Pázmány Péter Katolikus Egyetem
Jog- és Államtudományi Kar
Infokommunikációs Tagozat

Mit tudhat rólunk az internet?
A web 2.0-es szolgáltatások működése és jogi problematikája az adatvédelem tükrében

(TDK dolgozat)

Péter Krisztina
konzulens: Dr. Pogácsás Anett

Budapest 2016

Tartalomjegyzék:

“ A jelenlegi technológiai forradalmat nem a tudás és az információ központi szerepe jellemzi, hanem a tudás és információ alkalmazása, további tudás és újabb információ feldolgozó és kommunikációs készülékek létrehozására” Manuell Castells

1. Bevezetés

Napjaink technológiai fejlődése sok szempontból jelent társadalmunk életében paradigmaváltást. A hagyományos értelemben vett kommunikáció, versenyképesség, szellemi tulajdon és adatvédelem fogalmai megváltoztak. Ezen megújult tevékenységek közös forrása az internetre, azon belül a megosztásra alapuló oldalakra összpontosul. A folyamat terjedése, az internetes tartalom növekedése számszerűen is bizonyítható[1]: az interneten percenként keletkezik 1267,465 gigabyte adat. Ez körülbelül hat és fél perc alatt annyit tesz, mint az emberiség minden valaha elkészített filmjének mennyisége.[2] Ez a mennyiség rengeteg adatkezelést takar, ebből adódóan a dolgozat központi témája az adatvédelem. Célja a paradigmaváltás igazolása és a jogi szempontú megoldási mechanizmusok felvázolása. Az adatkezelés két új és lényeges dimenzióját vizsgálom. A web 2.0-es szolgáltatások és a Big Data jelenségét, amelyek működése egymással összefüggő. Fennállásuk bizonyítja, hogy ez az internetes dimenzió “ erőforrás” jellegű, a digitalizált közérdeket mutatja.[3]

1.1 Web 2.0-es szolgáltatások

. Az internet funkcióit tekintve sokszínű, de néhány kiemelkedő kategóriáról is beszélhetünk mint online ismeretségi hálózat, átfogó keresési felület, nagy mértékű adattárolás.[4] Ezen fogalmakat összefoglalóan web 2.0-es szolgáltatásoknak nevezhetjük. A fogalmat, Tim O’Reily definiálta először, figyelembe véve a web 2.0 legfontosabb funkcióit.[5] Eszerint a weboldalak izolált információ- és tartalomforrásokká alakulnak át, hasonulva az

[1] Cisco Visual Networking Index: Forecast and Methodology 2014-2019 white paper, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html (2016.10.10.)
[2] Németh Szabolcs: Az adataink jogi sorsa a halál után In: Tóth András (szerk.): Technológiai jog- Új globális technológiák jogi kihívásai,Patrocinium Kiadó., Budapest 2016, 262.
[3] Bocsok Viktor, Boldizsár Péter Ferenc, Loós Csaba, Major Tamás: A dolgok internete- Technológiai háttér, információbiztonsági és adatvédelmi aspektusok In: Infokomunikáció és Jog 12. évfolyam 2-3.szám, (2015) 57.
[4] Bartóki-Gönczy Balázs – Pogácsás Anett: A médiatartalom-szolgáltatásnak nem minősülő internetes tartalmak szabályozása. In: Koltay András – Nyakas Levente (szerk.): Magyar és európai médiajog. Wolters Kluwer, Budapest, 2015. 655-656
[5] http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (2016.02.13.)

asztali alkalmazásokhoz, mint például szövegszerkesztő, táblázatkezelő programok. Ezen felül társadalmi szempontból is kiemelkedő, hiszen kiindulási alapja maga a közösség, a felhasználó. Így lehetővé válik hogy a weben elérhető tartalmak szabadon felhasználható, és szerkeszthetőek legyenek, központi ellenőrzéstől mentesen. Ezáltal a felhasználó az információ birtokosa lesz, tehát önállóan szerkesztheti, közzé teheti.[6] A web 2.0 hatására az internet gazdasági, üzleti hatása megnövekedik. Lehetővé válik hogy a szoftverek folyamatos fejleszthetőséget érjenek el, az újdonságokról pedig közvetlenül a felhasználótól kaphatnak visszajelzéseket.[7] Ugyanakkor a web 2.0-es szolgáltatások használata alapján egyfajta "szűrőbuborék" alakul ki a profil számára, ami felvethet véleményszabadsággal vagy a tájékozatlansággal kapcsolatos nehézségeket.[8]

A Tim O'Reily által definiált fogalom rávilágít, hogy több közösségre alapuló szolgáltatás platformja, alakult ki egy szerteágazó online hálózat képében. Ez az online hálózat funkcióiban eltérő, azonban adatvédelmi szabályozását tekintve hasonló problémákat vet fel, hasonló belső felépítést eredményez.

1.2 A Big Data jelenség

A web 2.0-es szolgáltatások nagy előnye, hogy a legtöbb felületet ingyen használhatja a felhasználó. De a későbbiekben láthatóvá válik, hogy valójában adatvédelmi és fogyasztói szempontból "kattintással fizet".[9] Az online kereskedelem, az online piac megjelenésével megjelentek a digitális üzleti modellek.[10] A Big Data rendszer összetett és sok paradoxont rejt adatkezelés és fogyasztó tekintetében is, mégis hasznos a társadalom számára.[11] A modellnek teret adó web 2.0-es technológiák megadott személyes adatok, érdeklődéssel kapcsolatos következtetések, egyéb adatok (pl. IP cím, helymeghatározás) segítségével hozzák létre a monumentális Big Data adathalmazt. Ettől kezdve üzleti érdekekről és online gazdasági

[6] ld. The University of Melburn: Wikis, blogs and web 2.0 technology http://copyright.unimelb.edu.au/__data/assets/pdf_file/0011/1773830/wikisblogsweb2blue.pdf (2016.02.12)
[7] Cseh Gergely:A közösségi portálok árnyoldalai, In: Infokommunikáció és Jog X. évfolyam 2. sz. 2013. 91-92.
[8] vö. Tatay Eszter: A szűrőbuborék hatása a tájékoztatottsághoz való jogra In: Infokommunikáció és Jog XII. évfolyam 2-3.sz. 2015. 80-84.
[9] Szőke Gergely László: Infokommunikációs Szakmai Nap, beszámoló In: Infokommunikáció és Jog-12. évfolyam 4. sz. 2015. 158.
[10] Belényesi Pál: Digitális és technológiai piacok közgazdasági kérdései, In: Tóth i.m. 2016, 13-15.
[11] vö. Neil M. Richards, Jonathan H. King: Three paradoxes of big data, 66 Stanford Law Review Online 41 (2013) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325537 (2016.10.03.)

versenyről beszélünk[12], azonban a dolgozat a felhasználói, adatvédelmi oldalra összpontosít. A Big Data folyamatosan "mélyül" és a jelenséget sok kritika érheti. Hiszen sok személyesnek minősülő adatot kezelnek rólunk, a hozzájárulásunk keretein felül. Így felmerülhet a kérdés, egyáltalán létezni fog -e a jövőben megfelelő védelmet nyújtó adatvédelmi jog?

1.3 Célkitűzések

A dolgozat kiindulási alapja, hogy összevesse az adatvédelmet az előbb említett web 2.0-es technológiákat. Részletezi definiálásukat, besorolásuk problémáját, funkcióikat illetve az ehhez kapcsolódó adatvédelmi kihívásokat. Adatvédelem tekintetében az adatkezelés forrásait, jogi kereteit és az ehhez való hozzájárulás keretét vizsgálom. Írásomban láthatóvá válik, hogy a hatályos jogszabályok mellett a szolgáltatás rendelkezik szerteágazó, részletes adatvédelmi tájékoztatóval. De felgyorsult világunk működéséből kiindulva, ritka az a felhasználó, aki valóban ismeri a felhasználási feltételeket vagy az adatkezelési szabályozást. Így nem a tájékoztatáson alapuló, megfontolt hozzájárulásról beszélünk, hanem egy egyszerű "kipipálásról" a szolgáltatás használata előtt.

[13]Az általam kiválasztott kategóriák a tágabb értelemben vett web 2.0-es kategóriákat veszi sorra. Ezek az úgynevezett keresőmotorok (Google), a közösségi online kapcsolatokat fenntartó weboldalak (Facebook) valamint a nagymennyiségű adattárolást biztosító szolgáltatások (Cloud computing). Ezen technológiát és az internet egészét fedi leva nemrég szabályozott, ámde régóta jelen lévő cookie-val folytatott adatgyűjtés. Kiemelve a közösségi oldalak személyre szabott, hirdetésekhez kötődő eseteit. Ezen felül a dolgozat prezentálja az új kihívásokat az adattárolás kapcsán.. Például az IoT technológia szabályozatlanságát, illetve az online adatok sorsát a felhasználó halála után. Zárásként, a technológiákra reflektálva leírom az uniós szinteken történő adatvédelmi változások előzményét és újításait.

A dolgozat célja, hogy választ kaphassunk a feltett kérdésre. Létre jöhet -e egy stabil jogbiztonságot jelentő adatvédelem, a Big Data világában? Álláspontom szerint a hagyományos értelemben vett adatvédelem valóban eszköztelenné válik az új tehcnológiai

[12] v.ö. EDPS-BEUC Conference on Big Data, Brussels, 29 September 2016 "Check against delivery" http://ec.europa.eu/commission/2014-2019/vestager/announcements/big-data-and-competition_en (2016.10.02.)
[13] példaként a Facebook felhasználási feltételek részletes tájékoztatást biztosíthatnak https://www.facebook.com/legal/terms

platformokkal szemben.[14] A dolgozat bizonyítani fogja, hogy mint a technológiai jog szegmenseiből kiindulva, ezen a jogterületen is az "újrafogalmazására" van szükség mind a jogalkotó, mind a felhasználó szempontjait figyelembe véve. Fontos az elején tisztázni, hogy tényleges mindenre kiterjedő adatvédelmi megoldás még nem született. Így a dolgozat felméri a jelenleg végbemenő folyamatokat és felveti az aktuális és jövőbeni jogi megoldásokat.[15]

2. Google

A digitális világ "kapuőre". Az első web 2.0-es szolgáltatás, amelyet a leggyakrabban használunk a számítógép, okostelefon bekapcsolását követően. A felhasználónak az információk gyors és hatékony megtalálásában nyújt segítséget. A keresőmotorok működése általában az információ összegyűjtéséből és rendszerezéséből áll. Egy automatizált rendszerről beszélünk, amelyben adatgyűjtés megy végbe, minél nagyobb adatbázist létrehozva.[16] Ezen kívül a Google egyediesedési folyamata a közelmúltban kezdődött, a Google+ szolgáltatások megjelenésével. A fejlődést hordozza magában, hiszen a többi web 2.0-es oldalhoz hasonlóan itt is személyes adatok alapján egy saját profil jön létre. Alapvetően mégsem válaszolható meg az a kérdés mit várhatunk egy keresőtől. Ződi Zsolt infokommunikációs előadásában a fennálló helyzet paradoxonára világított rá: a szolgáltató minél inkább szubjektívvé válik a felhasználó izlése szerint, annál könnyebben zárhatja be őket saját világuk buborékába.[17]

A 29.es Munkacsoport ebben az esetben a keresőmotorok-hirdetés alapú- üzleti modelljét követik egy véleményezésben. A nyereségesség kiindulási pontja a hirdetés érvényesülésének hatékonysága, vagyis milyen gyakran tűnik fel a keresési eredményekben.[18] A "fizetés kattintásonként" elvből származik maga a bevétel a hirdetőnek, és lényegében a

[14] vö. Ivan K. Fong: Law and New Technology: The Virtues of Muddling Through, Yale Law & Policy Review: Vol. 19: Iss. 2, Article 5. (2000) http://digitalcommons.law.yale.edu/ylpr/vol19/iss2/5/ (2016.10.21.)
[15] vö. Neil M. Richards Jonathan H. King: Big Data and the Future for Privacy, Handbook of Research on Digital Transformations (Elgar 2016) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2512069 (2016.10.01.)
[16] Szabó Endre Győző, Bojnár Katinka, Buzás Péter: Új globális technológiák kihívásai a magyar jogban i.m. In: Tóth András (szerk.): Technológiai jog- Új globális technológiák jogi kihívásai,Patrocinium Kiadó., Budapest 2016, 88-89.
[17] vö. Polyák Gábor: A frekvenciaszűkösségtől a szűrőbuborékig Tóth i.m. (2016) 116-140.
[18] WP 148:1/2008. számú vélemény a keresőmotorokkal kapcsolatos adatvédelmi kérdésekről, 6.

felhasználó is “kattintással fizet” információért.[19] A felhasználó kattintása, keresése magába foglalja a keresőmotor adatkezelésének kezdetét. Hiszen a hirdetők alapvető célja, hogy megfelelő célcsoport felé legyenek irányítva, ebből adódóan a keresőmotorok ezt próbálják optimalizálni. Minden egyes lekérdezés célja a legnagyobb betekintés biztosítása. [20]

2.1 A kezelt adatok

A Google Adatvédelmi Irányelv felépítésének elsődleges pontjai, hogy meghatározza a szolgáltatás milyen adatot kezel, azt milyen módon használják fel. Ilyen kategória az automatikus szervernaplóból szerzett adat, eszközadat ,IP cím, helymeghatátozásból (GPS) származó adat, cookie és egyéb technológiák.[21] Ezen adatkezelések célja a szolgáltatás nyújtása, fenntartása, fejlesztése és védelme. Felkínálják a lehetőséget az egyénire szabott szolgáltatás elérésére.Tehát a profilhoz is felhasználja a regisztrált fél által megadott adatokat. A cookie-k és egyéb technológiák felhasználásával, a keresőmotorok üzleti modelljén túl a felhasználói élmény továbbfejlesztése a cél. Ezekből a technológiákból nem következtethetnek különleges személyes adatokra, például vallási, szexuális beállítottság.[22]

2.2 Keresőmotorok jogi kerete

Természetesen a keresőmotorok által lefolytatott adatkezelés is meghatározott jogi keretek között folyik. Európai Uniós jogforrások alapján elsődlegesen az alapjogi charta 8. cikke és az általános adatvédelmi rendelet elvei érvényesülnek. A 8. cikk a magánélet tiszteletben tartására hivatkozik.[23] Az adathalmaz tartalmazza a felhasználó érdeklődésének, kapcsolatainak nyomát, amely felhasználható kereskedelmi, bűnüldözési célra is. De a magánélet, a személyes adat értéke nem sérülhet. Hasonlóan definiálja ezt a kitételt a

[19] A Google a felhasználó ún. “szubjektív relevancia “ fogalmával dolgozik. a találatok megjelenésekor hat kategóriás fontossági sorrendet állít fel (vital-useful-relevant-slightly relevant- off topic-.useless) Hatnak rá a reklámozók által kifizetett összegek, hiszen a gazdasági verseny szempontjából nagy jelentősége van a sorrendnek, mivel a fogyasztó jellemzően arra a hirdetésre kattint, amelyet az első öt találat ad (Szőke i.m. 157.)
[20] Szőke i.m. 2015. 157.
[21] WP 148:1/2008. 6-7
[22] Google Adatvédelmi irányelvek https://www.google.hu/intl/hu/policies/privacy/
[23] (2) bekezdés “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.”

