ESZTERI DÁNIEL*

AZ EURÓPAI UNIÓS ADATVÉDELEM MINDENHOVÁ ELÉRŐ KEZE: A GDPR ALKALMAZÁSÁNAK KITERJESZTÉSE HARMADIK ORSZÁGOKRA, KÜLÖNÖS TEKINTETTEL AZ AMERIKAI EGYESÜLT ÁLLAMOKRA

https://doi.org/10.51783/ajt.2024.2.05

A személyes adatok védelméhez fűződő jog olyan az Európai Unió Alapjogi Chartájában[1] is nevesített, kiemelt védelmet élvező alapvető jog, amelynek alakulása, fejlődése mind a jogalkotásban, mind a jogalkalmazásban igen nagy jelentőségre tett szert az elmúlt két évtizedben.

A 2010-es évektől a nagyobb horderejű, a területet érintő események hatására a közvélemény is élénken elkezdett adatvédelmi kérdésekkel foglalkozni. Ez többek között az Európai Unió és az Amerikai Egyesült Államok közötti személyes adattovábbításokra és az azokkal kapcsolatos nemzetbiztonsági megfigyelési botrányokra vezethető vissza. A 2010-es évek végére pedig az egységes, közvetlenül alkalmazandó általános adatvédelmi rendeletnek, a GDPR-nak[2] köszönhetően az adatvédelem megkerülhetetlen jogterületté vált az Unióban, akár a legkisebb vállalkozások számára is.

Jelen tanulmány az Európai Uniós adatvédelmi jogfejlődés rövid bemutatásával indít. Ezek után a GDPR ún. extraterritoriális hatályával kapcsolatos szabályokat ismerteti, és összeveti azt a nemzetközi adattovábbításokra vonatkozó szabályokkal. Ennek során bemutatom, hogy a két egymással összefüggő és egymást kiegészítő szabályrendszer bevezetésének mi volt az indoka, hogyan függenek össze azok egymással, és mi adja a kettő közötti különbséget. Felvázolom továbbá a GDPR nemzetközi adattovábbítással kapcsolatos egyes legitim eszközeit is.

A tanulmány utolsó része az Európai Unióból az Amerikai Egyesült Államokba történő adattovábbítások problémájával foglalkozik, ugyanis az erre vonatkozó szabályozás többször megmérettetett, elbukott, majd újra megmérettetett az Európai Unió Bírósága előtt is. A cél annak áttekintése és igazolása, hogy az adattovábbítások terén irányadó szabályozás az USA vonatkozásában szemmel látható fejlődésen ment keresztül az elmúlt időszakban.

* PhD, osztályvezető, NAIH, 1055 Budapest, Falk Miksa utca 9–11.; kutató, HUN-REN TK Mesterséges Intelligencia Nemzeti Laboratórium, 1097 Budapest, Tóth Kálmán utca 4. E-mail: *daniel.eszteri@outlook.com*.

1 *Az Európai Unió Alapjogi Chartája* (2016/C 202/2) (a továbbiakban: Alapjogi Charta), 8. cikk.

2 *Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)* (közkeletű angol rövidítéssel a továbbiakban: GDPR).

Ettől függetlenül továbbra sem jelenthető ki teljes bizonyossággal, hogy minden problémát sikerült rendezni, és időtálló adattovábbítási rendszert sikerült alkotni.

1. AZ ADATVÉDELEM EGYSÉGES EURÓPAI UNIÓS SZABÁLYOZÁSA

1.1. A SZABÁLYOZÁS ELŐZMÉNYEI

A magánélet vagy – másik kifejezéssel élve – a magánszféra védelméhez való jog központi, meghatározó része a személyes adatok védelméhez fűződő jog. Egy adott élő emberhez (az adatvédelem terminológiája szerint: az érintetthez) köthető információk védelme a személyiségi jogok egyik fajtájaként a kiszolgáltatottság és egyéb visszaélések megakadályozására hivatott. A magánélet védelméhez való jognak és ezen belül a szűkebben értett adatvédelemnek az „anyajoga" az emberi méltósághoz való jog.[3]

A személyes adatok védelméhez fűződő jog legjelentősebb uniós jogalkotási terméke volt az 1995-ös Adatvédelmi Irányelv (a továbbiakban: Adatvédelmi Irányelv).[4] Az irányelv volt az alapja az 1995 utáni uniós tagállami jogalkotásnak, hiszen azt – annak természetéből fakadóan – az egyes tagállamoknak kötelezően át kellett ültetniük a nemzeti jogba.[5] Az 1990-es évektől az első magyar adatvédelmi törvényhez[6] hasonlóan sorban születnek meg Európában a nemzeti adatvédelmi törvények az Unió Adatvédelmi Irányelvének modellje után és implementációja során.[7]

Az Adatvédelmi Irányelvet azonban az ezredforduló után sok kritika érte. Ennek egyik fő oka az volt, hogy az elvek és szabályrendszer nemzeti jogokba történő átültetése a nemzeti sajátosságok (intézményrendszerek) különbözőségének figyelembevételével ugyan mindenhol megtörtént, de az adatvédelmi jogok és kötelezettségek vonatkozásában a teljes jogbiztonság uniós szinten mégsem valósult meg.[8] A másik nagy probléma az volt, hogy az irányelv által lefektetett szabályrendszer egyre kevésbé tudott reflektálni a technológiai fejlődés legújabb kihívásaira (pl. automatizált döntéshozatal), valamint az online szolgáltatások elterjedésével kapcsolatos kockázatokra. Az internetes szolgáltatások elterjedése kapcsán egyre jobban előtérbe került a harmadik országokba történő adattovábbítás következetesebb uniós szabályozásának igénye is.[9]

[3] Bendik Tamás – Sziklay Júlia: *Az adatvédelem hazai és európai uniós szabályozása és alapintézményei* (Budapest: Nemzeti Közszolgálati Egyetem 2019) 5.

[4] *A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv* (a továbbiakban: „Adatvédelmi Irányelv).

[5] Lásd Bendik–Sziklay (3. lj.) 10.

[6] Az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Avtv.)

[7] A szabályozás történetének részletes összefoglalását lásd: Szőke Gergely László: „Az adatvédelem szabályozásának történeti áttekintése" *Infokommunikáció és Jog* 2013/3. 109–110.

[8] Lásd Bendik–Sziklay (3. lj.) 11.

[9] Lásd a GDPR (6)–(7) preambulumbekezdéseit.

Az adatvédelem történeti fejlődését feldolgozó tanulmányában Szőke is rámutatott arra, hogy az online profilozás fejlődése, az egyre kifinomultabb direktmarketing-eszközök és helymeghatározás elterjedése mind olyan tendenciák, amelyek szabályozására egyre nagyobb igény mutatkozott. A felhőszolgáltatások elterjedése miatt pedig egyre jobban kicsúszni látszott az érintettek kezéből a személyes adataik „fizikai" ellenőrzésének lehetősége is.[10]

Mivel tehát a globalizáció hatására a személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt, egyre inkább igény mutatkozott egy új, uniós szinten is teljesen egységes adatvédelmi szabályozásra. Ennek az igénynek a végső terméke lett az Európai Unió általános adatvédelmi rendelete, a GDPR.

1.2. AZ EURÓPAI UNIÓS ADATVÉDELMI REFORM

Az Európai Unió adatvédelmi reformjának jogi kiindulópontja a Lisszaboni Szerződésre[11], továbbá ehhez kapcsolódóan az Alapjogi Chartára vezethető vissza. Az Alapjogi Charta 8. cikke önálló alapjogként biztosítja a személyes adatok védelméhez fűződő jogot, és meghatározza az ahhoz kapcsolódó alapvető elveket és követelményeket.

Habár az Alapjogi Charta formálisan nem vált az alapító szerződések részévé, azt a Lisszaboni Szerződés az alapító szerződések rangjára emelte, és azokkal megegyező jogi kötőerővel ruházta fel. Az egységes uniós adatvédelmi szabályozás kialakítására ezen általános uniós közjogi alapok mellett nyílt meg az út.[12]

Az Európai Bizottság (a továbbiakban: Bizottság) 2012. január 25-én terjesztette elő jogalkotási javaslatcsomagját, az úgynevezett „adatvédelmi csomagot". Ennek a részét képezte egy, az Adatvédelmi Irányelvet felváltó rendelet tervezete, amely az általános adatvédelmi szabályokat tartalmazta, valamint egy, a 2008/977/IB kerethatározat helyébe lépő irányelvre irányuló javaslat, amely a bűnüldözési célú adatkezelésekre koncentrált. A javaslatok tehát két eltérő jogforrásban kívánták szabályozni az adatvédelemre vonatkozó általános szabályokat és a bűnüldözési célú adatkezelésekre vonatkozó szabályokat. A szabályozás szükségességét a Bizottság szakpolitikai közleményében foglalta össze.[13]

A jogalkotási javaslatcsomagról az Európai Tanács az első álláspontját 2016. április 8-án fogadta el, majd az Európai Parlament 2016. április 14-i plenáris ülésén döntött az adatvédelmi csomag elfogadásáról. A jogi aktusok a 2016. április 27-én történő aláírásukat és az Európai Unió Hivatalos Lapjában 2016. május 4-én történő

[10] Lásd Szőke (7. lj.) 110.

[11] *A lisszaboni szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról (2007/C 306/01)* (a továbbiakban: Lisszaboni Szerződés).

[12] Lásd Bendik–Sziklay (3. lj.) 12.

[13] A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek és az Európai Gazdasági és Szociális Bizottságnak: A magánélet védelme az összekapcsolódó világban 21. századi európai adatvédelmi keret (COM(2012) 9 final), *https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012DC0009&from=HU.*

kihirdetésüket követően váltak az uniós *acquis* részévé,[14] mint a GDPR, valamint az ún. Bűnügyi Adatvédelmi Irányelv.[15]

A GDPR legjelentősebb újítása, hogy rendeleti szintű jogforrásként közvetlenül hatályosul és az közvetlenül alkalmazandó a tagállami jogrendszerekben, így főszabály szerint Unió-szerte egységes szabályozást eredményez.

A továbbiakban jelen tanulmány a GDPR szabályozási koncepciójának általános elemzésétől eltekint és kizárólag a harmadik országbeli alkalmazásával kíván foglalkozni. Ennek kapcsán az extraterritorialtás és a harmadik országok irányába történő adattovábbítás releváns rendelkezéseit és gyakorlatát tekinti át.

2. AZ EURÓPAI ADATVÉDELEM TERÜLETI HATÁLYÁNAK KITERJESZTÉSE AZ UNIÓN TÚLRA

2.1. AZ ADATVÉDELEM TERÜLETI HATÁLYÁNAK KITERJESZTÉSÉRE VONATKOZÓ IGÉNYEK FELMERÜLÉSE ÉS AZ EURÓPAI BÍRÓSÁG GDPR ELŐTTI VONATKOZÓ ESETJOGA

A GDPR további nagy újítása az addigi széttöredezett tagállami szabályozáshoz képest, hogy bizonyos adatkezelőknek[16] és adatfeldolgozóknak[17] akkor is kötelezően alkalmazniuk kell az előírásait, ha egyébként azok nem az Európai Unióban rendelkeznek tevékenységi hellyel, hanem harmadik országból nyújtanak szolgáltatásokat az Unióban tartózkodó érintetteknek. Ennek a kiterjesztő, ún. extraterritoriális hatályra vonatkozó szabályozásnak az igénye már a GDPR előtt is felmerült.

