SZEGEDI TUDOMÁNYEGYETEM
ÁLLAM- ÉS JOGTUDOMÁNYI KAR
DOKTORI ISKOLA

Mészáros János

Adatvédelem a XXI. században és az internet világában

c. doktori értekezésének tézisei

Témavezető:
Prof. Dr. Paczolay Péter
tanszékvezető egyetemi tanár

Szeged
2017

I. Az értekezés tárgya és célkitűzése

Az egyén digitális világban betöltött szerepének felértékelődése és a magánszférájának védelemre szorulása jelentik a dolgozat kiindulópontját, amelyet a disszertáns a magánszféra vizsgálatát követően az internet leggyakrabban használt szolgáltatásain (pl. Google, Facebook) keresztül mutat be, keresve a jogi és technikai megoldásokat a felmerült problémák megoldására[1].

A privacy fogalmának meghatározása különösen nehéz, mivel a "privát" szó jelentése is országonként eltérő és koronként változik, ezért dolgozatban annak történetét, az európai valamint az amerikai jogrendszerekben való érvényesülését vizsgálja meg a disszertáns.

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

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 található. Az információ, amely korábban adatmorzsákból volt összeállítható hosszas keresőmunka árán, így elérhetővé vált bárhol, bármikor, gyorsan és ingyen, akár inkognitóban is. A dolgozatban a felejtés jogának történeti és filozófiai hátterén túl az internetes keresőkön és a közösségi hálózatokon való érvényesülését vizsgálja meg a disszertáns, összekapcsolva az EU Bíróságának ítélkezési gyakorlatával.

A Facebook felhasználói tábora 2 milliárdhoz közelít, amellyel a világ egyik legnagyobb - nem állami - adatkezelője. A disszertáns a Facebook magánszférát érintő legfontosabb kérdéseit és problémáit helyezi vizsgálat alá, különösen az Európai Unió adatvédelmi szabályozásának a szemszögéből. A Facebook főként a felhasználók hozzájárulását használja fel jogalapként az adatkezeléseihez, azonban kérdéses, hogy annak feltételei (önkéntesnek, határozottnak, megfelelő

[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.

tájékoztatáson alapulónak és félreérthetetlennek kell lennie) maradéktalanul érvényesülnek-e, amelyet a disszertáns dolgozatban részletesen bemutat és mély elemzés alá helyez.
Az európai állampolgárok magánszférájára jelentős hatással van, hogy a leggyakrabban használt online szolgáltatások a személyes adataikat az Egyesült Államokba küldik, ahol azok biztonsága nincsen olyan mértékben biztosítva, mint az Európai Unióban. A Safe Harbor megszűnése és a Privacy Shield elfogadása, mint lehetséges adatküldési mód, csupán részleges megoldást eredményez, amely a dolgozatban bemutatásra kerül, különös tekintettel a közösségi hálózatokra és az internetes keresőkre. A személyes adatok Európán kívüli küldéséhez hasonlóan jelentős, azonban avval összevetve alulszabályozott problémát jelentenek az adatkezelő vállalatok felvásárlásával kapcsolatos aggályok, amelyek az adatkezelés módjának és céljának a megváltozását jelenthetik, amelyre legaktuálisabb példa a WhatsApp felvásárlása a Facebook által. A disszertáns célja továbbá jogi és technikai megoldásokat keresni a felhasználók magánszféráját érintő problémák orvoslására, amelyek a dolgozatban részletes bemutatásra kerültek.