95/46/EK irányelv 2. preambulumkezdése.[24] Fontos ennek a tiszeletben tartása, hiszen a keresőmotorok lényeges szerepet játszanak az internetes információáramlásban. A keresők, mint kapcsolattartók érvényre juttatják az információhoz való szabad hozzáférés és a véleménynyilvánítás és tájékodózási szabadság jogát. Utóbbi érdekeket az alapjogi charta 11. cikke írja elő.[25] Ahogy a web 2.0 szolgáltatások általában, itt sem határhoz kötöttség, hanem internet elvűség működik. Így EU-n EGT-n belül, vagy ezen tagállamokon kívüli helyszínen vagy külföldön található több helyszínről nyújtható a szolgáltatás. Ennek alkalmazhatóságával a 95/46/EK irányelv 4. cikke foglalkozik, a nemzeti adatvédelmi jog érvényesülése érdekében.[26]

Ha megállapítható az adatkezelő személye, meghatározható melyik állam joga alá tartozik. Valószínűsíthető, hogy ez a személy a keresőmotor működtetője. De az alkalmazott jog meghatározásánál elsődlegesen a tevékenység végzésének helye a mérvadó, nem az adatkezelő telephelye.[27]

2.3 A feledésbe merülés joga

Utóbbi megállapításból következik egy kifejezetten a Google adatkezelési problematikájával foglalkozó per. Kiindulási alapja, hogy az internetes keresőmotor működtetője felelős olyan harmadik fél által közzétett weboldalakért, amely személyes adatokat érint. Ha a név alapján indult keresés, és személyére vonatkozó információt talál, megkeresheti az adatkezelőt. Ha kérelmének nem ad helyet, fordulhat az érintett hatósághoz. Az uniós irányelv alapján szemben áll egymással a magánélethez való jog és az adatok szabad áramlásának társadalmi érdeke.[28] Az új általános adatvédelmi rendelet kiterjeszti az érintett jogait a jogtalan adatkezeléssel szemben. Hiszen a web 2.0-es szolgáltatások Big Data adatgyűjtése nagy kockázatot jelent. A keresőmotoroktól eltekintve más technológiák,

[24] " Az adatfeldolgozási rendszerek célja az emberek szolgálata, mivel a természetes személyek nemzetiségétől és lakhelyétől függetlenül tiszteleben kell tartaniuk e személyek alapvető jogait és szabadságait különösen a magánélet tiszteletben tartásához való jogukat, és hozzá kell járulniuk a gazdagási és társadalmi fejlődéshez, a kereskedelmi fejlődéshez, valamint az egyének jólétéhez."

[25] (1) [...] Ez a jog magában foglalja a véleményalkotás szabadságát, valamint az információk és eszmék megismerésének és közlésének szabadságát anélkül, hogy ebbe hatósági szerv beavatkozhatna, továbbá országhatárokra való tekintet nélkül.

[26] WP 148:1/2008. 8-10.

[27] Dénesné Orcsik Judit: A Google-nak törölnie kell az adatokat, ha kérjük, Ügyvédvilág 9. évfolyam 11. szám 2015. 14.

[28] Navratyil Zoltán: Internet és szólásszabadság: a "felejtés" joga és a "feledésbe merüléshez" való jog In: Iustum-Aequum-Salutare 11. évfolyam 2. szám, 2015, 100.

például közösségi oldalak vagy ún. "google/facebook életrajz" miatt is érhet negatív megítélés a felhasználót. Rengeteg beazonosíthatóságot elősegítő információhoz juthat más harmadik személy az érintett munkaképességről, anyagi vagy egészségi helyzetéről, Napjainkban gyakran felvetődnek ezzel kapcsolatos kérdések. Például a munkaadó alapozhatja e az interneten található adatokra a munkavállaló alkalmazását, vagy éppen az elbocsátását?[29] Valamint a szólásszabadságot megtestesítő technológia mennyiben korlátozhatja az érintett személyiségi jogait? [30] Az érintettnek joga van magánélet, valamint jóhírnevének védelméhez, így ebben a kontextusban merül fel a felejtéshez, feledésbe merüléshez való jog. Az alábbi Google példával a törléshez való jogot fogom konstatálni.[31]

2010-ben Mario Costeja González panaszt nyújtott be a spanyol adatvédelmi ügynökséghez a Google Spain és a La Vanguardia Ediciones SL napilap ellen.[32] Saját nevére keresett rá, aminek következtében rábukkant egy 1998. január és márciusra mutató linkre, ami társadalombiztosítási tartozás behajtására irányuló, lefoglalással kapcsolatos ingatlan-árverési közlemény volt. A panaszos kötelezni kívánta a katalán napilapot, hogy törölje vagy módosítsa az oldalakat, vagy a keresőmotor biztosítson olyan eszközt ami azonosíthatatlanná teszi őt és nem jelenik meg a keresési találatokban. Indoklása szerint a tartozását már kifizette, és az őt érintő lefoglalás több éve rendeződött, így nem releváns. Tehát ennek függvényében adatkezelési célja megszűnt.[33] A panasz tekintetében az AEPD (adatvédelmi hatóság) a La Vanguardia tekintetében elutasította a törlési kérelmet, de a Google Spain-t és a Google Inc.-et személyes adatokat védő eszközök alkalmazására kötelezte. De mivel a cég megtagadta a törlést, a férfi a bírósághoz fordult, és az előzetes döntéshozatali eljárásban az Európai Bíróság elé került az ügy. Az ítélet alapján az újságcikk nem került törlésre, de a keresőmotor spanyol üzemeltetője köteles volt kitörölni a találatok közül. A Bíróság megállapította, hogy a Google adatkezelést végez, és a spanyol leányvállalatot nevezte meg adatkezelőnek, a tevékenység végzésének helyéből adódóan.

[29] vö.:Németh Janka: Internet és közösségi háló mint munkaeszköz In Infokomunikáció és jog 10. évfolyam 1. szám 2013. 37-41. vagy Németh Janka: Az internet nem felejt közösségi média használatára alapított munkáltatói és munkavállalói felmondások In: infokomm és jog 10. évfolyam 2. szám 2013. 96-98.
[30] vö.: Láncos Petra: A közösségi média keretei között gyakorolt alapjogok korlátozásának alkotmányos kérdései Gazdaság és Jog 24. évfolyam 3. szám 2016. 8-12.
[31] Navratyil i.m. 102-104.
[32] Az Európai Unió Bírósága A C-131/12. sz. ügyben hozott ítélet 70/14. sz. sajtóközleménye, Luxembourg, 2014. május 13./http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070hu.pdf (2016.04.13)
[33] Orcsik i.m. 2015. 13.

Tehát a célját vesztett adatkezelés jogosan törölhető[34]. Ez a területi hatály kiterjesztésével kapcsolatos problematika később is felmerül az új általános adatvédelmi rendeletben, melyre később térek ki.

2.4 Az alkalmazott gyakorlat és nehézségei

Az ítéletet követően a Google Inc. rengeteg törlési kérelmet kapott. Az űrlap elérhető az interneten. Szükséges hozzá személyazonosságot igazoló okirat másolata is. A Google mérlegelési jogköre a magánélethez való jog és a nyilvánosság megismeréséhez fűződő jog összevetése. Valamint vizsgálatot folytat valóban elavult -e az adat, és közérdekhez fűződő érdekű -e. Ezt követően felmerülhet a kérdés, milyen adatokat törölhet a Google? Az előbbi szempontrendszertől függetlenül köteles a törlésre, ha az adatkezelés jogellenes. Az érintett kérésének indoka lehet az adatok hiányossága, téves tartalma. Azzal a feltétellel, hogy a törlést a törvény nem tiltja,az adatkezelés célja megszűnt, vagy a tárolási határidő lejárt. De törlést rendelhet elő bíróság vagy hatóság is. Ha a törlés jogos érdeket sértene, az adatkezelő nem törli, hanem zárolja. Ha a magyar székhelyű Google Kft. nem töröl ilyen adatot, a Nemzeti Adatvédelmi és Információszabadság Hatóság megállapítja a jogsértést, felszólítja ennek orvoslására vagy a közvetlen veszély megszűntetésére. 30 napos határidőn belül erről tájékoztatja a keresőmotor üzemeltető az adatvédelmi hatóságot. Ha a felszólítás ellenére nem teljesít, a hatóság nyilvános jelentést készíthet, vagy adatvédelmi, titokfelügyeleti vagy bírósági eljárást kezdeményezhet.[35]

Az előbb feltárt tények alapján elavult adatkezelés, vagy egyéb jogsértő cselekmény miatt bárki kérheti az adott területi leányvállalat intézkedését. Illetve a Google Adatvédelmi Irányelvek alapján bármelyik felhasználó fordulhat a Santa Clara megyei szövetségi vagy állami bírósághoz.[36]

A felhasználó a jogorvoslati lehetőségeken túl, a gyakorlati életben ütközhet nehézségekbe. Például törléshez való joggal kapcsolatban érkezett a magyar Nemzeti Adatvédelmi és Információszabadság Hatósághoz egy panasz. Vizsgálat indult azzal kapcsolatban, hogy a www.google.hu-ról a fent leírt eljárás szerint eltávolították az adatot, de

[34]Lehóczki Balázs: Az egyének védelme az interneten elérhető személyes adataik keresőmotorok általi kezelésének vonatkozásában- az Európai Unió Bírósága In: Acta Humana 2. évfolyam 2. szám 2014. 124-125.
[35] Orcsik i.m. 2015, 14.
[36] https://www.facebook.com/legal/terms/update erre hivatkozik a felhasználási feltételek 15. pont 1-2. bekezdése

a www.google.com-ról még nem. A spanyol jogesethez kapcsolódó dokumentumokra hivatkozva a Hatóság kifejtette az ezzel kapcsolatos adatvédelmi kötelezettségeket. Tehát a törlési kötelezettség az összes adatkezelési műveletet érinti. Biztosítani kell az érintett személyes adatainak védelmét az univerzális terjesztés és megismerhetőség ellen. A Google Inc. állítása szerint megfelelő intézkedést tett, mikor az európai domain nevekre korlátozva végezte el a törlést. Indoklásuk szerint bár lehetőség van a google.com használatára, egyre ritkábban használják. Azonban ez a gyakorlat nem megfelelő, hiszen minden releváns domainre,így a com.ra is ki kell terjednie.[37] A Google Inc. intézkedése a közösségi jog megkerülésének minősült. Az adatvédelmi hatóság többszöri felszólítása ellenére sem vált teljeskörűvé a törlési folyamat. .

A Google és más web 2.0-es technológiák alkalmazása során is lehetőség van a törlésre, vagyis a "felejtés" jogához és a "feledésbe merüléshez" való joghoz. A két jog definíciója nem azonos. A Google-el kapcsolatos perekben láthatóvá vált, hogy az elérni kívánt igény csak a honlapról való törlésre irányult. Nem terjedt ki harmadik felek megosztására. Tehát a feledésbe merülés joga egyfajta univerzális törlési kötelezettséget jelent. Az adatkezelő köteles a megosztó felek felhívására, és felelős a "feledésbe merülés" végrehajtásáért.[38]

3. Facebook

A közösség alapú szolgáltatások jelentősége nem vitatható. A facebook, vagy más közösségi oldalak elsődleges funkciója az ismeretségi hálózat kialakítása, fenntartása, a saját online világ felhasználói szerkesztése.[39] Folyamatosan nő a felhasználók száma, egyre több üzlet, marketingstratégia alapul a közösségi oldalakra. Minden ilyen folyamat adatkezeléssel jár, sőt a felhalmozott információk a Big Data megnevezés alá tartoznak, ennek hatását később részletezem, mint a web 2.0 egyik új kihívása. Adatvédelmi szempontból a Facebook kiemelkedő példának tekinthető, hiszen alapításától kezdve folyamatosak a fejlesztések (pl: facebook cookie szabadalom), a belső adatkezelési szabályozások, amelyek gyakran

[37] A Nemzeti Adatvédelmi és Információszabadság hatóság jelentése a Google Inc. személyes adatok védelmével kapcsolatos jogsértése tárgyáról, NAIH/2015/1775//V.
[38] Navratyil i. m. 2015, 101-103.
[39] WP163 5/2009. számú véleménye az internetes ismeretségi hálózatokról 4-5.

ellentmondtak a hatályos jogszabályoknak. Ennek ellenére az egyik leghatékonyabban működő adatkezelést végző közösségi felületnek tekinthető.[40]

3.1 Az adatkezelés összetevői

A Facebook profil adatkezelése a regisztrációval a felhasználó hozzájárulásával kezdődik. Adatkezelő ebben a tekintetben is a szolgáltató, hiszen meghatározza az adatkezelés célját, és többféle információt gyűjt. A Facebook adatkezelési szabályzat alapján elsődlegesen ezek a regisztráció során megadott kötelező adatok: név, születési dátum, neme kiválasztása, email és jelszó megadása. Az alapvető adatokon kívül megadható telefonszám, iskolai végzettség, munkahelyek, politikai és vallási nézetek, családi kapcsolat, családi állapot, képek videók mint egyéb kategória. Ezek az úgynevezett szenzitív, különleges személyi adatok. A szolgáltatás ezen felül észleli egy fotón vagy bejegyzésben való megjelölést. Ugyanilyen adminisztrátorok számára információ például egy adott csoporthoz csatlakozás, amely megjelenhet az érintett ún. tevékenységnapjójában, és felhasználó engedélyétől függően az idővonalán. Az adatgyűjtést lefedi az igénybevett szolgáltatások, fizetési eszközökből levont következtetés, vagy a csoport és eseményekből profilozott érdeklődési kör. [41]

A felhasználói szándékon és engedélyen kívül is gyűjtenek más forrásokból származó adatot az adott eszközről. Például operációs rendszer, hardver, készülékazonosító, internet jelerőssége, az eszköz helye IP cím, GPS és Bluetooth jel alapján. Ezen felül harmadik felek webhelyeinek használatáról adatgyűjtés, amennyiben van Tetszik gomb vagy Facebook-bejelentkezéshez lehetőség, illetve a közösségi oldal hirdetési vagy mérési szolgáltatását veszik igénybe. Ugyanilyen forrásnak tekinthető az olyan adatok, amelyek a Facebook által üzemeltetett vállalatokból származnak. (Instagram, Snapchat stb.) Ugyanúgy forrásnak tekinthető a cookie-k használata.[42] Amellett, hogy 2011. szeptember 22-én elnyert szabadalom miatt a kijelentkezés, vagy deaktiválódás után is fennmarad a böngészőben az adathalmaz.[43]

---

[40] ld. Amelia D Grubbs., "Privacy Law and the Internet using Facebook.com as a Case Study" University of Tennessee Honors Thesis Projects. (2011) http://trace.tennessee.edu/utk_chanhonoproj/1369 (2016.02.12.)
[41] Facebook adatkezelési szabályzat https://www.facebook.com/privacy/explanation
[42] v.ö.: Arnold Roosendaal: Facebook tracks and traces everyone:Like this! Tilburg Law School Legal Studies Research Paper Series, 2011 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563 (2016.02.08)
[43] Cseh i.m. 2013. 92.

