nemzeti jog biztosít. Ha a nemzeti jog szigorúbb adatvédelmi szabályokkal rendelkezik, akkor azt kell alkalmazni⁴²⁹. A BCR-nek tartalmaznia kell azt a fontos kötelezettségvállalást is, hogy a cégcsoport EU-n kívüli tagjainak cselekményeiért vagy a vállalat EU-ban található székhelyű központja vagy a cégcsoport egy európai tagja átvállalja a felelősséget és szükség esetén kártérítést fizet. A BCR betartását belső és külső audittal is ellenőriztetnie kell a vállalatnak. A cégcsoportnak együttesen és tagjainak külön is kötelezettséget kell vállalniuk, hogy az illetékes adatvédelmi hatóságokkal együttműködnek és ezen hatóságoknak a BCR értelmezésével és alkalmazásával kapcsolatos javaslatait alkalmazzák⁴³⁰.

A kötelező erejű vállalati szabályok jóváhagyása iránti kérelmezés és elbírálás során nemzeti adatvédelmi hatóság jár el, amely megvizsgálja, hogy a dokumentum megfelel-e a

⁴²⁹ Article 29 Data Protection Working Party: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 11639/02/EN WP 74 , 2003. 06. 03.

⁴³⁰ Article 29 Data Protection Working Party: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From “Binding Corporate Rules” 05/EN WP107, 2005. 04. 16.

Munkacsoport által felállított körülményeknek. A vizsgálati eljárásban egy vezető hatóság vesz részt, amely alapján nem szükséges minden egyes tagállamban külön-külön kérvényezni⁴³¹.

Az adatvédelmi rendelet rendelkezik az elbírás és panasz menetéről, amely alapján a fő hatóságként eljáró felügyeleti hatóság a döntéshozatali folyamat során koordinál az érintett felügyeleti hatóságokkal. Az érintett által benyújtott panasz részben vagy egészben történő elutasítására vonatkozó döntések esetében a döntést az a felügyeleti hatóság hozza meg, amelyhez a panaszt benyújtották.

A NAIH három típusba sorolja az eljárása formáit attól függően, hogy milyen minőségben jár el: 1. vezető hatóságként történő jóváhagyási eljárás; 2. nem vezető hatóságként történő, jóváhagyási eljárásban való részvétel; 3. eljárás egy, már engedélyezett BCR esetén.

A magyar szabályozásban használt „kötelező szervezeti szabályozás” elnevezés nem tükrözi egyértelműen, hogy csak gazdasági tevékenységet folytató vállalkozások élhetnek ezzel a lehetőséggel, amelyet az adatvédelmi rendelet is tisztáz⁴³².

⁴³¹ Horváth-Egri Katalin: A kötelező szervezeti szabályok (Binding Corporate Rules, BCR) és az együttműködési eljárás lehetőségei, Infokommunikáció és Jog, 2015. 4. szám 144-146.

⁴³² Maksó Bianka: Kötelező szervezeti szabályozás – az Infotv. legújabb adatvédelmi eszközének bevezetéséről, Infokommunikáció és Jog, 2015. 4. szám 144-146.

6.1.7 Általános szerződési feltételek

A megfelelő garanciák nyújtásához az általános szerződési feltételeknek (standard contractual clauses) „kellően ellensúlyozniuk kell a megfelelő védelem általános szintjének hiányát azáltal, hogy bármely adott helyzetben pótolják a védelem alapvető fontosságú hiányzó elemeit”⁴³³.

Az ilyen eszközök nemzetközi adattovábbításokban történő felhasználásának megkönnyítése céljából a Bizottság – az irányelv 26. cikkének (4) bekezdésével összhangban – jóváhagyott négy különböző, az irányelv 26. cikkének (2) bekezdésében foglalt követelményeket teljesítőnek ítélt általános szerződési mintafeltétel-csoportot. A mintafeltételek két csoportja az adatkezelők közötti adattovábbításra⁴³⁴, a másik kettő pedig az adatkezelő és az utasítása szerint eljáró adatfeldolgozó közötti adattovábbításra vonatkozik. E mintafeltételek mindegyik csoportja megállapítja mind az adatátadó, mind az adatátvevő kötelezettségeit. Ezek kötelezettségeket foglalnak magukban többek között az alábbiakkal kapcsolatban: biztonsági intézkedések, az érintett tájékoztatása érzékeny adatok továbbítása esetén, az adatátadó értesítése a harmadik országok bűnüldöző hatóságai által kérelmezett hozzáférésről vagy bármilyen véletlen vagy jogosulatlan hozzáférésről, valamint az érintettek saját személyes adataikhoz való hozzáférésehez, személyes adataik helyesbítéséhez vagy törléséhez való joga, továbbá az általános szerződési feltételek bármelyik fél általi megsértése esetén az érintettek kártérítésére vonatkozó szabályok. A szerződési mintafeltételek azt is előírják, hogy az uniós adatalanyok az adatátadó letelepedési helye szerinti tagállam adatvédelmi hatósága és/vagy bírósága előtt hivatkozhatnak a szerződési feltételek alapján őket – mint kedvezményezett harmadik személyeket – megillető jogokra. A szerződési feltételekben azért van szükség e jogokra és kötelezettségekre, mivel – a megfelelőség Bizottság általi megállapításának eseteivel szemben, – nem tételezhető fel, hogy a harmadik országbeli adatátvevő megfelelő felügyeleti és az adatvédelmi szabályokat végrehajtó rendszer hatálya alatt áll⁴³⁵.

⁴³³ 29. cikk alapján létrehozott Munkacsoport: Személyes adatok továbbítása harmadik országokba: Az európai uniós adatvédelmi irányelv 25. és 26. cikkének alkalmazása, 1998. 07. 24.

⁴³⁴ A Bizottság 2001. június 15-i 2001/497/EK határozata a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről, HL L 181., 2001.7.4., 19. o., és A Bizottság 2004. december 27-i 2004/915/EK határozata a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről, HL L 385., 2004.12.29., 74. o.

⁴³⁵ A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a 95/46/EK irányelv alapján, az Európai Bíróság C-362/14. sz. (Schrems-)ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról

6.2 Privacy Shield

Az Európai Unió Bírósága határozatában⁴³⁶ kimondta az Európai Bizottság azon határozatának érvénytelenségét, amely a Safe Harbor (biztonságos kikötő) rendszere alapján lehetővé tette személyes adatok továbbítását az Amerikai Egyesült Államokba. A Bíróság ítélete kiemeli, hogy a tagállami adatvédelmi hatóságok nem foszthatók meg attól a lehetőségtől, hogy a külföldre irányuló adattovábbítások kapcsán vizsgálják, vajon a célország megfelelő védelmi szintet biztosít-e.

Az Európai Unió Bírósága a bizottsági határozat érvénytelenségét többek között arra alapozta, hogy az Egyesült Államok hatóságai hozzáférhettek az Unió tagállamaiból továbbított személyes adatokhoz, és azokat akár a továbbításuk eredeti céljával összeegyeztethetetlen módon is kezelhették. A Bíróság a nemzetbiztonsági célú felhasználások kapcsán is hiányolta a garanciákat, például azt, hogy az érintett személyeknek nem volt olyan jogorvoslati lehetősége, amely az érintett jogainak gyakorlását (hozzáférés, helyesbítés, törlés) biztosította volna⁴³⁷. A döntés tehát nem a cégek magatartása, hanem az amerikai jogi környezet⁴³⁸ és a nem-amerikai állampolgárok számára biztosított jogok hiánya indokolta.

Az Safe Harbor érvénytelensége utáni jogi űr betöltésére azonnal megkezdődtek a tárgyalások az USA és az EU között, amelynek eredményeként született meg a Privacy Shield tervezete 2016 februárjában, amelyet a 29-es Munkacsoport megvizsgált, és a 2016. áprilisában kiadott állásfoglalásában⁴³⁹ az előrelépések mellett elsősorban a hiányosságoknak adott hangot.

A tervezet által biztosított védelmi szint megközelítőleg sem érte el az EU-ban elvártakat, így például az adatmegőrzéssel, automatizált döntéshozattal és az adatkezelés céljának korlátozásával kapcsolatos rendelkezések hiányoztak a tervezetből. További probléma volt, hogy az amerikai és európai fogalomhasználat eltérő, amely értelmezési kérdéseket vetett fel, egyes pontokat vitathatóvá, és megkerülhetővé téve.

Komoly továbblépés volt a Safe Harborhoz képest, hogy az EU állampolgárok is rendelkeztek panasztételi joggal és jogorvoslati lehetőségekkel, azonban az eljárások túl komplikáltak voltak

⁴³⁶ C-362/14 Maximilian Schrems v Data Protection Commissioner, Court of Justice of the European Union, 2015. 10. 07.

⁴³⁷ A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye az Európai Unió Bíróságának a Safe Harbor ügyben hozott ítéletéről, Budapest, 2015. október 6.

⁴³⁸ Az USA kormánya a PATRIOT Act értelmében bármikor kötelezhette a vállalatokat arra korlátozás nélkül, hogy kiadják az európai állampolgárok adatait, az érintett értesítése nélkül.

⁴³⁹ Article 29 Data Protection Working Party: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 16/EN WP 238, 2016. április 13.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

és nem biztosították a panaszos anyanyelvének használatát. A tagállami adatvédelmi hatóságok bevonását ajánlotta a Munkacsoport.

Az adatok továbbküldése az USA területéről harmadik államba szintén további szabályozásra szorult, amely magában kell, hogy foglalja a harmadik országban biztosított védelem vizsgálatát, a nemzetbiztonsági szervek adatigényléseit is figyelembe véve.

Az USA ügynökségeinek és hatóságainak az adatokhoz való hozzáférése⁴⁴⁰ is a megoldandó kérdések listáján maradt: bár szerepeltek biztosítékok és ígéret a tömeges és korlátozás nélküli adatkezelések elkerülésével kapcsolatosan, azok nem bizonyultak elég erősnek.

Az adatkezelések felügyeletét ellátó Ombudsman személye továbblépés, azonban a függetlensége kérdéses volt⁴⁴¹.

A Bizottság 2016. július 12-én elfogadta a Privacy Shield végleges verzióját⁴⁴², amelyben a javítások ellenére maradtak hiányosságok: többek között az automatikus döntéshozatallal kapcsolatos rendelkezések, az érintett tiltakozási joga, a Privacy Shield alkalmazhatósága az adatfeldolgozók esetében szabályozásra, illetve pontosításra szorulna⁴⁴³. Kifogásolta továbbá a 29-es Munkacsoport az Ombudsman függetlenségével és hatáskörével kapcsolatos rendelkezéseket, a tömeges és nem célzott adatgyűjtések elleni hatékonyabb biztosítékok hiányát.

A Privacy Shield az európai adatvédelmi jog alapelveit (pl. célhoz kötöttség, betekintéshez, helyesbítéshez való jog) törekszik érvényesíteni, amelynek legjelentősebb eredményei között említhetjük a programban résztvevő vállalatok komolyabb ellenőrzését és a megfelelő szankciókat.

Az érintettnek joga van információt kérni az adatkezelőtől arra vonatkozólag, hogy kezelik-e a személyes adatait, milyen joggalappal, azokat továbbküldték-e más adatkezelők részére. Különleges adatoknál opt-in szükséges, egyéb esetben opt-out is elégséges az adatok továbbküldéséhez. Az adatok továbbküldése esetén az adatkezelőnek szerződést kell kötnie, amelyben biztosítja, hogy a személyes adatok védelme ne csökkenjen.

Az európai állampolgárok jogorvoslati joga komoly előrelépés a Safe Harborhoz képest, amely nem biztosította az amerikai érintetteknek fennálló jogi védelmet az uniós polgárok részére.

⁴⁴⁰ Henry Farrell and Abraham Newman: The Transatlantic Data War, Europe Fights Back Against the NSA, Foreign Affairs, 2016. 01. 127-131.

⁴⁴¹ WP29 Press release 2016. 04. 16.

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf

⁴⁴² Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield

⁴⁴³ Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield

Az érintettnek joga van az adatkezelő vállalatnál közvetlenül panaszt benyújtani, amelyre az köteles 45 napon belül reagálni. Amennyiben a válasz vagy a megoldás nem kielégítő az érintett számára, abban az esetben alternatív vitarendezést vehet igénybe ingyenesen, továbbá a nemzeti adatvédelmi hatóságok segítségét is igénybe vehetik, amely különösen fontos az anyanyelvükön való segítségnyújtás miatt⁴⁴⁴.

A Privacy Shield szövegének jelentős része⁴⁴⁵ – 19 oldal - szól a titkosszolgálati adatgyűjtések korlátozásáról és a megfelelő biztosítékokról: többek között a nem célzott, tömeges adatgyűjtések elkerülése, a megfelelő jogalapok és engedélyek biztosítása, több felelős személy általi kontroll és a megkeresésekről szóló jelentések nyilvánosságra hozatala törekszik biztosítani az átláthatóságot és az adatgyűjtések korlátok közé szorítását. A rendelkezések komoly előrelépést jelentenek a Safe Harborhoz képest, azonban a teljes transzparencia hiú ábránd marad, amelynek elvárásához szükséges lenne, hogy azt a többi állam is legalább részlegesen teljesítse⁴⁴⁶.

Az ombudsman személye előrelépést jelent, különösen a tekintetben, hogy nem csupán a Privacy Shield-el kapcsolatos panaszokat, hanem az egyéb adatküldési módokon USA-ba került adatokkal kapcsolatos kérelmeket is vizsgálhatja⁴⁴⁷.

A részére küldött panaszoknak először megfelelő szűrőkön kell átmenniük, így a nemzeti adatvédelmi hatósághoz lehet azokat beadni⁴⁴⁸.

A Privacy Shield alapesetben megengedi a személyes adatok eltérő célból történő kezelését, amennyiben az kompatibilis az eredeti céllal, azonban az érintett bármikor tiltakozhat az ellen (opt-out). Különleges adatoknál azonban már szigorúbb a szabályozás, előírva az érintett előzetes hozzájárulását (opt-in)⁴⁴⁹.

⁴⁴⁴ Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176 final Brussels, 12.7.2016. 12-13.

⁴⁴⁵ Privacy Shield Decision 16-35.

⁴⁴⁶ Xavier Tracol, EU–U.S. Privacy Shield: The saga continues, Computer Law and Security Review Vol. 32. 2016. 776.

⁴⁴⁷ Privacy Shield Decision 34-35.

⁴⁴⁸ European Commission Directorate-General for Justice and Consumers: Guide to the EU – U.S. Privacy Shield, 2016.

⁴⁴⁹ Privacy Shield (22) Where a new (changed) purpose is materially different but still compatible with the original purpose, the Choice Principle gives data subjects the right to object (opt out). The Choice Principle does not supersede the express prohibition on incompatible processing. Special rules generally allowing for the opt-out "at any time" from the use of personal data apply for direct marketing. In the case of sensitive data, organisations must normally obtain the data subject's affirmative express consent (opt in).

A Facebook szintén a Privacy Shieldet használja a személyes adatai küldéséhez az Egyesült Államokba. Dolgozatom előző fejezetében kifejtettem, hogy a Facebook adatkezelései túlterjeszkednek a felhasználó hozzájárulásán és az adatgyűjtés időpontjában fennálló eredeti célokon, anélkül, hogy a felhasználótól arra külön hozzájárulást kérne, vagy tájékoztatást nyújtana.

A nem különleges személyes adatok esetében tehát a kompatibilitás vizsgálandó, amelyhez kiindulópontot adhat az Adatvédelmi Rendelet⁴⁵⁰, amely az következő szempontokat határozza meg: 1. kapcsolat az eredeti és az új cél között,

2. az adatgyűjtés körülményei,

3. az adatok jellege (különleges-e),

4. az érintettek milyen következményekkel járhat a további kezelés,

5. megfelelő garanciák megléte.

Az eredeti és az új cél között kapcsolat nehezen lelhető fel például a Facebook esetében a WhatsApp felvásárlása után megszerzett adatok felhasználása egyértelműen különbözik az eredeti céltól: a WhatsApp felhasználói személyes adataikat egy üzenetküldő szolgáltatás igénybevétele céljából, nem pedig egy közösségi hálózatnak adták meg.