II. A vizsgálati módszer és az értekezés felépítése

A disszertáns kutatási témájának 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 kizárólag Windows és Apple eszközökön fut teljes szolgáltatáskínálattal. A legnépszerűbb szolgáltatások és oldalak 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 találhatóak meg, azonban az alkotmányos védelem erősödése „elközjogiasítja” azt. A dolgozatban a magánszféra alkotmányos védelmén túl

elsősorban magánjogi oldalról került megközelítésre az adatvédelem érvényesülése és jogi szabályozása. A magánszféra és a személyes adatok védelme az alkotmányjog, polgári jog és büntetőjog anyagi jog szabályain keresztül került megvizsgálásra, a disszertáns az eljárásjogi szabályokat kizárólag a személyes adatok megsértése esetén alkalmazható jogérvényesítéssel kapcsolatban érintette. A disszertáns az értekezés megírása során törekedett a mértékadó hazai és nemzetközi szakirodalom bemutatására és kritikus értékelésére, a tudományos feldolgozáshoz történeti, jogtörténeti, komparatív, leíró/kutató, analitikus tudományos módszereket alkalmazva.

Összehasonlító jogi vizsgálatok során az Európai Unión kívül különösen az Egyesült Államok jogrendszerére koncentrált a diszertáns, mivel a digitális világ legjelentősebb vállalatai ezen állam területén rendelkeznek székhellyel.

A hatályos szabályozás elmélete (law in book) mellett dolgozatban kiemelt figyelmet kapott a jogalkalmazási gyakorlat (law in action) bemutatása, azon belül is különösen az Európai Unió Bíróságának ítélkezése, amelynek döntései (pl. Google Spain, Safe Harbor megszüntetése)[2] különös jelentőséggel bírnak az EU állampolgárok személyes adatainak kezelésével kapcsolatosan, továbbá az Egyesült Államok és az Európai Unió között fennálló viszonyban adatvédelem terén.

A dolgozat első része tartalmazza a magánszféra védelmének történeti és jogfilozófiai hátterét. Szociológiai megközelítésből az internetnek és a közösségi hálózatoknak a társadalom magánszféra iránti igényére gyakorolt hatása került megvizsgálásra. A disszertáns a dolgozatban kitér a technika és a jog kapcsolatának vizsgálatára is, amelynek során elsődleges célja az, hogy átlátható logikai tagolással rámutasson napjaink gyakorlatában felmerülő vitás kérdésekre és nehézségekre, valamint egyes jogalkotási és jogalkalmazási problémákra.

A fenti vizsgálati módszerek alkalmazásától az uralkodó tézisek igazolását vagy cáfolását várja a disszertáns, továbbá célja, hogy egyes szabályozási nehézségek kiküszöbölésére, egyszerűsítésére, ill. gyakorlati problémák megoldására javaslatkísérletet tegyen.

A kutatás egyes részeredményeit a disszertáns felhasználta publikációi, illetve tudományos előadásai során, törekedve arra, hogy az így megszerzett szakmai ismereteket, visszajelzéseket és tapasztalatokat maradéktalanul felhasználja a doktori értekezés megírása során.

---

[2] 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 Maximillian Schrems v Data Protection Commissioner, Court of Justice of the European Union, 2015. 10. 07.

III. Az értekezés tudományos eredményeinek összefoglalása

1) A személyiségi jogok, a magánszféra és az adatvédelem kapcsolata

A disszertáns vizsgálat alá helyezi a magánszféra, az adatvédelem, és az információs önrendelkezési jog kapcsolatát, továbbá rámutat, hogy az információs önrendelkezési jog folyamatosan gyengül, amelyet az adatvédelmi jog erősítésével lehet ellensúlyozni.
Az információs önrendelkezési jog és az adatvédelem gyakorlati érvényesülésén, továbbá történeti fejlődésén keresztül a szerző cáfolja, 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 adatvédelmi jog erősödése és „elközjogiasodása" mutatható ki, mivel az egyén védelemre szorul az egyre nagyobb és monopolhelyzetben lévő adatkezelőkkel szemben. A megfelelő védelemhez elengedhetetlen, hogy az „érintett-központú" szabályozás elmozduljon az „adatkezelő-központú" szabályozás felé[3].
Az adatvédelem intézménye kizárólag a magánszféra védelmén belül értelmezhető, míg az információs önrendelkezési jog az adatvédelmen belül helyezhető el.
A magánszféra védelmére való igény, az avval kapcsolatos szokások és jogszabályok hamarabb alakultak ki, mint az adatvédelem, amelyet a szerző annak történelmén és az adatvédelmi jogszabályok generációján keresztül mutat be.
Az önrendelkezési jog alapján megilleti az egyént az a jog, hogy döntsön a rá vonatkozó

[3] Szőke Gergely László: Az európai adatvédelmi jog megújítása, tendenciák és lehetőségek az önszabályozás területén, doktori értekezés, Pécs, 2014. 164.