Természetesen a közösségi oldalak adatkezelése is célzatos. Az online alapú kommunikációs platform szolgáltatást nyújt, felkínálja az online tartalom személyre szabásának lehetőségét. Ezen felül célja a továbbfejlesztése, kutatás és felmérések alapján. A felépítéséből kiindulva egyszerűsített lehetőséget ad meg, könnyítve a kapcsolattartást és hatékony működést.[44]

3.2 Közösségi oldalak jogi háttere

A közösségi oldalak működésének jogi besorolása alapján, EU-s szinteken ide tartozik a 98/48/EK által módosított 98/34/EK irányelvirányelv, amely besorolja az ismeretségi hálózat működését. A 98/34 EK 1. cikk (2) bekezdése szerint információs társadalommal összefüggő szolgáltatásnak minősül.[45] Szintén fontos jogforrás az általános adatvédelmi irányelv. A közösségi oldalak szolgáltatásai e rendelkezéseinek hatálya alá tartoznak. Abban az esetben is, ha a székhelyük az EGT területén kívül van. Ez ugyanúgy tevékenység végzésének helyéhez viszonyított kérdés mint a keresőmotorok és a cookie-k tekintetében. A 29. cikk alapján létrehozott munkacsoport véleménye iránymutató.[46]

A hatályos hazai jog keretein belül is bizonytalan a közösségi oldalak megítélése. Több jogszabályba is beleilleszthető a tevékenység.Elsőként az Elektronikus kereskedelmi szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv). A közösségi oldalak szolgáltatásával összeegyeztethető a 2§ f) pont szerint. Tehát információs társadalommal összefüggő szolgáltatás*:* "elektronikus úton, távollevők részére, rendszerint ellenszolgáltatás fejében nyújtott szolgáltatás, amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá."Ez a jogszabályi meghatározás nem korlátozza a közösségi oldalak működését. Ezen felül vonatkozhat erre a szolgáltatásra az elektornikus hírközlésről szóló 2003. évi C. törvény (Eht.). Gyakorlatilag a közösségi oldalak által nyújtott levelező szolgáltatás igazodhat ehhez a szabályozáshoz.[47]

A jogszabályok alkalmazása aszerint rétegződhet, hogy kit érint maga a szolgáltatás, vagyis a kommunikációs csatorna. Ez létrejöhet felhasználó-felhasználó között, felhasználó-szolgáltató, felhasználó és harmadik személy között. De minden esetben

[44] https://www.facebook.com/privacy/explanation
[45] 98/34/EK irányelve a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás megállapításáról
[46] WP163 5/2009. 5.
[47] Polefkó Patrik: Barátok és bizonytalanságok közt avagy a közösségi oldalakról adatvédelmi szemszögből 1. rész In: Infokommunikáció és Jog 8. évfolyam 3. szám 2010. 110-111.

szolgáltatói szerződés jön létre. Az Európai Unión belül információs társadalommal összefüggő szolgáltatást az úgynevezett származási ország elve alapján kell rendezni. Tehát azt a jogot alkalmazzuk, ahol ténylegesen, a technológiai feltételek biztosításán túlmenően nyújtják a szolgáltatást. Technológiai feltételnek minősül a honlap fenntartása, a tárhelykapacitás bérlése, vagy a szerver üzemeltetése. Adatvédelmi szempontból nehezen értelmezhető kérdés, hogy mi sorolható be magyar tartalomnak, tehát alkalmazhatóak -e a magyar adatvédelmi rendelkezések a felhasználó személyes adatainak kezelése kapcsán. Ezt a gyakorlatban az Infotv. megítélésétől függ. Leegyszerűsített esetkör szerint ha mindkét fél magyar, alkalmazható a magyar szabályozás, ha a szolgáltató EGT területen rendelkezik székhellyel, akkor az adott tagállamé. Ha valamelyik fél 3. kategóriát képvisel, úgy a nemzetközi magánjog szerint jogválasztásnak van helye.

Mivel szolgáltató és felhasználó közti szolgáltatás szerződésként is értelmezhető, a felek is megválaszthatják az alkalmazandó jogot. Ugyanakkor fontos kiemelni, hogy ebben a kontextusban is értelmezhető fogyasztói szerződésként, melynek alapját az 593/2008/EK 6. cikk (1) bekezdése képezi. Így a jogválasztás lehetőségénél figyelembe kell venni, hogy a fogyasztó hátrányára nem lehet eltérést megállapítani.[48]

3.3 A hozzájárulás korlátai, az adatkezelés jogalapja

Miután sorra vettem a jogi kereteket, vizsgálom az adatkezelés jogalapját. Az előzőekben leírt adatok gyűjtésének, mint magának az Infotv. által meghatározott adatkezelésnek is, két feltétele van: a hozzájárulás, és a tájékoztatás. A megfelelő tájékoztatás alapján a felhasználó regisztrációja önkéntes, határozottan, félreérthetetlenül kinyilvánítja a hozzájárulását. Ha ez írásbeli szerződés keretei között zajlik a hozzájárulás, akkor őt tájékoztatni kell minden releváns információról. Elsősorban a kezelendő adatok köre, az adatkezelés időtartama, felhasználásának célja, adatok továbbítása, jogorvoslati lehetőségek. A szerződésnek feltétlenül tartalmaznia kell, hogy az érintett aláírásával hozzájárul az adatkezeléshez.[49] Ez a közösségi oldalak platformján a regisztráció végén "bepipált" felhasználási feltétel és adatvédelmi nyilatkozat. A Polgári törvénykönyv szerint

[48] Polefkó i.m.l 1. rész I 2010. 110-112.
[49] vö.WP187 15/2011. számú vélemény a hozzájárulás fogalommeghatározásáról

szerződéses szempontból ez nem ütközhet problémába, de erről az Infotv. bővebben rendelkezik. A szabályozás szerint egyetlen pipával ellátott sor nem fedi le a hozzájárulást, a kellő információ ismeretét, vagy a garanciát jogellenes helyzet elhárításáról és megelőzéséről. Valamint általánosságban elmondható, hogy a felhasználók nagy része nem olvassa el ezeket a feltételeket és nincs tisztában az adatvédelemmel. Ezért fontos cél mind a Facebook mind más közösségi oldalak fejlesztésében, hogy a szolgáltatás során, leegyszerűsített formában a felhasználó megismerhesse saját adatkezelésének határait.[50]

Ezeket a határokat a regisztráló fél a belső szabályozáson, és a honlap felépítésén keresztül ismerheti meg. Miután a regisztráció megtörtént, kvázi egy szolgáltatási szerződés létrejött, a Facebook köteles fenntartani a tájékoztatást korlátainak és lehetőségeinek megismerését. Hiszen lényeges kitétel, hogy a szolgáltató kommunikáció platformot biztosít, amit a felhasználók szerkesztenek. Ebből adódóan lehetővé kell tenni számára, hogy az önkétes hozzájárulását bármikor visszavonhassa. Tehát biztosítani kell számára a leiratkozást, adattörlést, a kiegészítő szolgáltatás igénybevételének megszűntetését (egyes reklámok, hirdetések, alkalmazások). Célszerű tájékoztatni arról, milyen határidővel törlik a felhasználó adatait és mik azok az adatkezelési célok, ami alapján bizonyos ideig megőrzésre kerülhetnek a szolgáltatónál. Ezáltal a közösségi oldal különbséget tesz törlés, ideiglenes hozzáférhetetlenné tétel és a végleges törlés között. Bár a felhasználó maga szerkeszti saját virtuális világát, a szolgáltató fenntartja a jogot szerződésszegés esetén a profil használatának korlázozására vagy közösségből való kizárására. A rendszer az újraregisztrálás általi csalás kiszűrésére speciális cookie-kat fejlesztett ki.[51]

3.4 A felhasználó adatait védő opciók

A jogkövető felhasználó a későbbiekben is önmaga dönt a személyes és szenzitív adatok megadásáról, megosztásukról, láthatóságukról.[52] Ezt segíti a tevékenységnapló és a különböző adatkezelési tájékoztatók, irányelvek. Utóbbi útmutatók olyan speciális felhasználói kategóriához is szólhatnak mint a kiskorúak, szülők, tanárok. [53]

[50] Polefkó i.m. cikk 2. része, 2010 174.-175.
[51] Polefkó i.m. cikk 3. része, 2010. 210.
[52] Cseh i.m. 2013. 92-95.
[53] Facebook biztonsági központ https://www.facebook.com/safety/ és közösségi alapelvek https://www.facebook.com/communitystandards

A Facebook biztosít felhasználói felületet és védelmet. A regisztráció fontos eleme, hogy 13 év alatti kiskorú személy nem hozhat létre profilt.[54] A szolgáltató köteles őket speciális védelemben részesíteni. Ilyen példaként említhető a 2009. évi Hyves egyezség, melyet aláírt a Facebook, a Google és a Myspace. Ennek eredményeként jött létre a visszaélés bejelentése gomb. Az egyezmény meghatározása alapján a fiatal felhasználók személyes adatai főszabályként nem nyilvánosak, és nem lelhetőek fel keresőmotorok keresési találatai között. Minden funkciót, ami a magánéletük védelmét szolgálja jól láthatóan, könnyen elérhetően kell biztosítani[55]

Azonban a garanciák ellenére Facebook adatkezelésével kapcsolatban is felmerülhetnek visszaélések. Németország 2016 szeptemberében lépett fel a jogosulatlan adatbázis növeléssel szemben. Két szolgáltatás, a Facebook és a WhatsApp kapcsán végzéssel tiltották el a felhasználók személyes adatainak összevont kezelését. A közösségi oldal a WhatsApp felvásárlása után nem kerített sort a felhasználói adatbázis elkülönítésére, és a adatkezeléshez sem született jogalap, amelyhez a felhasználó hozzájárulhatott volna. Így a Facebooknak törölnie kellett az alkalmazásból szerzett adatokat. Ez 35 millió német felhasználót érintett.[56]

[54] ld. bővebben Kulcs a net világához! a Nemzeti Adatvédelmi és Információszabadság Hatóság tanulmánya a gyeremekek biztonságos és jogtudatos internethasználatáról, 2013. www.naih.hu/files/2013-projektfuzet-inter**net**.pdf
[55] Cseh i.m. 2013 94.
[56] https://net-jog.hu/2016/10/04/a-facebook-felrevezeti-a-felhasznalokat-nemetorszagban/ (2016.10.05.)

3.5 A Shrems ügy

A közösségi oldalak, és más web 2.0-es szolgáltatások szempontjából is kiemelkedő az adattovábbítás kérdése. A következőkben egy adattovábbítással és a Facebookkal kapcsolatos ügyet tárok fel, felhívva a figyelmet az ezzel kapcsolatos kihívásokra.

Az osztrák nemzetiségű Max Shrems kikérte az öszes kezelt személyes adatát a Facebooktól. Az így kapott hatalmas mennyiségű és eltérő minőségű személyes adatokkal szembesülve felkereste az ír adatvédelmi hatóságot. Ez a hatóság képviseli a Facebook európai képviseletét. Azzal kapcsolatban kereste fel őket, hogy vizsgálják meg az európai szabályokhoz mérten megfelelően kezelte -e a személyes adatait. Véleménye szerint a Facebook korlátlan hozzáférést nyújtott az amerikai titkosszolgálatoknak.[57] Az adatvédelmi hatóság a Safe Harbor jogalapra hivatkozva nem vizsgálta a kérdést 2000. július 26-a óta az EU Bizottság 2000/520/EK döntése alapján, amennyiben külföldre az adattovábbítás olyan amerikai vállalat részére történik, amely az USA Kereskedelmi Minisztériuma által vezetett listáján szerepel, kötött a jogszerű adattovábbításhoz. Ebbe a körbe tartozik a Facebook és a Google is. A Schrems ügy eljutott az ír Legfelsőbb Bíróságig, majd a Luxemburgi Bíróságig. Az ítélet szerint a Safe Harbor nem korlátozhatja vagy írhatja felül a hatóság vizsgálati jogosultságát arról, megfelelően kezelik -e a felhasználók személyes adatait.[58] Valamint érvénytelennek nyilvánították a megállapodást, mivel nem került sor az USA teljes jogrendszerének uniós adatvédelmi elvek szerinti vizsgálatára. Így az uniós adatvédelmi garancia nem állhat fenn, hiszen az amerikai hatóságok, mint a titkosszolgálatok szinte korlátlan megismerési joggal rendelkeznek. Az érintetti jogok mint a hozzáférés, törlés, helyesbítés, jogorvoslat, nem érvényesülhetnek. A bíróság megállapította, hogy az önkéntes vállaláson, szerződésen alapuló rendszer nem nyújt kellő védelmet, ha a harmadik ország jogszabályai ellentétes kötelezettségeket fogalmaznak meg. Tehát egy nemzetközi kikényszeríthető, ellenőrízhető kötelezettségvállalás lehet rá a megoldás. Az Európai

[57] Domokos Márton, Poefkó Patrik: Egy bírósági döntés következményei-avagy az Európai Bíróság ún. Schrems döntésének hatásai, a Safe Harbor sorsa és a felmerülő kérdések az adatvédelem területén In: Infokommunikáció és Jog 12. évfolyam 4. szám 2015. 123.

[58] A Nemzeti Adatvédelmi Hatóság beszámolója a 2015. évi tevékenységéről, 103-104 https://www.naih.hu/files/NAIH-BESZ-MOL--2015-MID-RES.pdf (2016.07.05)

Uniónak felül kellett vizsgálnia a Safe Harbor döntést, és megállapodásos egyezséget kívántak létrehozni.[59] Ennek eredményéről a későbbiekben lesz szó.

4. Cookie: az online marketing alapja

A felhasználók számára újdonságként hathat a weboldalakon megjelenő alábbi mondat: "Ez a honlap sütiket használ. A sütik elfogadásával kényelmesebbé teheti a böngészést. A honlap további használatával hozzájárulását adja a sütik használatához". Azonban a cookie, azaz a viselkedés alapú online marketing már hosszabb ideje létezik. Az ilyen marketing lényege az internethasználat nyomon követése, amellyel később létrehozható a felhasználó profilja. Ezen profil alapján érdeklődésének megfelelő reklámokat juttatnak el hozzá. A vizsgálat, az egyéni cselekvés felmérésének az eszköze lehet a honlapok többszöri felkeresése, kulcsszavak, interakciók. Az eredmény egy részletesen kidolgozott felhasználói profil a hirdető számára Ez a reklámozás jelentős gazdasági előnyökkel járhat, de elsődlegesen a magánélet tiszteletben tartását, és az adatvédelemhez való jogot kell figyelembe venni.

