JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

Eötvös Loránd Tudományegyetem

Állam- és Jogtudományi kar

Évfolyamdolgozat

A felhő alapú számítástechnika adatvédelmi kérdései

Szerző:

Boros Andor

Konzulens:

Dr. Vissy Beatrix

Budapest,

2015. május 15

I. Bevezetés

Az elmúlt évek egyre intenzívebb technikai fejlődése, új technológiai megoldások születése, az internet-penetráció gyors ütemű növekedése és az ehhez alkalmazkodó (alkalmazkodni próbáló) társadalomban bekövetkezett változások jelentős kihívások elé állítják a magánszféra védelmének egyik legfontosabb jogi leképeződését, az adatvédelmet.

A technológiai változások közül különösen a mobil és a felhő alapú számítástechnika, a Big Data, valamint a közösségi média[1] produkálják az utóbbi években az IT szektor legnagyobb növekedését létrehozva egy olyan információra és innovációra épülő „digitális világot", amely lényeges kihívások elé állítja a korábbi évtized technikai megoldásaira épülő adatvédelmet. E technológiai újítások részben egymásra épülnek, összefonódnak. Éppen ennek köszönhető, hogy a felhő alapú számítástechnika kiemelkedik a fenti területek közül, ugyanis az mind önmagában (külön szolláltatásként), mind pedig a többi egyre inkább elválaszthatatlan összetevőjeként is megjelenik.

A felhő alapú számítástechnika széles körű elterjedése következtében egyre nagyobb hangsúllyal merülnek fel az adatvédelmi kockázatok. Ezek kezelése, illetve minimalizálása érdekében pedig rendkívüli jelentőségű egy a technológiai változásokra gyorsan reagáló, így technológia-semleges szabályozási környezet.

Az adatvédelmi kérdések relevanciája vitathatatlan, különösen a jelenleg zajló adatvédelmi reform fényében. Az Európai Bizottság által 2012-ben beterjesztett, a jelenleg hatályos irányelv helyébe lépő általános adatvédelmi rendelettervezet hosszas előkészítő munka eredménye. A kérdés érzékenységét, illetve fontosságát jól mutatja, hogy az érintettek (adatkezelők, hatóságok, jogvédők) között azonnal heves vita bontakozott ki, amely nem csak egyes részletszabályokat, hanem a rendeleti formában történő szabályozás kérdését is érinti. A vita elhúzódásából viszont arra

---

1 Az amerikai International Data Corporation (IDC) informatikai és számítástechnikai vállalat 2013-ban közzétett tanulmánya alapján e szolgáltatások alkotják az ún. harmadik platformot, amely az innováció egyfajta újabb lépcsőjeként értelmezhető az IT-szektorban meghatározva a következő évtized fejlődési irányait.
http://www.idc.com/getdoc.jsp?containerId=prUS25285614 (utolsó letöltés: május 1.)

következtethetünk, hogy valamennyi szereplő felismerte a szabályozási környezet reformjának szükségességét, így nem hagyják a reformtörekvéseket kifulladni.

A felhő alapú technológia gyors terjedése, valamint az európai adatvédelmi reform együttesen különösen fontosság teszik az ezzel történő foglalkozást.

A dolgozatban a felhő alapú számítástechnikának a magánszféra-védelemre, illetve annak egy speciális jogi leképeződésére, az adatvédelemre gyakorolt legfontosabb hatásait és az ennek folyományaként felmerülő kihívásokat kívánom bemutatni. A jelenlegi adatvédelmi szabályok egy része nem megfelelően vagy egyáltalán nem alkalmazható a számítási felhő jellegadó technológiai megoldásai miatt. Ennek megfelelően az adatvédelmi rendszer számítási felhő által igényelt reformját a jelenleg is zajló európai adatvédelmi rendelettervezet segítségével kívánom bemutatni, rámutatva arra, hogy olyan átfogó változtatásokra van szükség, amelyek az eddigiektől jelentősen eltérő hangsúlyokat, szabályozási megoldásokat és jogintézményeket állapítanak meg. A dolgozat bemutatja a számítási felhő sajátosságait, annak adatvédelmi szempontból releváns technikai és üzleti megoldásait, illetve megvizsgálja az európai adatvédelmi rendszernek a számítási felhő által kiváltott legégetőbb problémáit és ezek megoldásának alternatíváit. Ennek alapján a dolgozatban foglalkozom többek között a személyes adat fogalmával, adatkezelő és adatfeldolgozó viszonyával és felelősségrendszerével, a harmadik országba történő személyes adatok továbbításának szabályaival.

II. A felhő alapú számítástechnika adatvédelmi szempontból releváns technológiai jellemzői

II.1. A felhő alapú számítástechnika meghatározása

A felhő alapú számítástechnika technológiai hátterének vizsgálata feltétlenül szükséges az adatvédelmi problémák áttekintéséhez és megértéséhez, majd a lehetséges megoldások feltárásához. A technológia jellege, költségei és elérhetősége alapvetően meghatározza magát a felhasználói kört, így magának az adatalanyoknak (érintetteknek) a körét és az ezeket fenyegető potenciális veszélyeket.

A közműszerű informatikai szolgáltatások[2] (*utility computing*), és ezek részét képező felhő alapú számítástechnika mögötti technológiai megoldások alapötlete nem új keletű.[3] Ugyanakkor e közműszerű megközelítés segíthet könnyebben megérteni felhő alapú számítástechnika legfontosabb tulajdonságait. Maga a közmű elnevezés arra utal, hogy az informatikai fejlődés ugyanolyan pályát futhat be, mint az áram- vagy vízszolgáltatás.[4] Ahogyan például a XIX. század második felében Nikola Tesla váltóárama forradalmasította az áramszolgáltatást lehetővé téve, hogy egy centralizált, nagy kapacitású erőmű hatalmas távolságokra lévő fogyasztókat is kiszolgáljon olcsó árammal, ugyanúgy a felhő alapú számítástechnika is lehetővé teszi, hogy a számítástechnikai erőforrások (a nagy teljesítményű processzorkapacitást igénylő számítási műveletektől a hihetetlen mértékű adattárolásig) az átlag felhasználó rendelkezésére álljanak (egy meghatározott ideig). Lehetőség nyílik arra, hogy a

2 A közműszerű IT szolgáltatás úgy határozható meg, mint egy olyan stabil, megbízható, tömegigényeket kielégítő szolgáltatása informatikai kapacitásoknak és funkcióknak, amely mögött korszerű, hatékonyan működtetett IT-infrastruktúrák állnak. (KRAUTH Péter: Közműszerű IT-szolgáltatás, http://www.nhit-it3.hu/__ujsite2/images/tagandpublish/Files/it3-2-1-10-u.pdf) (utolsó letöltés: 2015. V.1.)

3 Az informatika mint közmű fogalmát John MCCARTHY, a számítástechnika-kutatás egyik úttörője vezette be, amikor a Massachusettsi Műszaki Egyetemen (MIT) 1961-ben tartott beszédében kifejtette, hogy az informatika a jövőben az elektromos áramhoz, gázhoz, vízhez hasonló közműszolgáltatás lesz.

4 BŐGEL György: Az informatikai felhők gazdaságtana – üzleti modellek versenye az informatikában. In: Közgazdasági Szemle, LVI. évf., 2009. július–augusztus (676. o.)

felhasználók (haszon)bérbe vegyék ezeket az erősforrásokat éppen aktuális szükségletüknek megfelelően harmadik személytől anélkül, hogy hatalmas összegeket fektetnének a megvásárlásukba.

A felhő alapú számítástechnika megjelenésével nem csak egy új technológiát eredményezett, hanem egy új üzleti modellt is, amelynek sikeressége nagyban függ a versenyképességétől, előnyeitől.[5]

A felhő alapú számítástechnika gazdasági szférában is lecsapódó előnyei közé sorolható legfontosabb tulajdonságait tartalmazó definíció megfogalmazását igen sokan megkísérelték. Ennek ellenére egy átfogó, valamennyi szereplő által elfogadott definíció megalkotása komoly akadályokba ütközik. Meghatározásának nehézségét kettős (technikai és az üzleti) jellege, a különböző tulajdonságainak a túlzott középpontba állítása, valamint a folyamatosan változó technológiák okozzák.[6]

A szakirodalomban az egyik legtöbbet idézett definíciója az amerikai National Institute of Standards and Technology (NIST) által megalkotott, amely alapján:

A felhő alapú számítástechnika egy olyan modell, amely a felhasználók számára bárhol használható, kényelmes, igény szerinti hálózati hozzáférést biztosít olyan megosztott informatikai erőforrásokhoz (pl. hálózatok, szerverek, tárolókapacitás, alkalmazások, szolgáltatások), amelyek rövid idő alatt, minimális erőfeszítéssel vagy szolgáltatói közreműködéssel rendelkezésre bocsáthatók és felszabadíthatók.[7]

A következőkben a felhő alapú számítástechnika alatt az idézett definíciónak megfelelő technológiai és szolgáltatási modellt értem.

---

5 i.m. 674. o.

6 A felhő alapú számítástechnika definiálására tett kísérletek sokszínűségét emeli ki: Luis M. Vaquero, Luis Rodero-Merino , Juan Caceres, Maik Lindner: *A Break in the Clouds: Towards a Cloud Definition* http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf

7 Peter Mell and Timothy Grance: *The National Institute of Standards and Technology (NIST) Definition of Cloud Computing* (Szeptember 2011) http://csrc.nist.gov/publications/PubsSPs.html#800-145

II.2. A felhő alapú számítástechnika szolgáltatási modelljei

A felhőt mint szolgáltatást a korábbi évtized közepén indították el az IT-iparág legnagyobb szereplői (pl. Amazon, Google, Microsoft), amelyek hatalmas számítástechnikai erősforrásokkal rendelkeztek először csak saját igényeik, majd pedig a felhasználó közönség szükségleteinek kielégítésére is. Saját erőforrásaiknak és üzleti érdekeiknek megfelelően más-más szolgáltatási modelleket dolgoztak ki. [8]

A felhasználók[9] igényeinek megfelelően három fő szolgáltatásnyújtási modellt különböztethetünk meg[10]:

1. IaaS: Infrastructure as a Service – Infrastruktúra mint szolgáltatás

A legalacsonyabb szintű szolgáltatási modell, amely esetén a szolgáltató magát a technológiai infrastruktúrát (virtuális szervereket, távoli kiszolgálóegységeket) adja bérbe. A felhasználó egy olyan távoli infrastruktúrát vásárolhat időlegesen, amelyen saját (virtuális) szervereit futtathatja. Példaként említhető az Amazon EC2[11] vagy a magyar cloud.hu.[12] Ezek előnye, hogy a felhasználónak nem szükséges megvásárolnia a hardvert, nem kell viselnie az üzembe helyezés és üzemeltetés költségét. A felhasználó saját maga által kiválasztott, bármikor módosítható számítógép konfigurációt bérelhet.