Az adatvédelem extraterritoriális hatályú kiterjesztésének igényét tárgyalta többek között Kuner[18] vagy Svantesson,[19] akik közleményeikben már a GDPR alkalmazandóvá válása előtt rámutattak arra, hogy az extraterritorialitás igénye az adatvédelem területén a nemzetközi magánjog hasonló szabályozási filozófiájából eredeztethető. A Kuner által hivatkozott, a Nemzetközi Jogi Bizottságtól idézett meghatározás szerint a „területen kívüli joghatóság", nem más mint egy kísérlet arra, hogy nem-

[14] Lásd Bendik–Sziklay (3. lj.) 12.

[15] *Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről* (Bűnügyi Adatvédelmi Irányelv).

[16] A GDPR 4. cikk 7. pontja alapján adatkezelőnek minősül az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza [...].

[17] A GDPR 4. cikk 8. pontja alapján adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

[18] Christopher Kuner: „Extraterritoriality and International Data Transfers in EU Data Protection Law" *Legal Studies Research Paper Series* Paper No. 49/2015, *https://ssrn.com/abstract=2644237.*

[19] Dan Jerker B. Svantesson: *Extraterritoriality in Data Privacy Law* (Koppenhága: Ex Tuto, 2013). *https://doi.org/10.1093/idpl/ipu003.*

zetközi jogi szabályozás hiányában nemzeti jogszabályokkal, ítélethozatallal vagy végrehajtással szabályozzák az olyan külföldi személyek vagy vagyontárgyak jogállását, illetve az olyan határon túli cselekményeket, amelyek érintik az állam érdekeit.[20] Kuner kiemeli, hogy az extraterritorialitás problémája különösen az interneten folyó magatartások értékelésével kapcsolatban merül fel, mivel azokra egyi dőben több jogszabály is vonatkozhat, köszönhetően annak, hogy az adatkezelés elválik az azt végrehajtó vagy általa érintett felek földrajzi helyzetétől.[21]

Az adatvédelmi jog extraterritoriális hatályú alkalmazásának fő dilemmáját Czerniawski és Svantesson a következőképpen igyekszik megragadni: Egy adott állam vagy jelen esetben az Európai Unió területen kívüli joghatósági igényei azért észszerűek, mert ha az államok nem terjesztik ki adatvédelmi szabályozásukat a külföldi, harmadik országbeli felek magatartására, akkor a jelenlegi technológiai fejlettség mellett egyszerűen nem képesek biztosítani állampolgáraik jogainak hatékony védelmét. Ugyanakkor a széles körű extraterritoriális joghatósági igények vitathatatlanul észszerűtlenek is egyben, mivel az interneten szolgáltatók számára nem lehetséges, hogy magatartásukat a világ minden olyan országának jogszabályaihoz igazítsák, amellyel kapcsolatba kerülnek. Más szóval, az állami jog széles körű, területen kívüli alkalmazása végül ellehetetlenítheti a vállalkozások számára a határokon átnyúló kereskedelmet.[22]

A másik oldalon viszont jogosan merülhet fel a szabályozói igény azzal kapcsolatban, hogy az online szolgáltatók harmadik országba való letelepedésével ne lehessen kijátszani az egyes tagállamok és végső soron az Európai Unió szigorúbb adatvédelmi szabályait, csorbítva ezzel az uniós érintettek jogait.

Az adatvédelmi jog „területen kívüli" alkalmazásának igénye már a GDPR alkalmazandóvá válása előtt felmerült az Európai Unió Bíróságának (a továbbiakban: EUB) esetjogában is, szorosan kapcsolódva az ún. *megcélzás* fogalmának értelmezésével. A megcélzás fogalma gyakorlatilag annyit jelent, hogy egy szolgáltató a szolgáltatásait az Unióban tartózkodó érintettek részére is elérhetővé teszi jellemzően az interneten keresztül, tehát őket is célozza, viszont a tevékenysége központja (székhelye, telephelye) nem az Unióban, hanem egy harmadik országban található.

A megcélzás értelmezéséhez (a letelepedés fogalmával összefüggésben) az EUB 2015. október 1. napján kelt ún. Weltimmo-ítéletében[23] találhatunk iránymutatást. Ez a döntés a letelepedés fogalmát meglehetősen kiterjesztően értelmezte. Az EUB az ítéletben úgy határozott, hogy az Adatvédelmi Irányelv 4. cikk (1) bekezdésének a) pontját úgy kell értelmezni, hogy *„az lehetővé teszi az attól eltérő tagállam személyes adatok védelmére vonatkozó szabályozásának alkalmazását, mint ahol ezen adatok kezelője be van jegyezve, amennyiben ezen adatkezelő tartós jelleg-*

[20] Lásd Kuner (18. lj.) 6.

[21] Lásd Kuner (18. lj.) 7.

[22] Michal Czerniawski – Dan Svantesson: „Challenges to the extraterritorial enforcement of data privacy law – EU case study" in Martin Brinnen – Cecilia Magnusson Sjöberg – David Törngren – Daniel Westman – Sören Öman (szerk.): *Dataskyddet 50 år – historia, aktuella problem och framtid* (Stockholm: Eddy.se ab 2023) 128., *https://doi.org/10.53292/bd1fa11c.f5b3afbe.*

[23] C–230/14. sz. Weltimmo s.r.o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság ügyben 2015. október 1-én hozott ítélet [ECLI:EU:C:2015:639].

gel olyan, akár csekély mértékű valós és tényleges tevékenységet folytat e tagállam területén, amelynek keretében az adatkezelésre sor kerül."[24]

A fentiekben idézett megfogalmazás értelmezéséhez először is nézzük meg, hogy mi volt az ügy lényege, amelyben az ítélet megszületett: Az EUB előtti ügyben a szlovák bejegyzésű cég (Weltimmo s.r.o.) Magyarország állampolgárainak címzett, e tagállam nyelvén (tehát magyarul) megfogalmazott szolgáltatást kínáló weboldalt üzemeltetett, és e tevékenység következtében a szolgáltatása szinte teljes mértékben az említett tagállamra irányult. A konkrét ügyben az EUB ítélete kimondta, hogy a szlovákiai cég tényleges gazdasági tevékenységet nem is folytatott Szlovákiában, tehát abban az uniós tagállamban, ahol bejegyzett székhellyel rendelkezett. Követelései behajtása tekintetében viszont bankszámlát nyitott, és postafiókcímmel is rendelkezett Magyarországon, ahonnan a postát rendszeresen felvették és elektronikus úton továbbították számára, továbbá ügyvezetője magyar állampolgár volt, aki magyarországi érvényes lakcímmel rendelkezett, a cég a honlapján pedig magyar nyelven, magyarországi ingatlanok tekintetében kínált ingatlanközvetítői szolgáltatást.[25] Az EUB fenti ítélete alapján a magyar adatvédelmi hatóság eljárási joghatóságát megalapozta, hogy a vizsgált adatkezelő tartós jelleggel olyan, (akár csekély mértékű) valós és tényleges tevékenységet folytatott Magyarország területére irányítva az interneten keresztül, amelynek keretében személyes adatok (pl. a honlapon regisztrált felhasználók adatainak) kezelésére is sor kerül.[26]

Az EUB ebben az ítéletében tehát megállapította, hogy az Európai Unió más tagállamában bejegyzett székhellyel rendelkező adatkezelőnek Magyarország területére irányuló (internetes) szolgáltatásával kapcsolatos adatkezelések tekintetében a magyar adatvédelmi hatóság joghatósággal rendelkezik a vizsgálat lefolytatására. Igaz, ebben az ügyben két uniós tagállam joghatóságának kérdését vizsgálta az EUB, a döntés következményei azonban a GDPR megcélzás kritériumának szabályozásában is visszaköszönnek.[27]

Az EUB esetjogában tehát már a GDPR alkalmazandóvá válása előtt felmerült annak az igénye, hogy az egyik tagállamban tartózkodó érintetteket megillető adatvédelmi jogosultságokat ne lehessen kijátszani pusztán arra hivatkozva, hogy az adatkezelő vállalkozás nem rendelkezik székhellyel vagy fiókteleppel a tagállamban. Az internetes szolgáltatók üzemeltetésével számtalanszor kínálnak szolgáltatásokat az Európai Unióban tartózkodó érintetteknek harmadik országbeli vállalkozások. A GDPR ezekre az adatkezelőkre is kiterjeszti a hatályát, amelynek bemutatására a következő pontokban kerül sor.

[24] C–230/14. sz. Weltimmo s.r.o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság ügyben 2015. október 1-én hozott ítélet [ECLI:EU:C:2015:639] 41. pontja.

[25] A Nemzeti Adatvédelmi és Információszabadság Hatóság NAIH/2016/3274/8/H. sz. határozata, 9., *https://naih.hu/files/NAIH-2016-3274-H-hatarozat.pdf*.

[26] Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról* (Budapest: Wolters Kluwer Hungary Kft. 2021) 62.

[27] Lásd Péterfalvi–Révész–Buzás (26. lj.) 62–63.

2.2. A GDPR TERÜLETI HATÁLYÁRA VONATKOZÓ FŐBB RENDELKEZÉSEK

2.2.1. AZ EU-BAN TEVÉKENYSÉGI HELLYEL RENDELKEZŐ ADATKEZELŐK ÉS ADATFELDOLGOZÓK

Mielőtt rátérnék a GDPR harmadik országbeli adatkezelőkre és adatfeldolgozókra vonatkozó szabályaira, érdemes néhány szót ejteni az összehasonlítás miatt a rendelet „hagyományos" területi hatályára vonatkozó szabályairól is.

A rendelet területi hatályára vonatkozó alapvető előírások szerint[28] az Unió területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó a tevékenységi helyére vonatkozó bármely adatkezelést a GDPR-ral összhangban kell hogy végezze.

Az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók adatkezelése tehát fő szabály szerint a GDPR hatálya alá tartozik, függetlenül azon érintettnek lakóhelyétől és állampolgárságától, akinek a személyes adatait kezelik. Az adatkezelő vagy adatfeldolgozó nem hivatkozhat tehát arra, hogy kizárólag harmadik országbeli állampolgárok adatait kezeli, kizárólag őket célozza áruk vagy szolgáltatások nyújtásával és az ő viselkedésüket figyeli meg, ha egyébként az Unió területén rendelkezik tevékenységi hellyel, és az adatkezelést itt végzi.[29]

A fentiekre az alábbi példát hozza az Európai Unió tagállamainak adatvédelmi felügyeleti hatóságait tömörítő Európai Adatvédelmi Testület (European Data Protection Board, a továbbiakban: EDPB) vonatkozó iránymutatása: Egy francia vállalat közös gépkocsihasználati alkalmazást fejlesztett kizárólag marokkói, algériai és tunéziai ügyfelek részére. A szolgáltatás kizárólag ebben a három országban vehető igénybe, de minden személyesadat-kezelési tevékenységet a franciaországi adatkezelő végez. A személyes adatokat nem uniós országokban gyűjtik, ez esetben a személyes adatok kezelését viszont az adatkezelő Unión belüli tevékenységi helyén végzik. Tehát az adatkezelés ugyan Unión kívüli érintettek személyes adataihoz kapcsolódik, a GDPR szabályai szerint mégis annak rendelkezései vonatkoznak a francia vállalat által végzett adatkezelésre.[30]

A területi hatály szempontjából nincs jelentősége annak a tényezőnek sem, hogy az adatkezelő ezt a tevékenységet milyen jogi formában gyakorolja. Ugyanúgy meg kell tehát felelnie a GDPR előírásainak egy, az Unió területén tartózkodó érintettektől adatokat gyűjtő, utazó ügynöki tevékenységet végző egyéni vállalkozónak, mint annak a cégnek, amely kizárólag a bejegyzett székhelyén végez adatkezelést.[31]

[28] A GDPR 3. cikk (1) bekezdése alapján a GDPR előírásait kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy sem.