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, amelynek az adatkezelő köteles eleget tenni.

2) A személyes adatok védelméhez való jog ütközése alapvető jogokkal az Európai Unió Bíróságának joggyakorlatában

A disszertáns az Európai Unió Bíróságának joggyakorlatában az alapjogok (köztük a magánszféra és a személyes adatok védelme) és az alapvető szabadságok (személyek, áruk, szolgáltatások és a tőke szabad áramlása) védelmének viszonyát vizsgálja meg.
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.
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 tekintetében[5], amely a dolgozatban az EU Bíróságának legjelentősebb ügyein keresztül kerül bemutatásra.

[4] Sionaidh Douglas Scott: A tale of two courts: Luxemburg, Strasbourg 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>

Az Európai Unió Bírósága a bemutatott jogesetek jelentős részében nem adott konkrét választ az esetek eldöntésére, vagy nyitva hagyott több kérdést is, amelyet a tagállami törvényhozásoknak és jogalkalmazóknak kell megválaszolniuk.
A nemzeti törvényhozások és hatóságok döntései teljesen egységesek nem lesznek, amely 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-tól, továbbá lehetséges, hogy ugyanarra a keresésre más eredményeket kapunk majd Európában, mint a világ egyéb részein.

3) A felejtés joga

A disszertáns a felejtés jogának érvényesítésének 3 aspektusát mutatja be, a felmerülő problémákra megoldást keresve:
a) határvonal húzása az adatkezelők és adatfeldolgozók között 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.
A fejezetben több jogeseten 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.
A disszertánsnak ugyanakkor a technika jelenlegi állását és az internet gyakorlati működését

megvizsgálva cáfolnia 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, eltüntetni már 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 értékként („privacy by default"), amelynek egyik módja lehetne, hogy az adatok már a felvételkor lejárati időt kapnának, és annak leteltével névtelen adattá válnának – megszűntetve az érintettel való kapcsolatba hozhatóságot -, vagy törlődnének.

Az adatok kérelemre való eltávolításával, a felejtés jogának kérelemre való érvényre juttatásával kapcsolatosan megállapításra került, 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 tett a disszertáns a bankszektorban bevált módszereket alkalmazva.

A hatályos jogszabályokon és az EU Bíróságának döntésein keresztül bizonyításra került, hogy az internetes keresők adatkezelőnek minősülnek.

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 látszatmegoldást 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

kötelességeket ró, amelyek 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 kiemelésre kerültek a személyes ügyintézéssel és a közfeladatok Google-ra delegálásával kapcsolatos problémák, továbbá egy alternatív megoldási javaslat került kidolgozásra 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 tökéletese a kulcs a felejtés jogának az érvényesítéséhez, továbbá a többi alapjoggal való ütközésének a kezeléséhez, amely különösen fontos az érintettek jogainak védelme, továbbá a véleménynyilvánítás és a sajtószabadság biztosításához.

4) A Facebook adatkezelései

A Facebook adatkezelései jelentős részéhez jogalapként az érintett hozzájárulását használja fel, azonban a disszertáns rámutat, hogy a hozzájárulás alapvető követelményei (önkéntesnek, határozottnak, megfelelő tájékoztatáson alapulónak és félreérthetetlennek kell lennie) nem érvényesülnek maradéktalanul, így feltételezi, 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 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 a 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.

A disszertáns véleménye szerint minden egyéb adatkezelés esetén az érintett hozzájárulása lenne szükséges annak legitimálásához, amelynél a legfontosabb kérdés, hogy előzetes vagy utólagos lehet-e (opt-in vagy opt-out).