---

8 Racskó Péter: A számítási felhő Európa egén

9 Felhasználó alatt értendő jelen esetben az átlagembertől a multinacionális vállalatokig minden természetes és jogi személy.

10 ld. NIST def.

11 http://aws.amazon.com/ec2/

12 http://cloud.hu/

2. PaaS: Platform as a Service -Platform mint szolgáltatás

Az a szolgáltatási szint, amely lehetővé teszi a felhasználó számára, hogy saját alkalmazásait telepítse, fejlessze a szolgáltató platformját használva úgy, hogy a szolgáltató az infrastruktúra mellett egyéb szolgáltatásokat is nyújt (operációs rendszerek, fejlesztői és kiszolgáló szoftverek, programozási nyelvek adatbázis kezelők, futtató környezetek). Példaként említhető a Google App engine[13] és a Microsoft Azure[14] szolgáltatásai, amelyek lehetővé teszik a többnyire szakértő felhasználók számára, hogy teljes egészében az alkalmazásfejlesztésre tudjanak összpontosítani.

3. Saas: Software as a service – Szoftver mint szolgáltatás

A legmagasabb absztrakciós szintű szolgáltatás, amely estén a szolgáltató kész szoftvert bocsát a végfelhasználó rendelkezésére. Ilyen például a Microsoft Office 365, Dropbox, Google Gmail. A felhasználók többnyire egy egyszerű böngésző használatával, vagy egy alacsony rendszerigényű program segítségével tudják igénybe venni a szolgáltatásokat, amelynek köszönhetően egy kis teljesítményű személyi számítógéppel vagy mobil eszközzel is hihetetlen mértékű számítási és tároló kapacitást érünk el.

Természetesen e szolgáltatásnyújtási modellek egymásra épülhetnek. Így előfordulhat, hogy több szereplő is részese egy adott szolgáltatásnak. Példaként említhető a Dropbox tárhelyszolgáltató Saas szolgáltatása az Amazon IaaS szolgáltatásán alapul.

---

13 https://cloud.google.com/appengine/

14 http://azure.microsoft.com/hu-hu/

II.3. A felhő alapú számítástechnika kiépítési modelljei

A felhő alapú szolgáltatásoknak egy további csoportosítási módja a felhasználók közönségének nagysága szerint csoportosítható. E kiépítési modellek[15] az alábbiak:

1. Magánfelhő (Private Cloud)

A felhő infrastruktúráját kizárólag egy meghatározott szervezet érdekében üzemeltetik. Vagy a szervezet tulajdonában áll (akár annak telephelyén), vagy egy szigorú felügyelete, irányítása alatt álló szervezet számára kiszervezi a feladatokat. E modell áll a legközelebb a klasszikus kiszervezéshez, ahol egy szervezet a saját igényeinek kielégítésére hoz létre, vagy ad megbízást hagyományos IT-rendszer létrehozására. A magánfelhő hasonló elven működik azzal, hogy a felhő alapú technológia újításait, megoldásait használja (pl. virtualizáció). A skálázhatóság, az igényeknek megfelelő rugalmasság, a szolgáltatás alapú megközelítés miatt a magánfelhő költséghatékonyabb a hagyományos szerverparkok, illetve adatbankoknál, hiszen a technológiai eljárásokat úgy hajtják végre, hogy optimálisan kihasználják a rendelkezése álló erőforrásokat[16]. Előnyös lehet olyan szervezetek számára, amelyek területileg széttagolt IT rendszerrel rendelkeznek.

2. Közösségi felhő (Community Cloud)

A felhőn több olyan szervezet osztozik, amelyek egyfajta „közösséget” alkotnak tekintettel közös céljaikra, érdekeikre, biztonsági elvárásaikra. A magánfelhőhöz közel áll, azonban nem csak egy szervezet számára biztosítja a megfelelő erőforrásokat. Költségmegtakarítási célból

15 Az ún. kiépítési modelleket (Deployment Models) az Amerikai Szabványügyi Hivatal (NIST) állásfoglalása alapján rendszerezem, amely komplexebb, mint az adatvédelmi munkacsoportnak a felhő alapú számítástechnikával foglalkozó véleményben foglalt csoportosítás.

16 WP196. p. 28

előnyös lehet, ha több, hasonló profilú szervezet nem külön-külön, hanem együtt veszi igénybe e szolgáltatást. Tekintettel arra, hogy a szervezetek hasonló érdekekkel, célokkal rendelkeznek, az igényeik is hasonlóak (pl. azonos jogszabályi előírások miatt), ugyanakkor a magánfelhőhöz hasonlóan egyedi, személyre szabott szolgáltatásban részesülnek. Piaci és kormányzati szereplők is megjelenhetnek szolgáltatóként. A szolgáltatás igénybevevői közé sorolhatók a kormányzati szervek, egészségügyi intézmények, pénzügyi szervezetek.

3. Nyilvános felhő (Public Cloud)

A felhasználók széles körét megcélzó modell, bárki által igénybe vehető. A szolgáltató piaci, tudományos vagy kormányzati szervezet is lehet. E modell feleltethető meg leginkább a felhő-szolgáltatás széles körben elfogadott definíciójának.

4. Hibrid felhő (Hybrid Cloud)

A fentebb ismertetett modellek vegyítésének eredménye. Vegyes felhasználást tesz lehetővé, ezáltal is csökkentve a költségeket. A magánfelhőre épülő rendszerekben előfordulhat, hogy kivételes esetekben az igény meghaladja a rendelkezésre álló forrásokat. Mindez vagy a magánfelhő szolgáltatás hosszú távú bővítésével vagy a többletigény erejéig pl. nyilvános felhő szolgáltatás igénybevételével kiküszöbölhető. Az első esetben a bővítés többletköltséget eredményez akkor is, amikor elegendő lenne a kisebb kapacitás is, míg a második esetben csupán a kivételes esetekben előforduló erőforrásigény esetén merülnek fel többletköltségek. E vegyes használatra a „cloud bursting” (felhőszakadás) metaforát használja a szakirodalom.

Az ismertetett *kiépítési modellek* eltérő tulajdonságainak köszönhetően más-más területen rendelkeznek előnyökkel, illetve hátrányokkal. Ezek pedig egy skálán mozognak, melynek

végpontjai a magán és a nyilvános felhő. A méretgazdasági előny, hatékonyság tekintetében a nyilvános felhő a leginkább megfelelő választás, tekintettel arra, hogy szolgáltató oldalán megjelenő hatékonyság a felhasználók számára költségmegtakarításként jelentkezik. A magánfelhő esetében pedig ez a legkevésbé jelentkezik. A felhőszolgáltatás igénybevevő általi kontroll, illetve az adatvédelem, adatbiztonság szempontjából viszont a magánfelhő a leginkább megfelelő modell, míg a nyilvános felhő a legkockázatosabb és legkevésbé alakítható saját, speciális elvárásainknak megfelelően.

III. Személyes adatok és a felhő alapú számítástechnika

III.1. A személyes adat fogalma és annak eredete

A személyes adat fogalma az európai adatvédelmi rendszer központi eleme, ugyanis az nem csupán magának az adatvédelemnek a tárgyát jelöli meg, hanem egyszersmind meghatározza az európai adatvédelmi szabályok érvényesülésének, alkalmazhatóságának körét is. Ennek megfelelően amennyiben egy adat (információ) *személyes adat*nak tekinthető, annak jogszerű feldolgozása és kezelése csakis az érintett személy védelmét biztosító adatvédelmi alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek alkalmazásával történhet.

Az Adatvédelmi Irányelv 2. cikk a) pontja alapján *személyes adat „az azonosított vagy azonosítható természetes személyre ("érintettre") vonatkozó bármely információ; az azonosítható személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, szellemi, gazdasági, kulturális vagy társadalmi identitására vonatkozó egy vagy több tényezőre történő utalás révén;”*

E definíciót az Adatvédelmi Rendelettervezet és annak az Európai Parlament általi módosítása szinte szóról szóra átvette, amely alapján *„személyes adat az azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ. Az azonosítható*

személy olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító, például a név, egy azonosító szám, helymeghatározó adat, egyedi azonosító vagy az adott személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy társadalmi vagy nemi identitására vonatkozó egy vagy több tényezőre történő utalás révén;"[17]

A fentiek alapján látható, hogy az Adatvédelmi Rendelettervezet fenntartja a hatályos Adatvédelmi Irányelv objektív, magasan absztrahált, lehetőleg az azonosítható személyt érintő valamennyi információra kiterjedő fogalommeghatározását. Ahogyan az Európai Bizottság az Adatvédelmi Irányelv javaslatában[18] is kifejtette, az Európai Unió adatvédelmi rendszerének ezen általánosan megfogalmazott személyes adat fogalma az Európa Tanács 108. számú, 1981-ben elfogadott Egyezményén alapszik, melynek 2. cikke szerint *„személyes adat: bármely információ, amely egy azonosított vagy azonosítható egyénre vonatkozik (adatalany)"*.[19]

III.2. A személyes adat fogalma a felhő alapú számítástechnika vonatkozásában

III.2.a. Anonimizált és pszeudoanonimizált adatok

Az Adatvédelmi Irányelv személyes adat definíciójából a contrario következik, hogy amennyiben a közvetlen vagy közvetett azonosítása az adatalanynak nem lehetséges, vagyis maga az adat és az adatalany között nem létesíthető kapcsolat, akkor anonim adatról beszélhetünk, vagyis ennek feldolgozása, kezelése kívül esik az adatvédelem körén. A 29. cikk alapján létrehozott

17 AZ EURÓPAI PARLAMENT JOGALKOTÁSI ÁLLÁSFOGLALÁS-TERVEZETE

18 COM(90) 314 final (Commission Of The European Communities: COMMISSION COMMUNICATION on the protection of Individuals In relation to the processing of personal data In the Community and Information security) 19. p. http://aei.pitt.edu/3768/1/3768.pdf (utolsó letöltés: 2015. május 1.)

19 Az Egyezményt Magyarországon *az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló* 1998. évi VI. törvény hirdette ki.

adatvédelmi munkacsoport az Adatvédelmi Irányelv 26. preambulumbekezdésére[20] alapozva ugyanerre a következtetésre jut kiemelve annak fontosságát, hogy „minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására”[21].