[29] Lásd a GDPR (14) preaumbulumbekezdését.

[30] Európai Adatvédelmi Testület (EDPB): 3/2018. számú iránymutatás a rendelet területi hatályáról (3. cikk). 2019. 10., *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_consultation_hu.pdf*.

[31] Lásd Péterfalvi–Révész–Buzás (26. lj.) 59.

2.2.2. A GDPR EXTRATERRITORIÁLIS HATÁLYA

Az Unióban tevékenységi hellyel rendelkező adatkezelőkre és adatfeldolgozókra vonatkozó főszabály bemutatása után rátérnék a GDPR extraterritoriális hatályának ismertetésére, amely azt mondja meg, hogy mely esetben kell harmadik országbeli szervezeteknek is alkalmazniuk saját adatkezeléseikre a rendelet előírásait.

A GDPR az extraterritorális alkalmazásával kapcsolatos kérdéseket egyértelműen eldöntötte a rendeletnek az Európai Unió területén kívüli adatkezelőkre és adatfeldolgozókra való alkalmazhatóságára vonatkozó szabályok explicit rendezésével. Az EDPB vonatkozó iránymutatása a GDPR ezen előírását nevezi az ún. *megcélzás* kritériumainak.[32]

A GDPR tehát az Unióban tevékenységi hellyel nem rendelkező adatkezelőkre és adatfeldolgozókra is kiterjeszti a hatályát azokban az esetekben, ha a tevékenységeik áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, továbbá az érintettek Unión belül tanúsított viselkedésének megfigyelésével függenek össze.[33]

A GDPR ezen újítását Szabó ún. irányultsági szabálynak nevezi, amely figyelembe veszi a célpiacon, tehát jelen esetben az Unióban élő, tartózkodó személyek magánszférájának védelmét. A területi hatály kiterjesztése révén nem csupán az olyan adatkezelésekre kell alkalmazni a rendeletet, amelyekre az Európai Unió területén kerül sor, hanem azokra is, amelyek azon kívül történnek, és azok az Unióban tartózkodó érintettek adatainak kezelésével járnak együtt.[34]

A GDPR ad némi támpontot annak megállapítása érdekében, hogy az adatkezelő vagy adatfeldolgozó kínál-e termékeket és szolgáltatásokat az Unió területén lévő érintetteknek, tehát őket célozza-e meg az adatkezelése. Ezek szerint először meg kell bizonyosodni arról, hogy nyilvánvaló-e, hogy az adatkezelő vagy adatfeldolgozó az Unió egy vagy több tagállamában az érintettek számára szolgáltatásokat tervez nyújtani. A rendelet szerint nem tekintendő e szándék nyilvánvaló jelének az a puszta tény, hogy az adatkezelő, adatfeldolgozó vagy valamely közvetítő honlapja, e-mail-címe vagy más elérhetősége hozzáférhető az Unió területén. Ha viszont például az adatkezelő olyan nyelvet vagy pénznemet használ, amely egy vagy több tagállamban is általánosan használatos, és így lehetőséget biztosít termékeknek és szolgáltatásoknak az ezen a nyelven történő megrendelésére, vagy az Unióban tartózkodó fogyasztókra vagy felhasználókra tesz utalást, az egyértelműen jelezheti,

[32] Lásd EDPB (30. lj.) 15–16.

[33] A GDPR 3. cikk (2) bekezdés a)-b) pontjai alapján a GDPR előírásait kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, abban az esetben, ha az adatkezelési tevékenységek áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, vagy az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.

[34] Szabó Endre Győző: „Az Európai Unió Általános Adatvédelmi Rendeletében biztosított védelem szintjének elemzése." Doktori értekezés, Károli Gáspár Református Egyetem, 2019, 54. *https://corvina.kre.hu/phd/Szabo_Endre_Disszertacio.pdf.*

hogy az adatkezelő az Unió területén tartózkodó érintetteknek termékeket vagy szolgáltatásokat szándékozik kínálni.[35]

Fontos kivételszabály, hogy a szolgáltatások nyújtásához kapcsolódó adatkezelési tevékenységekkel összefüggésben a rendelkezés olyan tevékenységekre irányul, amelyek szándékosan, nem pedig akaratlanul vagy véletlenül céloznak meg az Unióban tartózkodó egyéneket. Erre a következő példát hozza az EDPB már hivatkozott iránymutatása: Egy ausztrál vállalat mobil hír- és videótartalom-szolgáltatást kínál a felhasználók preferenciái és érdeklődési köre alapján, amelynek használatával a felhasználók napi vagy heti rendszerességgel értesülhetnek az újdonságokról. A szolgáltatást kizárólag Ausztráliában tartózkodó felhasználóknak kínálják, akiknek az előfizetéskor ausztrál telefonszámot kell megadniuk. A szolgáltatás egyik ausztrál előfizetője Németországba utazik, és továbbra is használja a szolgáltatást. Az ausztrál előfizető ugyan az Európai Unióban való tartózkodása alatt veszi igénybe a szolgáltatást, az azonban nem az Unión belüli egyéneket „célozza meg", hanem kizárólag az Ausztrálián belülieket, így az ausztrál vállalat által végzett személyesadat-kezelés nem tartozik a GDPR hatálya alá.[36]

A GDPR tárgyi hatálya tehát rendkívül széles körben alkalmazandó az adatkezelőkre és adatfeldolgozókra, függetlenül attól, hogy az Európai Unióban van-e a tevékenységi helyük, vagy sem. A GDPR extraterritoriális hatálya lévén ugyanis annak alkalmazása kötelező az olyan adatkezelőkre és adatfeldolgozókra is, akik ugyan harmadik országban telepedtek le, azonban az Európai Unió területén tartózkodó, innen a szolgáltatásokat igénybe vevő érintettek személyes adatait kezelik, vagy az ő viselkedésük megfigyelését végzik.

A GDPR fentiekben bemutatott, rendkívül kiterjesztő területi hatályra vonatkozó rendelkezései további kiegészítésre kerülnek az adattovábbításra vonatkozó rendelkezésekkel. A harmadik országokba – vagy nemzetközi szervezetek részére – történő adattovábbítás általános szabályait a következő pontban tekintem át.

3. AZ UNIÓS ADATVÉDELEM EXPORTÁLÁSA A HARMADIK ORSZÁGOKBA TÖRTÉNŐ ADATTOVÁBBÍTÁSI SZABÁLYOKKAL

3.1. A HARMADIK ORSZÁGOKBA TÖRTÉNŐ ADATTOVÁBBÍTÁS SZABÁLYOZÁSÁNAK FEJLŐDÉSE A GDPR ELŐTT

Mielőtt rátérnék a GDPR jelenleg hatályos szabályozásának ismertetésére a harmadik országokba vagy nemzetközi szervezetek részére adattovábbítás kapcsán, tekintsük át röviden ennek a területnek a szabályozásával kapcsolatos jogfejlődést az elmúlt időszakban.

Az Európai Unió adatvédelmi szabályozása az Adatvédelmi Irányelv 1995-ös megalkotása óta írt elő különböző feltételeket a személyes adatok harmadik ország-

[35] Lásd a GDPR (23) preambulumbekezdését.
[36] Lásd EDPB (30. lj.) 17.

ba történő továbbítására. Ezeknek a szabályoknak az elsődleges célja annak a biztosítása, hogy amikor az uniós állampolgárok már begyűjtött személyes adatait az adatkezelők vagy adatfeldolgozók az Unió területén kívülre továbbítják egy ottani szervezetnek, akkor az adatokat megillető megfelelő szintű védelem is megmaradjon. A védelem ilyen szintű kiterjesztésének legfőbb indoka, hogy az internet és online szolgáltatások térnyerésével az Unióban letelepedett vállalkozások és egyéb szervezetek mindennapjainak részévé vált az, hogy harmadik országba továbbítanak általuk kezelt személyes adatokat.[37] Ezzel a gyakorlattal szemben pedig éles kritikaként fogalmazták meg már korában, hogy a személyes adatok olyan országokba történő továbbítása, ahol esetleg az azokat megillető védelem szintje, a helyi jogi szabályozásból és gyakorlatból következően alacsonyabb szinten van, mint az Európai Unióban, félő, hogy kiüresíti az érintett természetes személyeket megillető jogokat.[38]

Az adatvédelmi szabályozás ezért már viszonylag korán, az Adatvédelmi Irányelvben is a védelem kiterjesztését tűzte ki célul az Európai Unión kívüli területeken, és emiatt figyelemmel volt arra, hogy speciális szabályokat kell alkotni a harmadik országba történő adattovábbításokkal kapcsolatban. Az irányelvben az adattovábbítás általános elvének lényege az volt, hogy személyes adatok harmadik országbeli adatkezelőknek és adatfeldolgozóknak történő továbbítása esetén nem sérülhet az Unióban a természetes személyeket megillető védelem szintje.[39] A védelemnek egyébként nemcsak a harmadik ország irányába történő, hanem az onnan további vagy újbóli továbbítására is ki kell terjednie.[40]

Az Adatvédelmi Irányelv 25. és 26. cikkét magában foglaló IV. fejezete olyan rendszert hozott létre, amelynek célja, hogy a személyes adatok harmadik országokba történő továbbítását a tagállamok ellenőrizhessék. Ez a szabályrendszer kiegészítő jellegű az irányelv II. fejezete által létrehozott általános rendszerhez képest, amely a személyes adatok kezelése jogszerűségének általános feltételeit határozza meg.[41]

A harmadik országba történő adattovábbítás szabályai visszaköszönnek a GDPR alkalmazandóvá válása előtti olyan EUB ítéletekben is, mint az ún. Lindqvist ítélet[42] és az Amerikai Egyesült Államokba történő adattovábbítás problémáival kapcsolatban elhíresült Schrems I. ítélet is, amelyről a későbbiekben részletesen is szó lesz.[43]

Az irányelv alapelvként rögzítette, hogy személyes adatokat csak olyan harmadik országba lehet továbbítani, amely biztosítja a személyes adatok megfelelő szintű védelmét, ami a gyakorlatban annyit jelentett, hogy az adott harmadik ország köz-

[37] Lásd Péterfalvi–Révész–Buzás (26. lj.) 358.

[38] Christopher Kuner: „Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection". *University of Cambridge Faculty of Law Research Paper* No. 20/2021. 14–15., *https://doi.org/10.2139/ssrn.3827850*.

[39] Lásd Kuner (18. lj.) 8–9.