A fejezetben bemutatásra kerültek a Facebook adatkezeléssel kapcsolatos problémái, amelyek 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 alapbeállítássá tételén túl a Facebook olyan forrásokon keresztül is gyűjt személyes adatokat, amelyekről a felhasználóknak sok esetben nincsen tudomása és 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 félreérthetetlenség problémáját a felhasználó tudta és hozzájárulása nélkül zajló adatgyűjtésekkel került bemutatásra, amelyeknek eredete a hiányos és nem áttekinthető tájékoztató, amelynek homályos és megtévesztő részletei bemutatásra kerültek.

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, amelyek a fejezetben bemutatásra kerültek.

A Facebook történetének, működésének és bevételének vizsgálatát követően a szolgáltatás fizetőssé tételét a személyes adatok fokozott védelméért cserében csak korlátozottan tartja megvalósíthatónak a disszertáns.

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 minimális felhasználói díj fizetése sem jelenthet alternatívát.

Európában evvel szemben az 1,3 eurós felhasználónkénti havi átlagbevétel nem jelentene különösebb nehézséget a felhasználók jelentős részének, különösen Nyugat-Európában.

A disszertáns véleménye 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 szalaghirdetésekben, 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 archiválódna, vagy csupán közeli ismerősök számára lenne megtekinthető.

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 földrészeken 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, amelyre az EU Bírósága is kitér ítéletében. 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 félreérthetetlenségéről.

Az adatkezelési szabályzat teljes átvizsgálása után bizonyítást nyert, hogy a hozzájárulás feltételei nem teljesülnek maradéktalanul az adatkezelések jelentős részében.

A disszertáns a dolgozatban javaslatot tesz arra nézve, milyen módon lehetne az előzetes hozzájárulást (opt-in) megvalósítani a közösségi hálózatok esetében annak érdekében, hogy annak törvényes feltételei teljesülhessenek.

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 kéretlen 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 2018-tól az Adatvédelmi Rendelet alkalmazása során, amely mind az általános, mind a gyermekek hozzájárulásával kapcsolatban szigorúbb követelményeket támaszt, amelyek a fejezetben bemutatásra kerültek.

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 különleges adatokra, 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).

6) Személyes adatok küldése az EU területéről az Egyesült Államokba, különös tekintettel az internetes keresőkre és a közösségi hálózatokra

A személyes adatok küldése az Egyesült Államokba kiemelten fontos az információs társadalomban, azonban nem minden áron. Az NSA botrány és az 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 alternativái. 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 kérik 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 eltérő 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 evvel kapcsolatban a felhasználóktól. Hasonló a helyzet a Facebook vállalatcsaládon belül és más harmadik felekkel való adatmegosztása esetén.

7) A személyes adat, mint adásvétel tárgya

A disszertáns rámutat, hogy 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. Különösösen érintettek az uniós állampolgárok adatai, amelyek csak megfelelő védelemmel juthatnának el a felvásárlással érintett legnagyobb vállalatokhoz az Egyesült Államokba.

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 azonban igen: hiába ugyanaz a cég marad a személyes adatokért felelős szervezet, valójában az új tulajdonos irányítja és határozza meg a stratégiáját. A disszertáns a dolgozat 4. fejezetében kitért az adatkezelő meghatározásánál a több adatkezelő, valamint az adatkezelés céljának és módjának meghatározásával kapcsolatos problémákra, amely a tulajdonosváltozásnál is releváns lehet, mivel 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.

Mentális ok lehet, hogy cselekménye következményeit valamiért nem tudja teljes mértékig átgondloni 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 megértsen 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.

Az érintett, miután az adatkezelő 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 a disszertáns külön választotta 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.

A legnagyobb szolgáltatók egy országba való koncentrálódásával, és a felvásárlások gyakoriságának növekedésével különösen fontossá vált, hogy az Európai Unió erőssebben védje a felhasználók személyes adatait, amelynek első mérföldkövei az elfogadott Adatvédelmi Rendelet és a Privacy Shield.