Az Európai Parlament Adatvédelmi Rendelettervezettel kapcsolatban kiadott állásfoglalásának 23. preambulumbekezdése átveszi az Irányelvnek a Munkacsoport által is hangsúlyozott szabályozási koncepcióját kiegészítve azt a következőkkel: „*minden olyan módszert figyelembe kell venni, amelyet az adatkezelő vagy más személy* ***ésszerűen valószínűsíthető*** *módon felhasználhat az egyén közvetlen vagy közvetett azonosítására vagy kiválasztására. Annak megállapítására, hogy egy módszer ésszerűen valószínűsíthetően felhasználható-e az egyén azonosítására, minden objektív tényezőt tekintetbe kell venni, például az azonosítás költségeit és az azonosításhoz szükséges időt, figyelembe véve egyrészt a feldolgozás idején rendelkezésre álló technológiát, másrészt a technológiai fejlődést.”* [22]

Az Európai Parlament által javasolt objektív kritériumrendszer üdvözlendő. A személyes adatok védelméhez való jog mint alapjog érvényesülése nem függhet pusztán az adatfeldolgozó vagy adatkezelő szubjektív körülményeitől.

Az előbb kifejtettek alapján amennyiben egy felhőszolgáltató anonim adatokat kezel, kikerül az adatvédelmi szabályozás alól.

A pszeudonimizálás az anonimizáláshoz hasonlóan a személyazonosság elrejtését szolgálja. Legfőbb célja ugyanazon személyre vonatkozó adatgyűjtés lehetővé tétele oly módon, hogy magát a személyt meg kellene ismernünk.[23] Maga a pszeudonimizált adat tulajdonképpen álnevesített adatot jelent. Legtöbb esetben az elsődleges, közvetlen azonosítók (nevek, cím stb.) helyettesítéseként

---

20 Az Irányelv 26. preambulumbekezdése alapján „a védelem elvei nem alkalmazhatók az olyan módon anonimmá tett adatokra, ahol az érintett a továbbiakban nem azonosítható”

21 Irányelv 26. preambulumbekezdés

22 Az Európai Parlament jogalkotási állásfoglalás-tervezete az Adatvédelmi Rendelettervezet kapcsán, 23. preambulumbekezdés

23 WP 136, 19. p

közvetett azonosítókat (pl. számkódot) rendelünk az adatokhoz[24] többek között annak érdekében, hogy az az információ címzettje ne tudja az érintett személyt azonosítani.

Maga a pszeudonimizálás kétféleképpen is elvégezhető: visszafejthető (visszakövethető), illetve az ezt kizáró módon. [25]

Az olyan formában, amely lehetővé teszi azt, hogy egy kulcs segítségével visszafejthetők, felderíthetők legyenek a helyettesített elsődleges azonosítók bizonyos körülmények között.[26] Ez az eljárás különösen az elektronikus egészségügyi nyilvántartások (Electronic Healthcare Record – EHC) felhőben történő tárolása kapcsán,[27] illetve a gyógyszerek klinikai tesztelése során alkalmazandó.[28] Ez esetben az alapvető elvárás az, hogy a személyes (sokszor szenzitív) adatokat csak bizonyos személyek (pl. kutató, orvos) legyenek képesek meghatározott adatalanyokhoz kötni, még mások (pl. a felhőszolgáltatók, gyógyszeripari vállalkozások) számára a kezelt adatokat meg kell fosztani személyes jellegüktől.

A pszeudonimizálás továbbá elvégezhető oly módon is, hogy az adatalany és az adat közötti kapcsolatot végleg megszakítjuk. Ebben az esetben a közvetlen azonosítókat úgy kódoljuk (pl. egyirányú hash függvényekkel[29]), hogy azok többé nem visszafejthetők. [30]

A visszafelé követhető pszeudonimizált adatot olyan személyekre vonatkozó információnak tekinthetjük, akik közvetve azonosíthatók. Valójában a pszeudonim használata azt jelenti, hogy vissza lehet jutni az egyénhez oly módon, hogy az egyén személyazonossága felfedhetővé

24 Millard (2013), 170. p

25 WP 136, 20 p.

26 WP 136, 21. p

27 Bővebben lásd: Armin B. Cremers and Liangyu Xu: A Decentralized Pseudonym Scheme for Cloud-based eHealth Systems http://wob.iai.uni-bonn.de/Wob/Papers/HEALTHINF_2014_Full_Paper.pdf (utolsó letöltés: május 1.)

28 WP 136, 22. oldal

29 A telefonkönyvhöz hasonlóan egyik irányba igen könnyű keresni, viszont a visszafelé történő keresés nagyon nehéz. Továbbá szokás az ilyen egyirányú eljárásokat „csapóajtónak" (trapdoor function) is nevezni annak a jelzésére, hogy egy ilyen ajtón az egyik irányban könnyű keresztülhaladni, de az ellenkezőirányban annál nehezebb, s csak az illetékes képes erre, aki ismeri acsapóajtó nyitját. Bővebben: http://www.ms.sapientia.ro/~mgyongyi/Crypto/AsymmetricCryptoSyst.pdf

30 Millard (2013), 171. p

váljon, de csak előre meghatározott körülmények között. Ebben az esetben, noha alkalmazni kell az adatvédelmi szabályokat, az ilyen közvetett módon azonosítható információ feldolgozása tekintetében az egyént érintő fennálló kockázatok a legtöbb esetben olyan csekélyek, hogy e szabályok alkalmazása igazoltan rugalmasabb, mintha közvetlen módon azonosítható személyekre vonatkozó információkat dolgoznának fel.

III.2.b. A relatív és abszolút személyes adat értelmezés

Az személyes adat fogalmának relatív vagy abszolút jellege óriási jelentőséggel bír a felhő alapú számítástechnika szempontjából. A személyes adat abszolút és relatív értelmezésének középpontjában az adat és az érintett közötti kapcsolat helyreállíthatóságának, azaz az érintett közvetett azonosíthatóságának kérdése áll.[31] Az abszolút értelmezés alapján az adatot személyes adatnak kell tekinteni, amennyiben az adatalany és az adat között a kapcsolat megteremthető akár elvi síkon is (bármilyen eszközzel, bármilyen módon), tehát függetlenül attól, hogy adatkezelő valóban képes-e rá vagy sem.

Ezzel ellentétben a relatív értelmezés csupán azt tekinti személyes adatnak, ha ahhoz az adatkezelő *ténylegesen* is hozzáférhet. Vagyis ezen értelmezés szerint egy adat személyes adat jellegét az adatkezelő szempontjából kell vizsgálni: amennyiben az adatkezelő ténylegesen nem képes az általa kezelt adatokat az érintetthez kötni, úgy az adat e vonatkozásban (ezen adatkezelőnél) nem minősül személyes adatnak.[32]

A két megközelítés alapvetően meghatározza a személyes adat fogalmának kiterjedtségét és ezzel az európai adatvédelmi szabályok alkalmazásának a körét. Mindkét lehetséges értelmezési módnak megvannak az előnyei, illetve hátrányai. Az abszolút értelmezés a személyes adat

31 Dr. Szőke Gergely László et al. Munkahelyi adatvédelem, nemzeti jelentés-Magyarország, 11. oldal http://pawproject.eu/en/sites/default/files/page/web_national_report_hungary_hu.pdf (utolsó letöltés: 2015. V. 1.)

32 i.m. 11. oldal

fogalma alá vonja a lehető legtöbb adatot, ezzel ugyan biztosítva azt, hogy még véletlenül se kerüljön ki a szabályozás hatálya alól olyan adat, amely védelemre szorul. Ugyanakkor ezzel a kiterjesztő értelmezéssel az adatvédelmi szabályozás kötelezettségei olyan adatkezelőket is terhelhetnek, akiknek nincs módjuk megteremteni a kapcsolatot az adat és az adatalany között[33] (pl. ha az kezelt adatok erős kódolással vannak ellátva). Sőt abszurd módon ez ahhoz is vezethet, hogy úgy kellene az adatkezelőnek teljesítenie az adatalany felé a kötelezettségeit, hogy nem is képes kideríteni ki az adatalany.[34] A relatív értelmezés alapján a személyes adat fogalma az adatok jóval szűkebb körét öleli fel, így megtörténhet, hogy olyan adatok kerülnek az adatvédelmi szabályozás hatályán kívülre, amelyek kezelése mégis érintheti az egyén jogait. [35]

A kérdést maga az Adatvédelmi Irányelv nem rendezte, így az azt nemzeti jogokba átültető jogalkotó dönthette el, hogy mely értelmezést választja. E kérdés mentén a jelenleg hatályos, nemzeti jogszabályok megosztottak.[36] Többek között emiatt is szükséges egy egységes, európai szintű szabályozása az adatvédelemnek.

Magyarországon a korábbi adatvédelmi törvény (1992. évi LXIII. törvény) és az ahhoz kapcsolódó adatvédelmi biztosi gyakorlat az abszolút személyes adat értelmezés mellett foglalt állást.[37] Az Infotv. ezzel szemben a szűkebb értelmezést részesíti előnyben, ugyanis az adatkezelés elvei között rendelkezik a helyreállíthatóságról, amelyet a korábbi adatvédelmi törvény a személyes adat fogalmán belül tartalmazott.[38] Az Infotv. 4. § (3) bekezdése egy szűkítő fordulatot tartalmaz, amely alapján *„[a] személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel*

---

33 Douwe KORFF: EC Study on Implementation of Data Protection Directive 95/46/EC, 21. p http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 (utolsó letöltés 2015. V. 1.)

34 i.m 21.p

35 JÓRI András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, doktori értekezés, 86. p. http://ajk.pte.hu/files/file/doktori-iskola/jori-andras/jori-andras-vedes-ertekezes.pdf (utolsó letöltés: 2015. V.1)

36 Douwe KORFF: EC Study on Implementation of Data Protection Directive 95/46/EC, 22. p

37 JÓRI András (2005) p. 109-111. oldal.

38 Péterfalvi Attila (2012), p. 86

helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek."

Nem teljesen egyértelmű a helyzet az adatfeldolgozó viszonyában, ugyanis kérdésként merül fel, hogy személyes adatokat kezel-e az az adatfeldolgozó, amely az adatkezelő által történő titkosítás folyományaként nem tudja az érintetthez hozzárendelni az adatokat. A megoldás vitatott.

