KIS KELEMEN BENCE – HOHMANN BALÁZS

A SCHREMS ÍTÉLET HATÁSAI AZ EURÓPAI UNIÓS ÉS MAGYAR ADATTOVÁBBÍTÁSI GYAKORLATOKRA

1. BEVEZETÉS

Az Európai Unió és az Amerikai Egyesült Államok gazdasága adja a világ GDP-jének felét, a világkereskedelem egyharmadát, ezért a köztük fennálló kereskedelmi kapcsolatok meghatározó jelentőségűek a világpiac számára. Az EU Egyesült Államokba irányuló szolgáltatási exportja a szolgáltatási importhoz hasonlóan évek óta növekvő tendenciát mutat, ennek további támogatására a transzatlanti kereskedelmi és beruházási partnerségről 2013 óta zajlanak tárgyalások.[1] A kereskedelmi kapcsolatok szerves részét képezi az egyre növekvő adatáramlás,[2] mely egyben a személyes adatok cseréjét is jelenti, ezért gazdasági szempontból meghatározó jelentőségű az EU Egyesült Államokba irányuló adattovábbításra vonatkozó szabályozása.[3]

A személyes adatok magas szintű védelmének biztosítása, ugyanakkor a transzatlanti adattovábbítás megkönnyítése érdekében az Európai Unió Bizottsága 2000 júliusában hozott határozatában[4] megfelelő védelmet biztosító adatkezelőnek ismerte el az Egyesült Államok Kereskedelmi Minisztériuma által kiadott adatkezelésre vonatkozó elveket magukra nézve kötelezőnek elismerő szervezeteket, ezért lehetővé tette az európai személyes adatok továbbítását részükre (ún. Safe Harbor megállapodás).

Noha az Edward Snowden nevével fémjelzett megfigyelési botrány miatt a határozat felülvizsgálata már 2013 óta napirenden volt,[5] 2015 októberében az Európai Unió Bírósága a C-362/14. számú, Maximillian Schrems kontra Data Protection Commissioner ügyben hozott ítéletével végül érvénytelenné nyilvánította a keretrendszert,[6] komoly kihívás elé állítva ezzel az adatkezelőket, hogy más, az EU adatvédelmi irányelvének[7] megfelelő jogalapot biztosítsanak a transzatlanti adattovábbításra.

2016 februárjában megállapodás született az EU és az Egyesült Államok között a személyes adatáramlás új keretéről,[8] melynek eredményeként az Európai Unió Bizottsága 2016. július 12-én elfogadta az EU–USA Adatvédelmi Pajzsot.[9] A Safe Harbor helyére lépő megállapodás remélhetőleg megoldással szolgálhat az adatok biztonságával kapcsolatos aggályokra. Politikai nyilatkozatok terén szélesebb körű felügyeletet, bővebb ellenőrzési lehetőséget, hatékonyabb jogorvoslatokat ígérnek a szerződő felek.[10] Kérdéses azonban, hogy az adatkezelő szervezetek adatvédelmi követelményekre vonatkozó nyilvánosságra hozatali kötelessége, és az egyéb formális kötelezettség-vállalások mennyire jelentik a gyakorlatban is az adatvédelmi elvek megtartását.[11] Meg kell jegyeznünk, hogy egy ilyen rövid idő alatt kidolgozott „új" egyezmény kapcsán nehezen elképzelhető, hogy gyökeres változásokat hozhat az adattovábbítások, és főleg azok ellenőrzése gyakorlatába.[12] Ezért az EU–USA közötti „adatvédelmi pajzs" megállapodás, és az abból kibontakozó új rendszer tényleges érvényesülésig – sőt akár ezt követően is – kulcsszerepe lehet az Adatvédelmi irányelv EU-n kívüli adattovábbítást lehetővé tevő további jogalapjainak.

Az EU–USA közötti „adatvédelmi pajzs" megállapodás, és az abból kibontakozó új rendszer tényleges érvényesülésig – sőt akár ezt követően is – kulcsszerepe lehet az Adatvédelmi irányelv EU-n kívüli adattovábbítást lehetővé tevő további jogalapjainak.

A szerzők a Pécsi Tudományegyetem Állam- és Jogtudományi Karának joghallgatói.

A továbbiakban ezeket az alternatív megoldásokat – az adattovábbításoknak megfelelő jogi keretet nyújtó szerződéseket és egyéb, az érintett és az adatkezelő között létrejövő megállapodásokat – mutatjuk be, kiemelve az érintett hozzájárulásának problémakörét, melyet a Facebook hozzájáruláson alapuló adatkezelési gyakorlatának elemzésével szemléltetünk.

2. A HARMADIK ORSZÁGBA TÖRTÉNŐ ADATTOVÁBBÍTÁS AZ ADATVÉDELMI IRÁNYELVBEN

Az Adatvédelmi irányelv rögzíti, hogy a tagállami szabályozás csak olyan harmadik – az EGT tagállamain kívüli – országokba teheti lehetővé az adattovábbítási műveleteket, amelyek megfelelő védelmi szintet biztosítanak a személyes adatok kezelésére.[13] Az egyes országok adatvédelmi színvonalának megfelelőségét az Irányelvben meghatározott szempontok értékelése alapján az Európai Bizottság állapíthatja meg.[14] Ha egy ország adatkezelési szabályai nem összeegyeztethetőek az irányelvben lefektetett követelményekkel, az adattovábbítás csak az érintett egyértelmű hozzájárulásával, illetve egyéb szempontokhoz (szerződéshez, kiemelt közérdekhez, létfontosságú érdekhez) kapcsolódóan történhet,[15] ezek hiányában a Bizottság és a tagállamok kölcsönös kötelessége az adattovábbítás megakadályozása és a probléma megoldásához szükséges egyeztetések megkezdése.[16]

2.1. A biztonságos kikötő

A Safe Harbor keretrendszer létrehozásakor, 2000 júliusában az amerikai jogrendszer nem felelt meg azoknak az elvárásoknak, amelyeket az Adatvédelmi irányelv megkövetelt a biztonságos harmadik országoktól. Az érintett jogait középpontba helyező európai felfogás adatvédelmi szempontból szilárdabb, míg az amerikai megközelítés az üzleti szempontból rentábilisabb megoldásokat támogatta,[17] az üzleti környezet biztosítása a nyilvánosságra hozott dokumentumok[18] szerint prioritást élvezett az érintett kizárólagos döntési jogosultságának biztosítása felett. Ennek megfelelően törvényszerű volt az irányelv és a kereskedelmi érdekek összeütközése, ezért kulcsfontosságú volt egy olyan megállapodás létrehozása, amely a szükséges adatvédelmi garanciák érvényesülése mellett enged teret a transzatlanti kereskedelmi kapcsolatokhoz szükséges adattovábbításnak. A Safe Harbor ennek megfelelően a bizonytalanságok csökkentését és előreláthatóbb jogi és üzleti környezet biztosítását tűzte ki célként.[19]

A rendszer 7 alapelvből és 15 hivatalosan elismert „gyakran ismételt kérdésből" állt.[20] Az adatvédelmi elveket elismerő, önmagát tanúsító tengerentúli adatkezelő – az amerikai Kereskedelmi Minisztériumhoz történő egyszerűsített regisztráció után – jogosulttá vált a „biztonságos kikötő" használatára, tehát jogszerűen kezelhetett európai adatokat transzatlanti üzleti tevékenysége során.