Az adatgyűjtés körülményeit tekintve a hozzájárulás érvényessége kérdőre vonható a megfelelő tájékoztatás hiányában, a WhatsApp esetében pedig megtévesztés miatt egyértelműen érvénytelen, hiszen a felhasználók ígéretet kaptak arra, hogy adataikat nem fogják harmadik félnek kiszolgáltatni.

A Facebook-tól szóló fejezetben a célon túlterjeszkedő adatkezelés lehetséges hatásait alapos vizsgálatnak vettem alá, továbbá a felhasználó tudtával kezelt és a róla gyűjtött különleges adatokat elemeztem. A Facebook által kezelt adatok között jelentős mennyiségben találhatóak különleges adatok, továbbá az algoritmusok által magas bizonyossággal levonhatóak olyan

⁴⁵⁰ (4) Ha az adatgyűjtés céljától eltérő célból történő adatkezelés nem az érintett hozzájárulásán vagy valamely olyan uniós vagy tagállami jogon alapul, amely szükséges és arányos intézkedésnek minősül egy demokratikus társadalomban a 23. cikk (1) bekezdésében rögzített célok eléréséhez, annak megállapításához, hogy az eltérő célú adatkezelés összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték, az adatkezelő többek között figyelembe veszi:

a) a személyes adatok gyűjtésének céljait és a tervezett további adatkezelés céljai közötti esetleges kapcsolatokat;

b) a személyes adatok gyűjtésének körülményeit, különös tekintettel az érintettek és az adatkezelő közötti kapcsolatokra;

c) a személyes adatok jellegét, különösen pedig azt, hogy a 9. cikk szerinti személyes adatok különleges kategóriáinak kezeléséről van-e szó, illetve, hogy büntetőjogi felelősség megállapítására és bűncselekményekre vonatkozó adatoknak a 10. cikk szerinti kezeléséről van-e szó;

d) azt, hogy az érintettek nézve milyen esetleges következményekkel járna az adatok tervezett további kezelése;

e) megfelelő garanciák meglétét, ami jelenthet titkosítást vagy álnevesítést is.

következtetések a felhasználóról, mint például politikai és vallási nézetei, társadalmi helyzete, esetleg szexuális hovatartozása. A Facebook által alkalmazott Cookie és helyeghatározó technológiák által pedig további szenzitív információk tudhatók meg a felhasználóról.

A megfelelő garanciák továbbra is kérdésesek a Privacy Shield rendelkezéseit vizsgálva, amelyet jelen fejezetben fejtettem ki.

A Privacy Shield a személyes adatok továbbküldésével kapcsolatban is lényeges korlátozásokat tartalmaz. A személyes adatok küldése az USA-ban lévő adatkezelőtől bármely harmadik adatkezelő részére csak abban az esetben lehetséges, ha az határozott és korlátozott célból történik és szerződésen alapul, amely biztosítja az érintett számára a Privacy Shield-ben meghatározott védelmi szintet.

Fontos továbbá, hogy a szerződésben biztosítani kell az érintett részére a tiltakozási jogot (opt out), továbbá különleges adatok küldéséhez előzetes hozzájárulás szükséges (opt in)⁴⁵¹.

A különleges adatok esetében a Privacy Shield a továbbküldéshez és eltérő célból történő kezeléshez előzetes hozzájárulást követel meg, amelyet a Facebooknak a felhasználóktól be kellene szereznie.

A hozzájárulás beszerzése meg kell, hogy feleljen az alapvető követelményeknek, így megfelelő tájékoztatásnak kell megelőznie, amelyhez véleményem szerint nem kielégítő a felhasználói feltételek frissítése. Tudomásom szerint a Privacy Shield elfogadása óta nem érkezett a Facebook részéről a felhasználóknak előzetes hozzájárulással kapcsolatos megkeresése.

A fennálló helyzet így véleményem szerint ütközhet a Privacy Shield és az európai adatvédelmi jog rendelkezéseivel.

A Facebook oldalán lévő, Privacy Shield-el kapcsolatos tájékoztató alapján a Facebook hirdetési és mérési termékeket kínál, és az ilyen szolgáltatásokon keresztül személyes adatokat kaphat a hozzá nem tartozó partnerektől (az adatkezelőktől), amely esetben a Facebook Ireland

⁴⁵¹ (28) Under the Accountability for Onward Transfer Principle, any onward transfer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group) and (iii) only if that contract provides the same level of protection as the one guaranteed by the Principles, which includes the requirement that the application of the Principles may only be limited to the extent necessary to meet national security, law enforcement and other public interest purposes. This should be read in conjunction with the Notice and, in the case of an onward transfer to a third party controller, with the Choice Principle, according to which data subjects must be informed (among others) about the type/identity of any third party recipient, the purpose of the onward transfer as well as the choice offered and can object (opt out) or, in the case of sensitive data, have to give "affirmative express consent" (opt in) for onward transfers. In the light of the Data Integrity and Purpose Limitation Principle, the obligation to provide the same level of protection as guaranteed by the Principles presupposes that the third party may only process the personal information transmitted to it for purposes that are not incompatible with the purposes for which it was originally collected or subsequently authorised by the individual.

az adatfeldolgozó, és a Facebook Inc. további feldolgozó. Az ilyen adatok közé tartozhatnak például kapcsolattartási adatok, valamint magánszemélyeknek a partnerekkel és termékeikkel, szolgáltatásaikkal és hirdetéseikkel kapcsolatban szerzett élményeire vagy azokhoz kapcsolódó aktivitására vonatkozó információk⁴⁵².

A Facebook éles különbségtétele az adatkezelő, adatfeldolgozó, és további adatfeldolgozó között jelen helyzetben véleményem szerint megtévesztő lehet, és a valóságtól eltérő: az adatok kezelésének célját és módját valójában az Egyesült Államokban lévő Facebook Inc. határozza meg, nem pedig a Facebook Ireland.

A tájékoztatóban a Facebook fenntartja továbbá, hogy az adatokat a Facebook-vállalatcsaládon belül és harmadik felek – többek között szolgáltatók és egyéb partnerek – számára továbbíthatja, továbbá viseli a felelősséget a személyes adatok ilyen harmadik felek által az „Adatvédelmi pajzs” program alapelveinek nem megfelelően végzett feldolgozásáért, kivéve abban az esetben, ha nem a Facebook volt felelős az állítólagos károkozást előidéző eseményért. A vállalatcsaládon belül is szükséges lenne az előzetes hozzájárulások beszerzése különleges adatok esetében, a tiltakozási jogot pedig feltétel nélkül a felhasználók számára biztosítani és arról őket megfelelően tájékoztatni, amely hiányzik az említett tájékoztatóból.

⁴⁵² <https://www.facebook.com/about/privacyshield>

6.3 Következtetések

A személyes adatok küldése az Egyesült Államokba kiemelten fontos az információs társadalom korában, azonban nem minden áron. Az NSA botrány és EU Bíróságának ítélete rámutatott az uniós állampolgárok kiszolgáltatottságára, és jogaik szisztematikus megsértésére. A megoldás keresése különösen fontos, mivel a Facebook-nak, Google-nak, és a Microsoft-nak nincsenek európai alternatívái. A Safe harbor megszűnése és a Privacy Shield elfogadása komoly lépést jelentenek, azonban továbbra is hézagos a küldött személyes adatok védelme: az általános szerződési feltételek, szerződés teljesítése, felhasználó hozzájárulása és a kötelező erejű vállalati szabályok nem védik az érintett személyes adatait megfelelően, az említett adatküldési módok szintén felülvizsgálatra szorulnának.

A hiányosságok ellenére a Privacy Shield komoly előrelépés a Safe Harbor után, amelynek a gyakorlati megvalósulása fogja megmutatni az igazi erejét és gyengeségeit: az amerikai kormány valóban felhagy-e a tömeges adatgyűjtéssel, az ombudsman személyének lesz-e valós súlya, a programban résztvevő szervezeteken milyen precizitással és intenzitással kéri számon a Privacy Shield rendelkezéseit.

A Facebook elsőként vette igénybe a Privacy Shield-et a személyes adatok küldésére, azonban véleményem szerint a felhasználók tájékoztatása, és a Privacy Shield-ben előírt követelmények teljesítése nem teljes mértékig megfelelő: az adatok eredeti céljától kezelése esetén a kompatibilitás az elsődleges és a másodlagos célok között vitatható, továbbá a különleges adatok esetében előírt előzetes hozzájárulás is nehezen igazolható, mivel a Privacy Shield elfogadása óta elkülöníthető hozzájárulást nem kért ezzel kapcsolatban a felhasználóktól. Hasonló a helyzet a Facebook vállalatcsaládon belül és más harmadik felekkel való adatmegosztása esetén.

Az alábbi táblázatban foglaltam össze az egyes adatküldési módok előnyeit és hátrányait az adatkezelők szempontjából.

	előnyök	hátrányok
hozzájárulás	- könnyen igazíthatóak a felek érdekeihez	- egyes esetekben a hozzájárulás nem alkalmazható (pl. munkavállaló esetén, mivel hozzájárulás önkéntessége vitatható)

szerződés teljesítéséhez szükséges	- gyors és olcsó	- az adatkezelőt terheli a bizonyítási kötelezettség a „szükségességgel” kapcsolatban, amelyet bármikor vizsgálhatnak a nemzeti adatvédelmi hatóságok
Kötelező erejű vállalati szabályok	- nemzetközi szervezeten belül kényelmesen használható az adatok kezeléséhez	- a személyes adatok csak a szervezeten belül küldhetők - nincsenek minták - az egyes adatvédelmi hatóságok engedélyét kell kérni - az eljárás így drága és időigényes
Általános szerződési feltételek	- alkalmas bármilyen adat küldésére bárhova - a mintaszerződések el vannak készítve	- merev - a megoldás könnyen a Safe Harbor sorsára juthat
Privacy Shield	- könnyen teljesíthető egységes rendszer - a kisebb cégek is könnyen találhatnak mintákat a szervezeti és működési szabályzataikhoz, szerződéseikhez	- földrajzilag korlátozott, csak az Egyesült Államokba irányuló adatküldésre alkalmazható - még kiforratlan - egy újabb titkosszolgálati adatgyűjtéssel kapcsolatos botrány az USA-ban veszélybe sodorhatja ezt a megoldást is

2. táblázat: az egyes adatküldési módok előnyeit és hátrányait az európai adatkezelők számára

7. A személyes adat, mint adásvétel tárgya

Az online szolgáltatások adásvétele különösen jelentős adatvédelmi szempontból, mivel az adatkezelő, vagy a számára utasítást adó tulajdonos személye megváltozhat.

Mivel napjainkban a cégek adásvétele sok esetben csak kisebb részben a szolgáltatás, nagyobb részben az adatbázis miatt történik (pl.: a Facebook megvásárolta a Whatsapp-ot, Microsoft a Skype-ot), így különösen fontos, hogy a személyes adatok védelmének szintje ne csökkenjen. Komplette üzleti tevékenységek eladása alapvetően kétféle módon valósulhat meg: a gazdasági társaság felvásárlásával, vagy kizárólag az üzleti tevékenységet megtestesítő jogok és eszközök átvételével (pl.: szoftver, felhasználókkal megkötött szolgáltatási szerződés, domain név, védjegy).

Az egyik mód a szolgáltatás és az adatbázis megszerzésére, ha az adatkezelő cég teljes mértékig megvásárlásra kerül, így annak csak a tulajdonosa változik meg. Ebben az esetben az adatkezelő személye tulajdonképpen nem változik, viszont kérdésként merül fel a felhasználók tájékoztatásának a szükségessége⁴⁵³.

A jogi személy legfőbb ismérve, hogy a tagoktól elkülönült szervezettel rendelkezik, és működése független a tagok társaságba való belépésétől és kiválásától. Az üzletész átruházása (például adásvétel, öröklés címén) csupán a tag személyét érintő változás, mialatt a jogi személy – és az adatkezelő személye is – változatlan marad. A jogutódlással (például átalakulás, szétválás, egyesülés) a jogutód társaságot illetik a jogelő gazdászgi társaság jogai és terhelik a jogelő társaság kötelezettségei. A jogutódlással az adatkezelések is teljes terjedelmében a jogutódra szállnak át.

Péterfalvi Attila adatvédelmi biztosként kiadott korábbi állásfoglalása alapján az adatkezelő az adatkezelés körülményeiben bekövetkezett változásról köteles tájékoztatni [Avtv. 6. § (2) bekezdése szerint] az érintetteket. Ide tartoznak az adatkezeléssel kapcsolatos tényeket – mint például az adatkezelő személyét vagy az adatkezelés célját – érintő változások⁴⁵⁴.

A tagok személyében bekövetkezett változás a tagok és a társaság belső jogviszonyában jelent változást, és nem jelenti a társaság külső jogviszonyának – ideértve az érintettel fennálló és

⁴⁵³ Csiky András, Jambrik Gergely: Online szolgáltatások átruházásával kapcsolatos adatvédelmi kérdések és a követeléskezeléssel kapcsolatos adatkezelés, Infokommunikáció és jog, 2014. 3. 138.

⁴⁵⁴ Péterfalvi Attila adatvédelmi biztos 728/K/2006-3. ügyszámú állásfoglalása

adatkezelést igénylő jogviszony – megváltozását. Mégis elképzelhető olyan adatkezelés, ahol az adatkezelés céljára és jellegére tekintettel jelentősége van annak, hogy az adatkezelést végző jogi személy milyen tagsággal rendelkezik.

Péterfalvi Atilla álláspontja szerint a tájékoztatás minden adatkezelésben kiemelkedő jelentőségű. Ha az adatkezelés szempontjából jelentőséggel bír a jogi személy szervezetét vagy működését érintő változás, akkor a tájékoztatás elengedhetetlen. Ennek indoka, hogy az érintett a megváltozott körülmények ismeretében szabadon dönthessen arról, hogy kíván-e a továbbiakban az adatkezelésben részt venni vagy sem⁴⁵⁵.

Az egyik legfontosabb kérdés, hogy a korábbi adatkezelőnek adott hozzájáruló nyilatkozatok hatálya kiterjed-e a „tulajdonosváltást” követő adatkezelésre.

A jogutódlás esetében a törvény erejénél fogva átszállnak a jogutódra a jogelődöt megillető jogok és az őt terhelő kötelezettségek. A jogelőd adatkezelőnek adott hozzájárulások továbbra is jogalapot jelentenek az adatkezeléshez. Ugyanígy – Péterfalvi Attila álláspontja szerint – a tagok személyében bekövetkezett változás sem teszi a hozzájáruló nyilatkozatokat hatálytalanná, továbbá az érintett infotörvényben foglalt jogai alapján információs önrendelkezési jogával élve az adatkezelés bármely szakaszában elzárkózhat a további adatkezeléstől. Akár a „tulajdonosváltás” előtt, akár azt követően is.

Csiky András és Jambrik Gergely álláspontja szerint a tulajdonosváltás legfeljebb abban az esetben eredményezhet tájékoztatási kötelezettséget, amennyiben a tag személyéhez szorosan kötődött az adott szolgáltatás, ami a szolgáltatás során való személyes közreműködést jelenti, és amelynek jelentősége volt abban, hogy az érintett az adatkezelő szolgáltatását vette igénybe. Véleményem szerint minden esetben szükséges lenne az érintett tájékoztatása, mivel a tulajdonosnak – az üzleti érdekein keresztül – lehet ráhatása az adatkezelő döntéseire. Az adatkezelő az a személy, aki az adatkezelés célját meghatározza, azonban amennyiben a tulajdonos utasítására cselekszik, kérdésessé válik az adatkezelői minőségének önállósága.

Szerződésátruházásról abban az esetben beszélhetünk, amennyiben kizárólag egy tevékenység kerül átruházásra, így az adatkezelő személye megváltozik.

A szolgáltatási szerződés megkötésekor – jellemzően a regisztráció során – az érintett elfogadja az adatvédelmi szabályzatot is, amely az Infotv. két jogszabályhelyén alapulhat:

1. Az általános szabály (Infotv. 5. § (1), amely alapján személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul.

⁴⁵⁵ Péterfalvi Attila adatvédelmi biztosnak az iWiW felvásárlásával kapcsolatos ügyben adott válasza (Ügyszám: 741/A/2006-3.)

2. Különös szabály (Infotv. 6. § (4) alapján, ha az adatkezelés célja az adatkezelővel írásban kötött szerződés végrehajtása. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

Az általános szabály alapján az adatvédelmi szabályzat elméletileg külön kerül elfogadásra, míg a különös szabály esetében az adatkezelési szabályzat a szolgáltatási szerződés részét képezi és a felek avval együtt fogadják el.