Egyes vélemények szerint[39] abban az esetben, ha „erős" kódolási eljárást követően kerülnek az adatok az adatfeldolgozóhoz, már nem alkalmazandó ezen adatokra az európai adatvédelmi szabályozás. Ebben az esetben csupán az kulccsal rendelkező adatkezelő marad annak hatálya alatt, míg az adatfeldolgozó már nem. Mindez azt eredményezné, hogy az adatkezelők a lehető legtöbb kezelt adat vonatkozásában kódolással éljenek, hiszen érdekeltek lennének ebben többek között a harmadik országba történő adattovábbítás megkönnyítése érdekében is.

A Nemzeti Adatvédelmi és Információ Hatóság ezzel szemben, állásfoglalásában kifejezte azon véleményét, amely szerint „amíg az adatok vonatkozásában az adatkezelő számára fennáll annak a lehetősége, hogy az adatokat azonosított vagy azonosítható természetes személlyel kapcsolatba hozza, akkor az adatok személyes adatoknak minősülnek, függetlenül attól a körülménytől, hogy valamilyen „kódolási" eljárás következtében az adatok az adatfeldolgozó számára nem köthetőek meghatározott természetes személyhez".[40] A vélemény indokolásában viszont már árnyaltabb megközelítéssel találkozhatunk, ugyanis a NAIH attól teszi függővé, hogy a személyes jellegétől megfosztott adatokon végzett „adatfeldolgozás" azzal jár, hogy egyébként később az adatkezelő által azonosítható természetes személyekre nézve következtetések levonását eredményezi-e, illetve egyébként kihathat-e az érintettek helyzetére. Amennyiben igen az adatvédelmi szabályok alkalmazandók.

39 Millard (2013), p. 176

40 NAIH-2512-2/2012/V ügyszámú

Természetesen bizonyos esetekben a kódolás nem lehetséges, ugyanis amennyiben például az adatok feldolgozásához veszünk igénybe egy felhőszolgáltatók, bizonyos műveletek csak a kódolatlan adatokon végezhetők el.

III.2.c. Titkosítás a felhőben

A személyes adat fogalmának előbb kifejtett lehetséges értelmezéseinek lehetséges következményei a felhő alapú számítástechnikára nézve legmegfelelőbben az adatok kódolása kapcsán szemléltethető.

Az adatvédelmi irányelv 29. szakasza alapján létrehozott adatvédelmi munkacsoport számítási felhővel kapcsolatos 05/2012. számú véleményében kiemeli a titkosítás fontosságát, amely nagymértékben hozzájárulhat a személyes adatok bizalmas kezeléséhez.[41] Hasonló következtetésekre jut az Egyesült Királyság adatvédelmi hatósága, az ICO (Information Commissioner's Office), amely felhő alapú számítástechnikával kapcsolatos jelentésében a titkosítás fontossága mellett a titkosítás visszafejthetőségét biztosító kulcs gondos megőrzésére és kezelésére is felhívja a figyelmet.[42]

A titkosítás tekintetében az előbb említett jelentések hangsúlyozzák, hogy arra az adattovábbítás során is nagy hangsúlyt kell fektetni mind a felhő alapú számítástechnikát igénybevevő és a felhőszolgáltató közötti, mind a felhőszolgáltatáson belül a különböző adatközpontok közötti adattovábbítás során.

41 WP 196, p. 17

42 ICO: Guidance on the use of cloud computing p. 14
https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf (utolsó letöltés: 2015. V. 1.)

A Munkacsoport véleménye szerint a titkosítási eljárás[43] nem teszi visszafordíthatatlanul anonimmá a személyes adatokat[44], hiszen a cél a későbbiekben a visszafejtés.

A felhő alapú számítástechnika vonatkozásában a kérdés a szolgáltatási modellek és azok egymásra épülő réteges szerkezete szempontjából bír kiemelkedő jelentőséggel.

Abban az esetben, ha egy felhőszolgáltató (Cloud Service Provider) egy olyan szoftver alapú szolgáltatást (SaaS) kínál, amely egy másik felhőszolgáltató alkalmazásfelületet bizítosító szolgáltatására (PaaS) épül, előfordulhat, hogy a SaaS szolgáltató olyan módon titkosítja, anonimizálja az adatalany személyes adatait, hogy azokhoz a PaaS szolgáltató nem tud hozzáférni, hiszen nem rendelkezik a megfelelő kulccsal. Az abszolút személyes adat értelmezés alapján ebben az esetben a PaaS szolgáltató is személyes adatokat dolgoz fel, hiszen az anonimizált adatok és az adatalany közötti kapcsolat elvi szinten megteremthető, annak ellenére, hogy maga a szolgáltató gyakorlatilag erre nem képes, hiszen nem rendelkezik a megfelelő kulccsal.

IV. Ki a felelős a felhő alapú számítástechnika vonatkozásában a személyes adatokért?

IV.1. Az adatkezelő és adatfeldolgozó fogalma általában

Az adatkezelő és az adatfeldolgozó fogalma az európai adatvédelmi rendszer központi fogalmai közé tartoznak.

A 29. cikk alapján létrehozott adatvédelmi munkacsoport az „adatkezelő" és „adatfeldolgozó" fogalmáról szóló 1/2010. számú véleményében kifejtette, hogy az „*adatkezelő fogalmának első és legfontosabb szerepe annak meghatározása, hogy ki felelős az adatvédelmi*

43 Jelen esetben egyfajta visszafordítható, visszafejthető anonimizálási eljárást értek alatta.

44 WP 196, p. 17

szabályok betartásáért, és hogy az érintettek a gyakorlatban hogyan tudják érvényesíteni a jogaikat. Más szóval: a felelősség elosztása".[45]

Az Irányelv 2. cikk d) pontja alapján adatkezelőnek minősül „*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*".

Egy adatkezelő dönthet úgy, hogy saját maga végzi az adatkezelést (pl. saját szervezetén belül), azonban lehetősége van arra, hogy e tevékenységek egészét vagy annak egy meghatározott részét külső szereplőre ruházza. A gazdasági szükségszerűség, melynek következtében bizonyos tevékenységek elvégzése szakcégek, szakemberek részére történő átadással, kiszervezéssel hatékonyabban elvégezhető vezetett az adatfeldolgozó fogalmának a megjelenéséhez.[46]

Az Irányelv által meghatározott fogalom meghatározása alapján az adatfeldolgozó „*az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, amely személyes adatokat dolgoz fel az adatkezelő nevében*". Az Irányelvet a magyar jogrendszerbe átültető Infotv. lényegét tekintve hasonlóan határozza meg a fogalmát[47], azonban mellőzi a *hatóság* és *intézmény* használatát, hiszen a jogi személy fogalma azt már magába foglalja, illetve a kiegészíti azt a *jogi személyiséggel nem rendelkező szervezetekkel*. Az Irányelv nem definiálja az adatfeldolgozás fogalmát, ezzel szemben az Infotv. definíciójából[48] észrevehető, hogy érdemi döntés nem igénylő, technikai műveletek elvégzését jelenti[49]. Az Irányelvvel ellentétben az Rendelettervezet a magyar szabályozáshoz hasonlóan

---

45 WP 169, p. 6

46 Az adatkezelő fogalma a magyar jogrendszerbe a korábbi adatvédelmi törvény (Avtv.) 1999-es módosításával kerültbe. ld. Péterfalvi (2012) p. 71.

47 Infotv 3. § 17. pont: „*adatfeldolgozó*: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkezi szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi"

48 Infotv. 3. § 17. pont „*adatfeldolgozás*: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik."

49 Péterfalvi (2012) p. 71.

már definiálja[50] az adatfeldolgozás fogalmát azzal, hogy egyfajta példálódzó felsorolást is tartalmaz az elvégzendő műveletekre. Ugyanakkor vita tárgyát képezheti, hogy szükséges-e az *adatfeldolgozás* fogalmának a meghatározása[51], hiszen az adatkezelési *érdemi döntést* leszámítva elviekben bármely művelet elvégzése kiszervezhető.

IV. 2. Adatkezelő és adatfeldolgozó a felhő alapú számítástechnika vonatkozásában

A felhő alapú számítástechnika vonatkozásában a felhasználótól az infrastruktúra szolgáltatóig (IaaS) számos szerepelőről beszélhetünk. Amennyiben e szereplőket, illetve azok szerepét az európai adatvédelmi szabályozás fogalomrendszerében igyekszünk vizsgálni, szükségesnek mutatkozik az adatkezelő és az adatfeldolgozó fogalmak vizsgálata a felhő alapú szolgáltatások szereplőire vetítve. Kérdésként merülhet fel, hogy a felhő alapú számítástechnika mint egy modern, rohamosan fejlődő IT iparág viszonyaira alkalmazhatóak-e még az elmúlt évszázadban kidolgozott fogalmak, és ha igen, akkor szükségesek-e módosítások az eredeti koncepción.

Mindenekelőtt érdemes megvizsgálni, hogy milyen szerepbe illeszthető be a felhőszolgáltató.

IV.2.a. A felhőszolgáltató mint adatfeldolgozó

A felhő alapú számítástechnika vonatkozásában az esetek többségében a felhő-szolgáltatás igénybevevője tekinthető adatkezelőnek, aki meghatározza az adatkezelés célját, dönt

50 Rendelettervezet parlament által módosított szövegének 4. cikk 3. pontja: „adatfeldolgozás: a személyes adatokon vagy adatállományokon automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, azaz gyűjtés, rögzítés, rendszerezés, strukturálás, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés".

51 Majtényi (2006) p. 124.

annak módjáról és végrehajtja, vagy végrehajtatja azt. A felelősség elosztása tekintetében tehát ebben az esetben elsősorban az igénybevevőt mint adatkezelőt terhelik az adatvédelmi irányelvben, illetve az azt átültető nemzeti jogszabályokban meghatározott kötelezettségek.

Az Irányelv 17. cikk (3) bekezdése alapján amennyiben az adatkezelő egy adatfeldolgozót (jelen esetben egy felhő-szolgáltatót) szeretne igénybe venni, az adatfeldolgozásra egy olyan szerződésnek vagy jogi aktusnak kell vonatkoznia, amely az adatfeldolgozót az adatkezelővel szemben köti. A szerződés továbbá tartalmazza, hogy: (1) az adatfeldolgozó kizárólag az adatkezelő utasításai járhat el, és (2) az adatfeldolgozónak a személyes adatok megfelelő védelme érdekében végre kell hajtania a technikai és szervezési intézkedéseket a nemzeti jogszabályoknak megfelelően.