Ez az analízis nem kizárólagosan felhasználó-hirdető szerinti két komponensű folyamat. A reklámforgalmazó rendszer főbb szereplői a reklámhálózat-szolgáltatók. A segítségükkel kapcsolódhat össze közvetítő a hirdetővel. A közvetítő a honlap tulajdonosa, a hirdető pedig az adott termék vagy szolgáltatás népszerűsítője. A bevétel céljából a közvetítő reklámozási felületet biztosít a honlapján. [60]

4.1 A nyomon követés elemei és célja

Az online alapú analízis tárgya egy nyomon követő cookie az érintett végberendezésen. Ezt a tárolt adatot az egységesség miatt nevezik cookie-nak, de funkcióit tekintve több fajta alfanumerikus szöveg létezik. A nyomon követés akkor indul, mikor a felhasználó első alkalommal belép az adott oldalra A cookie-k élettartama változó. Lehet tartós cookie, például a Facebook esetében, vagy lejárati idővel rendelkező vagy manuálisan törölhető. A hagyományos cookie elutasítását vagy érintett általi törlését az ún. flash cookie (

[59] 29-es Cikk szerinti Munkacsoport nyilatkozata a Schrems-ügy következményeiről https://www.naih.hu/files/2016-02-08-nyilatkozat_forditas_SCHREMS.pdf (2016.07.04.)
[60] WP171 2/2010. számú vélemény a viselkedés alapú online reklámról 1-11.

helyi megosztott objektum). Ez az eljárás respawning, újraszármaztatás. Ebből is látható a nyomon követés sokrétűsége.[61]

A nyomon követés eredményeként jön létre egy felhasználói profil, szintén különböző azonosító típusból. A profil prediktív vagy explicit módon épülhet fel. Prediktív az egyéni és kollektív felhasználói viselkedés hosszantartó megfigyelése[62]. Például a felkeresett oldalak, hirdetések kattintások. A reklámhálózat-szolgáltatók, nyomon követési technikák és adatbányász szoftverek együttes alkalamazásával jöhet létre ilyen profil. Abban a kérdésben, hogy a felhasználót milyen hirdetések érdekelhetik a meglátogatott honlapokból és a korcsoportra vonatkozó következtetésekből állapítják meg. Az explicit profil olyan személyes adatokból áll, amelyet a felhasználó ad meg a szolgáltatónak a regisztráció során. Természetesen a két módszer összefüggésben áll, együttesen működik egy web 2.0-es szolgáltatásban. A cookie analízisen alapuló profil folyamatosan kiegészíthető olyan halmozott adatokkal, következtetésekkel. Az online reklámozási rendszerek a felhasználókat különböző csoportokba sorolhatják, érdeklődési körök függvényében. A végberendezések az IP-cím és Wifi hozzáférési pontok használatával is elkészíthetik a célprofilt.

A cookie-k által végzett adatgyűjtés célhoz kötött. Az analízis funkciója három szintű. [63] Ilyen funkció a célzott hirdetések küldése, az adatgyűjtés a weboldal használatával kapcsolatban és a felhasználói élmény növelése.Szemmel látható, hogy az internetes világot "behálózta" a cookie alapú online analízis. Ezért fogyasztóvédelmi és adatvédelmi bizonytalanságok miatt is releváns volt a részletes szabályozás. A következőkben technológia jogi kereteit vizsgálom

4.3 Az analízis jogi háttere

EU szinten több irányelvre is hivatkozhatunk. Kiindulási alapként a 2002/5817 irányelv 5. cikkének (1) bekezdése általánosan védi a felhasználók közti kommunikáció bizalmas jellegének fenntartását. A cookie-k és ehhez hasonló eszközökről a cikk (3) bekezdése rendelkezik. Ezt a szabályozást bővíti, módosítja a 2002/58, azaz a módosított elektronikus adatvédelmi irányelv. Erre hivatkozik a 29.es Munkacsoport véleményezése. A

[61] WP171 2/2010. i.m. 6-7
[62] WP 171 2/2010. i.m. 8.
[63] Domokos N. Márton: Sütiszörny megérkezett! A cookie-k használatának jogi szabályozása, Jogi Fórum, (2012) 3-5. http://www.jogiforum.hu/publikaciok/490 (2016.03.18)

cikk tárgyi hatálya szerint a jogszerű az előfizető vagy felhasználó végberendezésén az adattárolás, ha tájékoztatáson alapul a hozzájárulás. Ehhez kötött az adattárolás és a tárolt információhoz való hozzáférés. Tekintettel arra, hogy a cookie-k végberendezésen tárolt információnak minősülnek, e hatály alá tartoznak. Így ha az érintett ellátogat egy partnerhonlapra, a reklámhálózat-szolgáltató hozzáférhet. A technológiasemlegességből adódóan a cookie-k vagy típustól függetlenül más hasonló eszközök tárolása, későbbi használata és hozzáférése is ez a szabályozás vonatkozik. Ennek nem feltétele, hogy a cookie a 95/46/EK értelmezése szerinti személyes adatnak minősüljön. Bár a cookie mint végberendezésen tárolt adat a magánszféra részét képezheti, ezért a 95/46/EK tárgyi hatálya alá is tartozik. Valamint attól függetlenül, hogy a cookie-t elhelyező személy adatkezelő vagy adatfeldolgozó, szintén alkalmazandó az 5. cikk (3) bekezdés. Ezt az állítást az irányelv (24) preambulumkezdése ragadja meg: "(...) felhasználóinak végberendezései és az azokon tárolt minden adat a felhasználó magánszférájának részét képezi, amelynek az Emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény alapján védelmet kell élveznie. " A 29. cikk alapján létrehozott munkacsoport ehhez kapcsolódó véleményében szintén a 95/46/EK tárgyi hatálya alá tartozik, attól függetlenül, hogy a cookie nem minősül személyes adatnak. Abból adódóan, hogy a viselkedésalapú reklámmódszerek során adatfeldolgozás történik. Az egyedi azonosítók vagy az IP-címek gyűjtése segítséget nyújt az érintett egyedi azonosításában, abban az esetben is ha a név ismeretlen. Valamint a cookie-k segítségével, az online analízis fő funkciójaa felhasználó érdeklődési, vásárlási körének befolyásolása. Ez összekapcsolható a felhasználó által megadott explicit profillal, amely az érintett azonosításához vezethet.

Magyarországon a cookiekra vonatkozó szöveget az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht) 155§ (4) bekezdés tartalmazza.[64] Azonban az Eht.-re való hivatkozás a gyakorlati életben nehézségekbe ütközhet. Hiszen e törvény hatálya nem feltétlenül fedi le a weboldalak üzemeltetését, a cookie által biztosított szolgáltatások nyújtását. 1§ a) pont szerinti megnevezésében.[65] Így ebben a kérdésben ismét az Ekertv. információs társadalommal összefüggő szolgáltatásaihoz kapcsolódó szabályozáshoz

[64] "Egy előfizetőnek vagy felhasználónak elektronikus hírközlő végberendezésén csak az érintett felhasználó vagy előfizető világos és teljes körű-az adatkezelés céljára is kiterjedő- tájékoztatását követő hozzájárulás alapján lehet adatot tárolni vagy az ott tárolt adathoz hozzáférni."

[65] " a Magyarország területén végzett vagy területére irányuló elektronikus hírközlési tevékenységre, valamint minden olyan tevékenységre, amelynek gyakorlása során rádiófrekvenciás jel keletkezik,"

fordulhatunk.[66] Ezen felül ebben a kérdésben is mérvadó az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv). Például az adatkezelési alapelvek, adatgazdák jogaira vonatkozó rendelkezések tekintetében.[67]

[66] 2§ f) pont: Információs társadalommal összefüggő szolgáltatás: elektronikus úton, távollevők részére, rendszerint ellenszolgáltatás fejében nyújtott szolgáltatás, amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá

[67] Domokos i.m. 1-2.

4.4 A cookie-k jogalapja

Miután feltártam a cookie technológiájú adatkezelés célját, jogi szabályozását, e téma gyakorlati, jogalapot adó tevékenységét tárom fel. A web 2.0-es szolgáltatásokhoz kapcsolódóan itt is kiemelkedő a felhasználó tájékoztatásának és hozzájárulásának szerepe.

A 5§ (3) bekezdés alapján a felhasználó hozzájárulása kiterjed a cookie elhelyezésére, adatgyűjtésre. A hozzájárulás akkor érvényes, ha az adott esetre vonatkozó tájékoztatást az érintett megkapta. A személyes adat gyűjtését megelőzően kell ismertetni a technológiát, hogy teljes mértékben tisztában legyen annak feltételeivel. Valamint fontos kitétel, hogy a hozzájárulás visszavonható legyen. Figyelembe véve, hogy megfelel -e a gyakorlat az irányelv előbb említett szakaszának.

Egy adott honlapon, ahol megjelent egy hirdetés, amint elhelyeztek cookie-t, a felhasználót tájékoztatják. Ismereteket szerezhet arról, hogy a böngészőben is beállítható, ellenőrizhető a cookie-k megjelenése. A tájékoztatót a közzétevő és a reklámszolgáltató teszi lehetővé saját általános szerződési feltételeikben vagy adatvédelmi szabályaikban. Ez tartalmazza a viselkedés alapú online marketing alapfelhasználát és a böngésző beállítását. A gyakorlat így ellentétben állhat az 5. cikk (3) bekezdéssel meghatározott adatgyűjtés előtti előzetes tájékoztatás és hozzájárulás kérésével. Hiszen a felhasználó regisztráció során történő hozzájárulása nem terjed ki a cookie-k használatára. Ebben az esetben a 2002/58. irányelv (66) preambulum-bekezdésére lehet hivatkozni. Tehát technikailag lehetséges az adatkezeléshez való hozzájárulási szándék kifejezése böngésző vagy egyéb alkalmazás megfelelő beállításával. A felhasználó visszavonhatja a harmadik féltől származó cookie-k használatának engedélyét illetve módosíthatja saját profiljának érdeklődési körét. Így a (66) preambulum-bekezdés nem kivételt jelent a hozzájárulás-tájékoztatás jogalapja alól, hanem flexibilis, gyakorlatias megoldást nyújt.[68]

Természetesen a legtöbb esetben fontos az előzetes hozzájárulás léte ez jobban idomul az 5. cikk (3) bekezdésben leírtakhoz. Tekintettel arra, hogy a hozzájárulás az adatfeldolgozás jogi alapja, a 29. Munkacsoport is megerősítette ezt a nézetet: “A technológiai fejlesztések is szükségessé teszik a hozzájárulás gondos vizsgálatát. A gyakorlatban a 95/46/EK irányelv 7. cikkét nem mindig alkalmazzák megfelelően, különösen nem az internet összefüggésében, ahol a hallgatólagos hozzájárulás nem mindig jelent

[68] WP194 4/2012. számú vélemény a sütikhez való hozzájárulás alóli mentességről 2-6.

egyértelmű hozzájárulást. Mint ahogy az Irányelv 7. cikkének a) pontja előírja. Az, hogy az érintettek határozottabban képviselhessék álláspontjukat azt megelőzően, hogy mások személyes adataikat feldolgoznák, kifejezett hozzájárulást (és így hozzájárulási mechanizmust) igényel minden olyan feldolgozáshoz, amely hozzájáruláson alapul." A munkacsoport 1/199. ajánlásában javasolja az egyedi üzenetek használatát. Tehát a cookie-k esetén a felhasználót tájékoztatni kell azok fogadásáról, tárolásáról, küldéséről, annak céljáról és időtartamáról. A tájékoztatás után fenntartható a felhasználó számára a lehetőség, hogy szeretné -e ,ha profilt készítenének róla a reklámozás céljából. A megvalósítás problémája többszintű. Egyrészt a tájékoztatáson alapuló beleegyezés ezek szerint egyszeri és visszafordíthatatlan. Másrészt a felhasználó maga elfelejti a hozzájárulását, de jogosult lenne adatvédelmi intézkedésekre. A 29. cikk alapján létrehozott munkacsoport megoldási mechanizmusként három opciót javasol. Először is mint a cookie-t, az ehhez kapcsolódó hozzájárulást is korlátozni kell. Meghatározott időszakot követően, a reklámhálózat-szolgáltatónak új hozzájárulásra lesz szüksége. Emellett fontos a hozzájárulás visszavonhatóságának fenntartása. Illetve kiemelkedő jelentőségű az internethasználó felhasználóbarát, eredményes, közvetlen, rendszeresen ismétlődő tájékotatása.

A 04/2012. számú vélemény figyelembe véve az adatkezelés jogalapjának gyakorlatiasságát, kitér a hozzájárulást nem igénylő esetekre is. Az 5. cikk (3) bekezdés szerint két esetben mentesül a tájékoztatáson alapuló beleeggyezés alól. Elsőként azok a cookiek amelyek közlést továbbítanak. A második eset, amikor az előfizető vagy felhasználó kifejezetten kéri és a szolgáltatás nyújtásához feltétlenül szükséges. Például az internetes áruházakban jellemző cookie a "kosárba" gomb, vagy a biztonsági cookie, vagy a jelszóval védett munkamenethez használt cookie.[69] Összességében látható, hogy a viselkedés alapú online analízis alapját képező technológia összetett. Több célt szolgál a cookie használata, így egy hozzájárulás nem fedi le az egész mechanizmust. Tehát mind a jogi háttérnek, mind a gyakorlatnak utol kell érnie a folyamatos fejlődést.