Ez jelentette azt az alapvető problémát, amely végül a fent említett Schrems- ügyben csúcsosodott ki, és a Bizottsági határozat érvénytelenné nyilvánításához vezetett. A szervezetek önkéntesen léphettek a Safe Harbor-keretrendszerbe, és jelentősebb külső kontroll nélkül, saját belső szabályozóikkal kellett megfelelniük az adatvédelmi szabályoknak. Ugyan az USA Szövetségi Kereskedelmi Kamarája (Federal Trade Commission) gyakorolt

némi hatósági szerepkört a „tisztességtelen vagy megtévesztő cselekmények és üzleti gyakorlat" felmerülése esetén, ám az adatkezelő szervezetek rendszeresen megszegték a vállalt kötelezettségeiket. Gyakran a Safe Harbor elveket magukra kötelezőnek el nem ismerő adatfeldolgozókat vettek igénybe, vállalatcsoporton belül továbbították a dolgozók adatait, vagy európai személyes adatokhoz nyújtottak hozzáférést az amerikai titkosszolgálati szerveknek.[21] Pozitívumként említhetjük azonban, hogy láthatóvá tette a legnagyobb amerikai adatkezelőket, s némiképp ösztönözte őket a transzparenciára is az adatkezelési módszerek tekintetében.

2.2. Alternatív megoldások a transzatlanti adatáramlás biztosítására

Az EU álláspontja szerint[22] a biztonságos kikötő érvénytelenné nyilvánításától az adatvédelmi pajzs életbe lépéséig tartó átmeneti időszakban az általános adatvédelmi szerződési feltételek, illetve a kötelező erejű vállalati szabályok[23] jelenthetik a transzatlanti adattovábbítás kizárólagos jogi alapját, de azt követően is alkalmazhatóak maradnak. Fontos kiemelnünk azonban, hogy az alternatív megoldásokat még nem vizsgálta az EU Bírósága előzetes döntéshozatali eljárás keretében. Ebből kifolyólag jogi helyzetük, megítélésük, s ebből adódóan alkalmazásuk meglehetősen ingatag lehet, mely akadályozhatja széles körű elterjedésüket.[24] Természetesen ezen jogalapok alkalmazása esetén is lehetősége van a tagállami adatvédelmi hatóságoknak vizsgálni az adattovábbítások jogszerűségét, és a 29. cikk szerinti Adatvédelmi Munkacsoport[25] is folyamatosan vizsgálni köteles a követelmények érvényesülését.

Adatvédelmi szerződési feltételek

Az Adatvédelmi irányelv lehetőséget biztosít arra is, hogy a Bizottság olyan szerződési feltételeket fogadjon el (Modellszerződések, Standard Contractual Clauses, a továbbiakban: SCC) melyek az adattovábbítási műveleteket érintő szerződések kötelező tartalmát képezik, ha a megfelelő védelem ezzel is biztosítható.[26]

A szerződési feltételek legfontosabb szerepe az, hogy közvetítsék az Irányelv által meghatározott alapelveket a felek olyan szerződéses viszonyába, ahol az adott harmadik országbeli adatkezelő vagy feldolgozó az ország megfelelő adatvédelmi szintjének hiányában tevékenykedik, így az EU-ban tartózkodó érintett személy személyes adatainak védelmét csak ezek a kikötések tudják garantálni. Ennek megfelelően segítik egységesíteni az egyes szerződéseket, biztosítani azokat a garanciális szabályokat, amelyek minimálisan elvárhatóak adatvédelem szempontjából. Hátránya azonban, hogy bármilyen tökéletes szerződési feltétel a visszájára fordulhat, ha az nem a felek tájékozott hozzájárulásán alapul, például az érintett európai személy nem tudatosan hagyja jóvá, hanem csak egy regisztrációs folyamat vagy általános szerződési feltételek részeként, a szerződési feltétel valós tartalmának, hatásainak ismerete nélkül.

Az egyes szerződési feltételek meghatározásában kulcsszerepet játszik az Európai Bizottság, amely az irányelv felhatalmazása alapján[27] kijelölheti e feltételek körét, s jóváhagyhatja az egyes szerződési feltételeket.

A Bizottság két határozatában[28] állapította meg a szerződési feltételeket egyrészt az adatkezelők, másrészt az adatfeldolgozók vonatkozásában. Megismételte az irányelv legfőbb adatvédelmi elveit, így a célhoz kötöttséget, az arányosságot, az átláthatóságot, és többek között a továbbítás korlátozásának jogát. azért, hogy megelőzze, hogy a felek kiszerződjenek a megfelelő garanciákkal körülbástyázott védelem alól úgy, hogy arról az érintettnek nincs tudomása (pl. automatikus bejelölt jelölőnégyzet általi szerződéskötéssel).

A határozatot 2004 végén a joggyakorlat során felhalmozott tapasztalatok alapján felülvizsgálták.[29] A módosítások leginkább az adatkezelők és adatfeldolgozók felelősségét (egyetemes helyett saját felelősség vállalása), választási lehetőségeit érintette, csökkentve az SCC-k garanciális jellegét. 2010 végén a Bizottság az akkora már tömegesen felmerülő problémákra nem az eredeti határozat módosításával, hanem egy új határozat[30] elfogadásával válaszolt, s a korábbi enyhítés után szigorított a szabályozáson, de a fent említett problémákat nem tudta érdemben orvosolni.

Természetesen a szerződési feltételek alkalmazása csak akkor alapozhatja meg az adattovábbítás jogszerűségét, ha az tartalmilag is megfelelő garanciákat biztosít. Annak a felelőssége azonban továbbra is az adatkezelőt terheli, hogy az adattovábbítások ténylegesen meg is feleljenek az irányelv által lefektetett követelményeknek.

A kötelező erejű vállalati szabályok[31]

A legtöbb adattovábbítással kapcsolatos kihívás mögött az áll, hogy ugyan az adatok elsődleges kezelője európai központtal rendelkezik, de adatok további kezelését, feldolgozását már nem ez a szervezet (leányvállalat), hanem az elsődleges adatkezelő cégcsoportján belül egy másik, harmadik országban működő szervezet végzi.

Az adatok biztonságát ilyen esetben leginkább egy olyan belső, kötelező erejű vállalati szabályozás biztosíthatja, amely a cégcsoporton belüli adatkezelők- és feldolgozók részéről kerül elfogadásra és ellenőrzésre egyoldalú jognyilatkozattal. Az adatvédelmi szabályzat ez esetben hasonló szerepet tölt be, mint a szerződési feltételek, az Adatvédelmi irányelv követelményeinek érvényesülését szolgálja szervezeti belső szabályozóként. A szabályzat létrehozásában nagy szerepe van a tagállami hatóságoknak, akik engedélyező, a BCR jóváhagyásában döntő szereplőként lépnek be a folyamatba.

Egyértelműen látszik, hogy az EU szervei, s különösen a 29. cikk szerinti adatvédelmi munkacsoport igyekszik a vállalatcsoportok BCR-kezdeményezéseit ösztönözni.[32] A BCR előnyének lehet tekinteni, hogy azt a szervezet saját magának dolgozza ki, s ezért erősebben kötődik hozzá, törekszik teljesítésére. Hátránya is ugyanitt keresendő – a saját szervezeti szabályok megkönnyítik a kiskapuk beépítését, a szabályok be nem tartását, ezért kiemelten fontos szerepe van az engedélyező és ellenőrző hatóságoknak abban, hogy ezeket megelőzzék.

Derogációs rendszer

Az átmeneti helyzetre kiadott bizottsági iránymutatás harmadik helyen a derogációs rendszert nevesíti, mely tulajdonképpen az Irányelv 26. cikke (1) bekezdésében felsorolt olyan kivételeket jelenti, amelyek esetén abban az esetben is megengedhető az adattovábbítás, ha a harmadik ország adatvédelmi szintje nem éri el az elvárásokat, s ezért a Bizottság ezt nem tudta megállapítani (ahogy az Egyesült Államok esetében sem).