I. Objectives and Thematic Outline of the Dissertation

The data subjects' situation in the online environment has significantly changed and their privacy needs stronger protection. The primary goal of the dissertation is to outline the emerging need for the online privacy protection through the most popular online services like Google and Facebook. The secondary goal is to find technological and legal solutions for the online privacy protection.

It is challenging to define privacy, since its meaning is changing through the ages and countries. The history and the current situation of privacy protection is outlined in the thesis, especially in the European Union and United States.

One of the fundamental goals of the EU – the common market – has been established, which had a significant effect on the role of the EU Court of Justice: the protection of fundamental rights – especially in the online environment – became more important than the protection of the 4 freedoms which is proved through important cases of the EU Court of Justice.

The internet search engines and social networks recalled the need for the right to be forgotten since they provide the possibility to find information anytime and anywhere in an anonym way, for free. The philosophical and historical background of the right to be forgotten is elaborated in the dissertation, and it is followed by the elucidation of the role of Google and Facebook, connected with the jurisdiction of the EU Court of Justice.

There are almost 2 billion Facebook users, which makes it one of the biggest data controllers on the world. The dissertation outlines the most significant privacy issues of the Facebook from the EU data protection law's point of view. The Facebook applies mostly the users' consent as a legal base for its data processing activities, but it is questionable if the consent complies with the requirements (freely given, specific, informed and unambiguous), which is examined in the dissertation.

It has a significant impact on the EU citizens' data protection rights that their data is sent to the United States where the protection of their data is not as strong as in the EU. The end of Safe Harbor and the birth of the Privacy Shield cannot adequately solve the situation, since the other transfer methods are still not safe enough. Another significant problem is the acquisition of the data controllers, especially the big online companies, where usually the data base is most important

reason for buying the company. The current example is the acquisition of the WhatsApp by Facebook, which led to the change of their data protection terms.

II. Research methods

The research topic of the thesis has significant importance, since a big of the private life is moved to the online environment because of the technological development and the internet.

The use of the most popular programs (e.g. Windows, Apple OS) and services (Google, Facebook) is inevitable, and there are not many alternatives of them. This situation leads to the need for stronger data protection for the data subject.

The roots of the data protection law can be found in the civil law, but the constitutional protection pushes it to the field of public law.

The data protection law is approached more likely from the civil law side in the dissertation. The protection of privacy is elaborated through civil, criminal and constitutional law. The author elaborated the most relevant national and international literature by applying historical, comparative and descriptive analysis. During the comparative analysis the US law was mostly compared with the EU law since the biggest online companies are in the US.

Both the relevant law (law in book) and the jurisprudence (law in action) were outlined, highlighting the jurisdiction of the EU Court of Justice, since they have significant effect on the EU citizens' privacy rights.

The first part of the dissertation consists the historical and philosophical background of privacy. The effects of the social networks and the internet on the users were elucidated from social perspective. The PhD student also elaborates the connection between law and technology, which helps to point out the most important law making and jurisdiction issues.

The above mentioned research methods lead hopefully to the prove of the hypothesizes and new technological and law solutions.

The PhD student used his research findings for previous publications, university presentations, where he got many useful feedbacks which helped to finish the dissertation.

III. Summarization of the results of the thesis

1) The connection among the rights relating personality, privacy and data protection

The author places the connections among the informational self-determination, rights relating personality, privacy and data protection under research, and points out that the informational self-determination is constantly getting weaker which can be balanced with the stronger of data protection law.

It is proved through the working of informational self-determination in the real life and it's historical development that these two rights are different, they just partly overlap each other.

By the informational self-determination, the individual has the right to decide about the information concerning him, while the data protection law mainly restricts the data controller's activity.