Az Irányelv 17. cikk (2) bekezdése alapján „az adatkezelő – amennyiben az adatfeldolgozás az ő nevében történik – köteles olyan adatfeldolgozót választani, aki a technikai biztonsági intézkedések és az elvégzendő adatfeldolgozásra vonatkozó szervezési intézkedések tekintetében megfelelő garanciákat nyújt, továbbá köteles biztosítani az említett intézkedések teljesítését".

Az Irányelv idézett rendelkezései tehát teljes egészében a felhő alapú szolgáltatás igénybevevőjét terheli a felelősség az olyan felhőszolgáltatók kiválasztásáért, amelyek a személyes adatok védelme érdekében képesek a megfelelő technikai és szervezési intézkedések végrehajtására, illetve elszámoltathatóak.[52]

E megközelítés köszön vissza látszólag a Rendelettervezet 30. cikkében is, azonban közelebbről megvizsgálva jól látható, hogy az adatfeldolgozás biztonságának növelése érdekében már nem csak az adatkezelőt kötelezi elsődlegesen az adatok védelmét szolgáló megfelelő technikai és szervezési intézkedések megtételére, hanem kiterjesztve azt, immár az adatfeldolgozó is kötelezetté válik.[53]

---

52 WP196, p. 16.

53 Rendelettervezet 30. cikk (1) bekezdés: „Az adatkezelõ és az adatfeldolgozó, a technika állására és a végrehajtás költségeire tekintettel, a 33. cikk szerinti adatvédelmi hatásvizsgálat eredményeit figyelembe véve végrehajtja a megfelelõ technikai és szervezési intézkedéseket az adatfeldolgozás kockázatainak megfelelõ védelmi szint biztosítása érdekében."

Magából a Rendelettervezet szövegéből is észrevehető, hogy az adatfeldolgozó immár a közte és az adatkezelő között létrejövő szerződésre és annak tartalmára tekintet nélkül válik kötelezetté[54]. Ez egyfajta elmozdulást jelenthet a korábbi felelősség megosztás tekintetében, az adatkezelő mellett egyre nagyobb hangsúlyt kap az adatkezelő felelőssége is.

A felhő alapú számítástechnika esetében az adatfeldolgozás biztonsága körében a felhőszolgáltatók mint esetleges adatfeldolgozók kötelezettségei is növekedhetnek. Mindez üdvözlendő lépés tekintettel arra, hogy így a felhőszolgáltató mint adatfeldolgozó és az azt igénybevevő mint adatkezelő közötti szerződésre tekintet nélkül történik. A következőkben a hatályos szabályozásból eredő problémák bemutatás érdekében, érdemes megemlíteni a nyilvános felhőkre jellemző (public cloud) *take it or leave it* elvet, illetve annak negatív hatásai.

A felelősségnek az adatkezelő és az adatfeldolgozó közötti elosztása tekintetében a jelenleg hatályos Irányelvnek a fentebb idézet 16. és 17. cikke egyértelműen az adatkezelőt tekinti elsődleges kötelezettnek. Az adatfeldolgozónak pedig – igazodva a kisebb mértékű felelősségéhez – kizárólag az adatkezelő utasításai szerint kell eljárnia. A felhőszolgáltatás tekintetében egyes vélemények szerint meglehetősen mesterséges[55] lehet e viszonyrendszer fenntartása, ugyanis a szolgáltatást igénybevevő (adatkezelő) a felhőszolgáltató (adatfeldolgozó) erőforrásait saját maga használja, így a felhőszolgáltatótól nem vár el aktív magatartást. Ennek ellenére véleményem szerint szükséges e distinkció fenntartása, hiszen az igénybevevő nem a saját szervezetén belül dolgozza fel a személyes adatokat (nem a saját erőforrásait használja, a feldolgozást kiszervezi), így függetlenül a felhőszolgáltató aktív vagy passzív magatartásától, a felhőszolgáltató a kiszervezés folytán adatfeldolgozóvá válik.[56]

Az adatkezelő felelőssége a szolgáltatók közötti választás lehetőségén, illetve az utasításadási jogon alapszik. Ez teszi lehetővé, hogy az adatkezelő kiválaszthassa az adatok védelme

54 E megközelítést támasztja alá a Rendelettervezet indokolása is, amely a következőképpen rendelkezik:

55 Millard (2013) p. 198.

56 E tekintetben a felhőszolgáltatásokhoz hasonló a **tárhelyszolgáltatók** helyzete, akik ugyanúgy csupán passzív magatartásra kötelezettek, ennek ellenére a 29. cikk alapján létrehozott adatvédelmi munkacsoport 1/2010-es véleményében egyértelműen adatkezelőnek tekinti őket.

szempontjából leginkább megfelelő felhőszolgáltatót, amely az utasításai szerint fog eljárni. A felhőszolgáltatások (különösen a nyilvános felhőszolgáltatások) tekintetében azonban gyakran találkozunk szabványosított, előre elkészített és így nem tárgyalható szerződéssel (*take it or leave it contracts*). E problémakör vizsgálatához érdemes megvizsgálnunk a felhőszolgáltatások egy másik csoportosítási módját is, amely az II.3 részben került bemutatásra.

Észrevehető, hogy a felhőszolgáltatások esetében a különböző *kiépítési modellek* szerint alakul az adatkezelő utasításadási lehetőségének a terjedelme. Az adatkezelő az adatfeldolgozás során elvégzett műveletek feletti legnagyobb befolyással, kontrollal a *magánfelhő* esetében rendelkezik. Ebben az esetben viszonylag könnyen értelmezhető az adatfeldolgozót terhelő kötelezettség, mely szerint kizárólag az adatkezelő utasításai alapján dolgozhatja fel e személyes adatokat. Ezzel szemben a *nyilvános felhők* standardizált infrastruktúrával[57] és egy kész „szolgáltatási csomaggal" rendelkeznek. A méretgazdaságosságot, illetve az abból eredő hatékonyságot ez biztosítja. Ha a nyilvános felhőszolgáltatók minden egyes ügyfél számára külön kialkudott és személyre szabott informatikai megoldásokat biztosítanának, akkor nagy valószínűséggel elveszítené legnagyobb előnyét, a költséghatékonyságát és rugalmasságát.

Amint fentebb említésre került, az utasítási jog az adatfeldolgozó és az adatkezelő viszonyában a felelősségtelepítés egyfajta leképeződése. Abban az esetben viszont, ha a technológiai és gazdaságossági kérdések miatt az utasításadás csak szűk körben érvényesülhet, célszerű más megoldást találni, hiszen az elsődleges cél nem az adatkezelő utasításadási jogának a biztosítása, hanem a személyes adatok védelme az adatfeldolgozás során. Ennek érdekében megoldásként több alternatíva is kínálkozik.

Az egyik megoldás, hogy a felhőszolgáltatót adatfeldolgozó helyett adatkezelőnek vagy közös adatkezelőnek[58] tekintjük, így ennélfogva reá is vonatkoznának az adatvédelmi szabályokban

57 Millard (2013) p. 199-200

58 A rendelettervezet 24. cikke határozza meg a közös adatkezelő fogalmát. Ebben az esetben úgy tekinthető, hogy a nyilvános felhőszolgáltató, mivel szabványosított szerződéseket használ, az adatfeldolgozás módjának meghatározása során maga is aktív szerepet tölt be.

meghatározott kötelezettségek. Ezzel kapcsolatosan azonban a 29. szakasz alapján létrehozott adatvédelmi munkacsoport szerint „az a tény, hogy a szerződést és az üzletre vonatkozó részletes rendelkezéseit a szolgáltató, és nem az adatkezelő készíti el, önmagában nem ad kellő alapot arra a következtetésre, hogy a szolgáltatót kell adatkezelőnek tekinteni, mindaddig, amíg az adatkezelő szabadon fogadja el a szerződés rendelkezéseit és így teljes felelősséget vállal értük.”[59]

Ezen álláspont ellenére jól látható az egyensúlytalansági állapot, amely az igénybevevő mint adatkezelő és a felhőszolgáltató mint adatfeldolgozó adatvédelmi felelőssége és tényleges cselekvési lehetőségei közötti aszimmetrikus helyzetből ered. [60]

E problémát enyhítheti a Rendelettervezet 26. cikk (4) bekezdése, amely alapján amennyiben az adatfeldolgozó az adatkezelő utasításaitól eltér a személyes adatok feldolgozása során vagy az adatfeldolgozás módját és célját meghatározó féllé válik[61] az adatfeldolgozó az adatfeldolgozás tekintetében adatkezelőnek minősül és rá a rendelet közös adatkezelőkre vonatkozó szabályait kell alkalmazni.[62]

További megoldás lehet az adatfeldolgozó felelősségének a növelése.

A Rendelettervezet 26. cikke ugyanakkor megtartja a felelősségelosztás Irányelvben meghatározott megközelítését azzal, hogy konkrét kötelezettségeket is felsorol az adatkezelő számára.[63] Az utasításadási jog tekintetében azonban precízebben fogalmaz és szűkíti, illetve

---

A francia adatvédelmi hatóság (La Commission Nationale de l'Informatique et des Libertés -CNIL) ajánlásában hasonló álláspontra helyezkedett. Ehhez ld. http://www.cnil.fr/english/news-and-events/news/article/cloud-computing-cnils-recommendations-for-companies-using-these-new-services/

59 WP169 p. 29.

60 Pl. egy kis vagy közepes méretű vállalkozás mint felhasználó és egy felhőszolgáltató óriás (pl. Amazon, Google) közötti egyensúlytalanság.

61 Pl. a szabványosított szerződések révén a felhőszolgáltató nem enged teret az adatkezelő utasításainak.

62 A Bizottság által javasoltot jelentősen módosító Európai Parlament által javasolt szövegbe a LIBE bizottságnak köszönhetően került be „*vagy az adatfeldolgozás módját és céljait meghatározó féllé válik*” feltétel.