Legfontosabb derogációs esetként jelölhetjük meg az érintett hozzájárulását, melyet a tanulmány további részében bővebben elemzünk. A további okok jellemzően valamely nyomós és egyben jogos magán-, illetve közérdekhez kapcsolódnak, így az érintett vagy más személy érdekét szolgáló szerződés megkötéséhez, teljesítéséhez, jogi érdek vagy közérdek érvényesítéséhez, létfontosságú érdek vagy a szükséges és arányos nyilvánosság biztosításához szükséges.

3. AZ ÉRINTETT HOZZÁJÁRULÁSÁN ALAPULÓ ADATTOVÁBBÍTÁS

3.1. A hozzájárulás korlátai és korlátlansága

Az érintetti hozzájárulás, mint jogalap az adatvédelmi szabályozási modellek második generációjában vált általánosan elterjedtté, amikor az Adatvédelmi irányelv nevesítette azt.[33] Ekkor-

tól beszélhetünk ugyanis az információs társadalom kialakulásáról, ahol fontosabbá vált az adatok védelme, ugyanakkor szabad áramlásuk elősegítése is. Fontos kiemelni, hogy a hozzájáruláson alapuló adatkezelések száma, jelentősége a tagállamok között is jelentős eltéréseket mutat. Az információs önrendelkezési jogon alapuló szabályozással bíró országokban az érintetti kontroll szerepe lényegesen nagyobb, ilyen többek között Németország és 2012-ig hazánk is ennek tekinthető. Viszonyításképpen más országokban az érintetti kontroll szerepe csekélyebb, csak egy, a többivel azonos súlyú jogalapnak minősül, mint például az Egyesült Királyságban.[34]

Az utóbbi években egyre több kritika érte a hozzájárulást és az érintetti kontrollt, mint egyes szerzők szerint mára jelenlegi formájában meghaladott intézményt. Solove a Harvard Law Review-ban megjelent cikkében rámutat arra, hogy a Big Data, a Web 2.0 és a különböző biztonsági intézkedések megsértése felveti a hozzájárulás – mint az 1970-es évek óta változatlan adatkezelési jogalap – túlhaladott.[35] Mindezeket a szerző a hozzájáruló személyében és az adatgyűjtés rendszerében meglévő problémákkal indokolja. Solove munkájában a „privacy self-management" kifejezést használja, amely lényegében a tájékoztatás, hozzáférés, és hozzájárulás, vagyis a notice&choice[36] megvalósulási formája. Ezek a kifejezések arra utalnak, hogy magánszféránk menedzselésekor nagyon fontos, hogy értesítsék (notice) azt a személyt, akiről adatot gyűjtenek, vagy felhasználnak, illetve, hogy lehetősége legyen eldönteni (choice) azt, hogy kívánja-e ilyen adatok gyűjtését és felhasználását. Solove elmélete szerint az érintetti hozzájárulással jogszerűvé tehető minden adatkezelés, továbbá az adat felhasználását ezt követően nem ítélhetjük meg erkölcsileg jónak vagy rossznak. A hozzájárulás problematikája azonban szerinte két pilléren nyugszik, az egyik a kognitív, a másik a strukturális problémák.[37] Kognitív problémák alatt azt érti, hogy az érintettek általában nem olvassák el az adatkezelési szabályzatokat, amennyiben ezt mégis megtennék nem értik azokat. Ha értenék, akkor sem rendelkeznének megfelelő háttértudással ahhoz, hogy adekvát döntést hozzanak, ha mégis akkor is szembesülnek bizonyos döntéshozatali nehézségekkel. Ez utóbbiak közé tartozik az ún. kötött racionalitás vagy *bounded rationality*, amikor az emberek képtelenek meglévő tudásukat az adott szituációra alkalmazni, a téma komplexitásából adódóan. Azonban még amikor jó döntéseket is hoznak a felhasználók, az sem mindig konzekvens.[38]

Solove elmélete szerint az érintetti hozzájárulással jogszerűvé tehető minden adatkezelés, továbbá az adat felhasználását ezt követően nem ítélhetjük meg erkölcsileg jónak vagy rossznak. A hozzájárulás problematikája azonban szerinte két pilléren nyugszik, az egyik a kognitív, a másik a strukturális problémák.

A strukturális problémákat három részre osztja. Az első problémakör az, hogy a személyes adatok túl széles skálájáról beszélünk egy-egy adatkezelés során, és az érintett nem képes megfelelő kontrollt gyakorolni adatai felett. Másodikként említi meg az „egyesülés" problémáját, magyarán azt, hogy az egyesével megadott apróbb adatok a Big Data-nak köszönhetően összegyűlnek és ezek elemzése az érintettre nézve szenzitív információkat is tartalmazhatnak. Harmadikként kell megemlékeznünk az ún. „bemeneti kárról" amely azt írja le, hogy az érintettek gyakran „vállalják" az adataik jogosulatlan kiadásával később bekövetkező kár kockázatát a gyors és azonnali előnyök elérése érdekében.[39]

Solove írásában a problémák megoldására nem azt javasolja, hogy hagyjuk el teljesen a hozzájárulás koncepcióját egy paternalista adatkezelés felé, hanem azt, hogy a jogalkotó egy a valóságban is érvényesülő rendszert dolgozzon ki, amely figyelemmel van a hozzájárulás fent lefektetett problémáira. A paternalista adatkezelés és adatvédelem értelmében az állam igyekszik „megvédeni" az érintettet saját akaratától függetlenül, illetve annak ellenében is. A magunk részéről úgy gondoljuk, hogy a Solove által vázolt megoldás nem feltétlenül megvalósítható, tekintettel arra, hogy a jelenlegi jogalkotási folyamatok mellett és a fentebb írt kognitív problémákra figyelemmel gyakorlatilag nem lehetséges olyan szabályozás, amely minden tekintetben az érintett akaratával egyező adatkezeléshez vezetne.[40] Célunk legfeljebb annyi lehet, hogy a lehető legtisztább módon követeljük meg a hozzájárulást az érintettektől.

Más szakirodalmi álláspontok sokkal paternalistább álláspontra helyezkednek. Ők úgy vélik, hogy a demokratikus társadalom alapvető kelléke a magánélet, illetve az adatok biztonsága, ezért a jognak néhány esetben felül kell írnia a hozzájárulást, amikor az túlzott veszélyekkel járna az egyénre és a társadalomra nézve.[41] Ez a gyakorlatban olyan különösen szenzitív adatokra vonatkozhat, amelyek, ha nyilvánosságra kerülnek olyan mértékű hatást gyakorolhatnak egy személy életére, amely elemi jelentőséggel rendelkezik. Néhány szerző egyenesen odáig merészkedik a paternalizmus útján, hogy az információs önrendelkezéshez való jogról, vagy annak amerikai megfelelőjéről (right to information privacy) nem lehet lemondani.[42]

Álláspontunk szerint azonban, támaszkodva Solove, Richards és Mazzone munkásságára,[43] erről a jogról teljes bizonyossággal le lehet mondani. Párhuzam vonható ugyanis a szólásszabadság és az információs önrendelkezési jog között. Mindkettő elidegeníthető szerződéses kötelezettségvállalás útján, hiszen a szerződés teljesítéséhez fűződő érdek adott esetben lényegesen nagyobb, mint az egyébként a hallgatáshoz, vagy esetünkben adatainak kezeléséhez hozzájáruló fél szólásszabadsága, vagy információs önrendelkezéshez való joga. Ez a megállapítás a gyakorlatra olyan hatással lehet, hogyha a fél teljes mértékben tudatában van annak, hogy mihez járul hozzá, nem hivatkozhat információs önrendelkezési jogára az adatkezeléssel szemben.[44]