The individual has weaker right of choice about that if he or she wants to participate in the online environment or not (e. g. groups for friends and for workplace, using Google Docs with colleagues, classmates, Electronic Exam and Class Application Systems) which leads to the weaker informational self-determination. It can results significant disadvantages on the fields of work, studying and private life if the individual chooses not to participate in the above mentioned communication methods. It can be witnessed that next to the weaker informational self-determination the data protection law is getting stronger and having more public law attributes, because the individual needs stronger protection against the big data controllers which are most likely in a monopole situation in the online environment. For reaching the appropriate level of protection, it would be necessary to move from the regulation protecting the individual to the regulation restricting the data controllers' activities.

The data protection can be placed only in privacy protection and the informational self-determination can be only placed in the data protection law. The natural need for privacy, the habits, customs and laws about it formed earlier than the data protection, which is introduced by it's generations and history in the dissertation. By the informational self-determination the individual has the right to decide the publicity of the information concerning him or her, while the data protection law regulates the data controller's activities.

The data protection law doesn't emerge barriers for the individual about how he can make his own personal data public, but the data protection law requires legal basis for the data controller's processings (e.g. consent, specified by law).
The broader meaning of data protection is also proven by the requirement of data security, which has to be done by the data controller, not by the data subject.

2) The clash between the protection of personal data and the four freedoms of the EU in the jurisdiction of the European Court of Justice

The EU Data Protection Directive tries to fulfill two, seemingly opposite goals: the protection of personal data and the free movement of data in the European Union.
Striking the balance between these two goals was challenging for the lawmakers in the member states and it is still demanding for the law enforcement to determine the priorities. One of the main pillars of the European Union, the European common market has already been well established, which had a significant effect on the jurisdiction of the EU Court of Justice: protecting the 4 freedoms became less important compared to the fundamental rights.
The EU Court of Justice had to draw the line in the field of protection of human rights between the member states' and the EU level, which will be presented in the dissertation through the most important cases of the CJEU.
The CJEU has not given clear answers in many important cases, which leaves a lot of room for the member states and it leads to the issue that the interpretation of the Member States will never be unified and the fragmented interpretation of the EU data protection law can easily lead to forum shopping.
The Google Spain case is especially crucial, because of the interpretation and implementation of the judgment can lead different levels of privacy protection in the EU.

3) The right to be forgotten

There are 3 crucial fields for the improvement of the right to be forgotten:

a) Strike the line between the data controllers and data subjects in the online environment,

b) Developing standards for the examination of the applications from the users to erasure of their data,

c) Developing a user-friendly, transparent system for the data subjects, which can ease the administrative burden of the authorities both EU and member state level.

It has been introduced in the Chapter that the online world significantly changed the right to be forgotten, which was a natural and crucial part of the person's life. The information, which was hard to find before the Internet and Google, can be accessed easily, free, fast and anonym now.

This situation can lead to a conflict between the right to privacy and the freedom of information.

It seems almost impossible to perfectly enforce the right to be forgotten, since there are many websites on the internet with unlawful content, which cannot be shut down even with international cooperation. If an unlawful content spread out on the internet, it is impossible to remove it.

The biggest difference between the physical and electronic storage of data is that it is worth to destroy the physically stored data (e.g. paper archives), while it is complicated and sometimes more expensive to delete the digital data, than let it be stored.

The solutions for this issue can be technological methods, which could provide the right to be forgotten from the beginning of the data processing (privacy by default). One of the methods would be if the data had expire date from the beginning and it would be archived, pseudonymized, or deleted after a period of time.

It was elucidated in the Chapter that it cannot be said generally that the right to be forgotten has a priority over the other rights, it needs to be evaluated in every individual case if which right prevails after a balancing test. Suggestions for formal and material methods were given in the dissertation for this balancing test.

It was proven through the European, national, and case law of the CJEU that the internet search engines are data controllers. The operator of the search engine counts as a data controller, since it determines the goals and methods of the data processing which gives the right to the data subject to apply for the operator directly, if he or she would like to delete the search results concerning him or her. If the data subject does not agree with the decision of the operator, he or she can appeal at data protection authorities.