63 Rendelettervezet 26. cikk (2) bekezdés. Itt érdemes megemlíteni, hogy az Európai Bizottság által benyújtott szöveg jelentős módosításokon ment keresztül.

konkretizálja azt. Mindemellett kifejezésre juttatja azt is, hogy az adatkezelő és az adatfeldolgozó nagyfokú szabadságot élveznek a feladatok meghatározása és elosztása tekintetében:

„Az adatkezelő és az adatfeldolgozó szabadon határozzák meg e rendelet követelményeivel összefüggő szerepeiket és feladataikat, ugyanakkor biztosítják, hogy az adatfeldolgozó: (…) b) kizárólag az adatkezelő utasítása alapján dolgozzon fel személyes adatokat, kivéve, ha az Unió vagy a tagállam jogszabályai másként rendelkeznek”[64]

V. Harmadik országba történő adattovábbítás

A határokon átnyúló adattovábbítás mértéke exponenciálisan nőtt az elmúlt évtizedekben[65]. Az adatfeldolgozás módja is megváltozott, így már nem pusztán két végpont közötti adattovábbításról beszélhetünk, hanem gazdasági, üzleti profitot eredményező, centralizáció helyett dekoncentrált hálózatban történő adatfeldolgozási folyamatoknak egy szükséges kellékéről.[66]

A határokon átnyúló adattovábbítás szereplőinek a köre is jelentősen bővült, akik immár elsődlegesen a világhálót, illetve az ún. Web 2.0-t (a felhő alapú számítástechnika mellett ide sorolhatóak a közösségi oldalak, blogok, keresőmotorok, stb.) használják.[67]

A nemzetközi kereskedelemben és az egyre erőteljesebben globalizálódó világgazdasági folyamatokban való részvételhez elengedhetetlen a harmadik országokba[68] történő adattovábbítás. Ugyanakkor a határon átnyúló adattovábbítás növekedésével egyre nagyobb hangsúlyt kap az ezt szabályozó jogi környezet.

64 Rendelettervezet 26. cikk (2) bekezdés b) pont. Az Európai Parlament módosította a Bizottság javaslatát, amely az Irányelvben foglaltakat vette át.

65 Kuner (2013) p. 2

66 Schwartz (2009) p. 4

67 Kuner (2013) p. 3

68 nem EGT tagállam

V.1. A hatályos szabályozási rendszer

A jelenleg hatályos Irányelv sem kíván gátat szabni az adattovábbításnak, csupán egy olyan rendszert igyekszik létrehozni, amely megfelelő módon képes egyensúlyozni a két érdek (gazdasági-adatvédelmi) között. Ennek következtében csak olyan harmadik országba nem továbbítható személyes adat, amely nem képes *„megfelelő védelmi szintet”* biztosítani. [69] E főszabály alól kivételként jelennek meg az Irányelv 26. cikk (1) bekezdésében taxatíve meghatározott feltételek, így valamelyik teljesülése esetén az adatkezelő – a megállapított „megfelelő védelem” elvétől eltérve – személyes adatokat továbbíthat harmadik országoknak. A megfelelő védelmi szint követelményével igyekszik rászorítani a jogalkotó egy az európai sztenderdeknek megfelelő szabályozási környezet létrehozására azon országokat, amelyeknek (gazdasági) érdekük fűződik az EGT térségből a hozzájuk történő személyes adattovábbításhoz.

Az Irányelv felhatalmazza a Bizottságot[70] arra, hogy határozatban[71] megállapítsa a megfelelő adatvédelmi szint meglétét országonként. Ennek alapján a Bizottság már több országról megállapította, hogy abban a személyes adatok védelmi szintje megfelelő (Egyesült Államok, Új Zéland, Uruguay, Izrael, Kanada, Argentína stb.).[72] Bár formálisan a határozatot a Bizottság hozza, annak előkészítésében egyéb szereplők is részt vesznek (pl. a 29. cikk alapján létrehozott adatvédelmi munkacsoport). Továbbá mind az Európai Parlament, mind a Tanács kérheti a határozat módosítását, vagy hatályon kívül helyezését.

Mindezeken felül az Irányelv lehetővé teszi, hogy tagállamok engedélyezzék a személyes adatok olyan harmadik országba irányuló továbbítását vagy továbbítás-sorozatát, amely nem felel meg a megfelelő védelmi szint követelményének, azonban „adatkezelő *megfelelő garanciákat*

69 Irányelv 25. cikk (1) bekezdés

70 Irányelv 25. cikk (6) és 26. cikk (4) bekezdés

71 Az EUMSZ 288. cikke alapján a határozat jogi természetét illetően: „a határozat teljes egészében kötelező. Amennyiben külön megjelöli, hogy kik a címzettjei, a határozat kizárólag azokra nézve kötelező, akiket címzettként megjelöl”. A határozatok címzettjei a tagállamok, így azok az Európai Unió kötelező jogi aktusának tekinthetőek.

72 http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelme, továbbá a kapcsolódó jogok gyakorlása tekintetében; ilyen garanciát jelenthetnek elsősorban a megfelelő szerződési feltételek". [73] Továbbá a Bizottságnak is lehetősége van egyes általános szerződési feltételekről megállapítani, hogy megfelelő biztosítékot nyújtanak. [74]

Az Irányelv hatályos szabályozási rendszerét összefoglalva tehát megállapítható, hogy alapvetően három féle jogalapra hivatkozva továbbítható személyes adat harmadik országba:

1. Főszabályként az Európai Bizottság ún. *megfelelőségi határozata* alapján (adequacy decision)[75]

2. A megfelelőségi követelmény alóli, az Irányelv 26. cikk (2) bekezdésében taxatíve felsorolt kivételek esetén

3. Az adatkezelő által teremtetett megfelelő garanciák esetén (pl. megfelelő szerződési feltételek, BCR)

V.2. A Rendelettervezet szabályozási rendszere

Úgy a Bizottság által benyújtott Rendelettervezet, mint annak az Európai Parlament által módosított változata jelentős változtatásokat tartalmaz a harmadik országba irányuló adattovábbítás vonatkozásában.

A Rendelettervezet V. fejezete szakít az Irányelv azon módszerével, amely főszabályként meghatározza, hogy csak akkor továbbítható személyes adat harmadik országba, ha az megfelelő védelmi szintet biztosít. Egyetlen főszabály meghatározása helyett egy általános elvvel találkozunk, amely szerint a személyes adatok továbbítása csak abban az esetben megengedett, ha az

73 Irányelv 25. cikk (2) bekezdés

74 Irányelv 26. cikk (4) bekezdés

75 Irányelv 25. cikk (1) bekezdés

adatkezelő és az adatfeldolgozó teljesíti az adattovábbításra vonatkozó szabályokat felölelő fejezet rendelkezései.

Érdemes kiemelni, hogy a Rendelettervezet immár a személyes adatoknak harmadik országból vagy nemzetközi szervezettől egy további harmadik ország vagy további nemzetközi szervezet részére történő továbbítására vonatkozó feltételekre is kiterjeszti a fenti általános megfelelőségi kötelezettséget, amely a felhőszolgáltatók tekintetében is kiemelkedő jelentőséggel bírhat.

A Rendelettervezet a harmadik országba történő adattovábbítás során alapvetően két jogalapot különböztet meg és az Irányelvhez hasonlóan az ezek alóli taxatíve felsorolt kivételeket.

Az *első* lehetséges jogalap a „megfelelő védelmi szint" követelménye[76], amely „alapján akkor kerülhet sor adattovábbításra, ha a Bizottság megállapítja, hogy a *harmadik ország, annak régiója vagy adatfeldolgozó ágazata*, illetve a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges további engedély." Annak ellenére, hogy látszólag e koncepció megegyezik az Irányelv megközelítésével, jelentős különbségek mutatkoznak.

A Rendelettervezet a korábbi földrajzi alapú megközelítés mellett egy adott országban ágazatonként is lehetővé teszi a Bizottság számára a megfelelő védelmi szint vizsgálatát. Várhatóan olyan országok vonatkozásában kiemelkedő jelentőségű lehet, amelyek egy általános adatvédelmi szabályozás helyett szektor specifikus, ágazati szabályokkal rendelkeznek. A Rendelettervezet továbbá konkrét szempontokat is meghatároz a Bizottság számára, amelyek alapján el kell végeznie a vizsgálatot.[77] Azok a szempontok, amelyek figyelembevételével a Bizottság értékeli a védelem szintjének megfelelő, illetve nem megfelelő mivoltát, kifejezetten magukban foglalják például a jogállamiságot, a bírósági jogorvoslatot és a független felügyeletet.

76 A Rendelettervezet 41. cikk

77 Rendelettervezet 41. cikk (2) bekezdés

A *második* lehetséges jogalap esetén –amennyiben a megfelelő védelmi szint követelménye nem biztosított– az adattovábbítás akkor megengedett, ha az adatkezelő vagy az adatfeldolgozó megfelelő biztosítékot nyújt jogilag kötelező eszköz útján. A Rendelettervezet a megfelelő biztosítékok egy példálódzó felsorolását adja, amelynek következtében ide sorolhatóak a kötelező erejű vállalati szabályok, Bizottság által elfogadott adatvédelmi előírásokat tartalmazó mintaszerződések, engedélyezett ad hoc szerződési feltételek stb. Bár e jogalap az Irányelv 26. cikk (4) bekezdésében is már nevesítve volt, új elemként jelenik meg, hogy egységes adatvédelmi feltételeket a tagállami felügyelő hatóságok is elfogadhatnak és ezeket a Bizottság általános érvényűnek nyilváníthatja. [78]

A harmadik jogalap az előző irányelvhez hasonlóan az előző jogalapok hiányában történő kivételes adattovábbítási lehetőségeket tartalmazza hasonlóan az Irányelv 26. cikk (1) bekezdéséhez.[79]

Összességében elmondható, hogy a Rendelettervezet az Irányelv adatvédelmi hagyományait követi az adattovábbítás terén is, azonban megfigyelhető egyfajta könnyítés, rugalmasság, hiszen egyetlen fő jogalap helyett egy *összetettebb rendszert* hoz létre, amelyben úgy bővíti a jogalapok körét, hogy megfelelően ötvözi a földrajzi alapú szabályozási megközelítést (*geographically-based approach*) és a szervezeti megközelítést (*organizationally-based approach*). A földrajzi alapú megközelítés esetében a védelmi szint megfelelősségének vizsgálata elsősorban területi alapon történik (pl. országok, régiók), míg a szervezeti megközelítés esetében a személyes adatokat harmadik országba továbbító személy vagy szervezet válik felelőssé.