[40] Árvay Viktor – Balogh Gyöngyi – Buzás Péter – Eszteri Dániel – Hackspacher Andrea – Kiss Ernő – Majsa Ágnes – Révész Balázs: *Az új általános európai adatvédelmi szabályozás és az adatkezelői kötelezettségek* (Budapest: Nemzeti Közszolgálati Egyetem 2018) 49.

[41] Lásd Péterfalvi–Révész–Buzás (26. lj.) 359.

[42] C-101/01. számú 2003. november 6-i Lindqvist ítélet [EU:C:2003:596] 63. pontja.

[43] C-362/14. számú 2015. október 5-i Maximilian Schrems kontra Data Protection Commissioner ítélet [EU:C:2015:650] 46. pontja.

jogi berendezkedésének hasonlóan magas szinten kellett védenie az érintettek személyes adatait, mint ahogy arra az Európai Unióban sor kerül.[44]

Ennek egyik garanciája volt az az eset, hogyha a Bizottság ún. *megfelelőségi határozatban* megállapíthatta egy harmadik ország vonatkozásában, hogy az megfelelő szintű védelmet biztosít a személyes adatok vonatkozásában.[45]

Az Adatvédelmi Irányelv rendelkezései alapján, amennyiben nem volt ilyen megfelelőségi határozat, lehetőség volt „eltérni" ettől az alapelvtől, vagyis személyes adatok továbbítására *különös helyzetek* (*„eltérések"*) fennállása esetén is sor kerülhetett. Ezen eltérések közül az irányelv összesen hat esetkört sorolt fel,[46] többek között például az érintett egyértelmű hozzájárulását az adattovábbításhoz, vagy ha az adattovábbítás az érintett és az adatkezelő között szerződés teljesítése érdekében szükséges.[47]

Az irányelv továbbá úgy rendelkezett, hogy sor kerülhet adattovábbításra harmadik országba akkor is, ha az adatkezelő egyéb megfelelő garanciákat teremt.[48] Az irányelv a megfelelő garanciák megteremtésére szolgáló eszközök, módszerek meghatározását azonban általánosságban a tagállami jogalkotókra bízta. Az általános szerződési feltételeket, vagy ahogy gyakran nevezik, *modellszerződést* azonban, mint a garanciák megteremtésére szolgáló eszközök egy példáját, az irányelv kifejezetten nevesítette. Ezek olyan általános szerződési feltételek, amelyekről a Bizottság határozatban állapította meg, hogy szerződésbe foglalásukkal, vagyis a felek szerződéses vállalásával a személyes adatot továbbító szervezet megfelelő garanciákat biztosít a harmadik országba történő továbbítás vonatkozásában.[49]

Szintén ilyen, a megfelelő garanciákat nyújtó eszköz a már régóta alkalmazott kötelező erejű vállalati szabályozás (angolul: Binding Corporate Rules, a továbbiakban röviden: BCR), amely kifejezetten multinacionális nagyvállalatokra alkotott adattovábbítási garanciarendszer. A BCR arra szolgál, hogy megfelelő garanciákat biztosítson, amikor egy vállalkozáscsoportba tartozó uniós adatkezelő az ugyanezen vállalkozáscsoportba tartozó, de harmadik országban letelepedett adatkezelő vagy adatfeldolgozó részére továbbít személyes adatokat. A BCR tehát egy nemzetközi vállalatcsoport által létrehozott belső szabályzat, amely a csoportba tartozó adatkezelőkre, adatfeldolgozókra kötelező. A BCR általános adatvédelmi kötelezettségvállalásokat tartalmaz, amelyeket a csoporttagok a megállapodás aláírásával vállalnak, és azokat követniük kell.[50]

A BCR-t, mint külön adattovábbítási eszközt az irányelv egyébként nem nevesítette. A BCR-okkal kapcsolatos kötelező tartalmi követelményeket, elvárásokat, csakúgy, mint a nemzeti engedélyezési, jóváhagyási eljárásokat megelőző együtt-

[44] Lásd Adatvédelmi Irányelv 25. cikk (1) bekezdés.
[45] Lásd Adatvédelmi Irányelv 25. cikk (6) bekezdés.
[46] Lásd Péterfalvi–Révész–Buzás (26. lj.) 358.
[47] Lásd Adatvédelmi Irányelv 26. cikk (1) bekezdés;
[48] Lásd Adatvédelmi Irányelv 26. cikk (2) bekezdés.
[49] Lásd Péterfalvi–Révész–Buzás (26. lj.) 359.
[50] Szőke Gergely László: „Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén." Doktori értekezés, Pécsi Tudományegyetem, 2015, 132–133. *https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/szoke-gergely-laszlo/szoke-gergely-laszlo-vedes-ertekezes.pdf.*

működési eljárást, az európai uniós adatvédelmi hatóságokat (a GDPR alkalmazása előtt) tömörítő ún. 29. cikk Szerinti Adatvédelmi Munkacsoport[51] (a továbbiakban: 29-es Munkacsoport) dolgozta ki, és rögzítette az általa elfogadott dokumentumokban. A magyar jogalkotó ezt a megfelelő védelmi szint megteremtésre alkalmas eszközt az Infotv.[52] 2015. évi módosításával[53] emelte jogszabályi szintre.[54] Ez a rész egyébként azóta deregulációval kikerült az Infotv.-ből, mivel a BCR jogintézményét a GDPR kifejezetten beemelte az adattovábbítás elismert eszközei közé összeurópai szinten, így a nemzeti szabályozás feleslegessé vált.

A továbbiakban látni fogjuk, hogy a GDPR szinte azonos logikán alapuló rendszert hozott létre a nemzetközi adattovábbítások szabályozása területén.

3.2. A HARMADIK ORSZÁGOKBA TÖRTÉNŐ ADATTOVÁBBÍTÁS SZABÁLYOZÁSA A GDPR-BAN ÉS ANNAK ELHATÁROLÁSA AZ EXTRATERRITORIÁLIS HATÁLYTÓL

Kuner a témával foglalkozó tanulmányában kiemeli, hogy az uniós adatvédelmi jog ambiciózus célokat tűz ki a természetes személyek adatainak az Unión kívülről származó fenyegetésekkel szembeni védelme érdekében, amelyeket a területi hatályra és a nemzetközi adattovábbításra vonatkozó szabályok ötvözésével kíván megvalósítani.[55] A Bizottság a GDPR megalkotására irányuló javaslatában is megállapította, hogy az érintettek jogait továbbra is biztosítani kell a személyes adatoknak az EU-ból/EGT-ből harmadik országokba történő továbbításakor, valamint amikor tagállami egyéneket céloznak meg, és adataikat harmadik országbeli szolgáltatók használják fel vagy elemzik.[56]

Szabó szerint az Unióban elért védelmi szintet a harmadik országba irányuló szabályok helyes és következetes alkalmazása megerősíti, mivel az adatok exportja ilyen esetben nem jár a védelem eróziójával. Arra is utal továbbá, hogy az Adatvédelmi Irányelvvel összehasonlítva a GDPR nem tekinthető egyértelmű előrelépésnek vagy visszalépésnek a védelem szintjét tekintve.[57]

Való igaz, hogy a GDPR a korábbi Adatvédelmi Irányelvhez képest – a normaszöveg egységességén túl – különösebb újításokat nem tartalmaz az adattovábbítás szabályaira. Az irányelvhez képest uniós szinten egységes rendeleti normaszöveg azonban véleményem szerint az egységes jogértelmezést ezen a területen is elősegíti.

[51] 29. cikk Szerinti Adatvédelmi Munkacsoport: Working document setting up a framework for the structure of Binding Corporate Rules (WP 154). 2008. *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf.*

[52] *Az információs önrendelkezési jogról és az információszabadságról szóló 2011. CXII. törvény* (Infotv.).

[53] *2015. évi CXXIX. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. CXII. törvény, továbbá egyes más törvények módosításáról.*

[54] Lásd Péterfalvi–Révész–Buzás (26. lj.) 359.

[55] Lásd Kuner (38. lj.) 5.

[56] Lásd: Európai Bizottság (13. lj.) 10. és Kuner (38. lj.) 5.

[57] Lásd Szabó (34. lj.) 64.

Maga a GDPR nem határozza meg explicite az adattovábbítás fogalmát, azonban a GDPR területi hatálya és a nemzetközi adattovábbítás kölcsönhatásról szóló EDPB iránymutatás szerint egy adatkezelés adattovábbításnak minősül, ha:

1. az *adatátadó* (adatkezelő vagy adatfeldolgozó) az adott adatkezelés tekintetében a GDPR hatálya alá tartozik; és

2. az *adatátadó* közlés útján továbbítja, vagy egyéb módon hozzáférhetővé teszi a személyes adatokat az *adatátvevő* (egy másik adatkezelő, közös adatkezelő vagy -feldolgozó) számára; és

3. az *adatátvevő* egy harmadik országban található vagy nemzetközi szervezet és attól függetlenül, hogy a GDPR hatálya alá tartozik-e.[58]

A fenti három feltétel konjunktív, tehát egyszerre valamennyinek teljesülnie kell ahhoz, hogy nemzetközi adattovábbításról beszélhessünk.

A jogviszony egyik szükséges szereplője tehát az *adatátadó* (angolul: *exporter*), amely a GDPR hatálya alá tartozó elkülönült jogalany (adatkezelő vagy adatfeldolgozó), aki az általa kezelt személyes adatokat továbbítja. A jogviszony másik, szintén szükséges szereplője pedig az *adatátvevő* (angolul: *importer*), amely a harmadik országban található elkülönült jogalany (adatkezelő vagy adatfeldolgozó), akinek a személyes adatokat továbbítják.

Nem minősül tehát adattovábbításnak, ha közvetlenül az uniós érintettektől (pl. saját kezdeményezésükre) történik a személyes adatok gyűjtése, beszerzése, vagy ha nem másik adatkezelő vagy adatfeldolgozó részére történik közlés. Ilyen esetekre egyébként a már hivatkozott EDPB iránymutatás több példát is hoz.[59]

Mint az előző pontokban már kifejtésre került, a GDPR extraterritoriális hatálya egyébként is kiterjed azon adatkezelésekre, amelyek az Unióban tartózkodó érintetteket célozzák meg. Ezekben az esetekben a védelem közvetlenül az extraterritoriális hatályra vonatkozó rendelkezésekből fakad. Adattovábbításról tehát csak azokban az esetekben beszélünk, amikor egy egyébként a GDPR hatálya alá tartozó szervezet az általa már valahogyan kezelt (általában az érintettektől közvetlenül begyűjtött) személyes adatokat *továbbadja* vagy *exportálja* egy harmadik országbeli elkülönült entitásnak, akit ebben az esetben adatátvevőnek nevezünk.

Ha az EDPB iránymutatásában meghatározott valamennyi kritérium teljesül, akkor harmadik országba vagy nemzetközi szervezet részére történő adattovábbításról van szó, és az adatátadónak meg kell felelnie a GDPR adattovábbításokra vonatkozó V. fejezetben foglalt feltételeknek. Ez a gyakorlatban annyit jelent, hogy a személyes adatoknak a harmadik országba vagy nemzetközi szervezet részére történt továbbítását az erre szolgáló garanciális eszközök egyikének felhasználásával kell foganatosítania.