Mivel az adatkezelés célját a szolgáltatási szerződés határozza meg, és annak megszűnésével az adatkezelés általában véget ér, így az adatvédelmi szabályzat járulékos jellegűnek tekinthető. Az üzleti tevékenység átruházása esetén a Ptk. szerinti szerződésátruházásról⁴⁵⁶ beszélhetünk, amelynek háttérszabályait az engedményezés és a tartozásátvállalás adják⁴⁵⁷.

A szerződésátruházás az új Ptk. új jogintézménye, amelynek célja a teljes szerződéses pozíció átruházása, amelynek bevezetésével a Ptk. azt a bonyolult szerződéses mechanizmust kívánta megszüntetni, hogy a felek engedményezéssel és tartozásátvállalással próbálják meg a szerződéses pozíciók cseréjét kezelni. A szerződéses szerepek komplett átruházására ugyanis az engedményezés és a tartozásátvállalás sem volt megfelelő jogi eszköz⁴⁵⁸.

A szerződésátruházás jogintézménye alapvetően azt a célt szolgálja, hogy egy meglévő, hosszú távú jogviszonyban az egyik fél személyét illetően kontraktuális alapon jogutódlás következzen be. A szerződéses jogviszonyban maradó fél az alapjogviszonyt létrehozó szerződésben vagy akár azt követően járul hozzá ahhoz, hogy a későbbiek során a másik fél személye megváltozzon, mely harmadik fél kiléte az alapjogviszony létrejöttékor még nem meghatározott vagy az átruházás csak mint lehetőség merül fel⁴⁵⁹.

A szerződésbe belépő felet megilletik mindazon jogok, és terhelik mindazon kötelezettségek, amelyek a szerződésből kilépő felet a szerződésben maradó féllel szemben a szerződés alapján megillették és terhelték⁴⁶⁰.

⁴⁵⁶ Ptl. 6:208. § (1) A szerződésből kilépő, a szerződésben maradó és a szerződésbe belépő fél megállapodhatnak a szerződésből kilépő felet megillető jogok és az őt terhelő kötelezettségek összességének a szerződésbe belépő félre történő átruházásáról

⁴⁵⁷ 6:210. § [Az engedményezés és a tartozásátvállalás szabályainak alkalmazása]

A szerződésátruházásra egyebekben a követelések és a jogok tekintetében az engedményezés, a kötelezettségek tekintetében a tartozásátvállalás szabályait kell megfelelően alkalmazni.

⁴⁵⁸ Bodzási Balázs: A Ptk. hatálybalépése után felmerült gazdasági igények hatása, *Fontes Iuris: Az Igazságügyi Minisztérium Szakmai Folyóirata*, 1 (3-4). 2015. 57-65.

⁴⁵⁹ Késmárki-Mészáros Gyöngyi: A szerződésátruházás jogintézményének rövid bemutatása, *Themis*, 2013. június 177-188.

⁴⁶⁰ Pázmándi Kinga, Pétervári Kinga, Sárközi Tamás, Verebics János: *Üzleti jog az új Polgári Törvénykönyv után*, Typotex Elektronikus Kiadó, Budapest 2014. 204.

A szerződésátruházáshoz tehát szükséges az érintett hozzájárulása is, amelyet általában előzetesen szereznek be a szolgáltatók a szolgáltatási szerződés megkötése során, amelyben kikötik a lehetséges átruházást a jövőben egy ismeretlen harmadik fél részére⁴⁶¹.

Kérdés továbbá, hogy a szolgáltatási szerződés átruházásához való hozzájárulás kiterjed-e az adatvédelmi szabályzatra is. Amennyiben az adatvédelmi szabályzat a szolgáltatási szerződés részét képezi, abban az esetben a hozzájárulás egyértelműen kiterjed azokra is. Amennyiben az adatvédelmi szabályzat a szolgáltatási szerződéstől külön okiratot képez, a járulékos jellege folytán szintén a hozzájárulás alá kell, hogy essen⁴⁶².

A NAIH engedményezéssel kapcsolatos álláspontjából⁴⁶³ is levezethető, hogy amennyiben a szerződés átruházása jogszerű, úgy a vevő adatkezelése is annak tekinthető, mivel „az engedményezés velejárója a követelés érvényesítéséhez szükséges adatok átadása”.

Összegezve kijelenthető, hogy célszerű a szolgáltatási szerződésben kikötni az átruházás jövőbeni lehetőségét és annak részleteit, valamint az adatok védelmi szintjének megtartását, és az átruházás előtt az érintetteket értesíteni, hogy élhessenek tiltakozáshoz való jogukkal, amennyiben úgy döntenek.

A NAIH eseti döntése alapján is szükséges a jövőbeni átruházás lehetőségének részletes, és megfelelő kikötése, mint például, hogy a vevő az adatokat a felhasználók által ismert és elfogadott célra használja majd fel⁴⁶⁴.

7.1 A célhoz kötöttség és szükségesség elve, mint az adásvétel korlátja

A cél az adatkezelés legfontosabb aspektusa, melynek megváltozása új adatkezelést eredményez, és ahhoz szükséges az érintett hozzájárulása. A célhoz kötöttség az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája.⁴⁶⁵ Az adatgyűjtés célját annak megkezdése előtt meg kell határozni, valamint arról az érintettet megfelelően tájékoztatni kell, hogy megalapozottan dönthessen, miként rendelkezik személyes

⁴⁶¹ Facebook adatvédelmi szabályzat (letöltés ideje: 2016. 11. 06.): Új tulajdonos.

Amennyiben szolgáltatásaink vagy a hozzájuk tartozó eszközök tulajdonjoga vagy irányítási joga részben vagy teljes egészében megváltozik, adataidat átadhatjuk az új tulajdonosnak.

⁴⁶² Csiky, Jambrik 140.

⁴⁶³ NAIH ajánlása a követeléskezelés, tartozásbehajtás, adósságbehajtás, faktoringtevékenység során alkalmazott követeléstechnikák adatvédelmi követelményeiről (2014. július 3)

⁴⁶⁴ NAIH 2013. 02. 08-án kelt határozata III. 3) pont (Ügyiratszám: NAIH-5888-13/2012/H)

⁴⁶⁵ 15/1991. (IV. 13.) AB határozat

adataival, kiadja-e azokat. Az érintettel úgy kell közölni az adatfeldolgozás célját, hogy megítélhesse jogait és kötelezettségeit, továbbá a céltól eltérő felhasználás esetén élhessen jogaival.

A cél nélküli adatkezelés és adatraktározás jogszerűtlen, még az érintett hozzájárulásával is jogellenes. Az adatkezelés céljának meghatározottnak, konkrétan és jogszerűnek kell lennie, így nem felel meg a célhoz kötöttség elvének, ha az adatgyűjtés célja túl tágan van megfogalmazva, egyedi célok nélkül. Magyarország az 1990-es évek elején az ország teljes lakosságát érintő adatfeldolgozó rendszert szeretett volna felállítani, melyhez a jogszabály az alábbi, semmitmondó célt határozta meg: „az állampolgár jogai érvényesítésének és kötelezettségei teljesítésének előmozdítása, az állami szervek, a gazdálkodó és társadalmi szervezetek, egyesületek, valamint magánszemélyek társulásai (a továbbiakban együtt: szervezetek) munkájának segítése”

Az Alkotmánybíróság a jogszabályt megsemmisítette, mivel a célja „alkalmatlan arra, hogy az adatfeldolgozásnak bármiféle irányt vagy határt szabjon, azaz hogy célhoz kötöttségről egyáltalán beszélni lehessen”⁴⁶⁶

Az adatkezelésnek minden szakaszában meg kell felelnie a céljának, mely nem csak az adatkezelő és harmadik személyek relációjában kötelező szabály, hanem az adatkezelő szervezetén belül is. Ebből következően az adatkezelő szervezetében is csak azok férhetnek hozzá az személyes adatokhoz, akiknek ez feltétlenül szükséges, és munkájuk az adatkezelés céljához kapcsolódik, (pl.: az áruházak pontgyűjtő rendszeréhez a számlázási osztály hozzáférhet, de az árubeszerzési osztály elvileg nem), mely által az adatkezelés nem lép ki az előre meghatározott mederből.

A Földhivatal az ingatlan-nyilvántartás alapján nem adhat információt arról, hogy egy konkrét személynek mennyi és milyen értékű ingatlanjai vannak, csupán egy konkrét ingatlan adatait szolgáltathatja ki, mivel az ingatlan-nyilvántartás célja az ingatlanforgalom biztonságának garantálása, nem pedig a lakosság vagyonának nyilvántartása. Fontos megjegyezni, hogy a célhoz kötöttség közérdekű adatokra⁴⁶⁷ nem értelmezhető, azok bárki számára cél nélkül hozzáférhetőek, szabadon felhasználhatóak.

⁴⁶⁶15/1991. (IV. 13.) AB határozat

⁴⁶⁷ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. § 5. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Hasonlóan a hitelkártyát biztosító vállalatok sem használhatják fel az adatokat a fizetési adminisztráción túl más tevékenységre, melyre többször volt már példa: a hitelkártya tulajdonosokat az American Express sorolta be vásárlási szokásaik alapján⁴⁶⁸, mely adatokat azután reklámozásra használt fel⁴⁶⁹.

Az adatvédelmi irányelv alapján a tagállamoknak lehetősége van arra, hogy másodlagos célra is megengedjék az adatkezelést, amennyiben az elsődleges adatkezeléssel összefügg, avval releváns, így például,⁴⁷⁰ ha az adatkezelő ügyféladatbázisát saját marketingre használja fel.⁴⁷¹

A magyar adatvédelmi szabályozás viszont szűken kezeli a másodlagos, releváns adatkezelést⁴⁷².

A szükségesség elve alapján csak olyan személyes adat kezelhető, mely a cél eléréséhez elengedhetetlen, így például egy autó vásárlásához nem szükségesek az egészségügyi adataink. Legszembetűnőbb példa a szükségesség elvére a bankok és biztosítók által a kockázatelemzéshez kért személyes adatok, melyek között különleges adatok⁴⁷³ is vannak: személyi azonosító adatokon túl a kereset, betegség, házasság fennállása, házastárs keresete, további hitelek fennállta, életbiztosítás meglétét is igénylik az ügyféltől.

Az adatkezelés célja az ügyfél hitelképességének vizsgálata, mely által a hitelintézet tisztább képet kaphat az ügyfél vagyoni és családi helyzetéről. A bank minél több információt kap a potenciális ügyfélről, annál személyre szabottabb ajánlatot tud számára nyújtani, mely adott esetben pozitív hitelelbírást és kedvezőbb kamatokat is jelenthet.

⁴⁶⁸ Dwyer v. American Express, 652 N.E.2d 1351 (Ill. App. 1995)

⁴⁶⁹ Daniel J. Solove – Paul M. Schwartz: Privacy, Information and Technology, Wolters Kluwer Law & Business, New York, 2011, 425.

⁴⁷⁰ Jóri, 2005, 217.

⁴⁷¹ Az Európai Parlament és a Tanács 95/46/EK irányelve, 6. cikk

(1) A tagállamok rendelkeznek arról, hogy a személyes adatok:

b) gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további feldolgozása nem végezhető e célokkal összeférhetetlen módon. A személyes adatok további feldolgozása történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat;

c) gyűjtésük és/vagy további feldolgozásuk célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek;

⁴⁷² 4. § (2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

⁴⁷³ 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 3. § 3. különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre vonatkozó személyes adat, b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

7.2. Facebook és a WhatsApp

Amikor a Facebook megvásárolta 2014-ben a WhatsAppot, az ügylet megkötésekor mindkét fél a nyilvánosságot arról tájékoztatta, hogy az adataik biztonságban vannak, azok kezelése adatkezelési szabályzatokban leírtak szerint fog folytatódni, nem kerülnek megosztásra.

2016-ban frissítette a WhatsApp a felhasználói feltételeit, amelyből – több kattintás és görgetés után – kiderült, hogy a felhasználói adatait mégis megosztja a Facebookkal. A hírre a brit és a hamburgi adatvédelmi biztos azonnal vizsgálatot indítottak.

Az adatok Facebookkal való megosztását a WhatsApp olyan indokokkal támasztotta alá, mint „a felhasználók számának pontos ismerete”, a „spam elleni küzdelem”, „jobb ismerős ajánlási rendszer és releváns reklámok mutatása”⁴⁷⁴.

A felhasználóknak csupán 30 napja volt arra, hogy döntsenek a személyes adataik sorsáról, és a döntés lehetősége nem volt egyértelmű. Véleményem szerint a tájékoztatás nem felelt meg az uniós adatvédelmi jogszabályoknak, továbbá a hozzájárulás még ettől függetlenül sem tekinthető megfelelőnek, mivel ott is el volt rejtve az opt-out lehetősége.

A felhasználói szabályzat változtatásairól szóló tájékoztatás legfontosabb pontjait mutató, a felhasználó számára rendelkezésre álló rövidített változat nem tartalmazta az adatok megosztását, arról információkat csak akkor kapott a felhasználó, ha a részletes információkat kérő gombra („read more”) kattintott, így az adatvédelmi szempontból legjelentősebb információk tulajdonképpen el voltak rejtve úgy, hogy arra egy átlagos felhasználó biztosan nem keres rá, vagy olvas tovább.

Az adatvédelmi tájékoztató továbbá megtévesztően fogalmaz: „a személyes adataid nem kerülnek megosztásra a Facebookon”. A felhasználó, amennyiben nem olvas tovább és merül el a részletekben, könnyen azt hiheti, hogy az adatai nem kerülnek megosztásra a Facebookkal, pedig azokat megkapja közösségi hálózat.

A hozzájárulással kapcsolatos probléma, hogy ahhoz szintén el kellett mélyedni egy további menüben, ahol külön lehetett kipipálni a megosztás lehetőségét vagy tiltását.

A visszautasítás esetén is küldésre kerülhetnek használattal kapcsolatos információk a Facebook részére a rendszer és a biztonság fenntartása érdekében, tehát semmilyen módon nem lehet megtiltani, hogy a Facebook a felhasználókkal kapcsolatos adatokhoz hozzáférjen.

⁴⁷⁴ Tim Cowen: Big Data as a Competition Issue: Should the EU Commission's Approach Be More Careful? European Networks Law & Regulation Quarterly Vol. 4. 2016. 21.

Lényeges továbbá, hogy a WhatsApp adatok nem csupán a Facebookkal, hanem annak a vállalataival (Facebook Family) is megosztásra kerülhetnek. Amennyiben a WhatsApp felhasználó többet szeretne tudni ezekről a vállalatokról – amelyek a számára személyes adatai, kontaktjai megosztásra kerülnek - szintén tovább kell keresnie a felhasználói feltételek között. A leírtak után ironikusan hangzik, hogy a WhatsApp szabályzata biztosítja a felhasználót arról, hogy a felhasználók adatait nem fogja megosztani vagy eladni hirdető részére.

A WhatsApp alkalmazással kapcsolatban fontos megjegyezni, hogy a telepítéskor hozzáférést kér a felhasználó telefonkönyvéhez, hogy az abban lévő személyekkel a felhasználó közvetlenül tudjon kommunikálni. A felhasználók többsége ehhez hozzájárul, így a Whatsapp olyan személyek telefonszámaival és egyéb adataival is rendelkezik, akik nem felhasználói sem a WhatsAppnak, sem a Facebooknak. A Facebook ráadásul ismerősök ajánlására is felhasználhatja a gyűjtött információkat, így olyan személyek is rátalálhatnak a felhasználóra a Facebookon, akiknek egyébként nem lett volna ennyire egyszerű, és a visszautasításuk a valós életben nem könnyű. Így merülhet fel olyan kellemetlen helyzet, hogy a felhasználót a főnöke ismerősnek jelöli Facebookon, akinek visszautasítása vagy függőben hagyása nem merül fel valós opcióként.

Bár a WhatsApp üzenetek küldése titkosított csatornán keresztül zajlik, így annak tartalmáról nem kerülhet információ továbbításra a Facebook részére, azonban az alkalmazás rendelkezik olyan információkkal, hogy a felhasználó kivel, mikor, hol, mennyi ideig és milyen eszközről kommunikált.