The decision of the CJEU in the Google Spain case was a milestone for the protection of the individuals but it resulted a half solution: it burdens the internet search engines with the duty to

remove the unlawful information, not the original sources of the information. The reasons behind it can be understood: it is hard or almost impossible to hold the webpage operators in foreign countries responsible and force them to remove content, whereas the most popular search engines have offices and representatives in the EU.

One of the biggest problems with this solution is that the search engines were not prepared for this situation. First, it is questionable, if it is their responsibility to decide if the requested information is lawful or not. Second it is difficult to decide the requests at an internet company except those cases when the user owns an official paper (e.g. judicial decision).

The PhD student elaborated an application method in the Chapter about the right to be forgotten. The elaborated method would give the data subjects stronger rights and more insurances, while eases the burden on the individual search engines. Multiple search engines, civil right groups would also participate in this process to protect the fundamental rights of the data subjects and the freedom of information.

4) Facebook

The Facebook uses the data subjects' consent for most of its data processing as a legal basis. The consent has to be freely given, specific, informed and unambiguous. It is pointed out in the Chapter that in most of the cases one or more requirements of the consent are missing thus the PhD student supposes that most of the Facebook's data processing are not lawful in the EU.

The social networks can basically use 3 legal bases in the EU for processing their users' personal data:

1. data subjects' consent,
2. processing is necessary for the performance of a contract,
3. processing is necessary for the purposes of the legitimate interests pursued by the controller or the third party.

The social networks can only use the "necessary for the performance of a contract" as a legal base if the contract is necessary for providing their service (e.g. the basic information about the users, uploading profile pictures).

Processing personal data for "legal interest" can be a legal basis also in limited situations, like the security of the system and other users.

The PhD student thinks that in any other situation the users' consent would be necessary, and the most important question would be if opt-in is necessary, or opt-out is also acceptable.

The problems surrounding Facebook's data processing are introduced in this chapter. The roots of this problems are the Facebook's interest which is to stimulate the users to upload and share as much information as they can to make the advertising system more precise and profitable.

The Facebook makes the information shared by default, but the real problem is that the it collects data from sources which are unknown for the users or they don't have control about it.

The consent, which is the most frequent legal basis for the data processing, has to be freely given, specific, informed and unambiguous. It has been proven through the Chapter that one or more requirements of the consent are missing, and in some situations even the legal basis is missing in the case of Facebook's data processing.

One of the biggest problems with the Facebook's data processing is that the users have minimal control about it. The "all or nothing" is not a real option for the people who would like to be Facebook users, and there is no other option for joining a social network which lets the user to keep in touch with his or her international friends. The consent cannot be really "freely given" if the service doesn't have a real alternative. There is no other option for international social network outside of Facebook.

There are many data collection activities without the knowledge of the users which leads to the problem of the requirement of the "specific and unambiguous" consent. The consent cannot be informed, since the Facebook's Terms and Data Policy is not clear, and contains many misleading information.

The Facebook's problems with the consent can be even bigger when the new General Data Protection Regulation (GDPR) comes into force in 2018. The GDPR will have stricter requirements with the consent (e.g. in the case of children).

After the introduction of Facebook's history, system, and economical model, making a paid system seems challenging, since in most of the places in the world the population wouldn't pay for it.

The general income per user is too high in the United States to substitute it with user payments, and in the developing countries it is not possible make a paid model work.

In the EU the 1,3 Euro average income per user could be easily replaced. The PhD student thinks that a middle way also exists: the 50% of the average income per user could be replaced with the users' payments, and the other 50% could be covered by "general" advertisement, without user tracking. Under general advertisement the PhD student means the regular ones (e.g. banners, pop-up ads), which can be seen on most of the webpages, and they are similar to the "offline" advertisements (e.g. posters on the street).

If the user chooses the "half-paid" solution, he or she could get a Facebook experience by giving just basic data (e.g. name, age, city), without behavioral advertising and secret data collecting.