78 Rendelettervezet indokolása p. 13

79 Rendelettervezet 44. cikk

V.3. Az adattovábbítás szabályozási rendszerei a felhő alapú számítástechnika vonatkozásában

A felhő alapú számítástechnika sokkalta dinamikusabb, mint bármilyen más adatfeldolgozás. Az adatfeldolgozás helye nagyon gyors ütemben változhat. Ahogyan a 29. cikk alapján létrehozott adatvédelmi munkacsoport véleményében[80] olvasható: „a számítási felhőben (…) az adatoknak gyakran egyáltalán nincs állandó helyük a számításifelhő-szolgáltató hálózatán belül. Előfordulhat, hogy az adatok délután 2 órakor az egyik adatközpontban vannak, délután 4-kor pedig a világ másik részén lévő másikban. Ennélfogva a felhőszolgáltató ritkán kerül olyan helyzetbe, hogy meg tudja állapítani az adatok aktuális, elhelyezkedését, tárolásuk vagy továbbításuk helyét". A gyakorlatban a felhőszolgáltató, függetlenül a székhelyétől, telephelyétől, számtalan szerverközponttal, rendelkezik a világban.[81] Ennek oka többek között, hogy így is igyekeznek csökkenteni a működési költségeiket, pl. olyan régiókat választanak, ahol alacsonyabb az elektromos áram költsége, a klíma megfelelő a szerverparkok számára, továbbá a térség rendelkezik megfelelő nagyságú internetcsomóponttal.

Tekintettel arra, hogy a felhő alapú számítástechnika úgy képes a lehető legköltséghatékonyabban működni, hogy nem helyi, hanem globális szinten nyújt szolgáltatásokat, a külföldre történő adattovábbítás, illetve ezáltal az EU viszonyában a harmadik országba történő adattovábbítás gazdaságilag elengedhetetlen a felhő iparág számára.

E problémakör vizsgálata során is érdemes differenciálni aszerint, hogy a felhőszolgáltató adatkezelői vagy adatfeldolgozói minőségében kezelendő, nyilvános vagy magánfelhőről van szó.

---

80 WP196 p. 19

81 Millard (2013) p. 256

V.3.a. Kötelező erejű vállalati szabályok

A kötelező erejű vállalati szabályok (*Binding Corporate Rules, a továbbiakban BCR*) olyan gyakorlati szabálygyűjtemények, melyeket a nemzetközi szervezetek állítanak össze és követnek, és amelyek az adatvédelmi elvek megvalósítására szolgáló belső intézkedéseket tartalmaznak.[82] E szabályok, magatartási kódexek tehát egy (jellemzően) nemzetközi vállalatcsoporton belül, függetlenül a konkrét helyszíntől (így EGT területén kívül is) biztosítják az uniós adatvédelmi szabályok, elvek betartását a vállalaton belüli adatáramlás során. E jogintézmény lényegéből következik, hogy a vállalatcsoportok egyoldalú kötelezettségvállalásaként, magánjogi eszközökkel kikényszeríthető, jogilag kötelező formában nyújt megfelelő biztosítékok a személyes adatok harmadik országba történő továbbítása során.

A BCR-ek jogalapját a jelenleg hatályos szabályozásban az Irányelv 26. cikk (2) és bekezdése képezi, amely „adatkezelő megfelelő garanciákat" az adatkezelőtől megfelelő garanciák megteremtése esetén lehetővé teszi olyan harmadik országba történő adattovábbítást, amely nem biztosít „megfelelő szintű védelmet". Tehát a jelenlegi szabályozás nem említi külön kategóriaként a BCR-eket, azokat csupán levezetni lehet. Emiatt a BCR jogintézményének kialakulásához és fejlődéséhez jelentősen hozzájárult a 29. cikk alapján létrehozott adatvédelmi munkacsoport tevékenysége. Az e témában kiadott munkadokumentumai[83] jelentősen alakították, fejlesztették e szabályok alkalmazási lehetőségét.

A BCR-ek alkalmazásával az Európai Unió adatvédelmi elveit és szabályai egy olyan szabályzat tartalmazza, amely a gyakorlatban is kötelező erővel rendelkezik. A 29. cikk alapján létrehozott adatvédelmi munkacsoport véleményében is hangsúlyozza, hogy a gyakorlati érvényesülés feltételeként a BCR-ek tartalmaznia kell pl. belső fegyelmi szankciókat, ha munkavállalói azokat megszegi, továbbá azt, hogy a vállalat oktatást szervezzen a BCR alkalmazásáról az adatfeldolgozást

82 WP 173 p. 7.

83 A BCR-ekkel foglalkozói munkadokumentumok elérhetőek a következő honlapon: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm

végző munkavállalóinak.[84] Tekintettel arra, hogy a jogérvényesítés a nemzetközi környezet, a joghatósági kérdések miatt igen komplex, a BCR-ek alkalmazása során biztosítani kell a megsértésük esetére az Európai Unió területén történő igényérvényesítést is.[85]

A harmonizáció azonban nem teljes e területen sem, a tagállamoknak csupán egy része fogadja el harmadik országba történő személyes adat továbbításának jogalapjaként a BCR-eket.[86] Magyarország a BCR-eket elutasító csoportba sorolható, így annak előnyeit a magyar adatvédelmi jog alá tartozó vállalatok nem élvezhetik, ugyanis az Infotv. 8. §-ban meghatározott jogalapok között nem szerepelnek a kötelező erejű vállalati szabályok és azok nem is vezethetőek le.

A Rendelettervezet 43. cikke ezzel szemben immár külön nevesíti és részletesen szabályozza a BCR-eket beépítve a (többek között az adatvédelmi munkacsoport által kidolgozott) korábbi gyakorlatot.

Megjegyezendő, hogy az Európai Bizottság javaslatában csupán az adatfeldolgozó vonatkozásában szerepelt a BCR-ek alkalmazásának a lehetősége, azonban az Európai Parlament által elfogadott javaslatban már bekerült az adatfeldolgozó is. Mindez örvendetes annak fényében, hogy a felhőszolgáltatók mind adatkezelőnek, mind feldolgozónak minősülhetnek, így szükségesnek mutatkozik mind a két kategória számára lehetővé tenni alkalmazásukat.

A fentiek alapján látható, hogy a BCR-ek alkalmazása kiváló lehetőséget biztosít felhőszolgáltatók számára az adattovábbítás során jelentkező problémák kezelésére, azonban csupán abban az esetben, amikor a vállalatcsoporton belül történik az adattovábbítás, esetleg alvállalkozók nélkül, hiszen a vállalatok közötti adatáramlásra már nem alkalmazhatóak. Ennélfogva a BCR-ek alkalmazása leginkább a vertikálisan integrált szervezettel rendelkező, kiszervezést nem alkalmazó

84 WP 74, p. 10

85 WP 74, p. 19

86 A tagállamok gyakorlatát ezzel kapcsolatban összefoglalja a 29. cikk alapján létrehozott adatvédelmi munkacsoport következő munkadokumentuma: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm

adatfeldolgozó és adatkezelői minőségben megjelenő felhőszolgáltatók számára lehet működő megoldás.

V.4. Szerződéses biztosítékok

A szerződéses feltételek jogalapja az Irányelv esetében –a BCR-ek jogalapjához hasonlóan– a 26. cikk (2) és (4) bekezdése képezi. A szerződéses feltételek a BCR-ek egyoldalú kötelezettségvállalásával szemben egy többoldalú konstrukcióként jelennek meg. Két formájukat különböztethetjük meg: a) általános szerződési feltételek, b) ad hoc szerződések

a) Általános szerződési feltételek

E kategóriába az Irányelv 26. cikk (4) bekezdése alapján, az Európai Bizottság által elfogadott azon általános szerződési feltételeket tartalmazó csomagok sorolhatók, amely adatkezelők, vagy adatkezelő-adatfeldolgozó viszonyában szabályozzák a nemzetközi adattovábbításokat biztosítva ezáltal az ahhoz szükséges megfelelő védelmi szintet.[87] Az Európai Bizottság ennek következtében hozott két határozatot az EGT területén belül és azon kívül letelepedett adatkezelők közötti általános szerződési feltételekről,[88] továbbá egy határozatot az adatkezelő és EGT területen kívüli adatfeldolgozó viszonyában.[89]

A Rendelettervezet Bizottság által benyújtott tervezetének a 43. cikke megtartja e kategóriát, sőt kiegészíti azt egy új elemmel[90], amely szerint a tagállami felügyelőhatóságok is

87 WP196, p. 21.

88 2001/497/EC és a 2004/915/EC Bizottsági határozatok

89 2010/87/EU Bizottsági határozat

90 Rendelettervezet 43. cikk (2) bekezdés c) pont

kibocsáthatnak ilyen általános szerződéses feltételeket, amennyiben azokat a Bizottság jóváhagyja. Az Európai Parlament által módosított szövegben azonban törlésre kerül a jelenleg hatályos szabályozást beépítő rendelkezés, így az Európai Bizottság közvetlenül már nem fogadhatna el általános szerződési feltételeket, csupán jóváhagyhatná őket.

A felhő alapú számítástechnikában szükséges a kétoldalú megállapodások alkalmazása, hiszen a szolgáltatási lánc adott esetben több szereplős lehet, vagyis egy felhőszolgáltató alvállalkozókat vehet igénybe, akik újabb alvállalkozókat stb. Az általános szerződési feltételek jelenleg azonban nem fednek le valamennyi élethelyzetet, csupán azok egy részét. Csupán abban az esetben alkalmazhatóak, ha a felhőszolgáltatót igénybevevő adatkezelő egy harmadik országbeli felhőszolgáltatóval mint adatkezelővel, vagy adatfeldolgozóval köt szerződést. Abban az esetben tehát, ha egy unióban letelepedett felhőszolgáltatóval köt szerződés, amely egy alvállalkozójának továbbítaná harmadik országba az adatokat (pl. uniós SaaS, amely egy harmadik országbeli IaaS-ra épül) már nem alkalmazhatóak. Ez mindenképpen egy megoldandó problémaként jelentkezik, hiszen az az abszurd helyzet áll elő, hogy egy adatfeldolgozónak érdemesebb egy harmadik országbeli adatkezelő felhőszolgáltatót választania, hiszen reá alkalmazhatók a Bizottság által mintaként meghatározott általános szerződési feltételek, míg egy az EU-ban letelepedett adatfeldolgozó megbízása esetén az már nem vehet igénybe e módszer alapján egy harmadik országbeli alvállalkozót. Annak fényében pedig még nagyobb problémaként jelentkezik, hogy a felhőszolgáltató jelentős része a harmadik országbeli Amazon, Microsoft, Google által kínált IaaS-ra, illetve PaaS-ra épül.[91]

b) Ad hoc szerződések

Az általános szerződési feltételekhez szorosan kapcsolódó típusról beszélhetünk, ugyanis ebben az esetben a felek állapodnak meg, szerződésükben rögzítik a megfelelő védelmi szintet

91 Millard (2013) p. 272

garantáló szabályokat, ezt követően pedig szükséges az adott tagállam felügyelő hatóságának a jóváhagyása.