Németországban a Hamburg tartományi adatvédelmi biztos közigazgatási végzéssel eltiltotta a Facebookot a WhatsApp felhasználói adatainak rögzítésétől és tárolásától. Az adatvédelmi biztos hivatalának közleménye szerint a Facebook nem tartotta be a WhatsApp felvásárlásakor - 2014-ben - tett azon ígéretet, hogy a két szolgáltatás felhasználóinak adatait elkülönítve kezelik. Véleménye szerint a Facebook félrevezette a felhasználókat és a nyilvánosságot, és megsértette a nemzeti adatvédelmi előírásokat. A Facebook a WhatsApp-felhasználók személyes adatait az érintettek felhatalmazása és bármiféle jogszabályi alap nélkül kezeli - áll a közleményben, amely szerint a Facebooknak törölnie kell a WhatsApp felhasználói adatbázisából beszerzett adatokat.

Martin Schemm tartományi adatvédelmi biztos kiemelte továbbá, hogy az Európai Unió Bírósága egy júliusi ítéletében megerősítette, hogy a helyi, nemzeti adatvédelmi előírásokat kell alkalmazni, amennyiben egy vállalkozás az adott országban működő telephelye révén használ fel adatokat, a Facebook-nál pedig éppen a hamburgi képviselő felelős a hirdetési üzletág német nyelvű tartalmaiért.

A tiltó közigazgatási végzés mintegy 35 millió német WhatsApp-felhasználó adatait védi. Nekik kell döntenüik arról, hogy felhasználói profiljukat összekapcsolják-e Facebook-profiljukkal. Ehhez a Facebooknak engedélyt kell kérnie tőlük, és ez nem történt meg – emelte ki az adatvédelmi biztos. Hozzátette, hogy a végzés annak a sok millió embernek az adatait is védi, akiknek elérhetősége szerepel a német WhatsApp-felhasználók kontaktlistáján.

A Facebook új tulajdonossal kapcsolatos rendelkezései

A Facebook új tulajdonossal kapcsolatos rendelkezései a felhasználói feltételek között véleményem szerint több ponton is aggályosak és homályosak: nemhogy az adásvétel tárgya nincsen tisztázva, de még az adásvétel ténye sem szükséges az adatok átadásához.

Új tulajdonos.

Amennyiben szolgáltatásaink vagy a hozzájuk tartozó eszközök tulajdonjoga vagy irányítási joga részben vagy teljes egészében megváltozik, adataidat átadhatjuk az új tulajdonosnak.

A „szolgáltatások tulajdonjoga” világos és érthető, az „eszközök tulajdonjoga” azonban már nehezen értelmezhető a személyes adatok átadására: „eszközök” alatt érthetjük a számítástechnikai háttérrel, például a szervereket, amelyeket folyamatosan selejteznek, tulajdonjukuk gyakran és könnyen változhat.

Amennyiben a szolgáltatással együtt értékesítik az eszközöket, abban az esetben érthető személyes adatok átadása, azonban csupán a számítástechnikai eszközök átruházása semmilyen alapot nem ad a felhasználók személyes adatainak átadására.

A megfogalmazásban azonban a „vagy” kötőszó szerepel, mely megadja a lehetőséget csupán az eszközök átruházására szolgáltatások nélkül.

Aggodalomra ad okot az irányítási jog teljes vagy részleges megváltozására vonatkozó rendelkezés is, mely alapján a tulajdonjog átruházása sem szükséges a személyes adatok átadásához, csupán az irányítás részleges időleges megszerzésével az lehetséges.

7.3 A Toysmart ügy

Az utóbbi évtizedek alatt hatalmas mennyiségű rendszerezett, elektronikusan nyilvántartott személyes adat cserélt gazdát cégek adásvétele, egyesülése, szétválása és átszervezése során. A

vállalatok számára különös jelentőséggel bír a személyes adatok birtoklása, mely számukra profittá konvertálható egyre könnyebben, köszönhetően a feldolgozáshoz szükséges technika megfizethetőségének.

A Toysmart⁴⁷⁵ egy online játékkereskedő cég volt az Egyesült Államokban, melynek a Disney volt a többségi tulajdonosa. A Toysmart 2001-ben csődbe ment, és legjelentősebb megmaradt vagyona a felhasználói adatbázisa volt, melyet megpróbált eladni, de azt a sorozatos botrányok és hosszas procedúra után a bíróság végül nem megtiltotta.

Amikor a Toysmart bejelentette, hogy befejezi a tevékenységét, megbíztak egy végrehajtással és árverezéssel foglalkozó céget (The Recovery Group), mely meghirdette a Wall Street Journalban és a Boston Globe-ban a felhasználói adatbázisukat, mely tartalmazta az ügyfelek nevét, címeiket, fizetési adatait és információkat gyermekeikről.⁴⁷⁶

Mivel a Toysmart online cég volt, így nem rendelkezett „hagyományos” árverezhető vagyonnal, számottevően nem volt ingatlan és ingó vagyona. Az egyetlen értékes tulajdona a fogyasztóinak az adatbázisa volt.

A listát 50.000 dollárért hirdették meg, mely csupán kis része volt a Toysmart teljes, 18 millió dollárnyi adóságának, azonban hatalmas károkat okozhatott volna az online kereskedelemnek, mivel a sikeres tranzakció kikövezte volna az utat más internetes cégek előtt is, akik pénzzé tették volna adatbázisukat.

Az eladással több jogi és morális probléma is volt: a Toysmart adatvédelmi irányelvében - melyet a felhasználók számára regisztráláskor rendelkezésre bocsátott - kötelezte magát arra, hogy az adatokat harmadik személlyel nem osztja meg, azokat diszkréten kezeli⁴⁷⁷, továbbá a vállalat rendelkezett „TRUSTe”⁴⁷⁸ tanúsítvánnyal és pecséttel, mely egy olyan szervezet, amely garantálja, hogy a pecsétjével és tanúsítványával ellátott cég a személyes adatokat bizalmasan és jogszerűen kezeli.

A TRUSTe nem tudott közvetlenül keresetet beadni a bíróságra és eljárást indítani a Toysmart ellen, azonban a Szövetségi Kereskedelmi Bizottság⁴⁷⁹ (Federal Trade Commission,

⁴⁷⁵ A Toysmart 1999 januárjában kezdte meg a játékok kereskedelmét, majd 1999 szeptemberében szerezte meg a TRUSTe tanúsítványt

⁴⁷⁶ A Toysmart a felhasználók gyermekeiről is gyűjtött információkat egy online dinoszauruszos játék során, szüleik engedélye nélkül.

⁴⁷⁷ „A személyes adatok, melyeket a látogatóink önként megadnak..., harmadik személlyel megosztva soha nem lesznek. Minden információ, mely a Toysmart birtokába került, csupán a felhasználói élmény személyre szabására lesz felhasználva. Amikor Ön a Tosmart.com-on regisztrál, biztosítva lehet arról, hogy az Önnel kapcsolatos információkat bizalmasan kezeljük.”

⁴⁷⁸ A TRUSTe egy olyan nemzetközi cég, mely globálisan nyújt adatvédelemmel kapcsolatos megoldásokat és szolgáltatásokat. Ügyfelei közé tartozik többek között az Apple, Microsoft, Disney, eBay és a HP.

⁴⁷⁹ A Szövetségi Kereskedelmi Bizottság egy szövetségi állami szerv az Egyesült Államokban, mely fogyasztóvédelmi és versenyhivatali hatósági feladatokat lát el (<http://www.ftc.gov/>).

továbbiakban FTC) figyelmét felhívta a jogsértésre, mely vizsgálatot indított és bíróságon megtámadta az ügyletet⁴⁸⁰.

Az FTC keresetében azt állította, hogy a Toysmart versenyellenes és megtévesztő üzleti magatartást folytatott, mely a kereskedelemre negatív hatással volt. A Bizottság utasította a Toysmartot és keresetében kérte a bíróságot, hogy tiltsa meg a felhasználói lista eladását.

A Szövetségi Kereskedelmi Bizottság és a Toysmart egyezséget kötött, mely alapján a Toysmart eladhatta volna a felhasználói adatbázisát, viszont csak olyan kvalifikált vevőnek („qualified buyer”), aki vagy amely elkötelezett a családbarát és tisztességes üzleti politika mellett, valamint hasonló tevékenységi területen helyezkedik el és tiszteletben tartja a felhasználók jogait. A gyakorlatban ez azt jelentette, hogy csak másik online játékkereskedő cégnek adhatta volna el a Toysmart az adatbázisát.

Az egyezséggel több probléma is volt. Az egyik, hogy a Toysmart a felhasználóinak nem biztosított az „opt-out” (tiltakozási, utólagos leiratkozási) lehetőségét, továbbá az egyezségről nem kérték ki a bíróság véleményét.

Később úgy módosították a megállapodást, hogy a Toysmart eladhatta a felhasználói adatbázisát egy másik Disney leányvállalatnak (a Buena Vistának), mely a megvásárlás után rögtön megsemmisíti a listát. Ennek az elsőre ésszerűtlen és a Disney számára előnytelen üzletnek a célja az volt, hogy a felhasználók és a Disney-t bíráló jogvédők megnyugodjanak, továbbá a Toysmart hitelezői is pénzt lássanak az ügyletből.

A bíróság ítélete végül annyiban változtatta meg az egyezséget, hogy a Buena Vistának úgy kellett a listát megvásárolnia, hogy az nem kerül át hozzá fizikailag, hanem a Toysmart megsemmisíti. Tehát a Toysmartnak a listát meg kellett semmisítenie, a Buena Vistának pedig fizetnie úgy, hogy nem kapott érte semmit.

Az üggyel kapcsolatos felháborodás rávilágított az internetes kereskedelem legnagyobb gátjára: a felhasználók bizalmatlanságára.

Az üggyel kapcsolatos botrány után csökkent az Egyesült Államokban az internetes vásárlás iránti kedv, mely becslések alapján 2,8 milliárd dollár kiesést is okozhatott az internetes kereskedelem forgalmából csak 1999-ben.⁴⁸¹

Több felhasználó is pert indított internetes kereskedők ellen különböző jogalapon, melyek közül leggyakoribb a szerződésszegés volt. Szerződésszegés esetén az Amerikai Kereskedelmi

⁴⁸⁰ <http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm> (2013. 01. 10.)

⁴⁸¹ Center for Democracy and Technology 1999-es felmérése alapján becsült összeg

Kódex⁴⁸² alapján a bíróságok előtt a felhasználóknak azt kell bizonyítaniuk, hogy a kereskedők adatvédelmi irányelvei, melyeket regisztráció során elfogadtak, egy fogyasztó és vállalkozó között létrejött szerződés részének tekintendők, mely alapján szerződésszegés történt.

A második leggyakrabban alkalmazott jogalap a felperesek kereseteiben a megtévesztés volt,⁴⁸³ mely során azt kellett bizonyítaniuk, hogy az adatkezelési irányelvek hiányosak és megtévesztésre alkalmasak voltak.

Végül egyes államokban jogalapként szolgálhatott továbbá, ha az ott hatályos kereskedelmi szabályok megszegésével (pl. megtévesztő üzletpolitika, fogyasztó megkárosítása) vádolták az online kereskedőt.

A Toysmart ügy kapcsán felmerült a kérdés, hogy mit tehet a TRUSTe, ha ilyen jogsértés történik, és mennyire jelent biztonságot a tanúsítványa és pecsétje a honlapokon.

A TRUSTe gyakorlatilag három dolgot tehet, ha az ügyfeleinél jogsértést tapasztal:

1. Megfosztja az ügyfelet a TRUSTe tanúsítványtól és a pecsét használatától.
2. Az ügyféllel kötött szerződés megszegéséért bíróságon pert indít.
3. Fogyasztóvédelmi szerveknél és gazdasági versenyhivataloknál eljárást kezdeményez.

7.3.1 A tulajdonjogi és az alapjogi megközelítés

A Toysmart jogásza (és több cég jogi képviselője) amellet érveltek, hogy a személyes adatokat célszerű lenne árunak tekinteni, mellyel minden természetes személy szabadon rendelkezhetne és ellenszolgáltatásért egy megfelelő biztosítékokkal ellátott szerződésen keresztül átruházható, hasznosításra rendelkezésre bocsátható lenne (tulajdonjogi megközelítés).

A jogvédők és a bíróság szerint is ez a megközelítés teljesen téves volt, mivel a magánszféra és a személyes adatok védelme elsőbbséget élvez üzleti érdekekkel szemben (alapjogi megközelítés).

A tulajdonjogi megközelítés szerint avval, hogy az online cégek megkapnák teljes körű rendelkezésre a felhasználók személyes adatait, a felhasználóknak csupán előnyére válna, mivel több szolgáltatást és kedvezményt kaphatnának érte, mely az érintettek részére pénzben mérhető előnyt is jelenthetne.

⁴⁸² United States Uniform Commercial Code U.C.C. §1-201 (3)

⁴⁸³ Restatement (2nd) of Torts, 537. §

Az alapjogi megközelítést képviselő fél szerint ez azért téves feltevés, mert a cégek felhasználhatják a személyes adatokat célhoz kötött hirdetések elhelyezésére, és a kedvezmények nem lennének arányban a magánszféra korlátozásával.

A tulajdonjogi megközelítés abból a téves feltevésből indul ki, hogy minden személy szabadon képes belépni szerződésekbe és meghatározni annak feltételeit.

Az alapjogi megközelítés a valós életet hozza ellenérvként: az egyén (érintett, fogyasztó) a gyengébb fél, aki nincs tárgyalópozícióban a nagy vállalatokkal szemben. Az érintett döntési alternatívája a valós életben - különösen az online világban – az „elfogadom” és „elutasítom” lehetőségekre szűkül.

A személyes adatot árunak tekintők avval érveltek, hogy az adatok „adásvétele” esetén is van az érintettnek több olyan (kötelmi) jogi védelme, mint az ellenszolgáltatás elve, ellenérték arányosságának elve, továbbá a jóhiszeműség és a rendeltetésszerű joggyakorlás követelményei.

A valós életben a felsorolt védelmek azért nem működnének, mert nincsen alkupozíció, és a vállalatok a jogi osztályaikon keresztül sokkal erősebb jogérvényesítési és tárgyalási pozícióban vannak, míg egy fogyasztónak jelentős anyagi és időbeli ráfordítást jelentene egy per lefolytatása, bizonytalan eredménnyel, addig ez egy vállalatnál a jogászok mindennapi feladata.

Azért is téves út a tulajdonjogi megközelítés, mert az érintett, miután a vállalat rendelkezésére bocsátotta a személyes adatait, az Egyesült Államokban és világ országainak jelentős részében már nem tudja követni azok útját és ellenőrizni, hogy kinek a birtokában vannak, kik tekintenek bele. Tehát az érintett a „szerződészerű teljesítést” nem tudná vizsgálni.

7.3.2 A „tulajdonjogi megközelítés” enyhébb változatának gyakorlati megvalósulása

„ha egy szolgáltatásért nem fizetsz, akkor Te nem a vásárló vagy, hanem maga az áru”, olvasható az Enliken honlapján.

Az Enliken⁴⁸⁴ egy internetes tevékenységgel foglalkozó cég, melyet az Egyesült Államokban alapítottak 2011-ben, és célja, hogy a felhasználók hasznosíthassák a személyes adataikat egy

⁴⁸⁴ www.enliken.com

sajátos módszer által, mellyel a felhasználók követni tudják adataik sorsát és még pénzt is kereshetnek (vagy takaríthatnak meg).

Interneten az érintettek használják többek között a szociális hálókat, videó megosztókat, híroldalakat és sok más ingyenes webes szolgáltatást, melyeken keresztül a cégek információt gyűjtenek róluk és azokat a felhasználók személyre szabott hirdetésekre, vagy eladják más cégeknek a felhasználók háta mögött. Nyilatkozatuk szerint ezt a folyamatot akarja megfordítani az Enliken.

Az Enliken szerint a felhasználók által önkéntesen átadott internetezési szokások és információk sokkal értékesebbek a hirdetőik számára, mint a rejtetten, vagy „kéz alól” szerzett adatok tömege. Az Enliken módszere úgy működik, hogy a felhasználó feltelepít a számítógépére egy programot, mely megfigyeli a böngészési tevékenységét és azt naplózza.