Meg kell emlékeznünk még az USA és az EU közötti különbségekre is a hozzájárulás kapcsán. Az Egyesült Államokban az adatkezelés mindaddig legális, ameddig a jog azt meg nem tiltja, vagyis amíg problémát nem okoz. Az Európai Unió egy paternalisztikusabb álláspontot vesz fel, ami sokkal szűkebb körben engedélyezi az adatgyűjtést, szigorú szabályok alapján. Példának okáért a félreérthetetlen, egyértelmű és kifejezett jelzők használatát említhetjük a hozzájárulás előtt.[45]

A magyar szakirodalom képviselői is eltérő álláspontot képviselnek a hozzájárulás kérdésében. Jóri kritikusan szemléli a hazai érintett-központú adatvédelmi rendszert, és felhívja a figyelmet arra, hogy a hozzájárulás kiszolgáltatottá teszi az érintetteket az adatkezelőknek, akik nem csupán potenciálisan több információval rendelkeznek az adatot szolgáltatónál, de gazdasági túlsúlyban is vannak.[46] Fellelhető azonban olyan magyar szerző is, aki az információs önrendelkezési jog és így az érintetti kontroll mellett tör lándzsát, ilyen Szabó, aki az általános önrendelkezési jog egyik szeletének tekinti az információs önrendelkezési jogot.[47]

3.2. Fogalmi tisztázások az adattovábbításhoz való hozzájárulás kapcsán

A rendszeres és szokásos félrefordításoknak köszönhetően az uniós jog és a nemzeti jog között gyakran igen kusza fogalmi hálózat alakul ki, ezért a problémafelvetésben feltett kérdés megválaszolásának okán célszerű kibogozni e hálót. Alapfeltevésként abból kell kiindulnunk, hogy az adattovábbítás, mint az adaton végzett művelet, adatkezelésnek minősül, így vonatkoznak rá az adatvédelemmel kapcsolatos kötelező erejű jogi dokumentumok általános részei is.[48]

Ennek megfelelően a 95/46/EK irányelv 7. cikke megkívánja az érintett *egyértelmű hozzájárulását* az adatkezeléshez.[49]

Legelőször tehát célszerű áttekinteni a hozzájárulás fogalmát, amelynek értelmezésében a szakirodalomra támaszkodunk.

Az „érintett hozzájárulása" a már idézett irányelv fogalom-meghatározása szerint az érintett kívánságának önkéntes, kifejezett és tájékozott kinyilvánítása, amellyel beleegyezését adja az őt érintő személyes adatok feldolgozásához.[50] A hozzájárulásnak tehát önkéntesnek, kifejezettnek, valamint tájékozottnak kell lennie, és nem utolsósorban csak és kizárólag saját magát érintő személyes adatok feldolgozására irányulhat, hiszen az információs önrendelkezési jog értelmében csak a saját személyes adataikról rendelkezhetnek a természetes személyek.

Önkéntesség alatt saját döntés következtében végzett cselekvést értünk, amelyet a személy szabad elhatározásából tesz és általában rövid ideig tart. Az önkéntes cselekedet fogalmát a büntetőjog is körbehatárolja, amely arra fókuszál, hogy a cselekedetnek szabad elhatározásból született tudatos cselekedetnek kell lennie.[51]

Kifejezett alatt egyértelműen, világosan és határozottan megnyilvánuló információt értünk. Jogilag szintén olyan aktust kell ez alatt érteni, amely tisztán kifejezi az információ átadójának akaratát, amely tévésben manifesztálódik.[52]

A „tájékozott" olyan személyt jelent, akinek kellő ismeretei, értesülései vannak valamiben.[53]

Ennek alapján az adatkezeléshez és így az adattovábbításhoz saját döntéseként, szabad elhatározásból végzett, egyértelműen, világosan és határozottan megnyilvánuló hozzájárulást kell érteni egy olyan személy által, aki kellő ismeretekkel rendelkezik arra nézve, hogy milyen formában történik az adatkezelés.

A magyar jogalkotás teljes mértékben átvette az irányelv szövegét, azonban olykor más terminusokat, illetve magasabb védelmi szintet alkalmaz.[54] Ennek megfelelően a magyar szakirodalom a hozzájárulás kapcsán is hasonló megállapításokat tesz, mint külföldi társai. Így lefekteti, hogy a személyes adatok kapcsán a hozzájárulást csak az érintett, vagy annak törvényes képviselője adhat írásban vagy ráutaló magatartással. Ezen túl három konjunktív elemet különböztet meg, amelyek közül akár egy is hiányzik, nem beszélhetünk jogszerű hozzájárulásról. E feltételek az önkéntesség, a határozottság és a tájékozottság.[55]

Önkéntesség kapcsán foglalkozik a magyar irodalom a hátrány kilátásba helyezésével. Egyértelműen jogszerűtlen a hozzájárulás, ha annak megtételére úgy vették rá az érintettet, hogy valamely hátrányt helyeztek kilátásba a hozzájárulás megtagadásának esetére. Azonban ha valamilyen előnyt helyez kilátásba az adatkezelő – főként marketing tevékenységként – a hozzájárulást általában jogszerűnek tekinti a jogalkalmazás.

Határozott (egyértelmű) alatt azt értjük, hogy az adott nyilatkozatból félreérthetetlenül következnie kell az adatkezelésre megadott hozzájárulásnak.

Végül a tájékozottságon mindig előzetes tájékoztatást kell érteni, az adatkezelés minden momentumára kiterjedően, illetve kellően specifikusnak kell lennie az adott személyre. A magyar jog továbbá írásbeli formát csak a különleges vagy szenzitív adatok kapcsán kíván meg.[56]

Az Adatvédelmi irányelv az adattovábbítással kapcsolatos hozzájárulásra[57] egy olyan terminust használ annak minőségi leírásához, amely a magyar szakirodalom alapján a generális adatkezeléshez tartozik. Az angol szöveg az „unambigous" szót használja, amelynek jelentése félreérthetetlen, egyértelmű. Megállapítható tehát, hogy a magyar jog ebben a kérdésben az alapvető adatkezeléshez való hozzájárulás kapcsán egy magasabb védelmi szintet alkalmaz az irányelvénél.

Fontos megjegyezni, hogy mivel a magyar jogalkalmazás szerint ráutaló magatartással egyértelműnek (határozottnak) tekintett a hozzájárulás a generális adatkezeléshez, ezért úgy véljük, hogy az EGT-n kívüli adattovábbításhoz való hozzájárulás uniós jog szerint szintén megvalósulhat a hozzájárulás ilyen formájával. Ezt az állításunkat arra alapozzuk, hogy az Irányelv szintén az „egyértelmű" szóval jelöli a hozzájárulás minőségét a külföldi adattovábbítások kapcsán.