Mindez megoldásként szolgálhat az általános szerződési feltételek alkalmazásánál említett problémára, vagyis a harmadik országbeli alvállalkozó adatfeldolgozónak történő továbbításra, azonban a tagállami felügyelőhatóságok dönthetnek az adott, konkrét kérdésben.

A megoldás tehát ugyancsak alkalmazható a felhőszolgáltatók harmadik országba történő adattovábbítására, azonban az általános szerződési feltételekkel ellentétben (amelyek minden tagállamra kötelezőek és így minden tagállamban alkalmazhatóak), szükség van egy előzetes engedélyezési eljárásra, amely során az adott tagállami felügyelőhatóság megvizsgálja a megfelelő védelmi szint meglétét.

A Rendelettervezet – üdvözlendő módon – a 42. cikk (2) bekezdés d) pontjában külön nevesíti e kategóriát mind az adatkezelő, mind az adatfeldolgozó által történő adattovábbítás esetére.

c) Mi minősül adattovábbításnak?

Sem az irányelv, sem a Rendelettervezet nem definiálja az adattovábbítás fogalmát, holott ez határozza meg, hogy mikor kell alkalmaznunk a rá vonatkozó szabályanyagot. Az OECD Adatvédelmi Irányelvek (OECD Privacy Guidelines) kissé tautológia ízű meghatározásában a „*személyes adatok határokon átívelő áramlásának jelentése személyes adatok nemzeti határok közötti mozgása*”.[92]A 108. számú Európa Tanácsi Egyezmény pedig személyes adatoknak „országhatárokon keresztül - bármely eszközzel - történő továbbításként” határozza meg az adattovábbítás fogalmát.[93] Mindkét megközelítés arra helyezi a hangsúlyt, hogy a személyes adatnak át kell lépnie a határt.

92 OECD Privacy Guidelines Első Rész, 1. c) bekezdés.
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

93 Counsel of Europe- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.I.1981) 12. cikk (1) bekezdés
http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

A nehézségek akkor kezdődnek, amikor alaposabban szemügyre vesszük az internet világát. Az adatok határokon átnyúló áramlása technikai értelemben nem csupán aktív magatartás eredményeként következik be, amikor a cél az adatok továbbítása, hanem akkor is, ha pl. egy weboldal elérhetővé válik más országokban élők számára és azok csupán megnyitják (letöltik) saját számítógépükre.

E problémakört is körüljárta az Európai Unió Bírósága a *Lindqvist* ügyben[94], amely többek között arra kereste a választ, hogy harmadik országba irányuló adattovábbításnak minősülhet-e személyes adatoknak egy hazai vagy más tagállam területén lévő szerverre történő feltöltése weboldalként, ha ennek következtében ezen adatokat minden, internetre csatlakozó személy számára hozzáférhetővé teszi, beleértve harmadik országokban tartózkodókat is. A Bíróság arra a következtetésre jutott, hogy különbséget kell tenni az aktív adattovábbítás és az adatoknak a szerverről történő letöltés következtében bekövetkező adatáramlás között, amelyre már nem vonatkoznak a harmadik országba történő adattovábbításra vonatkozó rendelkezései.

Megjegyezendő, hogy az ítélet érvelése nem tartalmaz egy technológia-semleges végkövetkeztetés. Véleményem szerint leginkább az adott konkrét helyzetre[95] (a weboldalon közzétett adatok harmadik országban történő megnyitása, letöltése kontextusban) értelmezhető az, hogy a harmadik országba történő adattovábbítás megkíván egyfajta aktív, tudatos magatartást. Amennyiben ezzel ellentétesen értelmezzük, vagyis elfogadnánk azt, hogy az ítéletben megállapított értelmezés elvi jelentőségű technológiától függetlenül, ezzel alkalmazni kényszerülnénk e megszorító értelmezést minden adattovábbításra (pl. a felhő esetére is). Amennyiben tehát általános jelleggel alkalmaznánk az ügyben lefektetett elvet, csupán az aktív magatartás eredményeképpen létrejövő adatáramlás minősülne az adatvédelmi Irányelv fogalomrendszere szerint „adattovábbításnak”. Az egyensúly megtalálása nehéz, hiszen a konkrét ügyben elfogadható, hogy a Bíróság az aktív magatartás hiányára hivatkozva igyekszik szűkíteni az adattovábbítás rendelkezéseit, ugyanis ha nem így tenne, az voltaképpen nem lenne összeegyeztethető az Internet (internetes oldalak) alapvető jellemzőivel.

94 C101/01. sz. ügy http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=HU

95 C101/01. sz. ügy 69-71. bek.

Látható, hogy az adattovábbítás meghatározása korántsem problémamentes. Ennek ellenére viszonylagos egyetértés figyelhető meg atekintetben, hogy az adattovábbítás elhatárolandó a kizárólag átmenő adatforgalomtól.[96] A kizárólag átmenő adatforgalom fogalmát az Irányelv 4. cikk (1) bekezdés c) pontja említi az alkalmazandó nemzeti jog meghatározásának vizsgálatakor. A 29. cikk alapján létrehozott adatvédelmi munkacsoport példaként említi azokat a távközlési hálózatokat (kábelek), amelyek csak azt biztosítják, hogy a közlések áthaladását biztosítják. Ugyanakkor ezeket szűken kell értelmezni és abban az esetben, ha többletszolgáltatás is kapcsolódik már hozzájuk, ugyanúgy alkalmazandók esetükben is az adatvédelmi szabályok[97].

VI. Összegzés

A dolgozat bemutatta, hogy a felhő alapú technológia számos adatvédelmi szabály esetében speciális kérdéseket vet fel. Ennek ellenére véleményem szerint az európai adatvédelmi reform során a technológia-semleges jogalkotási technikát fenn kell tartani. Ez azonban nem jelenti azt, hogy a korábbi szabályozás radikális reformja ne lenne elképzelhető.

A felhő alapú technológia hatalmas gazdasági és technológiai potenciállal rendelkezik. A technológia ismertetett jellemzőinek köszönhetően a következő években meghatározhatja, jelentősen befolyásolhatja az IT szektor fejlődését. Az Európai Unió gazdasági válságból történő kilábalásában is kulcsszerepe lehet. Mindemellett azonban figyelembe kell venni az Európai Unió világszinten is meghatározó adatvédelmi szabályozását, amely jelentősen befolyásolja a technológia európai térnyerését.

A dolgozatban bemutatásra kerülő három fő pillér (személyes adat fogalma, adatkezelő és adatfeldolgozó viszonya, harmadik országba történő adattovábbítás) alapján kijelenthető, hogy az

96 Kuner (2013) p. 15.

97 WP179 p.25

kilencvenes években elfogadott irányelv, illetve az azokat átültető (sokszor partikuláris szabályozást előidéző) tagállami jogszabályok nem kedveznek a felhő alapú számítástechnika térnyerésének. Azonban a Rendelettervezet, illetve különösen annak az Európai Parlament által módosított változata számos kérdésben kedvező szabályozási környezetet vetít előre, amelyet nem a szabályok fellazítása, hanem a kor követelményeihez igazodó, az adatvédelem hatékonyságának növelése jellemez.

VI. Felhasznált források

- BŐGEL György: Az informatikai felhők gazdaságtana – üzleti modellek versenye az informatikában. In: Közgazdasági Szemle, LVI. évf., 2009. július–augusztus
- Christopher KUNER: Transborder Data Flows and Data Privacy Law, Oxford University Press, Oxford, 2013. Cit: Kuner (2013)
- Christopher MILLARD (szerk.): Cloud Computing Law, Oxford University Press, Oxford, 2013. Cit: Millard (2013)
- COM (90) 314 final (Commission of the European Communities: COMMISSION COMMUNICATION on the protection of Individuals In relation to the processing of personal data In the Community and Information security) http://aei.pitt.edu/3768/1/3768.pdf
- Douwe KORFF: EC Study on Implementation of Data Protection Directive 95/46/EC,http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667
- Dr. SZŐKE Gergely László et al. Munkahelyi adatvédelem, nemzeti jelentés-Magyarország,http://pawproject.eu/en/sites/default/files/page/web_national_report_hungary_hu.pdf
- ICO (Egyesült Királyság Adatvédelmi Biztosának Hivatala): Guidance on the use of cloud computing https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf
- JÓRI András: Adatvédelmi kézikönyv : Elmélet, történet, kommentár, Osiris kiadó, Budapest, 2003 (Cit: Jóri (2003))
- JÓRI András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, doktori értekezés, http://ajk.pte.hu/files/file/doktori-iskola/jori-andras/jori-andras-vedes-ertekezes.pdf

- MAJTÉNYI László: Az információs szabadságok, Complex kiadó, Budapest, 2006. Cit: Majtényi (2006)
- Paul M. SCHWARTZ, Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment (2009) (http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf) cit: Schwartz (2009)
- PÉTERFALVI Attila (szerk.): Adatvédelem és információszabadság a mindennapokban, HvgOrac kiadó, Budapest, 2012. Cit: Péterfalvi (2012)

Jogforrások, vélemények

Az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről szóló 1998. évi VI. törvény

A 29. cikk alapján létrehozott munkacsoport véleményei:

WP74

Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf

WP 136

munkacsoport 4/2007 vélemény a személyes adat fogalmáról.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_hu.pdf

WP 169

1/2010. számú vélemény az „adatkezelő” és az „adatfeldolgozó” fogalmáról

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_hu.pdf

WP 173

3/2010 vélemény az elszámoltathatóság elvéről

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_hu.pdf

WP 196

Opinion 05/2012 on Cloud Computing

http://idpc.gov.mt/dbfile.aspx/WP196.pdf

Internetes források (utolsó letöltés: 2015. 05. 1)

- IDC Predicts the 3rd Platform Will Bring Innovation, Growth, and Disruption Across All Industries in 2015

  http://www.idc.com/getdoc.jsp?containerId=prUS25285614
- Commission Of The European Communities: COMMISSION COMMUNICATION on the protection of Individuals In relation to the processing of personal data In the Community and Information security

  http://aei.pitt.edu/3768/1/3768.pdf
- KRAUTH Péter: Közműszerű IT-szolgáltatás,

  http://www.nhit-it3.hu/__ujsite2/images/tagandpublish/Files/it3-2-1-10-u.pdf
- Dr. TÓTH Mihály és Randall K. NICHOLS: Aszimmetrikus kriptorendszerek (tansegédlet)

  http://www.ms.sapientia.ro/~mgyongyi/Crypto/AsymmetricCryptoSyst.pdf