A leírás alapján kizárólag olyan információkat rögzít a program, melyhez a felhasználó hozzájárult (pl.: milyen weboldalt nézett). A program a cég szerint más információkat (pl.: magánlevelezést, szenzitív adatokat) nem rögzít, csak amelyekbe a felhasználó beleegyezett.

Az Enliken üzleti partnerei (pl.: New York Times, Amazon) az Enlike programján keresztül látják, hogy a felhasználók mely oldalakat látogatják és milyenek az böngészési szokásaik, melynek ellenértékeként vásárlási kedvezményeket adnak a felhasználó részére, vagy ingyenes hozzáférést a fizetős tartalmakhoz.

A felhasználói felületen be lehet állítani, hogy milyen adatokat kíván a felhasználó megosztani. Az Enliken koncepciója a legkényesebb kérdést is felveti: normális-e, hogy a hétköznapi felhasználók „aprópénzért” rendelkezésre bocsátják a személyes adataikat, melyek útját elméletileg tudják csak követni.

Az Enliken elmondása szerint egy tiszta és átlátható helyzetet teremtenek, melyet a felhasználó irányít és ő dönti el előzetesen (opt-in), hogy milyen adatokat kíván megosztani, melyeken kívül semmilyen más információ nem hagyja el a számítógépét. Úgy vélik, hogy ezáltal megteremthetnek egy előzetes beleegyezésen alapuló hirdetési rendszert, mely a felhasználó számára hasznos és átláthatóságot biztosít, továbbá kedvező a vállalatoknak is, mert tiszta és értékes adatokat kaphatnak ahelyett, hogy kémkedniük kellene a felhasználók után.

Az Enliken szerint a módszerük különösen a nagy vállalatoknak kedvez (Apple, New York Times), mert azok hajlamosabbak tisztességesen megszerezni és kezelni adatokat, mivel sokkal szabálykövetőbben kénytelenek viselkedni. Ennek következményeképpen kevésbé alkalmaznak adathalászatot és adatvásárlást, így az ő részükre nyitja meg a személyre szabott hirdetés lehetőségét az Enliken. A vállalatok számára ez a módszer a hirdetések hatékonysága

miatt lehet vonzó, mivel az ilyen személyre szabott hirdetéseknel jelentősen nagyobb az esély arra, hogy a felhasználó a hirdetést megtekinti (CPM), vagy rákattint (CPC).⁴⁸⁵

Az Enliten programjának működését a fejlesztők olyan egyszerűre állították, hogy mindenki számára kezelhető legyen: a program beépül a böngészőbe (Internet Explorer, Mozilla Firefox, Google Chrome), és észrevétlenül működik addig, amíg nem akarnak beállításokat módosítani rajta.

7.4 Értékelő gondolatok

Az információs társadalomban a személyes adatok értéke jelentősen megnövekedett, amelynek következtében gyakran szembesülhetünk avval a helyzettel, hogy vállalatok olyan áron kerülnek felvásárlásra, amely nincsen arányban az általuk termelt bevétellel, egyértelművé téve a jogügylet célját: az adatállomány megszerzése.

Az adatkezelő személye a vállalatfelvásárlás esetében elméletileg nem változik meg, gyakorlatilag viszont igen: hiába ugyanaz a cég marad a személyes adatokért felelős szervezet, valójában az új tulajdonos irányítja és határozza meg a stratégiáját. A dolgozatom 4. fejezetében az adatkezelő meghatározásánál kitértem a több adatkezelő, valamint az adatkezelés céljának és módjának meghatározásával kapcsolatos problémákra, amely a tulajdonosváltásnál is releváns lehet, mivel a sok esetben a felvásárolt cégeknél csupán az adatkezelés módjának meghatározása marad meg.

Különösen problémásak az olyan esetek, amikor az új tulajdonos olyan változtatásokat hajt/hajtat végre az adatok kezelésén, amely szembemegy a korábbi adatkezelési gyakorlattal, és a felhasználó által elfogadott adatkezelési elveken, mint például a Whatsapp felhasználói adatainak megosztása az új tulajdonos Facebookkal.

⁴⁸⁵ A bannerek (hirdetések a honlapokon) árazása 3 elterjedt módszert követ:

Időszaki árazás: adott időszakra (általában napra vagy hónapra) fix összeget kell fizetnie a hirdetőnek a reklámjáiért. Ezen módszert csak akkor érdemes választani, ha pontosan ismertek adott oldal látogatottsági statisztikái, és így az időszaki költséget lebontva CPM-re olcsóbban kijön egy megjelenés, mint egyébként. Tisztán ezt a módszert főleg kis, magáncélú oldalak alkalmazzák, illetve elvétve olyan portálok, melyeknél titkosak a látogatottsági statisztikák (komoly oldal sosem működik kizárólag ilyen alapon).

Megjelenés alapú árazás (CPM – Cost per mil): ez a legelterjedtebb árazási típus, amikor a banner 1000 megjelenésének van egy fix díja, pl. 5000 Ft, vagyis megjelenésenként 5 forint. De szokás egyszerűn AV (Ad View), azaz megjelenés díjat is megszabni (főleg Magyarországon). Ez a két fajta megadási mód egyenértékű.

Átkattintás alapú árazás (CPC – Cost per click): a leginkább hatékony és követhető megoldás a hirdető részéről, de sajnos kevésbé elterjedt. Ekkor a hirdetőnek csak akkor kell fizetnie a hirdetésért, ha a látogatók ténylegesen rá is kattintottak, tehát „teljesítmény” alapon számolják adott reklám költségét.

A személyes adat nem egy áru, amelyet korlátlanul lehet eladni és venni, amelynek tulajdonjogáról csak úgy lemondhat az érintett, hiszen bármikor lehet olyan helyzetben, mentális, vagy anyagi okokból, hogy olyan döntést hozzon, amelyet később megváltoztatna.

Mentális ok lehet, hogy cselekménye következményeit valamiért nem tudja teljes mértékig átgondolni és mérlegelni, így például ha gyermekként hoz döntést, vagy nincsen olyan értelmi szinten, hogy a személyes adatainak sorsára gondoljon, vagy hogy egy hosszú adatvédelmi tájékoztatót megértse és átlásson, amely még egy átlag polgárnak is komoly kihívást jelenthet. Anyagi ok lehet, hogy valamiért szorult állapotba kerül, és számára a pillanatnyi csekély bevétel többet jelent személyes adatainak védelménél.

Azért is téves út a tulajdonjogi megközelítés, mert az érintett, miután a vállalat rendelkezésére bocsátotta a személyes adatait, az Egyesült Államokban és világ országainak jelentős részében már nem tudja követni azok útját és ellenőrizni, hogy kinek a birtokában vannak, kik tekintenek bele. Tehát az érintett a „szerződésszerű teljesítést” nem tudná vizsgálni.

A magyar szabályozást megvizsgálva külön választottam a cégek és a szolgáltatások adásvételének jogi hátterét, azonban a nagy online szolgáltatók esetében a cégek felvásárlása bír jelentőséggel. Mind a jogutódlás mind a szerződésátruházás esetében különösen fontos a tájékoztatási jog, hogy az érintettek élhessenek a tiltakozáshoz és törléshez való jogukkal, még az adatbázis megszerzése és az adatkezelés szabályainak esetleges megváltozása előtt.

8. Összegzés és a dolgozat új eredményei

8.1 Összegzés

A „privacy” szó jelentése a történelem során gyökeresen megváltozott és országonként eltérően fejlődött. Az ókori Európában az egyén politikai jogaitól kezdődően az Egyesült Államokban megvalósuló „én házam az én váram” megközelítésig folyamatosan formálódott.

Az adatvédelem intézményét kizárólag a magánszféra védelmén belül értelmezhetjük, míg az információs önrendelkezési jogot az adatvédelmen belül helyezhetjük el.

A magánszféra védelmére való igény, az avval kapcsolatos szokások és jogszabályok hamarabb alakultak ki, mint az adatvédelem, amelyet dolgozatomban annak történelmén és az adatvédelmi jogszabályok generációján keresztül mutattam be. A feltevés igazolásához különösen nagy segítséget jelentett Magyarország korábbi adatvédelmi biztosainak és a NAIH elnökének az állásfoglalásai, amelyek e kérdéskörben egyértelműen összezsengenek.

Az információs önrendelkezési jog és az adatvédelem gyakorlati érvényesülésén keresztül cáfoltam, hogy teljes mértékig fednék egymást.

Az önrendelkezési jog alapján megilleti az egyént az a jog, hogy döntsön a rá vonatkozó információk nyilvánosságra hozataláról, míg az adatvédelmi jog elsősorban az adatkezelőnek állít korlátokat az adatok kezelésével kapcsolatosan. Az egyén azon jogára vonatkozóan, hogy nyilvánosságra hozhasson magáról bármilyen információt, az adatvédelmi jog korlátot nem állapít meg, csupán az adatkezelőnek írja elő a jogalapokat (hozzájárulás, vagy jogszabály engedélye).

Az adatvédelem tágabb jelentését az adatbiztonság követelménye is alátámasztja: az adatvédelem része az adatbiztonság követelménye, amely alatt olyan szervezési és technikai követelményeket értünk, melynek az adatkezelő köteles eleget tenni (pl.: csak meghatározott személyek férhetnek hozzá az adatbázishoz egyéni jelszóval, vírusirtó és tűzfal telepítése).

Szabó Máté szerint is "itt egyértelműen az adatok fizikai és jogi védelmén van a hangsúly, nem pedig az önrendelkezésen, az alany döntési szabadságán".

Az Európai Unió elsődleges jogforrásaiban kitűzött egyik legfontosabb cél, a közös piac létrehozása - finomhangolásoktól eltekintve - megvalósult, mely az EU Bíróságának feladatkörére is hatással volt: egyre kevésbé fajsúlyos az alapvető szabadságok hangsúlyozása, míg az alapjogok védelme előtérbe került, amelyek között egyre nagyobb jelentőséggel bírnak

az információs társadalommal kapcsolatos jogok. Az EU Bíróságának joggyakorlatát – különösen a magánszférához való jog egyéb alapvető jogokkal való ütközését érintő ügyeket – megvizsgálva bizonyosságot nyert, hogy a magánsféra – azon belül is adatvédelem – kiemelkedő védelemben részesül.

A mindennapi gazdasági életben egyre gyakoribb, hogy a rugalmasság növelése, a pénzügyi és egyéb kockázatok csökkentése céljából a vállalatok kiszervezéseket hajtanak végre: a könyvelés, jogi képviselet és garanciális ügyintézés harmadik felekkel való megoldása mindennapossá vált.

Az alvállalkozók és a külső szolgáltatást nyújtó harmadik felek alkalmazása együtt jár avval, hogy az ügyfelek, alkalmazottak és további érintettek személyes adatai egyre több szervezethez jutnak el egy szolgáltatás megvalósítása során.

Az információs és kommunikációs technológia fejlődése megkönnyítette harmadik felek bevonását és az egymástól távol lévő szervezetek közötti kapcsolattartást.

Egyre gyakrabban merül fel a szigorodó adatvédelmi szabályok miatt, hogy a szerződés a felelősség áthárítása céljából más személyt jelöl meg adatkezelőnek, mint aki ténylegesen döntési jogosultsággal rendelkezik az adatok felett: különösen az internet világában, ahol a szolgáltatások esetén összemosódnak a szerepek, gyakran lépnek fel az oldal üzemeltetői adatfeldolgozóként, áthárítva a felhasználóra az adatkezelés felelősségét.

Még egy adatkezelő és adatfeloldozó között létrejött tiszta jogviszonyban is jogsértés esetén az adatfeldolgozó adatkezelővé válhat (pl. az adatok tárolásáért felelős adatfeldolgozó továbbküldi az adatokat harmadik félnek az adatkezelő engedélye nélkül, vagy marketing célokra használja fel).

Az adatkezelő fogalmi eleme az adatkezelés céljának és módjának a meghatározása. A két kifejezés pontos fogalmának tisztázása alapvető jelentőséggel bír: a cél megmutatja, hogy pontosan mit kell valamelyik félnek meghatároznia ahhoz, hogy adatkezelőnek tekinthessük. Az adatkezelők felelőssége a véleményem szerint egyetemleges, amelyet dolgozatomban vizsgálat alá helyeztem.

Az adatfeldolgozó két legfontosabb fogalmi eleme, hogy az adatkezelő személyétől teljesen el van különülve, és hogy az ő nevében és utasításai alapján végzi az adatfeldolgozást.

A mindennapi gazdasági életben a tipikusan adatfeldolgozással foglalkozó szervezetek és személyek (pl. adattárolást biztosító vállalat) mintaszerződésekkel rendelkeznek, amelyeket az ügyfelek (adatkezelők) jelentős része változtatás nélkül ír alá. Az adatkezelő meghatározásában fogalmi elem, hogy „meghatározza az adatkezelés célját és módját”, ám ebben az esetben az

adatfeldolgozó által előre megírt mintaszerződés kerül felhasználásra. Amennyiben a szerződés megfelel az adatvédelmi jogszabályoknak, amely által magában foglalja az adatkezelő utasítási jogkörét és az érintettek jogait, a szerződés érvényes és hatályos a felek között.

Attól, hogy az adatkezelő (pl. egy munkáltató) nincsen alkupozícióban a nála jóval nagyobb adatfeldolgozó vállalattal (pl. Apple felhő tárhelyének használata, Google levelezőrendszerén adatok küldése), ugyanúgy felelős azért, hogy olyan szerződési feltételeket fogadjon el, amelyek megfelelnek az adatvédelmi jogszabályoknak.

Az adatkezelő és az adatfeldolgozó elhatárolásának összegzéseként megállapítható, hogy a cél meghatározása fenn van tartva az adatkezelőnek: az adatfeldolgozó és más személyek nem vehetnek részt semmilyen szinten és mértékben a cél meghatározásában. A cél meghatározásában való legkisebb mértékű részvétel is az adatkezelői minőséget vonja maga után. A mód meghatározásában való részvétel már nem ennyire egyértelmű: olyan technikai és szervezési jellegű döntéseket meghozhat az adatfeldolgozó, amelyek az érintett jogaira és az adatokra nincsenek jelentős hatással. Az adatfeldolgozó az adatkezelőtől és a jogszabályoktól kapott szűk mozgástérben meghatározhatja például, hogy milyen fajta számítógépen, mely programokkal és biztonsági intézkedésekkel tárolja és dolgozza fel az adatokat, továbbá megszabhatja, hogy milyen szervezet és személyi kör végezheti a műveleteket az adatokon. Amennyiben az adatfeldolgozó az adatkezelőtől kapott és a jogszabály által megengedett határokat átlépi, adatkezelővé minősül át, annak minden kötelezettségét és felelősségét magával vonva.

Dolgozatomban több jogséten keresztül bemutatásra került, hogy az internet világa felborította az állampolgár magánszférájának részét képező felejtéshez való jog működését. Az információ, amely a 90-es évekig adatmorzsákból volt összeállítható hosszas keresőmunka árán, már elérhető bárhol, bármikor, gyorsan és ingyen, akár inkognitóban is, amelyhez különösen nagy segítséget jelentenek az internetes keresők.

A fennálló helyzet így ütközést eredményezhet az egyén személyes jogai (magánszférához való jog, felejtéshez, személye kifejlődéséhez és az újrakezdéshez való jog), a sajtószabadság és a társadalom tagjainak információhoz való joga között.

Dolgozatomban ugyanakkor a technika jelenlegi állását és az internet gyakorlati működését megvizsgálva cáfolnom kellett, hogy a felejtés joga maradéktalanul érvényesülhet, mivel az interneten jelentős számban vannak olyan jogsértő tartalmakat tároló és megosztó oldalak, amelyek ellen még nemzetközi egyezményekkel és hatósági együttműködéssel sem tudnak fellépni az illetékes hatóságok, továbbá ha egy jogsértő tartalom több szerveren elterjedt,

gyakorlatilag eltüntetni nem lehet.

A legfontosabb különbség a fizikai és az elektronikus tárolás között, hogy a fizikailag tárolt archívumokat pénzügyi megfontolásból a fenntartónak megéri megsemmisíteni, mellyel szemben az elektronikusan tárolt adatbázisokból egyes adatokat sok esetben drágább törölni, mint tárolni hagyni.