Nincs ez így azonban a magyar jog szerint, ahol *kifejezett* hozzájárulásról beszélhetünk, ami a fenti meghatározás alapján világos, határozott és egyértelműen tevőleges magatartás, amelyet szerintünk egy regisztráció, vagy puszta tovább görgetés semmiképp sem valósíthat meg. Ezalatt mindenképpen külön, tevőleges hozzájárulást értünk. Természetesen léteznek olyan nézetek is, amelyek a regisztrációs gombra való kattintást tevőleges magatartásnak fogadják el, amelynek során elfogadásra kerülnek a felhasználási és adatvédelmi szabályzatok, feltételek is. Ennek ellenére a szerzők a hagyományos felfogást támogatják, tekintettel arra, hogy egyrészt nincsen lehetőség a szabályzatok külön-külön elfogadására, másrészt a „regisztráció" gombra való kattintással véleményünk szerint nem kifejezetten ezekhez való hozzájárulását adja meg az érintett, hanem a szolgáltatás igénybevételére vállalkozik. Más lenne a helyzet, ha nem előre pipált boxotkat használna a Facebook, erről részletesen lásd a következő fejezetben.

3.3. A Facebook adattovábbítási gyakorlata és Schrems beadványai a hozzájárulás kapcsán

Max Schrems osztrák állampolgár – vagy, ahogy a sajtóban gyakran hivatkoznak rá, „privacy campaigner" – beadványa egészen az Európai Unió Bíróságáig jutott, amikor azt kifogásolta, hogy a Facebook Ireland Ltd uniós állampolgárok személyes adatait oszthatja meg az amerikai titkosszolgálatokkal – ahogy arra korábban Edward Snowden is több, bizonyítékokkal alátámasztott nyilatkozatában is rámutatott.[58]

A Bíróság korábban hivatkozott döntésében ugyan érvénytelenné nyilvánította a Safe Harbor megállapodást,[59] Schrems azonban nem elégedett meg ennyivel, és sikerén felbuzdulva három különálló panaszt nyújtott be a német, belga és ír adatvédelmi hatóságokhoz, amelyekben kérelmezte, hogy a Facebook állítása le az EU és USA közti adattovábbítását, mivel véleménye szerint az amerikai titkosszolgálatok továbbra is, az alternatív jogalapok szerinti adattovábbítás során is rálátással bírnak európai személyes adatokra. Kiemelendő, hogy Schrems azért ezekhez a hatóságokhoz nyújtott be panaszt, mert a nevezett államok (kiterjesztve ezt az összes német nyelvű facebookot képviselő GmbH-ra) az Facebook Ireland Ltd-n keresztül szintén a Safe Harbor alapján továbbították európai állampolgárok személyes adatait az USA-ba.[60]

Schrems mindhárom új kérelmében azt állítja, hogy a Facebook nem kér félreérthetetlen és kifejezett hozzájárulást ahhoz, hogy a Facebook Ireland Ltd (írországi székhely) átküldhesse az adatokat a Facebook Inc-nek, az adatok EGT-n kívüli harmadik országba (USA) történő továbbításához. Továbbá azt is kifogásolja, hogy a Facebook nem garantálja az uniós polgárok adatainak biztonságát az USA tömeges megfigyelési gyakorlatával szemben.

Schrems mindhárom új kérelmében azt állítja, hogy a Facebook nem kér félreérthetetlen és kifejezett hozzájárulást ahhoz, hogy a Facebook Ireland Ltd (írországi székhely) átküldhesse az adatokat a Facebook Inc-nek, az adatok EGT-n kívüli harmadik országba (USA) történő továbbításához. Továbbá azt is kifogásolja, hogy a Facebook nem garantálja az uniós polgárok adatainak biztonságát az USA tömeges megfigyelési gyakorlatával szemben („mass surveillance").[61] Az illetékes ír bíróság az ügyben 2016 júliusában az EU Bíróságához fordult előzetes döntéshozatali eljárás keretében.[62]

Fontos tehát megvizsgálnunk, hogy mit is jelent pontosan az ún. „explicit"[63] vagy „unambigous consent"[64], vagyis a *kifejezett és félreérthetetlen hozzájárulás*. Ezeket milyen *módon* és *mire* ad-

hatják meg a felhasználók, illetve egyik legfontosabb kérdésként arra is válasszal szolgálunk, hogy igaza van-e a magánélet kortesének, Max Schremsnek, tehát előreláthatóan milyen döntést hoz majd a Bíróság a kérdéses három ügy kapcsán.[65]

A beadványok igazolásához először is meg kell vizsgálnunk, hogy egy Facebook regisztráció során a felhasználó milyen feltételekkel regisztrál, illetve mibe egyezik bele, valamint milyen formában teszi ezt meg.

Első lépésként vegyük szemügyre a Facebook regisztrációs felületét. A regisztráció rendkívül egyszerű, illetve ingyenesen elérhető a Facebook kezdőoldaláról. A közösségi háló egy vezeték-, illetve keresztnév, e-mail, jelszó, születési idő és nem megadásával már el is érhető. A Regisztrációs gomb felett a következő tájékoztató olvasható: „*A Regisztráció gombra való kattintással elfogadod a Feltételeinket, és tudomásul veszed az Adatkezelési Szabályzatban foglaltakat, beleértve a cookie-k használatáról szóló tájékoztatót.*"

Egyértelmű tehát, hogy Facebook ráutaló magatartással hozzájárulást kér ahhoz, hogy az Adatkezelési Szabályzata alapján kezelje az érintett regisztráló adatait. Fenntartva azt a nézetünket, hogy a regisztrációs gombra való kattintás nem kifejezett hozzájárulás.

A Facebook Adatkezelési Szabályzatát olvasva a következő ellentmondásokra hívnánk fel a figyelmet. „*A Facebook részét képező vállalatcsaládon belül megosztjuk azokat az információkat, amelyekkel rólad rendelkezünk.*" E mondatból úgy tűnhet, hogy a Facebook BCR-eket használ, azonban nem szerepel a Bizottság által vezetett, BCR-eket alkalmazó vállalatok listájában.[66] Ugyan e fogalmi elhatárolódás nem okozhat olyan problémát, mint az alábbi esetek, azonban jól jelzi azokat a fogalmi zavarokat amelyeket a transzatlanti adatáramlás ébreszt.

Kevésbé megmagyarázható az Adatkezelési Szabályzat olyan jellegű tévedése, hogy még mindig az érvénytelen Safe Harbor megállapodásra alapítja az adatok továbbítását.[67] A szabályzat nem csupán egy érvénytelen megállapodást használ jogalapként az adatok továbbítására az EGT-n kívüli államokba, hanem megfelelő hozzájárulással sem rendelkezik az adatok transzatlanti áramlására, sem az újonnan regisztrálók, sem a korábban regisztráltak esetében. Természetesen itt is lehetnek olyan érvek, hogy a korábbi Safe Harbor keretrendszerre hivatkozik a szabályzat, ami az előzetes tájékoztatás szerepét töltheti be a hozzájárulás alapján történő adatkezeléshez, azonban ezt az EU nem ismeri el. A Facebook ugyanis ráutaló magatartással fogadtatja el a már korántsem hatályos Adatvédelmi szabályzatát, ami semmiképp sem felelhet meg a magyar adatvédelmi jog harmadik országba való adattovábbításnál előírt szabályainak, ami kifejezett hozzájárulásról rendelkezik. Megengedhetőnek tűnik azonban a továbbítás az Adatvédelmi irányelv vonatkozó rendelkezései szerint, ahol is az egyértelmű hozzájárulás megadása elegendő.

Álláspontunk az, hogy nem elegendő csupán egy hozzájárulás az adatkezelés teljes folyamatára nézve, hanem külön-külön hozzájárulást kellene kérni a generális adatkezelés, tehát az Adatvédelmi Szabályzatban lefektetett többi funkció ellátására és a külföldi adattovábbításra egyaránt, tekintettel az eltérő védelmi szintekre.