5. Cloud Computing: fogalma, adatvédelmi nehézségei

A web 2.0 szolgáltatás célja az internet alapú mobilitás elérése. A cloud computing az adattárolás mobilitását hordozza magában. Egyfajta gyüjtőfogalom az informatikai

[69] WP194 4/2012. 6-10.

szolgáltatások halmazához. Közös elemük, hogy a számítóközpontja nem a felhasználó vállalati vagy otthoni számítógépe, hanem egy távoli bárhonnan elérhető szerverközpont. Leggyakoribb felhő alapú szolgáltatás a levelezőrendszerek, tárhelyek és virtuális munkavégzési keret biztosítása. Ezek gazdaságos, személyre szabott rendszerek, tehát végbe megy személyes adat adatkezelése is, amely több aggályt is felvethet. A felhasználói adatok folyamatos mozgásban vannak, amelyről az adat birtokosa nem feltétlenül értesül.[70] A szolgáltató több olyan alvállalkozót is igénybe vehet, akik ügyfél közrehatása nélkül dolgozzák fel az adatokat. Például marketing felhasználás céljából. Ellenszolgáltatás igénye merülhet fel abban az esetben, ha összetett vállalati alkalmazás során alkalmazott felhő tartalmát le kívánják tölteni vagy adataikat törölni. Így a vállalkozásoknak és a közigazgatási szerveknek fel kell mérnie az általuk használt szolgáltatás bizonyos hátrányait. Ezzel szemben a szolgáltató kötelessége, hogy ellássa az ügyfeleket minden szükséges információval.[71]

Mi minősül adatvédelmi kockázatnak a cloud computing használata során? Az előbb leírt két szempont, tehát ellenőrzés és információ hiánya alapján csoportosíthatóak a példák. A felhasználó személyes adatokat bocsát a szolgáltató rendelkezésére, így többé nem gyakorol felette kizárólagos ellenőrzési jogot. Emellett fennáll a rendelkezésre állás és a sértetlenség hiánya is,tekintve hogy, a szolgáltató kezeli a felhőben lévő tartalmakat. Megfelelő példa erre, hogy a szolgáltató kiadja a személyes adatokat más bűnüldöző szervezetnek és a felhasználónak nincsen beavatkozási lehetősége. A másik probléma az adatkezelés átláthatatlanságának hiánya is több szempont szerint mutatkozik meg. A kellő információ hiányában a felhasználó nincs tudatában a fennálló veszélyekkel, kockázatokkal. így nem hoz megfelelő intézkedést. Ennek eredete lehet, ha az adatkezelő nincs tisztában a fennálló adafeldolgozási láncolattal, vagy az EGT-n belül és kívüli különböző szabályozásokkal. Az EGT-n kívüli harmadik országokban a különböző adatvédelmi elvek miatt nem megfelelő szintű az adatvédelem és egyes adattovábbítási műveletek jogellenesnek minősülhetnek. Az átláthatóság megőrzése érdekében a számítási felhőben szereplő adat érintettjét, a 95/46/EK 10. cikk előírása szerint tájékoztatni kell az adatkezelő személyéről, az adatfeldolgozás céljáról.

[70] https://www.naih.hu/adatvedelmi-szotar.html

[71] l.d.:Bogdan Radu: The use of web-based applications developed on cloud infrastructures-juridical implications for the juridical professions, Dimitrie Cantemir Christian University, National Strategies Observer No.2/Vol.1, 2015 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2787619 (2016.02.08)

A fenti leírások alapján a dolgozat következő soraiban felsorolom a számítási felhő jogi kereteit. Elsődleges keretet biztosít a 95/46/EK adatvédelmi irányelv minden olyan esetben amikor cloud computing útján történik személyes adat feldolgozása. Ugyanebben a körben alkalmazandó a 2002/58/EK elektronikus hírközlési ágazati és e-magánéleti irányelv által meghatározott szabályozás.

Hasonlóan mint más web 2.0-es szolgáltatás esetében, itt is fontos az alkalmazandó jog vagyis a területi hatályok meghatározása. Az alkalmazhatóságot megállapítható az általános adatvédelmi rendelet 4. cikke alapján, amely kiterjed az EGT-n belüli egy vagy több telephellyel rendelkező adatkezelő tevékenységére. Az EGT területén kívül levő szolgáltatásra szintén kihat az előbbi szabályozás, amennyiben az adatkezelő tevékenységét ahhoz a területhez köti. Az alkalmazandó jog a letelepedés és a tevékenység helyéhez köthető az irányelv 4. cikk (1) bekezdés a) pontja alapján. Ebben a kérdésben irreleváns, milyen típusú a cloud szolgáltatás, hiszen minden típusnál az adott országban, ahol letelepedett az adatkezelő kötve van az ottani adatkezelési szabályzatokhoz .A nem letelepedett adatkezelők esetére a 4. cikk (1) bekezdés c) pontja vonatkozik.

A cloud computing kérdéskörében felmerül az adatkezelő és az adatfeldolgozói szerep különbségeinek összemosódása és átláthatóságának hiánya. Mind az adatkezelő mind az adatfeldolgozó definícióját az Infotv. határozza meg, de a két fogalom jelen összemosódása a 10§ (3) bekezdés szerinti saját célú adatfeldolgozás tilalmát érintheti.[72] Uniós szabályozás szintjén e két fontos fogalomról értekezik a 29.es munkacsoport 1/2010. számú adatkezelő és az adatfeldolgozó fogalmáról szóló véleménye.Eszerint az adatkezelő fogalmával egyuttal azt is meghatározzuk, ki vállal felelősséget, illetve hogyan oszlik el. E szerepkörök meghatározásánál a felhő alapú szolgáltatás igénybevevőjéről és a szolgáltatóról beszélünk. A felhasználó meghatározza, milyen célú és milyen módszerű legyen az adatfeldolgozás, így ebben a helyzetben adatkezelőnek tekinthető. Idomulva az irányelv általi meghatározásához, vagyis 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".[73] Az igénybevevő a szolgáltatás használata előtt, regisztrációkor elfogadja az adatvédelmi jogszabályok, belső szabályozások betartását és ezek ismeretéről elméletileg felelősséget vállal. Az igénybevevőt követően a szolgáltató

[72] Bocsok i.m. 2015. 61-62.
[73] ld. WP169 1/2010. számú vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról

szerepét tekintve adatfeldolgozónak tekinthető. Biztosítja az adatfeldolgozás platformját és annak meghatározott módját, az irányelv szerint definiálva, vagyis "természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv amely személyes adatokat dolgoz fel az adatkezelő nevében". Azonban egyes körülmények szerint tekinthető közös vagy saját jogú adatkezelőnek, ha például saját céljára dolgozza fel az adatokat. Az igénybevevőn, szolgáltatón kívül létezhet egy harmadik fél, az alvállalkozó. Az alvállalkozó szerződő fél, szerepkörében szintén adatfeldolgozóként tekinthető. Így hozzáférésük lesz a felhasználó személyes adataihoz, erről a szolgáltató köteles értesíteni az igénybevevőt, részletesen megjelölve az alvállalkozó szolgáltatási típusát..

Az előzőek alapján fontos kitérni arra, felsorolás szintjén, hogy mik azok a garanciák, amelyek a felhasználónak biztosítják a személyes adatainak védelmét. Mindenek előtt szót kell ejteni a felek jogáról és kötelezettségéről. Fenn kell állnia egyfajta felhasználói tudatosságnak, tehát az igénybe vevő olyan felhő szolgáltatót, adatfeldolgozót válasszon, amely képes megfelelő technikai és biztonsági intézkedések alkalmazására.[74] Ezt a követelményt a 46/95/EK 17. cikk (2) bekezdése írja elő, a (3) bekezdés kötelezi a feleket a hivatalos szerződés megkötésére. A szerződés követelménye, hogy az adatfeldolgozó elfogadja az adatkezelő által meghatározott célt és módszert. Emellett a szerződésnek ki kell térnie a személyes adatok feldolgozásának tárgyára, terjedelmére, idejére, módjára és céljára. Szintén fontos pontja a szerződésnek az adatkezelő kérésére illetve a szolgáltatás végével történő adatmegsemmisítés feltételeinek részletezése. A szolgáltató köteles elősegíteni a felhasználó hozzáférési és törlési jogának gyakorlását. Ugyanezek a kötelezettségek vonatkoznak a szerződésben meghatározott esetleges harmadik félre. Minden szerződő fél köteles az együttműködésre illetve a szolgáltatás belső szabályozásának nyújtására, ismeretére, betartására. A jogok és kötelezettségek felsorolásából következnek az intézkedések, amelyek biztosíthatják a személyes adatok védelmét. Ezek a rendelkezésre állás, sértetlenség biztosítása, átláthatóság, célhoz kötöttség, beavatkozási lehetőségek, elszámolhatóság és hordozhatóság.[75]

[74] vö. Dimitra Kamarinou, Christopher Millard, W Kuan Hon: Privacy in the Clouds: an empirical study of the terms of service and privace policies of 20 Cloud service providers, Queen Mary University of London, School of Law Legal Studies Research Paper No 209/2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646447 (2016.10.10.)
[75] WP29 05/2012.számú vélemény a számítási felhőről, 2-19

6. A jogalkotás újabb kihívásai

A 21. században web 2.0-es szolgáltatások sok szempontú kihívást jelentenek. Bár az előzőekből látható, hogy adatvédelmi szempontból besorolható egy-egy technológia és közös alapot képez. Cél, adatkezelés, jogi keret, jogalap, gyakorlati problémák alapján. Azonban az aktualizált szempontrendszerrel szemben is léteznek újabb, szabályozatlan területek. Jelen dolgozat kihívásként kezeli a folyamatosan terjedő IoT technológiát. Valamint a már meglévő közösségi oldalakhoz kapcsolhatóan, az online adatok kezelését a felhasználó halála után. A következőkben érintőleges szinten rávilágítok a két eset problémájára, szabályozási lehetőségeire. Ezen példák is bizonyítani fogják, hogy a napjainkban végbemenő adatkezelés messze túllépi a hagyományos adatvédelem határait.

6.1 A dolgok internete, IoT

Kevin Ashton, a Procter&GAmble brand managere használta először az Internet of Things, a dolgok internete megnevezést. Ez magába foglalja tárgyak, eszközök, rendszerek és az emberek közötti kommunikációt. Lényeges eleme az összekapcsolt hálózatra kötött eszközök közötti információcsere, külső beavatkozás nélkül. Az ember felé közlés szintén egy eszköz által kezdeményezett rendszeren történik. A közvetítő rendszerből adódik, hogy fejlettebb technológia mint a M2M (Machine to machine) kommunikáció, hiszen a rendszer központi eleme és címzettje az ember. E technológia megjelenése feltételezi az internet és szolgáltatásokat kiszolgáló infrastruktúra fejlettségét. Ilyen infrastruktúra például a szoftverek, cloud. Ahogy a többi web 2.0 szolgáltatás során,az internet itt is kvázi erőforrásként szolgálja az információs társadalmat. Szerteágazó technológiáról beszélünk, hiszen egy már működő mechanizmusról beszélünk. Jogi szempontból releváns, új elemekben bővelkedő szerződések születnek felhasználó és szolgáltató között.[76]

Az IoT technológia besorolása szerint egyfajta adatátviteli infrastruktúra. Az EU és ITU (International Telecommunication Union) közreműködésével létrehozott IERC (European Research Cluster on the Internet of Things) meghatározása alapján képes adatgyűjtésre, feldolgozásra, továbbításra. Az információáramlást az internettől nem

[76] ld.Ian Walden, Guido Noto La Diega: Contracting for the "Internet of Things": Looking into the Nest, Queen Mary University of London, School of Law Legal Studies Research Paper No. 219/2016

elkülönülő globális dinamikus hálózat, például felhő biztosítja. Használata történhet ingyenes vagy viszterhes bérleti keretek alapján. Tehát magasan automatizált, informatizált ágazat, amely fejlődést hozhat ún. "okos" energetika, ipari-rendszerek, e-egészségügyi távdiagnosztika, biztonságtechnikai, e-egészségügyi, e-kormányzat területén.[77] Mint ahogy általában a web 2.0-es szolgáltatásoknál a cél az egyediesítés. Minél több alkalmazás, szolgáltatás nyújtása az érintett környezet-specifikus adatait figyelembe véve. Az adatokból nyerhető következtetés az érintett azonosításra alkalmas, így személyes adatokat kezel. [78] A 29.es Munkacsoport véleményezése 3 technológiát vizsgál meg részletesen. Például a testen hordható számítástechnikai eszköz mint okos óra, Google Glass okos szemüveg[79], az ún. számszerűsített én, mint az alvásmonitor egyénről életmódra jellemző adatokat generál. Végül ilyen népszerű kategória az "okos otthon" vagy "domotika" összekapcsolt rendszerrel internet és termosztát, világítás, sütő rendszerek között. Újszerűsége nem csak a technológiai megjelenésében, de az új adatvédelmi folyamatokban is megmutatkozik.

A dolgok internete működése, mint információcsere folyamata, nem természetes személyek között zajlik. Annak ellenére hogy automatizált, gépek közötti kommunikáció, ugyanúgy sor kerül a személyes adatok feldolgozására, kezelésére. A tárgyak működéséből nyert következtetések már érintik a természetes személy magánszféráját. Minél több a hálózatban résztvevő tárgyak száma, annál részletesebb a személyiségprofil.[80] Így az IoT magánszférát érintő kockázatot jelent, hiszen az automatizált rendszerben nem történik ellenőrzés. Valamint sok esetben a felhasználó nincs tisztában az adatkezelés tényével, így a folyamatot nem alapozza meg az érintett hozzájárulása. Adatvédelem szempontjából szintén jelentős momentum, hogy mivel nem ember végzi az adatkezelést, nincs rá garancia, hogy személyes adat nem kerül egyéb célú felhasználásra.[81] Hazai jogi szabályozás is korlátozza a besorolhatóságukat, mert az Infotv. csak a természetes személyt, jogi személyt vagy jogi személyiséggel nem rendelkező szervezetet tekint adatkezelőnek. Jelen esetben közvetlen emberi beavatkozástól mentes a működés. Ebből adódóan bizonyos szinteken szükséges változtatni a szabályozáson. Például kibővíteni az adatkezelő fogalmát és tevékenyését. Indokoltságát igazolja, hogy a fogalom kiterjeszthető arra a célra amelyet természetes

[77] Bocsok Viktor, Boldizsár Péter Ferenc, Loós Csaba, Major Tamás: A dolgok internete- Technológiai háttér, információbiztonsági és adatvédelmi aspektusok In: Infokomunikáció és Jog 12. évfolyam 2-3.szám , 57. (2015)
[78] WP223 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, 4.
[79] ld. NAIH beszámoló a 2013.évi tevékenységéről 44-45.
[80] Szabó i.m. In: Tóth i.m. 2016. 56-57.
[81] WP223 8/2014. 6-10.

személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet határoz meg, és végrehajtására ilyen technológiát üzemeltet. Jelentős az adatkezelés, hiszen az IoT eszköz több adatforrásból gyűjtheti. Erre példa egy passzív gépi forrás mint a szívritmus mérése. A hatályos adatvédelmi szabályozás, a technológiai semlegességből kiindulva a gép nem minősülhet adatkezelőnek,így felmerülhet e fogalom megváltoztatásának igénye.[82]

6.2 Az online adatok sorsa a halál után

A virtualizált térben a felhasználók egyedi platformokat teremthetnek meg. Ám a web 2.0-es szolgáltatások korlátlan lehetőségeitől eltérően a mi emberi életünk véges. De a felhasználóé végtelen? Felmerülhet a kérdés, mi történik saját illetve profilunkból összeállított személyes adatainkkal halálunk után? Valójában ez a kérdés önállóan, jogilag szabályozatlan, mind magyar mind az európai gyakorlatban. E fejezet alapját a NAIH által megfogalmazott ajánlás képezi, amely felméri a szabályozás szükségességét, bemutatva néhány működő mechanizmust mint megoldási lehetőséget.