Ha a már fentiekben említett három kritérium nem teljesül, akkor nincs szó adattovábbításról, és akkor a GDPR adattovábbításra vonatkozó szabályait tartalmazó V.

[58] Európai Adatvédelmi Testület (EDPB): 5/2021. számú iránymutatás az általános adatvédelmi rendelet 3. cikkének alkalmazása és V. fejezete szerinti, nemzetközi adattovábbításokra vonatkozó rendelkezések közötti kölcsönhatásról 2.0. változat. 2023. 7., *https://edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_hu.pdf*.

[59] Lásd EDPB (58. lj.) 9–10.

fejezete nem alkalmazandó. Ebben az összefüggésben azonban fontos emlékeztetni arra, hogy az adatkezelőnek vagy adatfeldolgozónak, ha egyébként a GDPR területi hatályára vonatkozó szabályai kiterjednek a tevékenységeire, továbbra is eleget kell tennie a rendelet többi rendelkezésének, és teljes mértékben elszámoltatható marad adatkezelési tevékenységeiért.[60] A GDPR területi hatálya és az adattovábbításokkal kapcsolatos szabályai között tehát különbség van, viszont mindkét jogintézmény célja az uniós érintetteket megillető védelmi szint erősítése. Ezek a jogintézmények a harmadik országbeli adatkezelőkre vonatkozásuk kapcsán kiegészítik, erősítik egymást.[61]

Az adattovábbítással kapcsolatban a GDPR szigorú, többlépcsős keretrendszert állít fel. Az EGT tagállamokon kívüli, harmadik országok tekintetében két csoport különíthető el: az adatvédelmi szempontból megfelelő szintű védelmet biztosító és nem biztosító államok.

Ez alapján az adatkezelőnek elsősorban meg kell vizsgálnia, hogy az adott harmadik ország megfelelő védelmi szintet biztosít-e, amely alapján a személyes adatok a továbbítást követően is részesülnek az európaival egyenértékű szintű védelemben. Amennyiben az adott ország nem biztosít ilyen szintű védelmet, akkor az adatkezelőnek vagy adatfeldolgozónak kell megpróbálnia a megfelelő garanciákat megteremtenie.[62]

Harmadik országba történő adattovábbításnál észben kell tartani, hogy a személyes adatokat továbbítani kívánó adatkezelőnek vagy adatfeldolgozónak be kell tartania a GDPR többi rendelkezését is, így különösen az alapelveket tartalmazó 5. cikkben és a jogalapokat tartalmazó 6. cikkben foglaltakat. Ez azt jelenti, hogy két lépésből álló tesztet kell elvégezni az adattovábbítás foganatosítása előtt: először is, az adatkezelés egésze megfelelő jogalappal kell hogy rendelkezzen, illetve jogszerűnek kell lennie; másodszor pedig az V. fejezetben foglalt követelményeknek is meg kell felelnie.[63]

A továbbiakban röviden ismertetésre kerülnek azok a garanciák, amelyek keretei között jogszerűen kerülhet sor nemzetközi adattovábbításra.

3.3. AZ ADATTOVÁBBÍTÁS EGYES LEGITIM ESZKÖZEI

3.3.1. ADATTOVÁBBÍTÁS MEGFELELŐSÉGI HATÁROZAT ALAPJÁN

Az első lehetőség a harmadik országokba történő adattovábbításra, ha az ország ún. megfelelőségi határozattal rendelkezik. Ez annyit jelent, hogy egy formális eljárás során a Bizottság megvizsgálta az adott harmadik ország jogi, ezen belül elsősorban (de nem kizárólagosan) adatvédelmi jogi berendezkedését, normarendszerét és annak gyakorlati érvényesülését, majd egy határozatban megállapította, hogy az adott országban a személyes adatok védelmének szintje ugyanolyan magas szinten

[60] Lásd EDPB (58. lj.) 3.
[61] Lásd Kuner (38. lj.) 28.
[62] Lásd Árvay–Balogh–Buzás–Eszteri–Hackspacher–Kiss–Majsa–Révész (40. lj.) 49.
[63] EDPB: 2/2018 sz. iránymutatás az (EU) 2016/679 rendelet 49. cikke szerinti eltérésekről. 2018. 3., *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_hu.pdf.*

van, mint az Európai Unióban, ezért ottani adatkezelők vagy adatfeldolgozók részére különösebb kockázatok nélkül továbbíthatóak az uniós érintettek személyes adatai.

A megfelelőség nem követeli meg azt, hogy a harmadik ország pontról pontra lemásolja, megismételje az uniós szabályozást. Az ilyen döntés meghozatala előtt azt a tesztet kell elvégezni, hogy az adatvédelmi szabályok tartalma, alkalmazása, hatékony kikényszeríthetősége és felügyelete összességében biztosítja-e a megkívánt védelmi szintet. Ezt az értelmezést az EUB már a GDPR hatályba lépése előtti 2015-ös Schrems I. ítéletében is hangsúlyozta.[64]

Sem korábban az Adatvédelmi Irányelv, sem jelenleg a GDPR nem tartalmaz különösebben egzakt meghatározást arra vonatkozóan, hogy mit jelent az, hogy egy adott harmadik ország megfelelő védelmi szintet biztosít. A GDPR csupán azoknak a tényezőknek a – nem kimerítő – felsorolását tartalmazza, melyeket ennek megítélésekor a Bizottságnak figyelembe kell vennie.

A Bizottság a harmadik országra vagy egy harmadik ország valamely területére vagy meghatározott ágazatára vonatkozó értékelés elkészítésekor figyelembe veszi azt, hogy az adott harmadik országban mennyire tartják tiszteletben a jogállamiságot, az igazságszolgáltatáshoz való jogot, valamint a nemzetközi emberi jogi normákat és előírásokat, valamint megvizsgálja az adott ország általános és ágazati jogszabályait, valamint közrendjét és büntetőjogát is.[65]

A követelmények megfogalmazásából következik tehát néhány alapvető elvárás, amelynek a megfelelőség megállapításához meg kell felelnie az adott harmadik országnak vagy nemzetközi szervezetnek. Ezek a követelmények iránymutatást adnak arra vonatkozóan, hogy a megfelelőséget mi alapján kell megítélni, mérlegelni.[66]

A Schrems I. ítéletben használt értelmezés szerint a „*megfelelő*" kifejezést úgy kell érteni, hogy a harmadik országnak az Unióban biztosított védelmi szinttel *lényegében azonos védelmi szintet* kell biztosítania az alapvető jogok és szabadságok számára, ezt megfelelő jogi és igazgatási eszközökkel kell biztosítania. Lényeg, hogy ezeknek az eszközöknek a gyakorlati alkalmazása az Unióban biztosított védelemmel lényegében azonos védelmet eredményezzen.[67]

A harmadik országnak különösen gondoskodnia kell a tényleges, független adatvédelmi felügyeletről és tagállami adatvédelmi hatóságokkal való együttműködési mechanizmusairól, továbbá biztosítania kell, hogy az érintettek tényleges és érvényesíthető jogokkal, valamint hatékony közigazgatási és bírósági jogorvoslati lehetőségekkel rendelkezzenek.[68]

Jelenleg összesen tizenöt olyan, az Európai Gazdasági Térségen[69] kívüli harmadik ország[70] van, amely rendelkezik érvényes megfelelőségi határozattal, ezért ezen

[64] C-362/14. számú 2015. október 5-i Maximilian Schrems kontra Data Protection Commissioner ítélet [EU:C:2015:650] 91–92. pontjai.
[65] Lásd GDPR 45. cikk (1)–(2) bekezdései.
[66] Lásd Péterfalvi–Révész–Buzás (26. lj.) 366–367.
[67] C-362/14. számú 2015. október 5-i Maximilian Schrems kontra Data Protection Commissioner ítélet [EU:C:2015:650] 72–74. pontjai.
[68] Lásd Péterfalvi–Révész–Buzás (26. lj.) 367.
[69] Az EGT tagjai az Európai Unió tagállamain kívül Norvégia, Izland és Liechtenstein is.
[70] Ezek az országok a következők a tanulmány kéziratának lezárása időpontjában: Amerikai Egyesült

országokba való adattovábbítások kapcsán a GDPR hatálya alá tartozó adatkezelőknek és adatfeldolgozóknak nem kell plusz garanciákat biztosítaniuk.

3.3.2. ADATTOVÁBBÍTÁS MEGFELELŐ GARANCIÁK ALAPJÁN

Amennyiben a Bizottság az adattovábbítás célországa vonatkozásában nem fogadott el megfelelőségi határozatot, úgy az adattovábbításra csak akkor kerülhet sor, ha az adatkezelő vagy adatfeldolgozó egyedileg dolgoz ki és nyújt megfelelő garanciákat. A GDPR ezen garanciák kapcsán kiemeli, hogy az érintettek számára hatékony jogorvoslati lehetőségeknek kell fennállnia.[71] A megfelelő garanciákat tehát mindig egyedileg kell biztosítania az adatkezelőnek vagy adatfeldolgozónak.

A garanciák megteremtésére szolgáló eszközök közül vannak olyanok, amelyek esetén az adattovábbítást az adott uniós tagállam adatvédelmi hatóságának egyedileg jóvá kell hagynia.[72] Kevésbe szigorú eset, amikor az adattovábbításhoz keretrendszerül szolgáló eszközt kell „csak" engedélyeztetni a hatósággal. Igaz, ezen utóbbi esetet a GDPR normaszövege a „külön engedélyt nem igénylő" adattovábbításokhoz sorolja, azonban fontos, hogy a keretrendszer engedélyezésére itt is szükség van.[73] Végül a hatóság külön engedélye nélkül is végezhető adattovábbítás, azonban ezekre is formális jogi keretrendszerben van lehetőség.[74]

Az alábbi táblázat a megfelelő garanciákat nyújtó eszközöket szemlélteti:

A felügyeleti hatóság külön engedélye nélküli garanciális eszköz	*A felügyeleti hatóság által jóváhagyott garanciális keretrendszer*	*A felügyeleti hatóság külön engedélyéhez kötött, jóváhagyott egyedi eszköz*
Közfeladatot ellátó szervek közötti kötelező erejű, ki kényszeríthető jogi eszköz [GDPR 46. cikk (2) bek. a)]	Jóváhagyott kötelező erejű vállalati szabályok (BCR) [GDPR 46. cikk (2) bek. b)]	Adatkezelő vagy adatfeldolgozó és a harmadik országbeli adatkezelő, adatfeldolgozó vagy a címzett közötti szerződéses rendelkezések [GDPR 46. cikk (3) bek. a)]
A Bizottság vagy az adatvédelmi felügyeleti hatóságok által elfogadott általános adatvédelmi kikötések [GDPR 46. cikk (2) bek. c)-d)]	Jóváhagyott magatartási kódex [GDPR 46. cikk (2) bek. e)]	Közhatalmi vagy egyéb, közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések [GDPR 46. cikk (3) bek. b)]
	Jóváhagyott tanúsítási mechanizmus [GDPR 46. cikk (2) bek. f)]	

Államok, Andorra, Argentína, Dél-Korea, Egyesült Királyság, Feröer-szigetek, Guernsey, Izrael, Japán, Jersey, Kanada, Man-sziget, Svájc, Új-Zéland, Uruguay. Lásd: *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.*

[71] Lásd GDPR 46. cikk (1) bekezdés.