Olyan technikai módszerek jelenthetnék a megoldást, amelyek az adatkezelés kezdetétől biztosítják a felejtés jogát, a feldolgozó rendszerbe beépítve, alapvető értéként („privacy by default”), amelynek egyik módja lehetne, hogy az adatok már a felvételkor lejáratí időt kapnak, és annak leteltével névtelen adattá válnának – megszüntetve az érintettel való kapcsolatba hozhatóságot -, vagy törlődnének.

Az adatok kérelemre való eltávolításával, a felejtés jogának kérelemre való érvényre juttatásával kapcsolatosan dolgozatomban rávilágítottam, hogy nem lehet általánosságban kijelenteni, hogy az egyén felejtéshez való joga élvezne elsőbbséget, azt konkrét esetben arányossági tesztnek eleget téve lehetséges csak megállapítani, amelyre javaslatot tettem a bankszektorban bevált módszereket alkalmazva.

Dolgozatomban a hatályos jogszabályokon és az EU Bíróságának döntésein keresztül bizonyításra került, hogy az internetes keresők adatkezelőnek minősülnek.

Az internetes keresők algoritmusai folyamatosan és szisztematikusan az internet publikus információi között kutatnak (amelynek jelentős része személyes adatokat is tartalmaz), így megvalósítják az adatvédelmi irányelv által meghatározott adatkezelés fogalmát, mivel adatokat gyűjt, elemez, tárol és rendszerez, amelyeket a megfelelő kérés alapján a felhasználó részére rendelkezésre bocsát a találati eredmények között.

A kereső üzemeltetője „adatkezelőnek” minősül, mivel az irányelv alapján ő határozza meg az adatkezelés célját és módját, így az érintettnek joga van a kereső üzemeltetőjét közvetlenül megkeresni, ha a keresőmotor által kiadott találatok olyan oldalra mutatnak, amely róla személyes adatokat tartalmaz, és amennyiben az üzemeltető nem teljesíti a kérést, az érintett felkeresheti a kompetens hatóságokat annak érdekében, hogy a találatokat eltávolítsák.

Az Európai Unió Bíróságának Google Spain ítélete mérföldkő volt az érintettek jogainak védelmében, azonban részben látszattmegoldást eredményezett: nem a jogsértő tartalmat létrehozó, feltöltő és megosztó személyt, hanem a tartalomhoz legrövidebb utat biztosító szolgáltatók felelősségét veti fel, így a tartalomhoz továbbra is hozzá lehet férni, bár jóval nehezebben.

A megoldás hátránya továbbá, hogy a Google és más internetes keresők számára olyan jogokat és köteleességeket ró, melyek gyakorlására és teljesítésére nincsenek felkészülve, és az esetek jelentős részében nem is az ő kompetenciájuk lenne: egy információ hitelességéről vagy annak jogsértő tartalmáról egy ügyfélszolgálaton aligha lehet pontos döntést hozni az olyan egyértelmű helyzeteket leszámítva, mint amikor az érintett jogerős bírósági döntéssel rendelkezik. Az eljárással kapcsolatban kiemeltem a személyes ügyintézással és a közfeladatok Google-ra delegálásával kapcsolatos problémákat, alternatív megoldási javaslatokat kidolgozva oly módon, hogy a nemzeti hatóságokra se háruljon különösen nagy ügyteher, továbbá más internetes keresők és civilek is részt vehessenek a folyamatban. Az eljárások és a bírálati szempontok tökéletesítése a kulcs a felejtés jogának az érvényesítéséhez, továbbá a többi alapjoggal való ütközésének a kezeléséhez, amely különösen fontos az érintettek jogainak védelme, továbbá a véleménnyilvánítás és a sajtószabadság biztosításához.

A legtöbb Facebook által végzett adatkezelés jogalapja a felhasználó hozzájárulása, amelynek önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak, és félreérthetetlennek kellene lennie. Dolgozatomban bizonyításra került, hogy több, Facebook által végzett adatkezelés esetében a 4 feltétel egyike, vagy maga a hozzájárulás is hiányzik.

Az egyik legjelentősebb probléma a Facebook adatkezeléseinél, hogy a felhasználónak minimális kontrollja van azok felett, mivel a Facebook „mindent vagy semmit” választási lehetőséget kínál csupán az érintetteknek, akik így kénytelenek vagy elfogadni azokat, vagy a regisztrációval, felhasználással felhagyni. A „mindent vagy semmit” választási „lehetőség” az érintett hozzájárulásának az önkéntességével kapcsolatban vet fel problémákat, mivel valós alternatívája nincsen a Facebooknak, ha az érintett a különböző földrészekén élő ismerőseivel szeretne kapcsolatot tartani egy közösségi hálózaton.

A Facebook-on regisztráció során alkalmazott megoldás a legkevésbé alkalmas arra, hogy az érintett akár minimális tájékoztatáson essen át, amely megoldásra az EU Bírósága is kitér ítéletében⁴⁸⁶. Amennyiben az alapbeállítás a személyes adatok megosztása, és a felhasználó csupán utólagosan dönthet úgy, hogy nem engedélyezi azok kezelését (opt-out), nem beszélhetünk a hozzájárulás félreérthetlenségéről.

Az adatkezelési szabályzat teljes átvizsgálása után bizonyítást nyert, hogy a hozzájárulás feltételei nem teljesülnek maradéktalanul az adatkezelések jelentős részében.

⁴⁸⁶ Case C-49/11, Content Services Ltd vs. Bundesarbeitskammer, Európai Unió Bírósága, 2012.

Dolgozatomban javaslatot teszek arra nézve, milyen módon lehetne az előzetes hozzájárulást (opt-in) megvalósítani a közösségi hálózatok esetében annak érdekében, hogy annak törvényes feltételei teljesülhessenek.

A Facebook történetének, működésének és bevételeinek vizsgálatát követően a szolgáltatás fizetössé tételét a személyes adatok fokozott védelméért cserében csak korlátozottan tartom megvalósíthatónak.

A Facebook átlagos felhasználónkénti bevétele az Egyesült Államokban „túl magas” ahhoz, hogy azt könnyűszerrel ki lehessen váltani a felhasználók befizetéseivel, míg Ázsiában és a világ jelentős részén a legminimálisabb felhasználói díj befizetése sem jelenthet alternatívát. Európában evvel szemben az 1,3 eurós felhasználónkénti havi átlagbevétel nem jelentene különösebb nehézséget a felhasználók jelentős részének, különösen Nyugat-Európában.

Véleményem szerint a középút is megtalálható lenne: lehetséges lenne egy olyan megoldás alkalmazása, amellyel a felhasználónkénti bevétel 50%-ban reklámbevételből, 50%-ban a felhasználó által fizetett összegből állna össze.

A felezett összegű reklámbevételt elérhetné a Facebook viselkedésalapú reklámozás nélkül, a felhasználóról csupán alapvető adatok megszerzésével, amelyeket a felhasználó önként adna meg (pl. nem, kor, lakhely).

Így létrejöhetne egy olyan helyzet, hogy már a felhasználó regisztrálásakor alapbeállításként le lennének tiltva teljes mértékben a helymeghatározáson és viselkedésen alapuló adatgyűjtések, továbbá a felhasználó személyes adatainak kiszolgálása a Facebook partnerei részére, és csupán böngészője oldalsávjában kapna reklámokat szalaghirdetésekből, amelyeket bármilyen weboldalon is látogatóként megkapna anélkül, hogy bármilyen érzékeny információt megadna magáról.

Mivel személyes adatokat feldolgozni csak az érintett hozzájárulásával, vagy jogszabály engedélyével lehetséges (pl. az érintett létfontosságú érdekeinek a védelmében), így az olyan személyekről adatok feltöltése közösségi hálózatra, akik nem járultak hozzá, nem jogszerű.

Az érintettnek a közösségi hálózathoz való csatlakozás nélkül nehéz tudomást szereznie arról, hogy történik-e vele kapcsolatban adatkezelés, így nem tudja gyakorolni olyan jogait, mint a betekintéshez, helyesbítéshez, vagy a törléshez való jog (mivel általában nem is tud a kezelésről). A problémát súlyosbítja, hogy a közösségi hálózat üzemeltetője nem értesítheti az érintettet, mivel az kényszerűen levélnek minősülhetne az elektronikus hírközlési adatvédelmi irányelv alapján, ugyanakkor az adatvédelmi irányelv is kiemeli, hogy az érintettnek joga van

tudomást szerezni a róla folyamatban lévő adatkezelésekről.

Az érintett tudomásszerzését és a jogainak gyakorlását nem lenne szabad regisztrációhoz kötni: a közösségi hálózatoknak biztosítaniuk kellene olyan ügyfélszolgálatokat, amelyek elérhetőek lennének a honlapjukról regisztráció nélkül is, és amelyen keresztül az érintettek gyakorolhatnák jogaikat, továbbá az arcfelismerő funkció alkalmazásának egyik előnye is lehetne, hogy kiszűrhető lenne az olyan személyekről fénykép feltöltése, akik nem felhasználói a közösségi hálózatnak.

A Facebook hozzájárulással kapcsolatos hiányosságai különösen problémásak lehetnek majd az Adatvédelmi Rendelet alkalmazása során, amely mind az általános, mind a gyermekek hozzájárulásával kapcsolatban szigorúbb követelményeket támaszt, amelyeket a fejezetben bemutattam.

A Facebook életkorhatára miatt a gyermekek jelentős része hamis adatot ad meg életkoráról: az Egyesült Államokban 2010-ben a 14 évesek 78 %-a, a 13 évesek 62 %-a, a 12 évesek 46 %-a használta a szociális hálózatot.

A gyermekek biztonságát és személyes adatait több módon is védhetnék a közösségi hálózatok: célszerű lenne, ha a 18 éven aluliak esetében nem engedélyeznék a közösségi hálózatok a különleges adatok megadását regisztráció során, mivel többek között a vallással és a politikai hovatartozással kapcsolatos véleményeik még kiforratlanok, azok visszaélésekre adhatnak okot. Fontos lenne továbbá, hogy a közösségi hálózat megfelelő módon ellenőrizze a felhasználók valódi életkorát, amelyre több technikai megoldás is rendelkezésre áll.

A felhasználók által feltöltött személyes adatok között különösen jelentős szerepet töltenek be a különleges adatok: a felhasználó adatlapjával kapcsolatosan a Facebook már a regisztráláskor rákérdez olyan szenzitív információkra, mint a politikai vagy vallási nézet. A különleges adatok a közösségi hálózatokon kizárólag az érintett kifejezett hozzájárulásával kezelhetőek, vagy ha ő maga hozza azokat nyilvánosságra.

A feltöltött képekkel kapcsolatban a jogi helyzet nem ennyire egyértelmű: a képekből is kiderülhetnek olyan különleges adatok az érintettekről, mint a vallásuk, politikai nézetük, etnikumuk, vagy akár a betegségük (pl. egy politikai gyűlésen készült fényképfelvétel egyértelműen kifejezheti résztvevők politikai nézeteit).

Az arcfelismerő szoftver az arc speciális tulajdonságai alapján abból egy mintát generál, benne a legfontosabb koordinátákkal (mint pl.: szemek, orr, száj és fül távolsága egymástól). Az ehhez szükséges információkat a felhasználó profilképeiből szerzi meg és olyan képekből, melyeken

a felhasználó meg lett jelölve.

2012-ben a Facebook megszerezte a face.com-ot, amely egy arcfelismeréssel foglalkozó cég, technológiájuk olyan szintű fejlettséggel bír, hogy képes az arcok felismerésére rossz fényviszonyok és képminőség esetén: még a szemüveg, smink, Halloween jelmez sem jelent akadályt feladata elvégzésében. A Facebook fotó könyvtárában 2013 szeptemberében 350 milliárd kép volt, amely naponta 350 millióval növekszik. Semmilyen szervezet a Világon nem rendelkezik ekkora adatbázissal: a Flickr 10 milliárd fotóval rendelkezik és 3,5 milliót töltenek fel naponta. A kormányok is csupán az igazolványképekkel, továbbá az igazságügyi és titkosszolgálati tevékenységükből eredő adatbázissal rendelkeznek.

Kijelenthető, hogy az arcfelismerő technológia első korlátja (a megfelelő adatbázis hiánya) kiküszöbölésre került a Facebook adatbázisával. A feldolgozás megfelelő sebességének elérése pedig csak idő kérdése a felhő alapú technológiának, az internet és a szerverek feldolgozási sebességének köszönhetően.

Dolgozatomban az arcfelismerésen túl rávilágítottam továbbá a harmadik oldalak által alkalmazott, Facebook fiókkal történő bejelentkezés adatvédelmi aggályaira.

A hiányosságok ellenére a Privacy Shield komoly előrelépés a Safe Harbor után, amelynek a gyakorlati megvalósulása fogja megmutatni az igazi erejét és gyengeségeit: az amerikai kormány valóban felhagy-e a tömeges adatgyűjtéssel, az ombudsman személyének lesz-e valós súlya, továbbá a programban résztvevő szervezeteken milyen precizitással és intenzitással kéri számon a Privacy Shield rendelkezéseit.

A Facebook elsők között vette igénybe a Privacy Shield-et a személyes adatok küldésére, azonban véleményem szerint a felhasználók tájékoztatása és a Privacy Shield-ben előírt követelmények teljesítése nem teljes mértékig megfelelő: az adatok eredeti céljától kezelése esetén a kompatibilitás az elsődleges és a másodlagos célok között vitatható, továbbá a különleges adatok esetében előírt előzetes hozzájárulás is nehezen igazolható, mivel a Privacy Shield elfogadása óta elkülöníthető hozzájárulást nem kért ezzel kapcsolatban a felhasználóktól. Hasonló a helyzet a Facebook vállalatcsaládon belül és más harmadik felekkel való adatmegosztása esetén.

Az üzleti életben egyre gyakoribb jelenség, hogy vállalatok olyan áron kerülnek felvásárlásra, amely nincsen arányban az általuk termelt bevétellel, sok esetben egyértelművé téve a jogügylet célját: a felhasználók személyes adatainak megszerzése. Az adatkezelő személye a vállalatfelvásárlás esetében elméletileg nem változik meg, gyakorlatilag viszont igen: hiába

ugyanaz a cég marad a személyes adatokért felelős szervezet, valójában az új tulajdonos irányítja és határozhatja meg a stratégiáját. A dolgozatomban 4. fejezetében az adatkezelő meghatározásánál kitértem a több adatkezelő, valamint az adatkezelés céljának és módjának meghatározásával kapcsolatos problémákra, amely a tulajdonosváltásnál is releváns lehet, mivel a sok esetben a felvásárolt cégeknél csupán az adatkezelés módjának meghatározása marad meg.

Különösen problémásak az olyan esetek, amikor az új tulajdonos olyan változtatásokat hajt/hajtat végre az adatok kezelésén, amely szembemegy a korábbi adatkezelési gyakorlattal, és a felhasználó által elfogadott adatkezelési elveken, mint például a Whatsapp felhasználói adatainak megosztása az új tulajdonos Facebookkal.

A személyes adat nem egy áru, amelyet korlátlanul lehet eladni és venni, amelynek tulajdonjogáról csak úgy lemondhat az érintett, hiszen bármikor lehet olyan helyzetben, mentális, vagy anyagi okokból, hogy olyan döntést hozzon, amelyet később megváltoztatna.

A magyar szabályozást megvizsgálva különválasztottam a cégek és a szolgáltatások adásvételének jogi hátterét, azonban a legnagyobb online szolgáltatók esetében a cégek felvásárlása bír jelentőséggel. Mind a jogutódlás mind a szerződésátruházás esetében különösen fontos a tájékoztatási jog, hogy az érintettek élhessenek a tiltakozáshoz és törléshez való jogukkal, még az adatbázis megszerzése és az adatkezelés szabályainak esetleges megváltozása előtt.

Napjainkban az állampolgár számára leszűkült a döntés lehetősége a tekintetben, hogy részt vesz-e a digitális életben: az egyetemeken elektronikus portáljain és munkahelyi csoportokban zajló információáramlás megkívánja a részvételt, komoly hátrányba kerülhet az érintett az említett rendszerek használata nélkül.

A döntési lehetőség csökkenését jelenti továbbá, hogy az egyes szolgáltatások területén monopolhelyezethez közeli állapot alakult ki a digitális világban: szociális hálózatok terén a Facebooknak nem létezik globális szinten vetélytársa, a Windows mellett a többi operációs rendszer eltölpül, a kereső szolgáltatások közül továbbra is a Google a legerősebb és legjobb találati aránnyal rendelkező.