Mindenek előtt fontos a téma szükségességét tárgyalni. Először is az ajánlástól elvonatkoztatva, egy amerikai példával érzékeltetve. Ez az ún. San Bernardino ügy. 2015 december 2-án két felfegyverkezett személy behatolt egy szociális központba, a kaliforniai San Bernardinoban. A sok áldozatot és sérültet követelő cselekményről az FBI nyomán kiderült, hogy több terrorszervezettel is szimpatizáltak. Mivel a két elkövető életét vesztette az egyetlen bizonyíték egy iPhone 5 típusú mobiltelefon volt. A készülék operációs rendszere lehetőséget adott a tulajdonosa számára, hogy egy négyjegyű kóddal lezárhassa a képernyőt. Ha 10 alkalommal hibás a próbálkozás, a telefonon található öksszes adat törlődik. Így az FBI és az Apple között komoly vita alakult ki, a beépített törlési mechanizmus kivédéséről. Ez később megosztotta az amerikai hatóságot, mert sokan nehezményezték a halott személyes adatainak megsértését. Az FBI jogszabályként a 230 éves All Writs Actre hivatkozott, e módon kívánta kötelezni az Apple-t egy kiskapu létrehozására.. Míg az Apple érve szerint egy ilyen művelet végrehajtásával megszűnne a garancia a személyes adatok védelmére.[83] Az FBI végül egy izraeli céggel törette fel a telefont.[84] Láthatóvá válik az ügy kettőssége, illetve a tény, hogy szabályozatlan ez a terület

[82] Bocsok 2015. i.m. 61.
[83] Tim Cook, az Apple vezérigazgatójának nyílt levele az üggyel kapcsolatban http://www.apple.com/customer-letter/ (2016.10.11.)
[84] Németh Szabolcs i.m. In: Tóth i.m. 2016. 269-270.

A hazai példa, amelyre az ajánlás egy gyilkossági ügy miatt jött létre, miután a meggyilkolt nőről az ügyben érintett külföldi férfi Facebook idővonalon osztott meg több képet, bejegyzést, magánbeszélgetést illetve hasonló adatok nyilvánosságra hozatalával zsarolta az élő rokonokat. Később a magánbeszélgetések törlésre kerültek, ám felmerült az adatkezeléssel kapcsolatos későbbi jogi probléma orvoslása.

Milyen jogszabályra hivatkozhatunk az előbb elhangzott és jövőbeni esetekben? Az Infotv. 3§ (2) bekezdés definiálja a személyes adat fogalmát. Ebből adódóan személyes adatnak minősül a magánszemélyekről készült online felületen megosztott kép, üzenet, a magánszemély profilja vagy más olyan online tartalom, amely az érintettel kapcsolatba hozható. Emellett az adatvédelmi törvény szabályozza az adatkezelés jogalapjának lehetőségeit Az Infotv. 5 § (1) bekezdés a) pontja határozza meg a személyes adatok kezelésének különböző lehetséges, miszerint jogos a művelet ha az érintett hozzájárul.

Ha a személyes adatnak minősülő online tartalom megosztásának nincsen megfelelő jogalapja, az érintett felhasználó kérheti az adatkezelőtől a törlést Sok közösségi oldal támogatja a törlés lehetőségét, amennyiben a felhasználó sérelmesnek tartja a tartalmat és jelenteni kívánja azt. Ez a lehetőség nem csak az érintett felhasználóra korlátozódik, hanem bárki élhet vele. A közösségi oldal üzemeltetője mérlegeli adatvédelmi, erkölcsi, etikai szempontok szerint a sérelmet keltő, uszító, vagy pornográf tartalmat. E szempontrendszerhez kapcsolódik, mint megerősítő tényező az Infotv által szabályozott önrendelkezési jog, amely minden érintett magánszemélyre vonatkozik. A NAIH ajánlással kapcsolatos esetben az érintett egy elhunyt személy volt, ezen jogait nem érvényesíthette, azonban törlésre kerülhettek közösségi bejelentés alapján, vagy a külföldi férfi önként törölte azokat. Azonban ezzel láthatóvá válik, hogy az Infotv. nem tartalmaz semmilyen szabályozást egy elhunyt személyes adataival kapcsolatban. Ismét fontos kiemelni, hogy a közösségi oldalakkal kapcsolatos adatkezelést nem a törvény, hanem a felhasználói hozzájárulás alapozza meg, erről az esetkörről viszont nincs rendelkezés. Az alábbi példához hasonló esetben csupán a kegyeleti jog fennállására hivatkozhat az elhunyt családja. Valamint az adatok védelme a halál után sem szűnik meg, így korlátlanul nem hozzáférhetőek, hiszen ennek garanciáját az Alaptörvény Szabadság és felelősség VI. cikk (2) bekezdés biztosítja, tartalmát az Infotv. részletezi. Emellett az elhunyt emlékének megsértésével kapcsolatban a Ptk. 2:50§ esetköre az irányadó. Bár léteznek hatályos jogszabályok a halál utáni személyiségi jogok érvényesítése a hozzátartozók által, ez mégsem oldja meg a

felhalmozódott személyes adatok sorsát. Csupán érinti azt, de gyakorlati megoldást nem nyújtanak. Nemzetközi gyakorlat csak néhány országban, például az USA-ban alakult ki, amelyet a következőkben fogok részletezni.

Az Egyesült Államokban jelenleg nyolc tagállamban létezik olyan szabályozás, amely bizonyos korlátok között, de biztosítja az elhunyt online adataihoz való hozzáférést. Ezen felül szövetségi szinten is rendezi a hozzáférési lehetőség jogát. A Uniform Fiduciary Access to Digital Assets Act-ot 2014. őszén fogadták el.

Természetesen a nyolc állam szabályozásában vannak közös jellemzők, hogy miként kell eljárni az adott levelezési oldal, közösségi oldal, blog és egyéb online tartalom szolgáltatójának. A felhasználó halálát követően az elhunyt vagyonának gondnoka vagy végrehajtója számára szükséges biztosítani a hozzáférést, vagy másolatot a szolgáltató által nyújtott fiókttartalomról. A tagállamok szabályozásában található a biztosíték, miszerint az elektronikus levelezési szolgáltató nem kötelezhető bármilyen információ nyilvánosságra hozatalára. A hozzáférést korlátozva, a hagyaték rendezése miatt engedheti, azonban az örökösöknek vagy hagytéki gondnoknak ekkor sem áll fenn helyesbítési vagy törlési jogosultsága. Kivéve Nevada tagállamban, ahol nioncs hozzáférési jog, csak a szolgáltatótól indítványozható a fiók törlése. Delaware államban az előbbiekben felsorolt két rendszer vegyítése érvényesül.. Ez abban nyilvánul meg, hogy a hozzáféréshez vagy törléshez való jogosultságot valamilyen hitelt érdemlő okmánnyal igazolni kell és írásbeli kérvényt kell benyújtania a szolgáltatónak. Ezt követően teljes egészében hozzáférhet az elhunyt felhasználói fiókjához és módosítás nélkül törölhet és másolatot készíthet az adatokról. Ha a szolgáltató ennek nem tesz eleget, az örökös jogosultságát a bíróságon is érvényesítheti.

A szövetségi szintű szabályozás, és a Uniform Ficuicary Access to Digital Assest Act az előbbihez hasonló vegyes rendszert alkalmaz. Hasonló tartalmú szövetségi tövény az Electronic Communications Privady Act, amelyben a szolgáltató biztosítja az előzőleg törvényileg meghatározott jogosultnak a hozzáférést. Tehát összegében megállapítható hogy az USA törvényi rendelkezései szerint, a jogosul örökös vagy gondnok kérheti az adatkezelőtől hogy az elhunyt online adatait megismerhesse. Ebben az esetben ugyanaz a jogosultság jön létre mint, amely a korábbi felhasználó és a szolgáltató között, regisztráció során létrejött.

Jelenleg az Európai Unió tagállamai nem hoztak létre ezzel a témával kapcsolatos önálló szabályozást. Így a magyar adatvédelmi hatóság az igazságügyi miniszternek küldött

ajánlásával kívánta megállapítani a vélhetően helyes nemzetközi gyakorlat kialakítását. Az állásfoglalás szerint az amerikai minta nem felelne meg az adatkezelés célhoz kötöttségének kritériumának. Hiszen az előbbi alapján nincs garancia arra, hogy az online személyes adat ne kerülne a végakarattól eltérő célú harmadik fél birtokába. Így ez nem egyeztethető össze az Európai Unió adatvédelmi elveivel. Az állásfoglalás több szempontból is vizsgálja a kérdést, ám a lényeges feltevés az, miszerint a felhasználó és az online tartalom üzemeltetője között létrejövő szolgáltatási szerződés a felhasználó halálával megszűnik. Így az Infotv. 4§ (1), (2), (3) bekezdése alapján, az adatkezelés céljának megszűnését követően az elhunyttal kapcsolatos személyes adatokat főszabály szerint törölni kell., de jelenleg nincs törvényi jogosultság az örökösök részére. Ezért az adatvédelmi hatóság megfogalmaz egy megoldási formát: az örökösnek, gondnoknak jogosultsága van arra, hogy felhívja a szolgáltató figyelmét az elhunyt adatainak törlésére, megsemmisítésére.Erre azért van szükség, mert a szolgáltató nem képes ellenőrizni hogy az adatkezelés célja megszűnt. Fontos tény, hogy ez a jogosultság nem fedi le a felhasználói profilhoz, levelezéshez, magán- vagy üzleti titokhoz való hozzáférést. Valamint a visszaélések elkerülése végett, az előbb leírt jogosultságot igazolni kell és fontos, hogy az elhunyt a profil alapján beazonosítható legyen. Ezt a mechanizmust bevezetve, nagyobb eséllyel lehetne elkerülni a célját vesztett így jogosulatlan adatkezelés fenntartása.[85] Bár a Ptk és a Btk. bizonyos szinteken érinti ezt az esetkört, a nagyobb jogbiztonság érdekében szükségszerű az önálló szabályozás és nemzetközi gyakorlat kialakítása.[86]

7. Az uniós adatvédelmi szabályozás újításai

Az előbbiekben igazoltam, hogy a web 2.0-es szolgáltatások igazi növekvő membránként veszik körbe életünket. Mind magánélet, mind a jogtudomány tekintetében. Folyamatos kihívásokat, újításokat rejt magában, ezt azonban a viszonylag gyorsan reagáló jogi szabályozásokra is követi. .A korábban felsorolt új technológiák is mutatják hogyan változtak meg az adatvédelem általános tézisei.Természetesen az érvényben lévő, de folyamatosan megújuló jogszabályok sem képesek teljesen lefedni a percenként megújuló

[85] A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az online adatok halál utáni sorsáról, 2015 https://www.naih.hu/files/Ajanlas_online-adatok-halal-utani-sorsarol.pdf (2016.08.09)

[86] Gyakorlatias megoldást nyújt a Facebook, ahol be lehet állítani hagyatéki kapcsolattartó felhasználót aki bizonyos szinteken kezelheti az elhunyt adatlapját (https://www.facebook.com/help/1568013990080948)

web 2.0-eseket. Ismét feltehető a dolgozatban megjelenített központi kérdés: Képes e a hagyományos értelemben vett adatvédelem lefedni a web 2.0-es Big Data adathalmazzal rendelkező technológiákat? Illetve csak a szolgáltatások belső szabályzata képes az adatvédelmi krízisek tisztázására? A következőkben azt vizsgálom, hogy az adatvédelmi jog EU szinten mennyit változott és milyen indokkal, technológiával reagált az újításokra. Ez alapján részletezem az adattovábbítással kapcsolatban történt változásokat a Safe Harbor és Privacy Shield példáján keresztül. Végül a 2018-ra hatályosuló új általános adatvédelmi irányelvet vizsgálom. Összpontosítva a változtatás indokára, az akkori rendelettervezet újításaira és annak ténylegesen megvalósult példáira.

7.1 Safe Harbor és Privacy Shield

A web 2.0-es alkalmazások adatkezelése különösen nagy védelmet igényel. Ebbe a körbe tartozik az adattovábbítás tevékenysége is. Ha az adattovábbítás nincs megfelelően szabályozva, a tömeges megfigyelés által veszélybe kerülhetnek a felhasználó személyiségi jogai. Például ilyen amerikai program volt a Patrict Act, ezt követően az ún. PRISM-program. Ennek jogellenességére hívta fel a figyelmet Edward Snowden, majd Maximillian Schrems. Alapvetően minden EU-USA adattovábbítás 2000 óta, Bizottság 2000/520/EK alapján a Safe Harbor rendszer szerint történik. Ez lényegében az országok és vállalkozások 'önbevallása" a megfelelő adatkezelés működéséről. Az USA területén lévő cégeknek el kellett fogadnia az ország Kereskedelmi Minisztériuma által meghatározott adatvédelmi követelményeket. Így az EU hatóságok megfelelő szintűnek minősítik az személyes adatok adattovábbításának védelmét.[87] A Safe Harborhoz csatlakozó amerikai cégek a 95/46/EK Adatvédelmi Irányelv keretrendszerét. A keretrendszer hét alapelve: adatvédelmi tájékoztatás, választási lehetőség, adattovábbítás harmadik fél részére, adatbiztonság, adatintegritás, hozzáférés, végrehajtás. A rendszerrel kapcsolatban a jogszerűség megingott, amikor 2013-ban az amerikai Nemzetbiztonsági Ügynökség (NSA) nemzetbiztonsági megfigyelési programján belüli információk nyilvánosságra kerültek. A helyzetet súlyosbította, hogy az NSA több állampolgár személyes adataihoz is hozzáfért. Az első tényleges kritika ekkor érte a Safe Harbort. Hiszen nincs garancia a biztonságra, csupán a meglétének feltételezése. A bírálatok nyomán, az Európai Bizottság vizsgálata alapján egy

[87] NAIH i.m. 2015. 103-104.

ajánlást tett közzé a Safe Harbor javítása érdekében. Az ajánlás lényege az átláthatóság elérése, az eljárási mechanizmusok kimutatása és a megfelelő végrehajtás létrehozása volt. Hiába volt pragmatikus és összetett az ajánlás, a Safe Harbor tényleges reformálására akkor még nem került sor. Ugyanebben az időszakban az Európai Parlament állampolgári jogok, bel- és igazságügyi bizottsága (LIBE Bizottság) egy jelentést bocsátott ki az USA által kibocsátott nemzetbiztonsági célú adatkezelésről. A jelentés konklúziója a kritikával megegyező. A Safe Harbor nem nyújt megfelelő adatvédelmi biztonságot az EU állampolgárok számára, így azonnali felfüggesztésre lenne szükség. Az LIBE egyik példája azon cégek adatkezelése, akik nem titkosítják tevékenységüket, így az amerikai titkosszolgálatoknak lehetősége van a személyes adatok elérésére. Azonban ez a jelentés sem segítette a konstrukció megrenoválását. Szintén 2013-ban a Galexia nevű ausztrál internetjogi és adatvédelmi tanácsadó cég kutatást végzett a Safe Harbor rendszer hitelességéről. A programban való részvételhez szükséges évenkénti céges önértékeléseket vizsgálták.Egy társaság önértékelést nyújt be a DOC részére, amivel igazolja, hogy megfelel a hét alapelvnek és a weboldalukon feltűntetik a tanúsítványt. A Galexia igazgatója Cristopher Connolly bírálja ezt a gyakorlatot. A bírálat alapja, hogy sok tagsági kérelem valótlan. Szám szerint 2008-ban 200, majd 2013-ra. Valamint a kutatás szerint több társaság engedély nélkül jelenítette meg weboldalán a Safe Harbor pecsétet vagy EU zászlót. Illetve a fogyasztók számára sem biztosítottak megfelelő tájékoztatást vagy vitarendezési lehetőségeket. A kritikát követte a fokozott ellenőrzés az USA Szövetségi Kereskedelmi (FTC) Bizottsága által

Ezen előzmények alapozták meg az Európai Unió Bíróságának ítéletét, amellyel 2015 október 6-án azonnali hatállyal érvénytelennek nyilvánították a Safe Harbor bizottsági határozatot. Így az USA-ba történő adattovábbítás jogalapjaként nem lehet rá hivatkozni.A harmadik országnak történő adattovábbítás alapulhat más jogalapra. Ezen kivételeket az Irányelv 25. cikk (6) bekezdés és a 26. cikk (1), (2) és (4) bekezdés. Ilyen kivétel például az úgynevezett “white list” megfelelő szintű védelmet nyújtó ország, amelyet a Bizottság határozata állapított meg nevesíti, amennyiben a belföldi jogszabályok engedik azt. A felsorolt kivételeken alapulnak a mintaklauzúlák, mint a Standard Contractual Clauses (SCC) és a Binding Corporate Rules (BCR) vagyis az általános szerződési kikötések és a kötelező szervezeti szabályok.[88] A BCR bevezetése az Infotv legfrissebb módosítása, amely 2015.