[72] Lásd GDPR 46. cikk (3) bekezdése szerinti eszközöket.

[73] A GDPR 46. cikk (2) bekezdés (b), (e) és (f) pontjai szerint ilyen eszközök a kötelező erejű vállalati szabályok, a magatartási kódexek és a tanúsítási mechanizmusok.

[74] Lásd a GDPR 46. cikk (2) bekezdés a), c) és d) pontjai szerinti eszközöket.

Jelen tanulmány a továbbiakban a megfelelő garanciákat nyújtó adattovábbítási eszközökre vonatkozó szabályok részletes bemutatásától eltekint, mivel azok összetettsége túlmutatna annak keretein.

3.3.3. KÜLÖNÖS HELYZETEKBEN BIZTOSÍTOTT ELTÉRÉSEK

A GDPR 49. cikke felsorolja azokat a helyzeteket, amelyek esetén az adattovábbításra sor kerülhet akkor is, ha a továbbítás célországára vonatkozóan nincs elfogadott megfelelőségi határozat, illetve az adatkezelő vagy adatfeldolgozó nem biztosít megfelelő garanciákat. Jelen tanulmányban eltekintek a hivatkozott cikkben található felsorolás részletes ismertetésétől, mivel egyrészt annak keretei nem teszik lehetővé a kellően részletes elemzést, másrészt a tanulmány célja sem az adattovábbítási intézmények kommentárszerű bemutatása.

E helyütt csak utalnék arra, hogy a GDPR 49. cikke által felsorolt helyzetek tehát kivételek azon főszabály alól, hogy személyes adatok harmadik országba történő továbbítására csak akkor van lehetőség, ha a megfelelő védelmi szint biztosított az adott országban, vagy ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújt. Ez alapján, illetve tekintettel a cikk címének megfogalmazására is („különös helyzetekben biztosított"), az ott található eltéréseket szűken kell értelmezni, annak érdekében, hogy a kivétel ne váljon szabállyá.[75]

3.4. AZ ADATTOVÁBBÍTÁSI HATÁSVIZSGÁLAT (TRANSFER IMPACT ASSESSMENT)

A harmadik országokba történő adattovábbítás fentebb ismertetett általános szabályozásával kapcsolatban a GDPR-nak új értelmezési kereteket adott az EUB 2020 nyarán a Schrems II. ítéletében.[76] Az ítélet, a korábbi Schrems I. döntéshez hasonlóan az Amerikai Egyesült Államokba történő adattovábbítások kapcsán született. Az EUB olykor élesen fogalmazva az ítéletben kiemelte többek között azt is, hogy a személyes adatok harmadik országokba történő továbbítása nem lehet az EGT-ben biztosított védelem aláásásának vagy gyengítésének eszköze. A döntés szerint a harmadik országokban biztosított védelmi szintnek nem *teljesen azonosnak*, hanem *lényegében azonosnak* (az eredeti angol kifejezés szerint: *„essentially equivalent"*) kell lennie az EGT-ben biztosított védelmi szinttel.[77]

Az ítélet szerint az adatátadóként eljáró adatkezelők vagy adatfeldolgozók feladata, hogy esetről esetre és adott esetben a harmadik országbeli adatátvevővel együtt-

[75] Lásd Árvay–Balogh–Buzás–Eszteri–Hackspacher–Kiss–Majsa–Révész (40. lj.) 49.

[76] C-311/18. számú 2020. július 16-i Data Protection Commissioner kontra Facebook Ireland Ltd. és Maximilian Schrems ítélet [ECLI:EU:C:2020:559].

[77] Európai Adatvédelmi Testület (EDPB): 01/2020 számú ajánlás azon intézkedésekről, amelyek kiegészítik az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében. 2021. 3., *https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_hu_0.pdf.*

működve ellenőrizzék, hogy a megfelelőségi határozattal nem rendelkező harmadik ország joga vagy gyakorlata hatással van-e a GDPR 46. cikke szerinti adattovábbítási eszközökben foglalt megfelelő garanciák hatékonyságára. Ezekben az esetekben az EUB továbbra is nyitva hagyta annak lehetőségét, hogy az adatátadók olyan kiegészítő intézkedéseket tegyenek, amelyek pótolják a harmadik ország védelmi szintjének hiányosságait, és így az uniós jog által előírt szintre emeljék azt. Az ítélet egyébként nem pontosította, hogy ezek milyen intézkedések lehetnek.[78]

Ennek az értékelésnek az elvégzését úgy nevezett adattovábbítási hatásvizsgálatokban (Transfer Impact Assessment, a továbbiakban röviden: TIA) kezdték el dokumentálni az adattovábbításokban érintett szervezetek. Ezek a hatásvizsgálatok jellemzően eseti alapon mérlegelik a külföldi védelem szintjének megfelelőségét, amikor az adatokat általános szerződési feltételek, BCR-ok vagy más, az EU által jóváhagyott mechanizmusok alkalmazásával továbbítják.

A TIA elvégzése során különösen fontos annak értékelése, hogy a harmadik országban fennálló jogi helyzet és gyakorlat bármilyen módon hatást gyakorolhat-e az igénybe vett adattovábbítási eszközök megfelelő garanciáinak hatékonyságára. Az értékelésnek a harmadik országbeli jogszabályokra kell összpontosítania, beleértve az ország bíróságainak és hatóságainak gyakorlatát is. A cél annak eldöntése, hogy az adattovábbítási eszközben foglalt garanciák képesek-e biztosítani a gyakorlatban a továbbított személyes adatok hatékony védelmét.

A TIA elvégzése során olyan kiegészítő intézkedések azonosítása és elfogadása szükséges, amelyek mellett a továbbított adatok védelmének szintje megfelel a *lényegi azonosság* követelményének. Az EDPB a témáról és a hatásvizsgálat elvégzéséről egyébként részletes ajánlást bocsátott ki, amely a kiegészítő intézkedések példáinak és a hatékonyságukhoz szükséges egyes feltételeknek a nem kimerítő jellegű felsorolását is tartalmazza.[79]

Igaz, a Schrems II. ítélet az Amerikai Egyesült Államokba történő adattovábbítások kapcsán született, azonban annak általános megállapításai érvényesek bármilyen olyan harmadik országba történő adattovábbításra, amelyik nem rendelkezik a Bizottság által kiadott megfelelőségi határozattal.

4. ADATTOVÁBBÍTÁS AZ AMERIKAI EGYESÜLT ÁLLAMOKBA: EGY VISSZATÉRŐ AKUT PROBLÉMA

Az Európai Unió és az Amerikai Egyesült Államok adatvédelmi szabályozása között több nagy különbség is mutatkozik. Így például az amerikai jogrendszerben nincsen általános adatvédelmi keretnorma, ezért alapvetően szektorális szabályokra épül az adatvédelem.[80] Ezért már korábban is az USA-ba történő adattovábbítások kapcsán a Bizottság speciálisabb, összetettebb helyzetet teremtető megfelelőségi határozatai voltak érvényben, amelyek azonban így sem tudták biztosítani a megfelelő védel-

[78] Lásd EDPB (77. lj.) 3.
[79] Lásd EDPB (77. lj.) 3. és 31–54.
[80] Lásd Szabó (34. lj.) 55.

mi szintet. A korábban érvényben lévő, azóta az EUB előtt elbukott megfelelőségi határozatok története az alábbiakban foglalható össze.

4.1. A SAFE HARBOR MEGÁLLAPODÁS ÉS ANNAK ÉRVÉNYTELENÍTÉSE

Korábban, a Bizottság által hozott határozat szerint az Amerikai Egyesült Államok megfelelő védelmi szintet biztosított abban az esetben, ha a személyes adatok továbbítása a határozat mellékleteit képező, a Bizottság és az USA Kereskedelmi Minisztériuma (Department of Commerce, a továbbiakban: DoC) között létrejött, ún. Safe Harbor megállapodásban meghatározott elvekkel összhangban történt. A megállapodás, illetve a határozat alapján létrejött az USA-ban egy keretrendszer, mely alapján valamely szervezetnek a Safe Harbor elvekhez való csatlakozására egy öntanúsítási rendszer alkalmazása révén került sor.[81]

Az amerikai egyesült államokbeli adatkezelők, adatfeldolgozók nagyon nagy számban végezték el az öntanúsítást, ezáltal számos, a számukra személyes adatot továbbító uniós adatkezelő és adatfeldolgozó hivatkozott arra, hogy az adott szervezet vonatkozásában az USA megfelelő védelmi szintet biztosít.

A keretrendszert azonban számos kritika érte, például annak önkéntes jellegére, valamint a hatékony jogorvoslat hiányára tekintettel. A helyzet akkor eszkalálódott, amikor 2013-ban kitört az ún. megfigyelési botrány (ez volt a titkosszolgálati dokumentumokat kiszivárogtató korábbi tisztviselő neve után Snowden-botrányként[82] elhíresült eset), mely alapján bizonyossá vált, hogy a személyes adatokhoz az USA hatóságai általi – például nemzetbiztonsági célból történő – hozzáférésére vonatkozó jogszabályokkal kapcsolatban megfogalmazott kritikák alaposak. Ezek többek között kiemelték, hogy az amerikai titkosszolgálatok teljesen parttalanul, az európai értelemben vett célhoz kötöttség elvét teljesen kiüresítve tárolták el, és fértek hozzá az internetes kommunikációs csatornákhoz és így többek között az Európai Unióból érkező személyes adatokhoz is.[83]

Ennek megfelelően a Bizottság megfelelőségi határozataként funkcionáló Safe Harbor megállapodást az EUB 2015. október 6-án a már többször hivatkozott Schrems I. ügyben hozott ítéletében érvénytelenné tette. Erre többek között az került sor, mivel a Bizottság határozatában nem indokolta meg kellően, illetve abban nem állapította meg, hogy az Amerikai Egyesült Államok belföldi joga vagy vállalt nemzetközi kötelezettségei alapján ténylegesen megfelelő védelmi szintet biztosít-e. Az

[81] A Bizottság 2000/520/EK határozata (2000. július 26.) 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.

[82] Glenn Greenwald – Ewen MacAskill – Laura Poitras: „Edward Snowden: the whistleblower behind the NSA surveillance revelations" *The Guardian* 2013. június 11., *https://theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.*

[83] A Bizottság 2013/0847 közleménye az Európai Parlamentnek és a Tanácsnak a védett adatkikötő működése az uniós polgárok és az EU-ban letelepedet vállalatok szempontjából, *https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013DC0847&from=NL.*

ítélet arra is rámutatott, hogy a megfelelőségi határozat megfosztotta, illetve korlátozta az uniós nemzeti adatvédelmi felügyeleti hatóságoknak a korábbi Adatvédelmi Irányelvből fakadó jogköreit.[84] Az EUB talán egyik legsarkosabb megállapítása az volt, hogy az USA nemzetbiztonsági szolgálatai *általános jelleggel, korlátozás nélkül hozzáférnek az elektronikus kommunikációk tartalmához, ezt pedig úgy kell tekinteni, hogy az a magánélet tiszteletben tartásához való, az Európai Unió Alapjogi Chartája 7. cikkében biztosított alapvető jog lényegét sérti. Erre pedig a megfelelőségi határozat semmilyen további garanciát, hatékony jogorvoslati lehetőséget nem biztosított.*[85] Mindezek alapján a megfelelőségi határozat érvénytelenségét mondta ki az ítélet, így az adattovábbítások kapcsán új eszközre volt szükség, mivel a Safe Harborra a továbbiakban az adatkezelők nem hivatkozhattak.