Kifejezett lenne a hozzájárulás, ha azt az érintett nem előre pipált boxok segítségével adhatná azt meg, ahogy az a 29. cikk szerinti Munkacsoport vonatkozó állásfoglalásában is szerepel.[68] E dokumentum alapján azonban az irányelvben szereplő félreérthetetlen, egyértelmű és sajátos hozzájárulás sem adható meg ráutaló magatartással, azonban kötelező ereje nem lévén e vélemény nem köti sem az uniós szerveket, sem a nemzeti hatóságokat, bíróságokat. Ebből kifolyólag lehetséges az, hogy a hatályos magyar törvény szerint az egyértelmű hozzájárulás a gyakorlatban ráutaló magatartással is megvalósítható.

Mindezeken túlmenően azonban álláspontunk az, hogy nem elegendő csupán egy hozzájárulás az adatkezelés teljes folyamatára nézve, hanem külön-külön hozzájárulást kellene kérni a generális adatkezelés, tehát az Adatvédelmi Szabályzatban lefektetett többi funkció ellátására és a külföldi adattovábbításra egyaránt, tekintettel az eltérő védelmi szintekre. Megjegyezzük, hogy az Infotv. szerint a generális adatkezeléshez ráutaló magatartás is elegendő, azonban semmiképp nem lehet elégséges az ilyesfajta hozzájárulás a különleges adatok kezelésére és a külföldi adattovábbításra nézve. Megjegyzendő, hogy az Infotv. nem írja elő kötelezően, hogy az adatkezelésekhez funkciónként külön hozzájárulásra van szükség, azonban a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlatából ez kitűnik, amely véleményünk szerint irányadó lehet a jövőre nézve.

A közösségi hálón megosztott különleges adatok kapcsán szintén külön hozzájárulás szükséges minden egyes adatkezelési cél kapcsán, itt is figyelemmel az eltérő védelmi szintre. Nem lehet ugyanis vélelmezni, hogy az oldalon megadott különleges adatra nézve fennáll az adatkezelésre vonatkozó hozzájárulás. Amennyiben azonban hozzájárulással rendelkezik a szolgáltató, akkor sem beszélhetünk generális beleegyezésről az összes különleges adatra vonatkozóan, hiszen mindez szembe menne a különleges adatok fokozott védelmét biztosító szabályokkal. A magunk részéről úgy véljük, hogy a gyakorlatban ez oly módon valósulhatna meg, hogy különleges adat csoportonként (pl. vallással, politikai véleménnyel, egészségi állapottal kapcsolatos adatok) előzetesen kellene kérni az érintett hozzájárulását az adatkezelési célokra. A Facebooknál ez különösen igaz lehet, hiszen a profilban megadható a politikai vélemény, pártállás, vallásos vagy más világnézeti meggyőződésre utaló adat, sőt még a szexuális életre vonatkozó (preferenciák) adatok is.

A fentiekre tekintettel álláspontunk szerint Schrems beadványai az irányelv alapján nem feltétlenül[69] járhatnak sikerrel csupán a hozzájárulás minőségével kapcsolatban, azonban figyelemmel arra, hogy jelen esetben mindenképp nemzeti jogokat is vizsgálnak majd a bíróságok, ezek ismerete elengedhetetlen a kimerítő válaszadás tekintetében. Míg a német és ír adatvédelmi törvény nem határozza meg az adattovábbításhoz szükséges hozzájárulás minőségét, addig a belga jogszabály az Irányelv teljes átvételére törekszik, és az egyértelmű jelzőt használja a külföldi adattovábbításokkal kapcsolatban.[70] Megjegyezzük továbbá azt is, hogy ha az adott eset a magyar Infotv. hatálya alatt történt volna, a nemzeti jog alapján elérhető lenne Schrems célja, vagyis a közösségi oldal EU–USA közötti adatforgalom megtiltása.

Jelentősen új jogi környezetet hoz 2018 májusában az EU Általános Adatvédelmi Rendelete, amely közvetlenül alkalmazandó lesz valamennyi tagállamban, megszüntetve a nemzeti jogok közötti eltérést. A Rendelet az EGT-n kívüli adattovábbítást a Bizottság megfelelőségi határozata, illetve a megfelelő garanciák hiányában – beleértve a kötelező erejű vállalati szabályokat is – az érintett hozzájárulása alapján csak akkor tekinti jogszerűnek, ha az érintett azt követően adta meg kifejezetten hozzájárulását a tervezett továbbításhoz, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról.[71]

A jogszabályhely tehát nem csupán *kifejezett hozzájárulást* ír elő a harmadik országba való adattovábbítás esetére, hanem olyan tájékoztatást is, amely nem kizárólag az adatkezelés módjára szól, hanem felhívja a figyelmet azokra a kockázatokra, amely az adattovábbítással járhatnak.

Amennyiben tehát az új, csak 2018-tól alkalmazandó adatvédelmi előírásokra tekintettel hozza meg döntését a Bíróság Schrems ügyében, lehetséges, hogy a hatályos jogszabályok értelmezése során is kiáll majd a kifejezett és tevőleges hozzájárulás mellett.

V. KONKLÚZIÓ

A Safe Harbor megállapodás érvénytelenné nyilvánítása kétségkívül napjaink egyik legnagyobb adatvédelmi vitáját kiváltó döntése, amely rendkívül sokféle jogalkalmazási nehézséget teremt a transzatlanti gazdasági kapcsolatokban.

Értékelve a fentieket általánosságban elmondhatjuk, hogy korunk embere gyakran hajlamos megfeledkezni személyiségi jogairól, információs önrendelkezési jogáról, amit egyes szervezetek, gazdasági társaságok kellő ügyességgel ki is használnak. Nem feledkezhetünk meg azonban – az ugyan kisebbségben lévő – olyan emberekről, akiknek igenis fontos, hogy milyen adatokat, és kik kezelnek róluk, illetve milyen információk jutnak esetlegesen olyan kormányok kezébe, amelyeknek az adott személy nem is állampolgára.

Fontosnak tartjuk az uniós állampolgárok számára is könnyen elérhető jogorvoslati lehetőségek létrehozását, a valóságban is érvényesülő garanciák mellett adataik védelme és zártan kezelése érdekében. A jogorvoslati rendszer központjának Európában kellene maradni, s felülemelkedve a nemzeti az adatvédelmi hatóságok tagállamonként eltérő, erőtlen jogosítványain, hatékony, adott esetben az adattovábbítás átmeneti felfüggesztésére is kiterjedő jogokkal lenne szükséges felruházni, melyek így megfelelő garanciát jelentenének a jogosulatlan, európai szabályokon túllépő gyakorlattal szemben.

Ezenfelül szükséges az amerikai kormányzat részéről egy szemléletváltás, amely elengedhetetlen az új „adatvédelmi pajzs" sikeres működéséhez. Ez alapján nagyobb figyelmet kell fordítani az adatvédelmi alapelvek tényleges átültetésére, s határt szabni a tömeges megfigyeléseknek. Mindez rendkívül kockázatos vállalkozásnak tűnhet a folyamatos nemzetbiztonsági kockázatokra tekintettel, de nem hagyható el, mert az egyének önrendelkezésének biztosítása nélkül nem tudnak működni azok a demokratikus, jogállami folyamatok, amelyeket pont az említett nemzetbiztonsági kockázatok ellen védenek.[72]

Javaslatunk a kialakult helyzetre nézve, – utalva ehelyütt a Bíróság sokszor kifejezetten nem pusztán jogalkalmazó, hanem jogfejlesztő tevékenységére – Schrems beadványai kapcsán az, hogy az EUB ne a kialakult jogalkalmazási gyakorlatot kövesse a hozzájárulási forma tekintetében, hanem az új rendelet szellemében, mintegy azt megalapozva hozzon határozatot. Egy ilyen jellegű döntés lándzsát törne az információs önrendelkezési jog, illetve az adatok fokozottabb védelme mellett az Európai Unióban.