[88] Domokos, Poefkó i.m. 2015. 123-132.

október 1-jétől lépett hatályba mint legújabb adatvédelmi eszköz.[89] 2016-ban az EU és USA tárgyalása során jött létre az új megállapodás, az úgynevezett Privacy Shield.[90]

A Privacy Shield adatvédelmi kötelezettsége és alapelvei nem különböznek elődjétől, és a kötelezettségvállalás ugyanúgy önkéntes alapú maradt. Azonban a 2016 nyarán elfogadott adattovábbítási rendszer több újdonságot hordoz magában. A megfelelő végrehajtás érdekében az amerikai Kereskedelmi Minisztérium jogköre kibővül, így a cégek szigorú felügyelet mellett csatlakozhatnak és végezhetik tevékenységüket. Jogsértés esetén a minisztériumnak joga van törölni a listáról. A Privacy Shield négy jelentős tartalmi elemében különbözik a Safe Harbortól. Elsődlegesen a rendszer alapján a személyes adatokat kezelő cégek, szervezetek szigorú kötelezettséget vállalnak és az előbbiekben leírt felügyelet alatt állnak. Szintén fontos pont, hogy rögzítésre került jogorvoslati lehetőség. Az adatkezelő szervezet számára érkező panaszokat 45 napon belül meg kell válaszolni az érintetteknek. Valamint ingyenesen vehető igénybe az alternatív vitarendezés. A panaszokat az adott nemzeti adatvédelmi hatóság és az USA kijelölt szervei együttműködve vizsgálja meg. Ezen felül a panaszosok számára lehetőség a választottbírósági út és az úniós állampolgároknak a közvetlen bíróság előtti jogérvényesítés.2016 február 24.-én elfogadták az amerikai bírósági jogorvoslatról szóló törvényt (Judical Redress Act) A Privacy Shield harmadik jelentős pontja a hozzáférés határának meghatározása. Az USA írásbeli kötelezetettséget vállalt, miszerint kormányzati szervei szükségesség és arányosságnak mértékében, felügyeleti mechanizmusok mellett férnek hozzá uniós állampolgárok személyes adataihoz. Kizárták azt a lehetőséget, hogy személyes adatokat tömeges megfigyelés alatt tartsa. Az ezt felügyelő mechanizmus a független ombudsmani hivatal,amely kivizsgálja az ezzel kapcsolatos panaszokat. Ebből következik a negyedik pont, a szigorú és átfogó évenkénti ellenőrzés.[91] A Privacy Shield céges és kormányzati szerv szintű kötelezettségvállalásának felülvizsgálatát az Európai Bizottság és az Egyesült Államok Kereskedelmi Minisztériuma közösen fogja végezni. Látható, hogy az új mechanizmus a szervezetek számára több feladatot, nagyobb kontrollt jelent. Negatív kritikák szerint hasonló problémával szembesülhetünk mint a Safe

[89] Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2015. évi tevékenységéről 52-56.
[90] Teljes megnevezése: New framework for transatlantic exchanges of personal data for commercial purposes: the EU- U.S. Privacy Shield (WP29 01/2016, 9.)
[91] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf (2016.09.26.)

Harbor esetében. Ezt a kormányzati megfigyelés megfelelő garanciájának hiányával indokolták.[92]

7.2 Az Európai Unió új adatvédelmi rendelete

A web 2.0-es szolgáltatások adatkezelésére is vonatkozó 95/46/EK Irányelv tekintetében is szükség volt radikálisabb változtatásokra. Ezt a változást 2012-ben indította el az Európai Bizottság, amikor az akkor hatályos irányelv felváltására közzétette a általános adatvédelmi rendelet tervezetét (későbbiekben: Rendelettervezet). A következő sorokban részletezem a hatályos irányelv problematikáját, valamint az új 2018-ra hatályosuló rendelet újításait.

Miért nem volt már képes a 95/46/EK szabályozása teljesen lefedni az újonnan érkező technológiákat? A változás jogossága több szemponttal is alátámasztható. Kiindulási pontként megállapítható, hogy jelenleg második technológiai platform az uralkodó. Újra és újra felbukkan a mobile computing, a mobil adattárolás, az applikációk adatkezelése. Ebből adódóan megjelentek olyan világméretű adatvédelmi kockázatok mint a cyberchrime kategóriája mint például a személyiséglopás, vagy internetes zaklatás.Így szigorodtak a személyes adatokat tároló eszközök védelmére vonatkozó szabályok és a használatukra vonatkozó iránymutatások, felhasználói útmutatók. Szintén újdonságként jelent meg a cloud computing alapú specifikus hozzáférés, vagy más specifikus azonosítási módszerek mint az arcfelismerés vagy más biometrikus adatok. Valamint kiemelt adatvédelmi kihívás, hogy sok web 2.0-es szolgáltatás összekapchsolja a különböző adatkezelők által kezelt adatokat. Erre kiváló példa a Facebook, az Instagram a Snapchat adatainak, vagy a helymeghatározási és cookie adatok összekapcsolódása a profillal. Újabb szabályozatlan területnek minősült az előző fejezetben tárgyalt IoT technológia az adatkezelő megnevezésének problematikájával. De ugyanolyan prioritással említhető példaként a globális piacon megjelenő elektronikus fizetőeszközökkel kapcsolatos adatkezelés, vagy az úgynevezett e-health. Ezek alapján összességében megállapítható a probléma forrása, hogy minden adatkezelés specifikussá vált, kevés a minden technológiára ráhúzható szabályozás. Mégis a mai világban folyamatos az egyedi adatkezelés és a nemzetközi szintű adattovábbítás. Így láthatóvá vált, hogy mind az

[92] vö. WP238 Opinion 1/2016 on the EU-USA Privacy Shield draft adequancy decision

adatkezelő mind az érintett érdeke hogy az összetett adatvédelmi kérdések szabályozásra kerüljenek.[93]

Felmerül a kérdés, sikerült e minden kihívásnak megfelelnie? Természetesen az adatvédelemmel kapcsolatos alapelvek és az irányelv célja változatlan maradt[94], mégis sok újdonság került bele a rendelettervezetbe[95] illetve az 5419/16.számű rendeletbe. Az előző rendelet korlátait tekintve szükségessé vált a területi hatályok kiterjesztése a nem EU-ban letelepedett adatkezelők tevékenységére is. A Google rész példájából kiindulva az adatkezelő vagyis a felelős meghatározása székhely helyett tényleges és valós adatkezelés alapján végezhető.[96] Egy adott adatkezelő tevékenységét csak egy meghatározot adatvédelmi hatóság felügyeli, ahol a tevékenységet végzik.[97]. A rendelet másik fontos pontja arról az esetkörről szól, mikor az Unió területén belül élő érintettek személyes adatait uniós területen kívül kezelik vagy dolgozzák fel. Ez esetben az adatfeldolgozó vagy adatkezelő egy képviselőt jelöl ki. Kiemelkedően fontos, ha az adatkezelés különleges nagymértékű adatkategóriára, büncselekménnyel kapcsolatos személyes adatokra vonatkozik és kockázatos az érintett, jogai és kötelezettségeit tekintve. [98] Ezt a területet a 27. cikk szabályozza részletesen.

A rendelet ezt követően a személyes adat meghatározására tér ki. Ez a definíció a web 2.0-es és egyéb technológiák megjelenését követően jelentősen kibővült. Ide tartoznak az úgynevezett online azonosító jelek, mint az IP címek, a cookiek vagy más az érintett személyével összefüggésbe hozható eszközadat, például egy pacemaker vagy fénykép mint biometrikus adat .[99] Bár a rendelkezésre álló adatok, különösen a Big Data hatás miatt felhalmozódtak, kezelésük lényegében a hagyományos adatvédelmi alapokra épül. Mindenek előtt a személyes adat kezelését meghatározott célhoz, időintervallumhoz kötni. De ezt a folyamatot a tájékoztatáson alapuló hozzájárulás indítja meg. A rendelet szerint a hozzájárulás írásbeli, szóbeli és elektronikus eszköz által tett nyilatkozat. Ebből adódóan ide tartozik egy adott weblapon lévő négyzet "bepipálása" is. Példája a közösségi oldalakon

[93] Domokos N. Márton: Az EU új adatvédelmi szabályozása – avagy „keep bangin' on the wall of Fortress Europe", Jogi Fórum, 2013 1-4. www.jogiforum.hu/files/adatvedelem/Az_EU_uj_adatvedelmi_szabalyozasa.pdf (2016.03.18.)

[94] 5419/16.számú rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (1)-(12)

[95] NAIH beszámoló a 2015. évi tevékenységéről 15-17.

[96] 5419/16 (22)-(25)

[97] 5419/16 (36)

[98] 5419/16 (80)

[99] 5419/16 (30)

történő regisztárció vagy a későbbi beállításokhoz való hozzájárulás.[100] Ahogy a cookiek esetkörében is említésre került, fontos, hogy a felhasználó tisztában legyen a hozzájárulás tartalmával illetve fennálljon a lehetőség annak visszavonására is. A hozzájárulás feltételeit illetve a gyermekekre vonatkozó rendelkezéseket a 7. és 8. cikk tartalmazza.

Az új rendelet reagálva a technológiai fejlődésekre, bővítette a jogosultságokat. A felhasználó joga, hogy az adatkezelőtől helyesbítés vagy az adat tárolásának megszűntetésére, különösen a gyermek álltal létrehozott online tartalom esetében. Ez a megszűntetés összefüggésben áll a elfeledtetési joggal, amelynek lényegi elemeit a keresőmotorokról szóló fejezetben részleteztem. [101] A könnyebb online adatáramlás biztosítása érdekében létrejött az adathordozhatóság joga is. Erre jó példa, hogy a meglévő facebook fiókunk, adataink alapján gyorsan használhatunk más szolgáltatásokat, mint az Instagram, Snapchat stb. Lényeges ezen felül meghatározni, hogy a felhasználó jogosult arra, hogy korlátozza az olyan automatizált adatkezelés hatályát, amely személyes jellemzők kiértékelésével jár, így akár joghatással is járhat. A rendelet a gyakorlatban példaként említi az online automatikus munkaerő toborzást, illetve a web 2.0-es szolgáltatások profilalkotását. A profilalkotás kockázata, hogy érinti a felhasználó munkahelyi teljesítményét, anyagi helyzetét, érdeklődési körét,egészségi állapotát vagy a helyváltoztatásának előrejelzését.[102] Ezen adatok, valamint a rendelet által meghatározott különleges adatok védelme elsődrendű. Fenntartására létrejött az Európai Adatvédelmi Testület minden tagállam egy felügyelő hatóságának vezetőiből, és az európai adatvédelmi biztosból álló képviselettel. Tanácsadási, véleményezési és közös adatvédelmet elősegítő feladatot lát el. A Testület felépítéséről, eljárásáról szól a rendelet 3. szakasz 68-76. cikke.

Az ideális modell után a rendelet kifejt egy új adatvédelmi meghatározást, amennyiben az adatkezelés nem biztonságos. Ez az úgynevezett adatvédelmi incidens fogalma. A felhasználó számára a megfelelő intézkedés hiányában vagyoni és nem vagyoni kárt okozhat. Példaként a személyazonosság lopása, adatok feletti rendelkezés elvesztése, jóhírnév megsértése,bizalmas adatok sérülése, valamint szociális vagy gazdasági hátrány.[103] Erre reagál az incidenst elhárítani célzó mechanizmus. Ha az adatkezelő tudomására jut, kötelessége jelenteni a felügyelő hatóság számára, késedelem nélkül vagy 72 órán belül

[100] 5419/16 (32)
[101] 5419/16 (65)-(67)
[102] 5419/16 (71)-(73)
[103] 5419/16 (85)

illetve ha késedelmes részletekben köteles közölni azt. Mindenképpen köteles tájékoztatni az érintettet az incidens mértékéről, esetleges hátrányos következményéről illetve javaslatokat tesz a hatás enyhítésére.[104] Ezzel az eljárással kapcsolatban részletes szabályozást nyújt a rendelet 33-34. Cikke.

Az új rendelet sokféle újdonságot mutat, láttatva hogy a cél egy összetett a gyakorlatban is jól működő adatvédelmi mechanizmus.[105]

8. Az adatvédelem reformja? Jogi és felhasználói oldal

Az uniós szabályozáson át bizonyításra került, hogy a jogalkotó is képes reagálni az új technológiákra. Ennek ellenére érezhető a bizonytalanság. A web 2.0-es szolgáltatások folyamatosan megújulnak, a Big Data adatbányászat egyre elismertebb lesz. Ez félelmet kelthet mind a felhasználóban, mind a jogalkotóban. Ahogy azt a dolgozat bevezető részében is kifejtettem, a megoldást az újradefiniálás jelentheti. Hiszen egy digitalizált belső szabályozásban és működésében "önállóan" kialakult világ nem követhető a hagyományos értelemben vett adat, személyes adat, adatkezelő vagy feldolgozó fogalmaival. De hangsúlyoznunk kell a biztonság fennállásának jelentőségét, csupán más dimenzióban.