This solution would create a situation where the users would have a safe user experience, without losing the control of their data. The location-based and behavioral advertising would be turned off, and Facebook wouldn't send the users' data to third partners.

The information what the user can get through the registration for Facebook is not suitable to reach the requirement of the informed consent.

Another issue is that the default setting is that all the user's activity is "public" and the user has to change the settings to restrict it, it challenges the requirement of "unambiguity" of the consent.

There are suggestions in the Chapter about the op-in solutions to make the Facebook's data processing lawful.

It poses a significant privacy issue that the information and pictures of people are shared on social networks, who are not users of the service, thus they are not able to know about it and object to the data processing. It is challenging to solve this issue since the data controller cannot trace and inform the data subject, because it could be spam, or unlawful identification by the EU law. The Data Protection Directive and the GDPR also states that the data controller has the right to know about the data processing concerning him or her.

The Facebook's age limit is the reason for many users decide to give fake data about their age. In the U.S. most of the kids under 14 are Facebook users despite the restrictions. There would be many ways to protect and restrict them, which are introduced in this Chapter. One of the easiest solution would be for example if children wouldn't be allowed to give sensitive data about themselves, and the face recognition could be also useful to detect them with other technical methods.

Among the data uploaded and shared by the users, the pictures are crucial, since the photos can show sensitive information, like race, religion, disease, political views. Facebook stores a gigantic photo database, which is worth more with the use of face recognition technology. It is elaborated in the Chapter what kind of privacy problems can be caused by the advanced photo recognition technology.

6) Sending personal data from the European Union to the United States, especially in the case of search engines and social networks

Sending personal data to the US is crucial in the age if information society, but it has to be restricted by the fundamental rights. The NSA Scandal and the decision of the CJEU showed that the EU citizens' rights were seriously violated.

Finding the solution is crucial, since there are no real alternatives for Facebook, Google and Microsoft in the EU. The end of Safe Harbor and the birth of Privacy Shield are big steps, but the protection of personal data sent to the US is still not strong enough: the standard contractual clauses, binding corporate rules, performance of a contract, and the consent transfer methods are not sufficient to protect the data subjects' rights. The above mentioned transfer methods are elucidated in the Chapter, and the PhD student suggests the revision of them, since they are more like a "gap" beside the Privacy Shield.

Facebook was one of the first companies applying for the Privacy Shield registration. The issues about the data processing of the Facebook and the requirements of the Privacy Shield are introduced in the Chapter. The PhD student proves that the Facebook does not comply with the Privacy Shield requirements adequately (e.g. processing data for secondary purpose, the consent for special categories of personal data and the sharing data inside the Facebook group).

7) Personal data, as good for sale

In the informational society the value of personal data has significantly increased, which is proved by the high sale prices of the online companies. The sale of the companies has sometimes only one reason, the user database.

It is elaborated in the Chapter that the acquisition of online companies can be problematic from the point of view of data protection law, since not just the owner is changing. The acquisition also means that there will be a new person who has significant influence on the goals and methods of the data processing. The EU citizens' data are especially in danger since they are stored in the biggest online companies in the US, where they were sent with a weak data transfer method by the Safe Harbor.

In theory, the data controller is not changing with the acquisition, but in practice, a new owner will have control over it in some degree. The issue of joint data controllers, the goals and methods were elaborated in the fourth Chapter which can be relevant to the issue of owner changing.

It can be especially problematic if the new owner changes the data processing in a way which does not comply with the original terms of data processing (e.g. Facebook bought the Watsapp and the user data was shared for commercial purpose).

It would be crucial for the data subjects to get sufficient information before the selling of their personal data. The personal data is not just a good which can be just sold and bought without limitation. The data subjects are not able to evaluate the risk of giving their personal data in every situation thus the data cannot be handled as a good, which lost its connection with the original owner. With the concentration of the biggest data controllers in one country, the EU should be stricter to protect the data subject, and the significant steps for that direction are the GDPR and the Privacy Shield.