4.2. A PRIVACY SHIELD MEGÁLLAPODÁS ÉS ANNAK ÉRVÉNYTELENÍTÉSE

A Schrems I. döntés következményeként beálló rendkívül bizonytalan helyzet megoldása érdekében a Bizottság szinte azonnal tárgyalásokba kezdett az USA-val annak érdekében, hogy létrehozzanak egy új keretrendszert. Ez az új megállapodás a Privacy Shield („Adatvédelmi Pajzs") elnevezést kapta, amely a Bizottság 2016. július 12-én kiadott megfelelőségi határozatában öltött testet.[86]

Az így létrejött Privacy Shield keretrendszer alkalmazása továbbra is önkéntes volt, vagyis öntanúsításon alapult, azonban kiegészült további garanciákkal. Ezek a garanciák több jogorvoslati lehetőség biztosítását tartalmazták az érintettek számára, kialakítottak egy ún. ombudsmani mechanizmust, illetve az uniós adatvédelmi hatóságokkal történő együttműködési eljárást.[87]

Az öntanúsítást elvégző szervezetekre vonatkozó és betartandó alapelvek hasonlóak voltak a korábbi Safe Harbor megállapodásban is szereplőkkel. A Privacy Shield ezek mellett megkövetelte, hogy az öntanúsítást elvégző szervezetek alávessék magukat számos vitarendezési, jogorvoslati mechanizmusnak, például a munkaviszony keretében gyűjtött humánerőforrás-adatok nemzetközi továbbítása során. Az érintett szervezetek kötelesek voltak együttműködni az uniós adatvédelmi felügyeleti hatóságok általi vizsgálat és panaszrendezés során.[88]

Nem kellett sok idő, és az EUB elé került a nagy reményekkel megalkotott Privacy Shield megállapodás is, mivel azt is számos kritika érte, többek között az elégtelen jogorvoslati lehetőségek, valamint az USA jogrendszerében fennálló, az adatvédelmet érintő korlátozások továbbra is aggasztó mértéke miatt.

[84] C-362/14. számú 2015. október 5-i Maximilian Schrems kontra Data Protection Commissioner ítélet [EU:C:2015:650] 79-106. pontjai.
[85] C-362/14. számú 2015. október 5-i Maximilian Schrems kontra Data Protection Commissioner ítélet [EU:C:2015:650] 92. pont.
[86] A Bizottság 2016/1250/EU végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről.
[87] Lásd Péterfalvi–Révész–Buzás (26. lj.) 371.
[88] Lásd Péterfalvi–Révész–Buzás (26. lj.) 371.

A Privacy Shield megállapodás 2017-es első felülvizsgálatáról az európai adatvédelmi hatóságokat tömörítő – az EDPB jogelődjének tekinthető – 29-as Munkacsoport jelentése is számos kritikus pontot emelt ki, különösen a nemzetbiztonsági megfigyelési programok és az ombudsmani mechanizmus kapcsán. Így például az újonnan kialakított ombudsmani mechanizmus csak papíron létezett, a hozzá beérkező panaszok eljárásrendje egy államtitoknak minősített dokumentumban volt részletezve, továbbá annak a végrehajtó hatalomtól való függetlenségével kapcsolatban is aggályok merültek fel. Az USA nemzetbiztonsági szervei általi hozzáférések célhoz kötöttsége és annak szabályozása (illetve leginkább annak hiánya) szintén továbbra is a kritikák kereszttüzében állt.[89]

Az EUB végül 2020. július 16-án az ún. Schrems II. ügyben hozott döntésében fogalmazta meg álláspontját. Az ítélet szerint az USA által alkalmazott megfigyelési programokra vonatkozó jogszabályok nem biztosítanak az érintettek számára olyan jogokat, amelyek az amerikai hatóságokkal szemben érvényesíthetőek a bíróságok előtt, vagyis az érintettek nem rendelkeznek hatékony jogorvoslathoz való joggal.[90]

Az ombudsmani mechanizmussal kapcsolatban megállapította továbbá az EUB, hogy az nem biztosít jogorvoslati lehetőségeket olyan szerv előtt, amely az Unióban az Alapjogi Charta 47. cikkében előírt garanciákkal lényegében azonos garanciákat nyújtana azon személyek számára, akiknek a személyes adatait az USA-ba továbbították. A döntés ezzel kapcsolatban külön kiemelte, hogy *„semmilyen* […] *utalás nincs arra vonatkozóan, hogy az ombudsmannak felhatalmazása lenne arra, hogy a nemzetbiztonsági szervezetekkel szemben kötelező erejű határozatokat hozzon.”*[91]

Az EUB már a korábbi Schrems I. döntésében is kimondott, az USA hatóságai általi tömeges megfigyelésekre alapuló megállapításait is megerősítette a Schrems II. döntésében is. Az ítélet hangsúlyozta, hogy a tömeges adatgyűjtés lehetősége, *„amely az EO 12333-on*[92] *alapuló megfigyelési programok keretében megengedi az Amerikai Egyesült Államokba továbbított adatokhoz való hozzáférést anélkül, hogy e hozzáférés bármiféle bírósági felügyelet alá tartozna, semmi esetre sem szabályozza kellőképpen egyértelműen és pontosan a személyes adatok ilyen tömeges gyűjtésének terjedelmét.”*[93]

Az EUB a fentiek miatt arra a megállapításra jutott, hogy a Bizottság megsértette a GDPR megfelelőségi határozatokra vonatkozó követelményeit, mivel olyan megfelelőségi határozatot adott ki az USA vonatkozásában, amely a valóságban

[89] 29. cikk Szerinti Adatvédelmi Munkacsoport: EU – U.S. Privacy Shield – First annual Joint Review (WP 255) 2017. 31–34 és 35–37., *https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782*.

[90] C-311/18. számú 2020. július 16-i Data Protection Commissioner kontra Facebook Ireland Ltd. és Maximilian Schrems ítélet [ECLI:EU:C:2020:559] 178–185. pontjai.

[91] C-311/18. számú 2020. július 16-i Data Protection Commissioner kontra Facebook Ireland Ltd. és Maximilian Schrems ítélet [ECLI:EU:C:2020:559] 196. pont.

[92] *Executive Order 12333 on United States Intelligence Activities* [1981. december 4.] *https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf*.

[93] C-311/18. számú 2020. július 16-i Data Protection Commissioner kontra Facebook Ireland Ltd. és Maximilian Schrems ítélet [ECLI:EU:C:2020:559] 183. pont

egyébként nem biztosítja a megfelelő védelmi szintet a személyes adatok továbbítása kapcsán. Hasonlóan a korábbi Safe Harbor megállapodáshoz, a Privacy Shield határozatról is kimondta ezért az EUB, hogy érvénytelen.[94]

Az ítélet folyományaképpen a 2020 nyara és 2023 nyara közötti nagyjából hároméves időszakban nem volt érvényes megfelelőségi határozat az EU–USA adattovábbítások viszonylatában. Ez a probléma egyébként nem egy hatósági döntésben visszaköszönt. Így például az ír adatvédelmi hatóság által kezdeményezett eljárásban a Meta Platforms Ireland Limited által nyújtott Facebook-szolgáltatáshoz kapcsolódó adattovábbításokat illetően 1,2 milliárd eurós bírságot szabtak ki azért, mert nem voltak megfelelőek azok a szerződéses rendelkezések, amelyek szerint a cég az EU-ból az USA-ba továbbította a Facebook-felhasználók bizonyos személyes adatait.[95] A végleges döntés nagy hangsúlyt helyezett arra, hogy mivel annak meghozatala idején az USA nem rendelkezett érvényes megfelelőségi határozattal az adattovábbításokról, ezért a plusz adatvédelmi garanciákat a Meta-nak kellett volna megteremtenie megfelelő szerződéses rendelkezésekkel, amelyek azonban nem érvényesültek a gyakorlatban.[96]

4.3. A DATA PRIVACY FRAMEWORK, AVAGY A JELENLEGI ADATTOVÁBBÍTÁSI KERETRENDSZER AZ EU ÉS AZ USA VONATKOZÁSÁBAN

Az USA elnöke 2022 októberében aláírta a 14086. számú végrehajtási rendeletet,[97] amely előírta olyan új, kötelező erejű biztosítékok bevezetését, amelyek szerint az amerikai hírszerző szolgálatoknak az uniós érintettek adataihoz való hozzáférései során a szükségesség és arányosság elve szerinti korlátok kell hogy érvényesüljenek. A végrehajtási rendelet előírja többek között olyan eljárási rend biztosítását, amely alapján az amerikai hírszerzési tevékenységet végző szolgálatok kizárólag meghatározott nemzetbiztonsági célok elérése érdekében végezhetnek megfigyelő tevékenységet. Ennek során figyelembe veszik minden személy magánélethez való jogát és polgári szabadságjogait, állampolgárságtól vagy lakóhely szerinti országtól függetlenül. A megfigyelés csak akkor hajtható végre, ha az egy jóváhagyott hírszerzési prioritás előmozdításához szükséges, és csak az adott prioritással arányos mértékben és módon. A végrehajtási rendelet ezek mellett előírt egy teljesen új eljárási mechanizmust, azon érintett személyek részére, akik az adataik kezelésével kapcsolatban jogorvoslattal kívánnak élni az amerikai nemzetbiztonsági hatóságok

[94] C-311/18. számú 2020. július 16-i Data Protection Commissioner kontra Facebook Ireland Ltd. és Maximilian Schrems ítélet [ECLI:EU:C:2020:559] 199–201. pontjai.

[95] Európai Adatvédelmi Testület (EDPB): 1/2023. számú kötelező erejű határozat az ír felügyeleti hatóság által benyújtott, a Meta Platforms Ireland Limited által a Facebook-szolgáltatásai számára végzett adattovábbításokról (az általános adatvédelmi rendelet 65. cikk). 2023, *https://edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_hu.pdf*.

[96] Data Protection Commissioner of Ireland IN-20-8-1. számú határozata, *https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf*.

[97] *Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities* [2022. október 7.], *https://state.gov/executive-order-14086-policy-and-procedures/*.

őket érintő megfigyelési tevékenységeivel kapcsolatban.[98] A rendelet megteremtette a hátterét annak, hogy a Bizottság új megfelelőségi határozat kiadását kezdje meg az USA vonatkozásában.

Végül hosszas tárgyalások és egyeztetések után 2023. július 10-én a Bizottság elfogadta az EU–USA adatvédelmi keretrendszerről (EU–US Data Privacy Framework, a továbbiakban röviden: DPF) szóló legújabb megfelelőségi határozatot[99], amely a GDPR 45. cikkével összhangban kimondja, hogy az USA az Európai Unióból a DPF keretrendszerben részt vevő amerikai szervezetek részére továbbított személyes adatok tekintetében megfelelő szintű védelmet biztosít.