Az említett szolgáltatók monopolhelyezete nem csupán versenyjogi szempontból lehet kérdéses, hanem adatvédelmi szempontból is aggályosnak tekinthető, mivel nagyobb mennyiségű és arányaiban több különleges adatot kezelhetnek (pl. vásárlási szokások, rokoni és kapcsolati hálók), mint egyes államok.

Véleményem szerint a gyakorlatilag monopolhelyzetben lévő adatkezelők szabályozása és az

érintett védelme a fogyasztóvédelmi megoldásokhoz hasonlóan valósítható meg. Pontosan meg kell határozni, hogy az adatkezelők mit tehetnek az állampolgárok adataival, továbbá az egyoldalúan módosított és hátrányos felhasználói feltételek ellen ugyanolyan szankciók lennének szükségesek, mint például egy áram-, vagy távközlési szolgáltató esetében.

A monopolhelyzet mellett különösen jelentős a „virtualizálódás” jelensége, mely által az egyén egyre több emberrel és szervezettel tart kapcsolatot teljes személytelenséggel, mely fordítva is igaz: a döntéshozó szervek (pl. hivatalok) felé az egyén csupán egy adathalmazként jelenik meg. A két folyamat következtében fontos különösen, hogy az egyén kontrollal rendelkezessen a külvilág felé áramló - hozzá kapcsolható - adatokról, mivel azok határozzák meg az életének egyre jelentősebb részét.

A technológia fejlődésének köszönhetően világunk leszűkült, amelynek gazdasági és magánéleti előnyeit minden nap élvezzük, ám evvel együtt a magánszféránk is csökkent, amelyet a jogalkotónak és jogalkalmazónak is védenie kell, különben a személyes adataink könnyen üzleti haszonszerzés tárgyává, vagy visszaélés eszközévé válhatnak.

8.2 Új eredmények

1. A magánszféra, az adatvédelem és az információs önrendelkezési jog kapcsolata számos nemzetközi és hazai kutatás tárgya volt már, azonban dolgozatomban a történeti fejlődésükön és dogmatikai elemzésükön túl online környezetben elhelyezve tekintetem át az érvényesülésüket: a közösségi hálózatok és internetes keresők adatkezeléseire és jogsértéseire adott jogalkotói, jogalkalmazói és társadalmi válaszokon keresztül jutottam el az alábbi eredményekhez.

Az adatvédelem a magánszféra védelmén belül helyezhető el, míg az információs önrendelkezési jog és az adatvédelem nem egyeznek meg teljesen egymással, azonban átfedés van közöttük.

Dolgozatomban bizonyításra került az információs önrendelkezési jog sorvadása, mivel az egyént egyre kevésbé illeti meg a választás lehetősége a tekintetben, hogy részt vesz-e a digitális életben (pl. munkahelyi és baráti csoportok a Facebookon, dokumentumok közös használata a Google rendszerén munka- és osztálytársakkal, ETR, Neptun stb.). A munka, tanulás és magánélet során komoly hátrányokkal jár, ha az egyén információs önrendelkezési jogával élve nem vesz részt az említett kommunikációs csatornák használatában.

Az információs önrendelkezési jog gyengülésével párhuzamosan az adatvédelmi jog erősödésére és „elközjogiasodására” mutattam rá dolgozatomban, mivel az egyén védelemre szorul az egyre nagyobb és monopolhelyzetben lévő adatkezelőkkel szemben.

2. Az EU Bíróságának joggyakorlatát – különösen a magánszférához való jog más alapvető jogokkal való ütközését érintő ügyeket - megvizsgálva bizonyosságot nyert, hogy a magánszféra – azon belül is az adatvédelem - kiemelkedő védelemben részesül, akár az áruk, tőke és szolgáltatások szabad áramlásával szemben is.

3. Dolgozatomban tisztáztam az adatkezelő és az adatfeldolgozó elhatárolását a felhőszolgáltatók, közösségi hálózatok és internetes keresők működése során. Az adatok kérelemre való eltávolításával, a felejtés jogának kérelemre való érvényre juttatásával kapcsolatosan dolgozatomban rávilágítottam, hogy nem lehet általánosságban kijelenteni, hogy az egyén felejtéshez való joga élvezne elsőbbséget, azt konkrét esetben arányossági tesztnek eleget téve lehetséges csak megállapítani, amelyre javaslatot tettem a bankszektorban bevált

módszereket alkalmazva. Az eljárással kapcsolatban kiemeltem a személyes ügyintézésrel és a közfeladatok Google-ra delegálásával kapcsolatos problémákat, alternatív megoldási javaslatokat kidolgozva oly módon, hogy a nemzeti hatóságokra ne háruljon különösen nagy ügyteher, továbbá más internetes keresők és civilek is részt vehessenek a folyamatban. A megoldások úszerű megközelítést jelentenek a felejtés jogának érvényesítéséhez.

4. A dolgozat kifejezetten hiánypótló a Facebook hozzájárulással kapcsolatos problémáinak vizsgálatával, amely során bizonyításra került, hogy több, Facebook által végzett adatkezelés esetében a hozzájárulás feltételei (önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak és félreérthetetlennek kellene lennie) nem teljesülnek maradéktalanul, vagy maga a jogalap is hiányzik.

Bizonyítottam a célhoz kötöttség sérelmét több Facebook által végzett adatkezelés esetében, továbbá javaslatokat tettem avval kapcsolatban, hogy milyen módon lehetne azokat orvosolni, Dolgozatomban újdonságként egy olyan megoldás megvalósítását vetettem fel, amely során a bevételük 50%-át tenné ki a felhasználó befizetése, míg a maradék 50%-ot adatbányászat nélküli „szokásos” reklámokkal is elérhetné a szolgáltató. A „félíg fizetős” megoldás egy opció lenne, amellyel azon felhasználók élhetnének, akik hajlandóak áldozni viselkedés alapú reklámozás nélküli rendszer használatáért.

A részben fizetős, magánszférát erősebben védő megoldás megvalósíthatóságát a Facebook régiónkénti bevételeivel támasztottam alá, vagy vettem el.

Így létrejöhetne egy olyan helyzet, amellyel már a felhasználó regisztrálásakor alapbeállításként le lennének tiltva a helymeghatározáson és viselkedésen alapuló adatgyűjtések, továbbá a felhasználó személyes adatainak kiszolgálása a Facebook partnerei részére, és csupán böngészője oldalsávjában kapna reklámokat, amelyek bármilyen weboldal böngészése során megjelennek anélkül, hogy információt adna meg magáról.

6. A személyes adatok megszerzése vállalatfelvásárlások által nem túl hangsúlyos, sem a magyar, sem az angol nyelvű jogirodalomban. A probléma megközelítése aktuális és újszerű, mivel a WhatsApp adatkezelésének megváltozása a Facebook általi felvásárlás következtében jelenleg is vizsgálat alatt áll több európai adatvédelmi hatóság által, továbbá a Privacy Shield megvalósulása folyamatban van, amellyel az uniós állampolgárok személyes adatai eljuthatnak a felvásárlással érintett legnagyobb vállalatokhoz.

Köszönetnyilvánítás

Végül, de nem utolsósorban szeretnék köszönetet mondani Paczolay Péter Professzor Úrnak, aki abban a megtiszteltetésben részesített, hogy elvállalta a dolgozatom témavezetését, Szőke Gergely Adjunktus Úrnak, az SZTE ÁJTK Politológiai Tanszék és Doktori Iskola összes munkatársának és mindazoknak akik véleményükkel hozzájárultak a dolgozatban megfogalmazott következtetések levonásához.

Irodalom

Szakirodalmi források

Alan Westin: Privacy and Freedom, New York: Atheneum, 1967.

Balogh Zsolt György - Polyák Gábor - Rátai Balázs - Szőke Gergely László: Munkahelyi adatvédelem a gyakorlatban, Infokommunikáció és jog, 2012. (9. évf.) 50. sz. 97.

Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski, and Maša Galič: A Typology of Privacy, 2016. 09. 22.

Bíró Gyula: Kriminalisztika, Debreceni Egyetem ÁJK. Lícium-ART Könyvkiadó Kft., Debrecen, 2010.

Bocsok Viktor, Boldizs Péter, Loós Csaba, Major Tamás: A dolgok internete – technológiai háttér, információbiztonsági és adatvédelmi aspektusok, Infokommunikáció és Jog, 2015. 2-3.

Bodzási Balázs: A Ptk. hatálybalépése után felmerült gazdasági igények hatása, Fontes Iuris: Az Igazságügyi Minisztérium Szakmai Folyóirata, 1 (3-4). 2015.

Brad and Debra Schepp: How find a job on LinkedIn, Facebook, MySpace, Twitter and other social networks, New York, 2012.

Brian Leiter: Cleaning Cyber-Cesspools: Google and Free Speech, Harvard University Press, 2010.

Bunny Sandefur: The best practice of forgetting, Emory International Law Review, Vol. 30 Issue 1, 2015.

C-491/01 Queen v. Secretary of State for Health, ex parte British American Tobacco (Inv) Ltd & Imperial Tobacco Ltd, 2002. 12. 10.

Carolyn Abram: Welcome to Facebook, everyone, The Facebook Blog, 2006. 09. 26.

Caitlyn Kuhs: Need for Informed Consent in the Age of Ubiquitous Human Testing, Loyola of Los Angeles Law Review Vol. 49. 2016.

Cesare Bartolini, Lawrence Siry: The right to be forgotten in the light of the consent of the data subject, Computer Law and Security Review 32. 2016. 223-224.

Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176 final Brussels, 12.7.2016.

Csiky András, Jambrik Gergely: Online szolgáltatások átruházásával kapcsolatos adatvédelmi kérdések és a követeléskezeléssel kapcsolatos adatkezelés, Infokommunikáció és jog, 2014.

Daniel J. Solove – Paul M. Schwartz: Privacy, Information and Technology, Wolters Kluwer Law & Business, New York, 2011.

Daniel J. Solove, Paul M. Schwartz - Privacy Law Fundamentals, 2015.

Daniel J. Solove: Nothing to Hide, The False tradeoff between Privacy and Security, Yale University Press, New Haven & London, 2011.

Daniel J. Solove: Understanding Privacy, Harvard University Press, 2008.

David Flaherty: Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, U.S.: The University of North Carolina Press. 1989.

David Lindsay: The right to be forgotten in European Data Protection Law, in: Emerging Challenges in Privacy Law - Comparative Perspectives, 2014.

Domokos Márton, Polefkó Patrik: Egy bírósági döntés következményei - avagy az Európai Bíróság ún. Schrems döntésének hatásai, a Safe Harbor sorsa és a felmerülő kérdések az adatvédelem területén, Infokommunikáció és Jog, 2015. 4. szám

Edward Lee: Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten, UC Davis Law Review, Vol 13. 2015.

Edward P. Sisk: Technical Difficulties: Protecting Privacy Rights in the Digital Age, Criminal and Civil Confinement Vol. 42. 2016.

Eli Pariser: The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think, 2011.

Emmanouil Bougiakiotis: The enforcement of the Google Spain ruling, International Journal of Law and Information Technology, 2016, Vol. 24

Eszteri Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései, Infokommunikáció és Jog, 2015. 2-3.

EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance, Chris Connolly, Galexia, Strasbourg, October 7. 2013.

F. Ható Katalin: Adatbiztonság, adatvédelem, SZÁMALK Kiadó, Budapest, 2001.

Farnell, Lewis R.: Greek Hero Cults and Ideas of Immortality. Kessinger Publishing, 2004.

Finszter Géza: A bűnügyi nyilvántartások helyzete és fejlesztési lehetőségei. In: Kriminológiai tanulmányok, 2006. 43. köt.

Frank Pasquale: Asterisk Revisited: Debating a Right of Reply on Search Results, Journal of Business and Technology Law, Volume 3, Issue 1, Article 5. 2008. 85.

Gyenei Laura: Újabb kihívások az uniós emberi jogi bírászkodás területén, Iustum Aequum Salutare II. 2006/3–4.

Henry Farrell and Abraham Newman: The Transatlantic Data War, Europe Fights Back Against the NSA, Foreign Affairs, 2016. 01.

Horváth-Egri Katalin: A kötelező szervezeti szabályok (Binding Corporate Rules, BCR) és az együttműködési eljárás lehetőségei, Infokommunikáció és Jog, 2015. 4. szám

Imran Naseem: Facebook Cash Manuscript, 2012.

Jane R. Bambauer: All Life Is an Experiment. (Sometimes It Is a Controlled Experiment.), Loyola University Chicago Law Journal Vol. 47. 2016.

Janet Lowe: Secrets of the World's Greatest Billionaire Entrepreneurs, Sergey Brin and Larry Page, John Wiley & Sons, Inc., 2009, 250-270.

John Battelle: Keress, HVG Kiadó Zrt, Budapest, 2006.

John Haydon: Facebook Marketing for Dummies, Published by: John Wiley & Sons, Inc, 2013.

Jordan D. Brougher: The right to be forgotten: applying European privacy law to American electronic health records, Indiana Health Law Review Vol. 13:2, 2016.

Jóri András: Adatvédelmi kézikönyv, Osiris Kiadó, Budapest, 2005.

Jóri András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2009.

Julia Kerr: What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What It Means for the Future of the Right to be Forgotten, Chicago Journal of International Law, Volume 17, Number 1 Article 7, 2016.

Julia Powles: The Case That Won't Be Forgotten Loyola University of Chicago Law Journal 583, 2015.

Justin Levy: Facebook Marketing (third edition), Que Publishing, Indianapolis, 2012.

Lenkovics Barnabás - Székely László: A személyi jog vázlata, Eötvös József Könyvkiadó, Budapest, 2001.

Késmárki-Mészáros Gyöngyi: A szerződésátruházás jogintézményének rövid bemutatása, Themis, 2013.

Lothar Determann: Determann's Field Guide to International Data Privacy Law Compliance, Edvard Elgar Publishing Limited, 2012.

Majtényi László: Adatvédelem, információszabadság, Alkotmány- és Jogpolitikai Intézet, Budapest, 1997.

Maksó Bianka: Kötelező szervezeti szabályozás – az Infotv. legújabb adatvédelmi eszközének bevezetéséről, Infokommunikáció és Jog, 2015. 4. szám

Mező István: Személyes adatok védelme az Európai Unió jogában és Magyarországon, Miskolc, 2007.

Nagy Ferenc: Anyagi büntetőjog, általános rész II, Szeged, 2014.

Navratyil Zoltán: Internet és szólásszabadság: a „felejtés” joga és a „feledésbe merüléshez” való jog, Iustum Aequum Salutare, XI. 2015. 2.

Orla Lynskey: From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection 's identity Crisis, in: European Data Protection: Coming of Age, Springer Science+Business Media Dordrecht, Brussels, 2013.

Paczolay Péter: Az emberi jogok egyetemessége, in: Ünnepi Kötet Lábady Tamás 70. születésnapja alkalmából, szerk.: Csehi Zoltán – Koltay András – Landi Balázs – Pogácsás Anett, Pázmány Press, Budapest, 2014.

Paul M. Schwartz: Privacy and Democracy in Cyberspace, 52 Vanderbilt Lawreview, 1999.

Paulan Korenhof, Jef Ausloos, Ivan Szekely, Meg Ambrose, Giovanni Sartor, Ronald Leenes: Timing the Right to Be Forgotten, A study into “time” as a factor in deciding about retention or erasure of data, Computers, Privacy and Data Protection Conference 2014.

Pázmándi Kinga, Pétervári Kinga, Sárközi Tamás, Verebics János: Üzleti jog az új Polgári Törvénykönyv után, Typotex Elektronikus Kiadó, Budapest 2014.

Péterfalvi Attila: Adatvédelem és információszabadság a mindennapokban, HVG-ORAC Lap-Könyvkiadó Kft., Budapest, 2012.

Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (1. rész), Infokommunikáció és Jog, 38. szám

Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (2. rész), Infokommunikáció és Jog, 40. szám

Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (3. rész), Infokommunikáció és Jog, 41. szám

Polefkó Patrik: Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (4. rész), Infokommunikáció és Jog, 42. szám

Rachel L. Finn, David Wright, Michael Friedewald: Seven Types of Privacy, European Data Protection: Coming of Age, 2013.