Jegyzetek

1 Elina Villup, Aydan Bahadir: Transatlantic relations: USA and Canada. 2016. november (http://www.europarl.europa.eu/ftu/pdf/en/FTU_6.6.1.pdf 2016.11.15.)

2 Joshua P. Meltzer: Examining the EU safe harbor decision and impacts for transatlantic data flows. 2015. november 3. (https://www.brookings.edu/testimonies/examining-the-eu-safe-harbor-decision-and-impacts-for-transatlantic-data-flows/ 2016.06.12.)

3 Európai Bizottság: A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK a 95/46/EK irányelv alapján, az Európai Bíróság C-362/14. sz. (Schrems-) ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról. Brüsszel, 2015. november 6. COM(2015) 566 final. 2. o.

4 Bizottság 2000. július 26-i 2000/520/EK határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő" adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről, HL L 215., 2000.8.25., 7. o.

5 Martin A. Weiss, Kristin Archick: U.S.– EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service, 7-5700, 2016. 8–9. o. (https://www.fas.org/sgp/crs/misc/R44257.pdf 2016.06.13.)

6 A Bíróság ebben az esetben előzetes döntéshozatali eljárás keretében egy szekunder uniós jogi aktus érvénytelenségét mondta ki, amelyet ennélfogva az alapügyen eljáró tagállami bíróság nem vehet figyelembe az ügy eldöntése során. Az érvénytelenségi döntés – noha nem azonos a semmissé nyilvánítással – más tagállami bíróságok számára is irányadónak tekinthető, amint azt a Bíróság a 66/80. sz. International Chemical Corporation ügyben kimondta. Lásd: Mohay Ágoston: Az előzetes döntéshozatali eljárás. In: Mohay Ágoston – Szalayné Sándor Erzsébet (szerk.): Az Európai Unió joga (Harmadik, átdolgozott kiadás), Dialóg Campus, 2015, 172. o.

7 Az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK irányelve (a továbbiakban: Adatvédelmi irányelv).

8 Az EU–USA adatvédelmi pajzs létrehozásával megállapodás született az Európai Bizottság és az Egyesült Államok között a transzatlanti adatáramlás új keretéről. Strasbourg, 2016. február 2. (http://europa.eu/rapid/press-release_IP-16-216_hu.htm 2016.07.12.)

9 A BIZOTTSÁG VÉGREHAJTÁSI HATÁROZATA (2016.7.12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről. Brüsszel, 2016.07.12. C(2016) 4176 final.

10 Az Európai Bizottság elindítja az EU–USA adatvédelmi pajzsot, amely erőteljesebb védelmet biztosít a transzatlanti adatáramlásoknak. Brüsszel, 2016. július 12. (http://europa.eu/rapid/press-release_IP-16-2461_hu.htm 2016.07.15.)

11 Domokos Márton, Polefkó Patrik: Egy bírósági döntés következményei – avagy az Európai Bíróság ún. Schrems döntésének hatásai, a Safe Harbor sorsa és a felmerülő kérdések az adatvédelem területén. *Infokommunikáció és Jog,* 2016/64. 123–126. o.

12 Natasha Lomas: Europe And US Seal „Privacy Shield" Data Transfer Deal To Replace Safe Harbor. 2016.02.02. (http://techcrunch.com/2016/02/02/europe-and-us-seal-privacy-shield-data-transfer-deal-to-replace-safe-harbor 2016.06.12.)

13 Adatvédelmi irányelv 25. cikk (1) bek.

14 Adatvédelmi irányelv 25. cikk (6) bek.

15 Adatvédelmi irányelv 26. cikk (1) bek.

16 Adatvédelmi irányelv 25. cikk (4)–(5) bek.

17 Schwartz, Paul M.: The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harward Law Review.* Vol. 126., 2013, 1985. o.

18 U.S.-EU Safe Harbor Framework Documents https://build.export.gov/main/safeharbor/eu/eg_main_018493 (2016.01.28.)

19 Robert S. LaRussa: Privacy and FAQ Letter. 2000. július 17. (https://build.export.gov/main/safeharbor/eu/eg_main_018486 2016.07.28.)

20 U.S. DEPARTMENT OF COMMERCE: Safe Harbor Privacy Principles. 2000. július 21. (https://build.export.gov/main/safeharbor/eu/eg_main_018475 2016.07.28.)

21 NSA paying U.S. companies for access to communications networks. https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html (2016.06.13.)

22 Európai Bizottság: A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK a 95/46/EK irányelv alapján, az Európai Bíróság C-362/14. sz. (Schrems-) ügyben hozott ítéletét követően a személyes adatoknak az Európai Unióból az Amerikai Egyesült Államokba történő továbbításáról. Brüsszel, 2015. november 6. COM(2015) 566 final 4. o.

23 Binding Corporate Rules, a továbbiakban: BCR

24 Peers, Steve: Live. Die. Repeat. The 'Privacy Shield' deal as 'Groundhog Day': endlessly making the same mistakes? http://eulawanalysis.blogspot.hu/2016/02/live-die-repeat-privacy-shield-deal-as.html (2016.02.02.)

25 Az Adatvédelmi irányelv 29. cikke alapján létrehozott munkacsoport a tagállamok nemzeti adatvédelmi felügyelő hatóságainak vezetőiből, az EU adatvédelemért felelős szerveinek képviselőiből és a Bizottság egy képviselőjéből áll, szerepe konzultatív, tehát ajánlásokat és véleményeket ad közre, melyek segítségével a Bizottság figyelmét fel tudja hívni az egyes problémás adattovábbítási gyakorlatokra.

26 Adatvédelmi irányelv 26. cikk (4) bek.

27 Irányelv 26. cikk (4) bek.

28 Az Európai Bizottság 2001. június 15-ei 2001/497/EK határozata és Az Európai Bizottság 2001. december 27-ei 2002/16/EK határozata.

29 Az Európai Bizottság 2004. december 27-i 2004/915/EK határozata.

30 Az Európai Bizottság 2010. február 5-i 2010/87/EU határozata.

31 Lásd erről bővebben: Horváth-Egri Katalin: A kötelező szervezeti szabályok (Binding Corporate Rules, BCR) és az együttműködési eljárási lehetőségei. *Infokommunikáció és Jog,* 2015/64. 143–146. o.

32 A Munkacsoport által kiadott dokumentumok segítséget nyújtanak a szervezetek számára a BCR kialakítása során, lásd Article 29 – Data Protection Working Party: Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules forInternational Data Transfers, WP74 (11639/02/EN) 2003. június 3.

33 Az érintetti hozzájárulás történetének megismeréséhez a szabályozási generációk tükrében lásd Szőke Gergely László: Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén, HVG-ORAC Kiadó, Budapest, 2015. 37–52. o.

34 Szőke: *i. m.* 50. o.

35 Daniel J. Solove: Introduction: Privacy Self-management, *Harvard Law Review,* 2013, Vol. 126. 1880. o.

36 Az USA adatvédelmi szabályai alapvetően a notice&choice rendszerre épülnek.

37 Solove: *i. m.* 1881. o.

38 Solove: *i. m.* 1883–1888. o.

39 Solove: *i. m.* 1888–1893. o.

40 Szőke: *i. m.* 48–49. o.

41 Tekintettel arra, hogy az adatvédelem – csakúgy mint a környezetvédelem – mind az egyénre, mind a társadalomra egyformán hatással van. Lásd Sólyom László: Egy új szabadságjog: az információszabadság, *Valóság,* 9. sz. 1988, 31. o.