Természetesen az értékek megőrzése elengedhetetlen. Meg kell őrizni a közérdekű, publikus adat és a privát személyes adat elkülönítésének jelentőségét. Ezen adatok megőrzése alapját képezi a védelemnek. Szintén maradandó az identitás megőrzése. Fontos, hogy a felhasználó tisztában legyen azzal ki ő és mit akar a világ felé közvetíteni. Állíthatnánk, hogy a jogalkotó számára ez irreleváns, de az újradefiniálás alanya maga a közösségre alapuló online szolgáltatás és piaci verseny. Így a technológiai jognak el kell fogadni a tényleges belső szabályozások és felhasználói útmutatók létét, mint az értékek megőrzésének eszközét. Ezek az elemek tartják fenn az adatvédelem gyakorlatát[106]

Mi lehet a probléma a tényleges szabályozással? Az adatvédelmi hatóság alapjogi azon belül ombudsman jellegű felügyeletet biztosít. Így az eszköztár jogilag kötelező erővel nem bíró ajánlás, állásfoglalás vagy kötelező erővel bíró hatósági aktus. Európai uniós szinten ilyen felügyeletre példa a Privady Shield-hez kapcsolódó ombudsmani hivatal vagy a nem EGT területen tevékenykedő adatkezelő képviselője. Bár elméletileg fennáll

[104] 5419/16 (86)-(88)
[105] v.ö. Domokos i.m. 4-40.
[106] ld. Neil M. Richards Jonathan H. King i.m. 2014.

mechanizmus a védelem fenntartására, kérdéses, hogy ez a gyakorlat képes e megfelelően helytállni. Létrejöhet az a paradox helyzet, hogy a technológiasemlegesség megtartásába "kapaszkodva" pont a védelem jogi háttér frissítését engedik el[107]. Az új rendelet is tanúskodik róla, hogy bár reagálunk a technológiára, mégis megmaradt az online térben merev, hagyományos adatvédelmi szerepkör, Például a korábban említett IoT rendszereknél, mert nem tudunk elvonatkoztatni attól, hogy gép és gép végez adatkezelést.

Mit tehet a felhasználó? Lényegében választhat igénybe veszi -e a web 2.0-es szolgáltatásokat. Dönthet úgy, nem járul hozzá, hogy felhasználják adatait, hirdetések és következtetések létrehozására. Nem kíván tartalmat megosztani vagy része lenni a Big Data hálózatnak. Ez elméletileg megvalósulhat egy számítógép és internet nélküli világban. Képes a mai ember informált maradni mind kommunikációban mind a munkájában az internet használata nélkül? Természetesen nem. Napjainkban az online felület nélkül létező ember a fogyasztói társadalomnak és egyúttal a fejlődésnek fordít hátat (pl: smart home vagy ún smart grids kialakítás[108]. Ahogy a jog területén, itt is fontos hogy ne egy társadalmi szintű paranoia akadályozza a fejlődés elfogadásának útját. A felhasználónak bizonyos szinteken tisztában kell lennie adott szolgáltatás adatkezelésével és saját védelmének lehetőségeivel. [109]

9. Lezárás

Az online piac, amelyre a web 2.0-es technológiák épülnek képviselik a versenyképességet és a fogyasztói élmény növelését. A hirdetők érdekét képviseli a keresési találatok sorrendje, és a kialakult szűrőbuborék rendszerek. A Big Data adathalmaz eszköze alapján az adatbányászat és profilozás mindennapos folyamattá vált.

Ezzel párhuzamosan van jelen az adatvédelem, amelynek célja a felhasználó személyiségéhez fűződő jogainak védelme. Ez a jog szemben áll a fogyasztói társadalom, a közérdek igényeivel. A közösség alapján létrejövő tartalom szolgáltatói kötelesek jogosultságot bizosítani az egyénnek. Mind jóhírnév megőrzésének, mind véleményszabadságnak vagy tájékozottságának érdekében. A dolgozat olyan opciókat mutatott be, mint a keresőmotoroknál a törlés joga vagy a közösségi oldalaknál a feledésbe

[107] vö. Jóri András: Első oldal In: Infokommunikáció és Jog 12. évfolyam 4. szám (2015)
[108] Szuchy Róbert: Energetika-Intelligens rendszerek In: Tóth i.m (2016). 275-291.
[109] vö. Szőke i.m. (2015) 158.

merüléshez való jog. Ugyanilyen opció a felhasználó saját tartalmának szabad szerkesztése, amely a technológiák egyediesítésére alapoz (Facebook, Cloud, Google+).

A felhasználó és szolgáltató vizsonyát, az adatkezelés kezdetét a hozzájárulás adja meg. A web 2.0-es szolgáltatások jól mutatják, immár a kipipálás is hozzájárulást jelent. Minden technológia alapját a megfelelő tájékoztatás képezi. Ennek fontos elemei a hagyományos adatvédelemből erednek (személyes adat, cél, adatkezelő és feldolgozó) mégis jóval nagyobb adathalmazról kell megfelelő tudásanyagot biztosítani. Például a cookiek használatával kapcsolatban.

A kialakult rendszer kritikája maga az egyensúly hiánya. Általánosságban elmondható, hogy a felhasználó nem ismeri adatkezeléssel érintett jogosultságait, a szolgáltató sokszor hiányosan tájékoztatja és nem biztosít igényérvényesítő lehetőségeket. Ezen felül a Big Data adatkezelés miatt a szolgáltatók, hirdetők több olyan információhoz jutnak, amely nem feltétlenül érinti a hozzájárulás keretét vagy az adatkezelés célját. Például a cookie, helymeghatározás, IP cím vagy más adatból nyert következtetésekből adódó profilozás. Lényegében ennek egyetlen fékező ereje maga a felhasználó döntése és a web 2.0-es szolgáltatás adatkezelési szabályzata, felhasználási feltételei.

Utóbbi kijelentés a jog korlátját is jelenti. Komoly nehézségekbe ütközik az új technológiákra való megfelelő reakció és egy mindent átfogó részletes szabályozás. Ennek elérését segítik a nemzetközi egyezmények, az uniós tagállamok megállapodásai. Azonban a megfelelő erősségű jogalkalmazás és végrehajtás ugyancsak bizonytalanságba ütközik.

Tényleges, minden szinten működő gondolatmenet vagy szabályozás egyelőre nem született. Ettől függetlenül az előző fejezet szkeptikus nézőpontjától elvonatkoztatva végső célom, hogy a dolgozat pozitív kicsengéssel záruljon.Mind a web 2.0-es szolgáltatásokkal kapcsolatban, mind az adatvédelem megújulásával kapcsolatban. A jövő jogalkotói számára fontos célkitűzés lesz a hagyományos értékek megőrzése, de az új technológiai reformok befogadása. A felhasználói és a szolgáltatói oldal célkitűzése is a tudatosság elérése lesz. Felhasználói oldalon tájékozottság, szolgáltatói oldalon határozott és felhasználóbarát belső szabályozások szintjén. Az idealizált kép távolinak tűnhet, mégis ez alapozza meg a filozófiát, hogy ne rettegjünk a felhalmozódott online adataink “árnyékától”.

10. Irodalomjegyzék

Magyar források:

1) Bartóki-Gönczy Balázs – Pogácsás Anett: *A médiatartalom-szolgáltatásnak nem minősülő internetes tartalmak szabályozása,* In: Koltay András – Nyakas Levente (szerk.): *Magyar és európai médiajog,* Wolters Kluwer, Budapest, 2015.
2) Belényesi Pál: *Digitális és technológiai piacok közgazdasági kérdései*, In: Tóth András (szerk.): *Technológiai jog- Új globális technológiák jogi kihívásai*,Patrocinium Kiadó., Budapest 2016.
3) Bocsok Viktor, Boldizsár Péter Ferenc, Loós Csaba, Major Tamás: *A dolgok internete- Technológiai háttér, információbiztonsági és adatvédelmi aspektusok* In: *Infokomunikáció és Jog* 12. évfolyam 2-3.szám 2015.
4) Cseh Gergely: *A közösségi portálok árnyoldalai.* In: *Infokommunikáció és Jog* X. évfolyam 2. sz. 2013.
5) Dénesné Orcsik Judit: *A Google-nak törölnie kell az adatokat, ha kérjük, Ügyvédvilág* 9. évfolyam 11. szám 2015.
6) Domokos N. Márton: *Sütiszörny megérkezett! A cookie-k használatának jogi szabályozása, Jogi Fórum,* 2012.
7) Domokos Márton, Poefkó Patrik: *Egy bírósági döntés következményei-avagy az Európai Bíróság ún. Schrems döntésének hatásai, a Safe Harbor sorsa és a felmerülő kérdések az adatvédelem területén* In: *Infokommunikáció és Jog* 12. évfolyam 4. szám 2015.
8) Domokos N. Márton: *Az EU új adatvédelmi szabályozása – avagy „keep bangin' on the wall of Fortress Europe", Jogi Fórum*, 2013.
9) Jóri András: *Első oldal* In: *Infokommunikáció és Jog* 12. évfolyam 4. szám 2015.
10) Kulcs a net világához! a Nemzeti Adatvédelmi és Információszabadság Hatóság tanulmánya a gyeremekek biztonságos és jogtudatos internethasználatáról, 2013.
11) Láncos Petra: *A közösségi média keretei között gyakorolt alapjogok korlátozásainak alkotmányos kérdései Gazdaság és Jog* 24. évfolyam 3. szám 2016.
12) Lehóczki Balázs: *Az egyének védelme az interneten elérhető személyes adataik keresőmotorok általi kezelésének vonatkozásában- az Európai Unió Bírósága* In: *Acta Humana* 2. évfolyam 2. szám 2014.

13) NAVRATYIL Zoltán: *Internet és szólásszabadság: a "felejtés" joga és a "feledésbe merüléshez" való jog* In: *Iustum-Aequum-Salutare* 11. évfolyam 2. szám, 2015

14) Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2013. évi tevékenységéről

15) Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2015. évi tevékenységéről

16) A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az online adatok halál utáni sorsáról

17) NÉMETH Janka: *Internet és közösségi háló mint munkaeszköz* In *Infokomunikáció és jog* 10. évfolyam 1. szám 2013.

18) NÉMETH Janka: *Az internet nem felejt közösségi média használatára alapított munkáltatói és munkavállalói felmondások* In: *Infokommunikáció és Jog* 10. évfolyam 2. szám 2013.

19) NÉMETH Szabolcs: *Az adataink jogi sorsa a halál után* In: TÓTH András (szerk.): *Technológiai jog- Új globális technológiák jogi kihívásai*, Patrocinium Kiadó., Budapest 2016

20) POLYÁK Gábor: *A frekvenciaszűkösségtől a szűrőbuborékig*, In: TÓTH András (szerk.): *Technológiai jog- Új globális technológiák jogi kihívásai*, Patrocinium Kiadó, Budapest 2016

21) POLEFKÓ Patrik: *Barátok és bizonytalanságok közt avagy a közösségi oldalakról adatvédelmi szemszögből 1-3. rész* In: *Infokommunikáció és Jog* 8. évfolyam 3. szám 2010. ; 7. évfolyam 5. szám 2010. ; 7. évfolyam 6. szám .2010.

22) SZABÓ Endre Győző, BOJNÁR Katinka, BUZÁS Péter: *Új globális technológiák kihívásai a magyar jogban* i.m. In: TÓTH András (szerk.): *Technológiai jog- Új globális technológiák jogi kihívásai,* Patrocinium Kiadó., Budapest 2016

23) SZUCHY Róbert: *Energetika- Intelligens rendszerek* In: TÓTH András (szerk.): *Technológiai jog- Új globális technológiák jogi kihívásai*, Patrocinium Kiadó., Budapest 2016

24) TATAY Eszter: *A szűrőbuborék hatása a tájékoztatottsághoz való jogra* In: *Infokommunikáció és Jog* XII. évfolyam 2-3.sz. 2015.

25) SZŐKE Gergely László: *Infokommunikációs Szakmai Nap, beszámoló,* In: *Infokommunikáció és Jog*-12. évfolyam 4. sz. 2015.

Normák:

1) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv)
2) 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások egyes kérdéseiről (Ekertv)
3) 2003. évi C. törvény az elektronikus hírközlésről (Eht.)
4) 95/46EK adatvédelmi irányelv
5) New framework for transatlantic exchanges of personal data for commercial purposes: the EU- U.S. Privacy Shield
6) 5419/16.számú rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
7) Az Európai Unió Alapjogi Chartája

Külföldi források:

1) BOGDAN Radu: *The use of web-based applications developed on cloud infrastructures-juridical implications for the juridical professions*, Dimitrie Cantemir Christian University, National Strategies Observer No.2/Vol.1, 2015.
2) EDPS-BEUC Conference on Big Data, Brussels, 29 September 2016. *"Check against delivery"*
3) FONG, Ivan K.: *Law and New Technology: The Virtues of Muddling Through*, Yale Law & Policy Review: Vol. 19: Iss. 2, Article 5. 2000.
4) GRUBBS, Amelia D.:*Privacy Law and the Internet using Facebook.com as a Case Study* University of Tennessee Honors Thesis Projects 2011.
5) KAMARINOU Dimitra, MILLARD Christopher, HON Kuan W: *Privacy in the Clouds: an empirical study of the terms of service and privace policies of 20 Cloud service providers,* Queen Mary University of London, School of Law Legal Studies Research Paper No 209/2015
6) RICHARDS Neil M, KING Jonathan H.: *Three paradoxes of big data,* 66 Stanford Law Review Online 41 2013.

7) Richards Neil M, King Jonathan H.: *Big Data and the Future for Privacy*, Handbook of Research on Digital Transformations Elgar 2016.
8) Roosendaal Arnold: *Facebook tracks and traces everyone:Like this!* Tilburg Law School Legal Studies Research Paper Series, 2011.
9) The University of Melburn: *Wikis, blogs and web 2.0 technology*
10). Walden Ian, La Diega Noto Guido: *Contracting for the "Internet of Things: Looking into the Nest,* Queen Mary University of London, School of Law Legal Studies Research Paper No. 219/2016

29.-es Munkacsoport véleményezések:

1) WP 148:1/2008. számú vélemény a keresőmotorokkal kapcsolatos adatvédelmi kérdésekről
2) WP163 5/2009. számú véleménye az internetes ismeretségi hálózatokról
3) WP169 1/2010. számú vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról
4) WP171 2/2010. számú vélemény a viselkedés alapú online reklámról
5) WP187 15/2011. számú vélemény a hozzájárulás fogalommeghatározásáról
6) WP194 4/2012. számú vélemény a sütikhez való hozzájárulás alóli mentességről
7) WP223 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről
8) WP238 Opinion 1/2016 on the EU-USA Privacy Shield draft adequancy decision

Linkek:

1) https://ssrn.com/en/
2) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
3) http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html
4) http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html
5) https://www.facebook.com/legal/terms
6) https://www.facebook.com/privacy/explanation
7) https://www.google.hu/intl/hu/policies/privacy/
8) https://www.facebook.com/safety/
9) https://www.facebook.com/safety/groups/teens/

10) https://www.facebook.com/communitystandards
11) https://www.facebook.com/help/1568013990080948
12) http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf
13) https://net-jog.hu/2016/10/04/a-facebook-felrevezeti-a-felhasznalokat-nemetorszagban/