Roger Clarke, “Introduction to Dataveillance and Information Privacy, and Definitions of Terms”, Xamax Consultancy, Aug 1997. <http://www.rogerclarke.com/DV/Intro.html>

Rebecca Lipman: Online Privacy and the Invisible Market for Our Data, Penn State Law Review, 2016.

Ross E. Campbell: Comment, Progress in Involuntary Commitment, 49 WASH. L. REV. 617, 640 (1974).

Rotem Medzini: Prometheus Bound: An Historical Content Analysis of Information Regulation in Facebook, ew University of Jerusalem, Faculty of Social Sciences, School of Public Policy, Students; Haifa Center for Law and Technology, 2016.

Samuel D. Warren and Louis Brandeis: The Right To Privacy, Harvard Law Review, 1890.

Sebastian Schweda: Right to Be Forgotten Also Applies to Online News Archive, Supreme Court Rules, European Data Protection Law Review Volume 1, Issue 4. 2015.

Shaniqua Singleton, Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD, 44 Ga. J. Int’l & Comp. L. 2015.

Shaniqua Singleton, Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD, 44 Ga. J. Int’l & Comp. L. 2015.

Simon Éva: Egy XIX századi tanulmány margójára, in: Információs Társadalom, szerk.: Simon Éva, Gondolat Kiadó, 2005. évfolyam 2. szám

Sionaidh Douglas Scott: A tale of two courts: Luxemburg, Strasbourg and the growing European human rights acquis. Common Market Law Review, 2006/43.

Szabó Máté Dániel: Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival, in: Információs Társadalom, szerk.: Simon Éva, Gondolat Kiadó, 2005. évfolyam 2. szám

Székely Iván, Jog ahhoz, hogy elfelejtsenek és töröljenek, Információs társadalom 13. évf. 3-4. sz. 2013.

Székely Iván: A felejtés joga az információs társadalomban, Információs Társadalom 10. évf. 3-4. sz. 2010.

Szőke Gergely László: Az érintettek és az adatkezelők adatvédelmi attitűdje – európai tapasztalatok, Infokommunikáció és Jog, 2014. 4.

Szőke Gergely László: Az európai adatvédelmi jog megújítása, tendenciák és lehetőségek az önszabályozás területén, doktori értekezés, Pécs, 2014.

Takis Trimidas: The ECJ and the Draft Constitution: A Supreme Court for the Union? Federal Trust Constitutional Online Paper 05/04

[<www.fedtrust.co.uk/uploads/constitution/05_04.pdf>](http://www.fedtrust.co.uk/uploads/constitution/05_04.pdf)

Tatay Eszter: A szűrőbuborék hatása a tájékozottsághoz való jogra, Infokommunikáció és Jog, 2015. 2-3.

Tim Cowen: Big Data as a Competition Issue: Should the EU Commission's Approach Be More Careful? European Networks Law & Regulation Quarterly Vol. 4. 2016. 21.

Tom Taulli: How To Create The Next Facebook, Apress, 2012.

Vékás Lajos (szerk.): A Polgári Törvénykönyv magyarázatokkal, CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2013.

Viktor Mayer-Schönberger: Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, Princeton and Oxford, 2009.

Viktor Mayer-Schönberger: Delete: The Virtue of Forgetting in the Digital Age, Princeton: Princeton University Press, 2009.

W. Gregory Voss, Céline Castets-Renard: Proposal for an International Taxonomy on the Various Forms of the 'Right to Be Forgotten': A Study on the Convergence of Norms, 14 Colorado Technology Law Journal 281 (2016) (Issue 14.2), 2016.

Xavier Tracol, EU–U.S. Privacy Shield: The saga continues, Computer Law and Security Review Vol. 32. 2016. 776.

Xavier Tracol: “Invalidator” strikes back: The harbour has never been safe, Computer Law and Security Review Vol. 32. 2016. 356-358.

Online Források

Amanda Lenhart, Kristen Purcell, Aaron Smith, and Kathryn Zickuhr: “Social media & mobile Internet use among teens and young adults,” Pew Internet and American Life Project report, 2010. 02. 03.

http://www.pewinternet.org/~media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplevels.pdf

Andrew Leonard: The Internet’s next victim: Advertising, Salon, 2012. 09. 02.

http://www.salon.com/2013/09/02/the_internets_next_victim_advertising/

Angelina Bouc: Hacker Community Raises Reward Money for Khalil Shreath After Facebook Denial, 2013. 08. 21. <http://guardianlv.com/2013/08/hacker-community-raises-reward-money-for-khalil-shreath-after-facebook-denial/>

Az adatvédelem története, Adatvédelmi biztos már megszűnt honlapjának legutolsó mentett változata, 2011. 12. 31.

Barbara Brandtner - Allan Rosas: Human Rights and the External Relations of the European Community: An Analysis of Doctrine and Practice, in: European Journal of International Law, 14 April 2014. (<http://ejil.oxfordjournals.org/>)

Ben Popper: Facebook now has more than a billion mobile users every month, The company is making nearly twice as much per user as it did one year ago, 2014. 04. 23.

<http://www.theverge.com/2014/4/23/5644740/facebook-q1-2014-earnings>

Blackstone's Commentaries on the Laws of England, Book the Fourth - Chapter the Sixteenth: Of Offenses Against the Habitations of Individuals

Brendan Van Alsenoy, Valerie Verdoodt, Rob Heyman, Jef Ausloos and Ellen Wauters: From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms, 2015

Carol Huang: Facebook and Twitter key to Arab Spring uprisings: report, TheNational, 2011.

06. 06. <http://www.thenational.ae/news/uae-news/facebook-and-twitter-key-to-arab-spring-uprisings-report#ixzz3AB7jvokd>

Complaint against Facebook by the Federal Trade Commission, Commissioners: Jon Leibowitz, Chairman, J. Thomas Rosch, Edith Ramirez, Julie Brill

<http://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>

Dan Levine; McBride, Sarah: Facebook to pay \$10 million to settle suit. Reuters, 2012. 06.

16. <http://www.reuters.com/article/2012/06116/net-us-facebook-settlement-idUSBRE85FON120120616>

Daniel Ionescu: Facebook Adds Facial Recognition to Make Photo Tagging Easier.

PCWorld, 2010. 12. 16.

http://www.pcworld.com/article/213894/facebook_adds_facial_recognition_to_make_photo_tagging_easier.html

EC study on implementation of data protection directive (Study Contract ETD/2001/B5-3001/A/49)

comparative summary of national laws by Douwe Korff (consultant to the European Commission), Human Rights Centre, University of Essex, Cambridge, 2002. 09, 80.

Eurostat: Az információs társadalomra vonatkozó statisztika – háztartások és magánszemélyek (letöltés dátuma: 2016. április 25.)

http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals/hu

Eszter Hargittai, Jason Schultz, and John Palfrey: Why parents help their children lie to Facebook about age: Unintended consequences of the ‘Children’s Online Privacy Protection Act, in: First Monday, Volume 16, 2011. 11. 07.

<http://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075>

Federal Trade Commission: Operators of Online "Virtual Worlds" to Pay \$3 Million to Settle FTC Charges That They Illegally Collected and Disclosed Children's Personal Information, 2011. 05. 12. <http://www.ftc.gov/news-events/press-releases/2011/05/operators-online-virtual-worlds-pay-3-million-settle-ftc-charges>

Facebook Partners With Shadowy ‘Data Brokers’ To Farm Your Information, Sherbit Blog, April 16, 2015

<https://www.sherbit.io/facebook-partners-with-shadowy-data-brokers-to-farm-your-information/>

Graham Cluley, Facebook changes privacy settings for millions of users facial recognition is enabled. Sophos naked security, 2011. 06. 07.

<http://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/>

Heather Timmons: China will unblock Facebook, Twitter and The New York Times to boost its new free trade zone, Quartz, 2013. 09. 24.

Jason Mick: Google: Yes, we "Read" Your Gmail, 2013. 08. 15.

<http://www.dailytech.com/Google+Yes+we+Read+Your+Gmail/article33184.htm#sthash.55NWTmdH.DzspukoP.dpuf>

John Paul: "Facebook Hits 1 Trillion Pageviews", ReadWriteWeb. 2011. 08. 24.
http://web.archive.org/web/20110911044951/https://www.readwriteweb.com/archives/facebook_hits_1_trillion_pageviews.php

Joshua Gardner: Computer expert hacks into Mark Zuckerberg's Facebook page to expose the site's vulnerability after his security warnings were dismissed, 2013. 08. 18.
<http://www.dailymail.co.uk/news/article-2396628/Mark-Zuckerbergs-Facebook-page-hacked-Khalil-Shreateh-expose-site-vulnerability.html>

Mark Milian (January 19, 2012). 60 apps launch with Facebook auto-share. CNN.
<http://www.cnn.com/2012/01/18/tech/social-media/facebook-actions-apps/index.html>

Mary Madden, Aaron Smith: Reputation Management and Social Media. Pew Internet, 2010. 05. 26. <http://pewinternet.org/Reports/2010/Reputation-Management/Part-2/Attitudes-and-Actions.aspx>

Mernyó Ferenc: Családi állapota: halott, Népszabadság online, 2010. 07. 24. http://nol.hu/tud-tech/csaladi_allapota_halott

Passport failure shows the folly of Microsoft's ways, Zdnet, 2005. 01. 04.
<http://www.zdnet.com/passport-failure-shows-the-folly-of-microsofts-ways-3039183062/>

Pepitone Julianne: Facebook settles FTC charges over 2009 privacy breaches. CNN, 2011. 11. 29. http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.html

Robyn Peterson: Who Owns Your Identity on the Social Web? Mashable, 2011. 10. 11.
<http://mashable.com/2011/10/21/web-identity/>

Sean Lane, et al. v. Facebook, Inc., Blockbuster Inc., Fandango Inc., Hotwire, Inc., STA Travel Inc., Overstock.com, Inc., Zappos.com, GameFly, Inc.

Segall, Laurie (March 23, 2012). Facebook strips 'privacy' from new 'data use' policy explainer. CNN Money. <http://money.cnn.com/2012/03/22/technology/facebook-privacy-changes/index.htm>

Jogszabályok, határozatok

Az Európai Unió Alapjogi Chartája

Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. 05. 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről

Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól ("Elektronikus kereskedelemről szóló irányelv")

Az Európai Parlament és a Tanács 2001/29/EK irányelve (2001. május 22.) az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolásáról

Az Európai Parlament és a Tanács 2004/48/EK irányelve (2004. április 29.) a szellemi tulajdonjogok érvényesítéséről

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)

Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (1995. október 24.)

Az Európai Unió Tanácsának 93/13/EGK irányelve (1993. április 5.) a fogyasztókkal kötött szerződésekben alkalmazott tisztességtelen feltételekről

1949. évi XX. törvény, a Magyar Köztársaság Alkotmánya

Magyarország Alaptörvénye

1959. évi IV. törvény a Polgári Törvénykönyvről

1987. évi XI. törvény a jogalkotásról

1999. évi LXXII. törvény a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

1993. évi LIX. törvény az állampolgári jogok országgyűlési biztosáról

1995. évi LXV. törvény az államtitokról és a szolgálati titokról

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

1996. évi CXII. törvény (Hpt.) a hitelintézetekről és a pénzügyi vállalkozásokról

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

2001. évi CXX. törvény (Tpt.) a tőkepiacról

2007. évi CXXXVIII. törvény (Bszrt.) a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2013. évi V. törvény, a Polgári Törvénykönyvről

2/1990. (II. 18.) AB határozat

8/1990. (IV. 23.) AB határozat

20/1990. (X. 4.) AB határozat

5/1991. (IV. 13.) AB határozat

15/1991. (IV. 13.) AB határozat

34/1992. (VI. 1.) AB határozat

46/1995. (VI. 30.) AB határozat

84/1995. (VII. 6.) OGY határozat

Legfelsőbb Bíróság 1/2008. PJE határozat

2043/2009. PEH

361/2009 (XII. 30) Kormányrendelet a körütekintő lakossági hitelezés feltételeiről és a hitelképesség vizsgálatáról

BVerfG 65, 1, („Volkszählungsurteil”)

BDT2002. 692.

BH2011. 248.

A Fővárosi Ítéltábla Polgári Kollégiuma 1/2013. (VI. 17.) számú határozata

A Minisztertanács 25/1986. (VII. 8.) és 102/1990. (VII. 3.) MT számú rendelete

ENSZ Emberi Jogi Bizottság általános állásfoglalása, No. 34, CCPR/C/GC/34, Genf. 2011. 09.

The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information,

<http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf>

OECD irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, magyar nyelvű áttekintés: <http://www.oecd.org/sti/ieconomy/15590228.pdf>

Guidelines for the Regulation of Computerized Personal Data Files, elfogadva 1990. december 14-én az ENSZ Közgyűlése által

Bizottság 2000. július 26-i 2000/520/EK határozata 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

The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce, 2002. 12. 13.

The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce, 2004.10.20.

Javaslat az Európai Parlament és a Tanács rendeletére a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet)

Article 29 Working Party Opinion 13/2011 on Geolocation services on smart mobile devices”, WP185, 16 May 2011, 13-14.

A 29-es Munkacsoport 8/2001 véleménye a személyes adatok feldolgozásáról a foglalkoztatás kontextusában és összefoglalás, 2001. 09. 13.

Article 29 Working Party: Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, 2002. 10. 24, 6.

Article 29 Working Party Opinion 2/2010 on online behavioral advertising, 22 June 2010, WP 171

Article 29 Working Party Opinion 15/2011 on the definition of consent, 13 July 2011, WP187

Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking

A 29-es Munkacsoport 5/2004 véleménye a nem kívánt, közvetlen üzletszerzésre irányuló tájékoztatásról a 2005/58/EK irányelv 13. cikkéről, WP 90, 2004. 02. 27.

Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy and its implementing Commission Regulation (EC) No 259/2008

Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 2009. 06. 12.

Article 29 Data Protection Working Party, Letter from the Article 29 Working Party to Google on Google Privacy Policy, 23 September 2014, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm#2014.

European Commission’s Expert Group on Cloud Computing Contracts Unfair Contract Terms in Cloud-Computing Service Contracts, 1. (letöltve: 2016. 04. 27.) http://ec.europa.eu/justice/contract/files/expert_groups/unfair_contract_terms_en.pdf

A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a védett adatkikötő működése az uniós polgárok és az EU-ban letelepedet vállalatok szempontjából, Brüsszel, 2013.11.27.

Németországi Szövetségi Köztársaság Alaptörvénye

Egyesült Államokbeli jogszabályok:

Az elektronikus kommunikációk során a magánszférát védő törvény, Electronic Communications Privacy Act of 1986 (ECPA), Pub.L. 99–508

A videó felvételekkel kapcsolatos magánszférát védő törvény, The Video Privacy Protection Act of 1988 (VPPA), Pub.L. 100–618

Kaliforniai Fogyasztóvédelmi Törvény, Californian Civil Code § 1750 and § 1770

Children's Online Privacy Protection Act of 1998

Health Insurance Portability and Accountability Act

Jogesetek

Guest Beer Provision, Supply of Beer (Tied Estate) Order 1989 SI 1989/2390

Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989)

Rotaru v. Romania, no. 28341/95, ECHR, 2010. 05. 04.

C-491/01 Queen v. Secretary of State for Health, ex parte British American Tobacco (Inv) Ltd & Imperial Tobacco Ltd, 2002. 12. 10.

Semayne's Case(1604) Michaelmas Term, 2 James 1 In the Court of King's Bench, first published in the Reports, volume 5

Pollard vs. Photographic Co.: 40 Ch. Div. 345

C-491/01 Queen v. Secretary of State for Health, ex parte British American Tobacco (Inv) Ltd & Imperial Tobacco Ltd, 2002. 12. 10.

Joined Cases C-465/00, C-138/01 & C-139/01, Österreichischer Rundfunk, 2003. 05. 20.

Case C-101/01 Bodil Lindqvist, 2003. 11. 06.

Case C-73/07 Satakunnan Markkinapörssi and Satamedia, 2008. 12. 16.

Times Newspapers Limited v. the United Kingdom, no. 3002/03 and no. 23676/03, ECHR, 2009. 05. 10.

C-28/08 P Commission v Bavarian Lager, 2010. 06. 29.

C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, judgment, 2010. 11. 09.

C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014. 05. 13.

C-49/11 Content Services Ltd vs. Bundesarbeitskammer Court of Justice of the European Union, 2012.

BVerfG [German Constitutional Court] 27 February 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007