42 Ezt az álláspontot képviseli Steve Peers professzor, amikor az EUB egy 2014-es döntésével hozza párhuzamba az információs önrendelkezési jogot. Peers, Steve: The party's over: EU data protection law after the Schrems Safe Harbor Judgement, *EU Law Analysis,* http://eulawanalysis.blogspot.hu/2015/10/the-partys-over-eu-data-protection-law.html (2016.01.30.) Vö. Az Európai Unió Bíróságának

C199/12–C201/12. sz. egyesített ügyek X, Y és Z kontra Minister voor Immigratie, Integratie en Asiel, 2013. július 11.
43 Solove: *i. m.* 1894. o. Vö. Mazzone, Jason: The Waiver Paradox, 97 *NW. U. L. REV.* 2003, 801, 801–02. o.
44 Volokh, Eugene: Freedom of Speech and Information Privacy: The Troubling Implications, of a Right to Stop People from Speaking About Me, 52, Stanford Law Review, 2000, 1049, 1063. o. Idézi: Solove, Daniel J. – Richards, Neil M.: Rethinking Free Speech and Civil Liability, 109 COLUM. L. REV. 2009, 1650, 1676. o. Idézi: Solove: *i. m.* 1894. o.
45 Schwartz, Paul M.: The EU–U.S. Privacy Collision: A Turn to Institutions and Procedures, 126 Harvard Law Review, 2013, 1966, 1971–76, 1992–2001. o. Vö. Kosta, Eleni: Consent in European Data Protection Law, Brill, 2013.
46 Jóri András: *Adatvédelmi kézikönyv,* Osiris, Budapest, 2005, 62. o. és Jóri András – Bártfai Zsolt: Vitás kérdések az adatvédelmi törvény értelmezése körül, *Infokommunikáció és Jog,* 2005, 5. sz. 161. o. Hasonló álláspontra jutnak más szerzők is, lásd Attila Kiss – Gergely László Szőke: Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. in: Serge Gutwirth – Ronald Leenes – Paul de Hert (eds.): Reforming European Data Protection Law. Springer, 2015. pp. 319–321., p. 317.
47 Szabó Máté Dániel: *Az információs hatalom alkotmányos korlátai,* Miskolci Egyetem, Miskolc, 2012, 31–32. o. Vö. Szőke: *i. m.* 84–85. o.
48 Péterfalvi Attila (szerk.): Adatvédelem és információszabadság a mindennapokban, HVG-ORAC Lap- és Könyvkiadó, 2012, Budapest, 68. o.
49 Érdekességként jegyezhető meg, hogy az irányelv angol szövege az *„unambigous"* szót használja, a hozzájárulás minősítését illetően.
50 Irányelv 2. cikk h) pont.
51 West's Encyclopedia of American Law, edition 2. S.v. „Voluntary Act." (http://legal-dictionary.thefreedictionary.com/Voluntary+Act 2016.01.25.) Vö. Magyar Értelmező Kéziszótár 2003, Akadémiai Kiadó, Budapest, 1027. o.
52 Burton's Legal Thesaurus, 4E. S.v. „explicit." (http://legal-dictionary.thefreedictionary.com/explicit 2016.01.25.) Vö. Magyar Értelmező Kéziszótár, 674. és 1164. o.
53 Magyar Értelmező Kéziszótár, 1296. o.
54 Az információs önrendelkezési jogról és az információ szabadságról szóló 2011. évi CXII. törvény, 3. § 7. pont, 5. § (1) bekezdés a) pont, (2) bekezdés a) pont, 8. § (1) bekezdés a) pont.
55 Péterfalvi: *i. m.* 65. o.
56 Péterfalvi: *i. m.* 65–66. o.
57 Adatvédelmi irányelv 26. cikk.
58 Samuel Gibbs: Max Schrems demands Facebook stop EU to US data transfer due snooping, The Guardian, Tech, 2015. december 3. (http://www.theguardian.com/technology/2015/dec/03/max-schrems-demands-facebook-stop-eu-us-data-transfer-snooping 2016.01.25.)
59 Az Európai Unió Bíróságának ítélete a C-362/14. sz. ügyben, 2015. október 6.
60 Ez kitűnik a Schrems által beadott panaszokból is. Ezek egyenként ld. "PRISM 2.0" - Complaints after the Judgment C-362/14 (http://www.europe-v-facebook.org/EN/Complaints/PRISM_2_0/prism_2_0.html 2016.06.13.)
61 *Uo.*
62 Bővebben: Schrems v. Data Protection Commissioner (https://epic.org/privacy/intl/schrems/#schrems2 2016. 11 .05.)
63 A kifejezést használja az Európai Parlament és Tanács Rendeletének tervezete, az Általános Adatvédelmi Rendeletről, Brüsszel, 2015. december 15. 15039/15 44. cikk (1) bekezdés a) pont, 144. o.
64 A kifejezést használja az Európai Parlament és Tanács 1995. október 24-ei 95/46/EK irányelv (a továbbiakban: Irányelv) 26. cikk (1) bekezdés a) pont és az Európai Unió Bíróságának ítélete a C-362/14. sz. ügyben, 2015. október 6. az irányelvre való hivatkozáskor.
65 Rapid Press Update: Facebook & NSA-Surveillance: Following „Safe Harbor" decision, Irish Data Protection Commissioner to bring EU-US data flows before CJEU again (http://www.europe-v-facebook.org/PA_MCs.pdf 2016.06.13.)
66 Lásd List of companies for which the EU BCR cooperation procedure is closed (http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm 2016.01.30.) Facebook Adatvédelmi Szabályzat (https://hu-hu.facebook.com/privacy/explanation 2016. 06. 13.) A szabályzat 2015. január 30. napján íródott angol nyelven, s azóta folyamatosan hatályba tartott. Lásd https://www.facebook.com/legal/terms (2016.06.13.)
67 Facebook Adatvédelmi Szabályzat, https://hu-hu.facebook.com/privacy/explanation (2016.06.13.) és a szabályzat. https://www.facebook.com/legal/terms (2016.06.13.)
68 Article 29 Working Party „Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114), 2005. november 25., 10. o. Figyelemmel az „Opinion 5/2004 on unsolicited direct marketing communications under Article 13 of Directive 2002/58/EC" (WP 90), 2004. február 27., 3.2. pontra.
69 Sikerrel járhatnak azonban arra tekintettel, hogy a Facebook nem nyújt kellő védelmet az uniós állampolgárok adataira vonatkozóan. E kérdés megválaszolására azonban nem vállalkozunk, hiszen külön tanulmány témája is lehetne a feltett kérdés.
70 Data Protection Act of Ireland, 1988, F30[11 4(a) (i) (II). Bundesdatenschutzgesetz (BDSG) (Deutschland) 4c. § (1) 1. 08/12/1992 Act of 8 December 1992 on protection of privacy in relation to processing og personal data (Belgium), Art 22. § 1, 1°.
71 Általános Adatvédelmi Rendelet, 49. cikk (1) bekezdés a) pont. Az angol szöveg az *explicit consent* kifejezést használja.
72 29. cikk szerinti Adatvédelmi munkacsoport felismeri az Egyesült Államok kormányzata részéről 2014 és 2015 között tanúsított erőfeszítéseket a nem amerikai állampolgárokat érintő adatok védelme terén, azonban még mindig vannak aggályai a négy alapvető garancia terén, különös tekintettel a jogorvoslati jog területére. Lásd Statement of the Article 29 Working Party on the consequences of the Schrems Judgement, 2016. február 3. (http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf 2016.02.18.)