A DPF keretrendszerben részt vevő egyesült államokbeli szervezetek részére történő adattovábbításra anélkül kerülhet így sor, hogy a GDPR 46. cikke szerinti adattovábbítási eszközökre kellene támaszkodni, tehát ezekre az adattovábbításokra nem kell további kiegészítő intézkedéseket alkalmazni.

4.3.1. EGY RÉGI-ÚJ MEGOLDÁS: AZ ÖNTANÚSÍTÁSI RENDSZER

A DPF a Privacy Shield-hez és a Safe Harbor-hoz hasonlóan megtartotta az öntanúsítási mechanizmust, tehát az adattovábbításban érintett amerikai szervezetek a továbbiakban is úgy fogadhatnak személyes adatokat adattovábbítás keretei között az Európai Unióból, ha előtte végigmentek az öntanúsítási lépéseken, és megkapták ennek megfelelően a DPF tanúsítványt.

A DPF tanúsítvánnyal rendelkező szervezetek listáját a DoC a rendszeresen frissülő honlapján teszi közzé, amely szabadon elérhető és ellenőrizhető bárki számára.[100] A tanúsítvány kiállításához szükséges kritériumrendszer követelményei szintén bárki számára elérhetők a DoC honlapján.

A DPF-be való belépéshez a szervezetnek az USA Szövetségi Kereskedelmi Bizottsága (Federal Trade Commission, a továbbiakban röviden: FTC), az USA Közlekedési Minisztériuma (Department of Transport, a továbbiakban röviden: DoT) vagy más vizsgálati és végrehajtási hatáskörrel rendelkező szerv ellenőrzése alá kell tartoznia. A DPF-be belépő szervezetnek nyilvánosságra kell hoznia adatvédelmi szabályzatát, és teljes mértékben elszámoltathatónak kell lennie annak végrehajtása kapcsán. Az elvek be nem tartása kapcsán az FTC vizsgálati jogkörrel rendelkezik, és ennek keretein belül, mint egyfajta tisztességtelen vagy megtévesztő kereskedelmi gyakorlatot és cselekményeket – akár bírság kiszabásával is – szankcionálhatja.[101]

A DoC emellett nyilvántartást vezet és tesz elérhetővé a nyilvánosság számára azokról az egyesült államokbeli szervezetekről, amelyek korábban öntanúsítással

[98] Lásd: *https://whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.*

[99] *COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.*

[100] Lásd: *https://dataprivacyframework.gov/list.*

[101] Lásd: *https://dataprivacyframework.gov/framework-article/OVERVIEW.*

rendelkeztek, de már eltávolították őket a DPF listájáról. A DPF listájáról való törlés azt jelenti, hogy az ilyen szervezetek nem állíthatják, hogy megfelelnek a DPF-nek, és kerülniük kell minden olyan nyilatkozatot vagy félrevezető gyakorlatot, amely azt sugallja, hogy részt vesznek abban. Az a szervezet, amely továbbra is azt állítja, hogy részt vesz a DPF-ben, vagy más ezzel kapcsolatos megtévesztő nyilatkozatokat tesz, miután eltávolították a listájáról, az FTC, a DoT vagy más hatóságok eljárásait vonhatja maga után, és ezek következményeképp szankcionálható.[102]

A DoC vonatkozó eljárásai, hatáskörei és az öntanúsítási mechanizmus az USA-ba történő adattovábbítás kevésbé kritizált részei közé tartoznak, az azokkal kapcsolatos kifogások kevésbé hangsúlyosan jelentek meg az irodalomban és az EUB döntéseiben. A védelmi szinttel kapcsolatos főbb kritikák inkább az USA nemzetbiztonsági szerveinek adathozzáféréseivel és az ezzel kapcsolatos jogorvoslati hiátusokkal voltak kapcsolatosak. Az erre vonatkozó új szabályokat a következő pontban mutatom be.

4.3.2. AZ ÚJ JOGORVOSLATI MECHANIZMUS

Azoknak a személyeknek, akiknek adatait a megfelelőségi határozat alapján továbbítják az USA-ba, több jogorvoslati mechanizmus is rendelkezésükre áll a DPF alapján. Ezt akár közvetlenül az USA-beli adatokat átvevő szervezetnél is megtehetik a GDPR szerinti érintetti joggyakorlási kérelem[103] keretében, de emellett természetesen elérhető számukra az a hagyományos út is, hogy panaszukat előterjesztik az illetékes európai adatvédelmi hatóságnál. A nemzetbiztonsági célú adatkezelések kapcsán az érintettek számára külön jogorvoslati mechanizmus is rendelkezésre áll.

A személyes adataik USA-ba történő továbbításához használt eszköztől függetlenül az uniós érintettek panaszt nyújthatnak be nemzeti adatvédelmi hatóságukhoz, hogy igénybe vegyék a nemzetbiztonsági és bűnüldözési területén alkalmazandó új jogorvoslati mechanizmust. A nemzeti adatvédelmi hatóság pedig gondoskodik arról, hogy a panaszt átadják az EDPB-nek, amely továbbítja a panaszt a panasz kezelésére illetékes egyesült államokbeli hatóságnak. Az adatvédelmi hatóság biztosítja továbbá, hogy az érintett tájékoztatást kapjon a panaszkezelési folyamatról, ideértve a benyújtott panasz kapcsán lefolytatott vizsgálat eredményeit is.

Ahhoz egyébként, hogy egy panasz kivizsgálásra a hatóságok által befogadható legyen, az egyéneknek nem kell bizonyítaniuk, hogy az adataikat az amerikai hírszerző ügynökségek ténylegesen gyűjtötték, azokat megismerték, azokhoz hozzáfértek.[104]

A nemzetbiztonsági célú adatkezelésekkel összefüggésben kialakított jogorvoslati mechanizmus kétlépcsős rendszert vázol fel, miután az európai érintett panaszát az európai adatvédelmi hatóságok – az EDPB útján – továbbították az USA-ba.

[102] Lásd: *https://dataprivacyframework.gov/framework-article/OVERVIEW*.
[103] Lásd a GDPR 12–22. cikkei.
[104] Európai Adatvédelmi Testület (EDPB): Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023. 2–3., *https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf*.

A jogorvoslat első szintjén a Nemzeti Hírszerzési Igazgató Hivatalának polgári szabadságjogok védelméért felelős tisztviselője (Civil Liberties Protection Officer in the Office of the Director of National Intelligence, a továbbiakban röviden: CLPO) végzi a panaszok első vizsgálatát, aki felelős azért, hogy az amerikai hírszerző szervezetek betartsák a magánélet védelméhez fűződő és alapvető jogokat. A jogorvoslati mechanizmus második szintjén az érintettek az USA Főügyésze (Attorney General) által létrehozott, az USA Igazságügyi Minisztériumának Department of Justice, a továbbiakban röviden: DoJ) szervezetén belül működő Adatvédelmi Felülvizsgálati Bírósághoz (Data Protection Review Court, a továbbiakban röviden: DPRC) fordulhatnak fellebbezési kérelemmel a CLPO döntése ellen. Természetesen az is előfordulhat, hogy nem az érintett, hanem a vizsgált hírszerző szerv kérelmezi a DPRC felülvizsgálati eljárását. A DPRC döntésében akár az adatok törlését is elrendelheti, amely kötelező és végleges az előtte lévő panasszal érintett adatkezelésre vonatkozóan. A DPRC döntése ellen fellebbezni vagy további jogorvoslattal élni nem lehet.[105]

A DPRC jogállása kapcsán a keretrendszer elfogadása előtt megfogalmaztak olyan szakmai kritikákat, amelyek szerint az nem felel meg a bíróságok függetlenségével kapcsolatos uniós sztenderdeknek. A kritikák alapján a DPRC a DoJ szervezetének részeként ugyanis nem független a végrehajtói hatalomtól. Azonban a DPRC elhelyezése a végrehajtó hatalmon belül szándékos és szükségszerű az USA belső joga miatt. Ennek oka, hogy az USA alkotmánya a rendes bíróságok előtti eljárás kapcsán megköveteli azt, hogy az eljárást indítványozó felperesnek tudnia kell bizonyítani, hogy „tényleges" sérelmet szenvedett el, amely valamely az alperes által okozott olyan tényleges, konkrét kárban vagy jogsérelemben kell testet öltsön, amelyet a bíróság valószínűleg orvosolni tud. Az USA bíróságai előtti kereshetőségi joggal kapcsolatban ezt a kritériumot nevezik az ún. „standing requirement"-nek. Az USA hírszerzési tevékenységeivel kapcsolatos panaszoknál viszont erre ritkán van lehetőség, mivel a panaszos rendszerint nem tudja bizonyítani az őt ért megfigyelés tényét. Az USA bíróságai így jellemzően elutasították az ilyen típusú kereseteket. Ezzel szemben a végrehajtó hatalmi ágon belüli „bíróság" akkor is elbírálhatja az érintetti panaszokat, ha a panaszosok nem rendelkeznek a III. cikk szerinti kereshetőségi joggal.[106] A DPRC jogállása és annak a végrehajtói ágba történő betagozódása az USA közjogi rendszerén belül tehát szükségszerű. Az ettől eltérő jogálláshoz valószínűleg az USA alkotmányát kellene módosítani.

Az EDPB vonatkozó, a Bizottság által a megfelelőségi határozat elfogadása előtt kikért véleménye, nagyrészt elfogadta a DPF előírásait, és azokat elégségesnek tartja a megfelelő védelmi szint garantálására. Azt azonban az EDPB is megjegyezte, hogy a felvázolt jogorvoslati rendszer megváltoztatása vagy az eljárási szabályok

[105] Európai Adatvédelmi Testület (EDPB): 5/2023. sz. vélemény a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről. 2023. 58., *https://edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_hu.pdf*.

[106] Lásd: *https://dataguidance.com/opinion/international-overview-dprc-regulations*; *https://law.cornell.edu/wex/standing*.

módosítása után szükséges lehet a keretrendszer újraértékelése.[107] Maga a DPF egyébként tartalmaz annak rendszeres felülvizsgálatára vonatkozó előírásokat, így elfogadása után egy évvel, majd később minden negyedik évben felül kell vizsgálni annak hatékonyságát és gyakorlatban való érvényesülését.[108]

Az EDPB hangsúlyozta, hogy az USA kormánya által a nemzetbiztonság területén bevezetett valamennyi biztosíték (beleértve a jogorvoslati mechanizmust is) az USA-ba továbbított valamennyi személyes adatra vonatkozik, függetlenül az alkalmazott továbbítási eszköztől. Tehát az európai érintettek nemcsak a DPF keretében, hanem bármilyen eszköz keretében továbbított személyes adattal kapcsolatban kérhetnek jogorvoslatot. Arra a kérdésre jelenleg nehéz válaszolni, hogy a DPF a jelenlegi formájában vajon megfelelő védelmi szintet biztosít-e, és nem fogja-e azt megsemmisíteni az EUB. Az ezzel kapcsolatos szerzői konklúzió a következő, záró pontban olvasható.

5. KONKLÚZIÓ

A tanulmány első felében bemutattam, hogy az Európai Unióban a széttöredezett nemzeti, majd tagállami szabályozások először az 1995-ös Adatvédelmi Irányelv egységesítési törekvései mentén kerültek közelebb egymáshoz, majd a GDPR 2018-tól való alkalmazásával váltak teljesen egységessé uniós szintén. Az Unió adatvédelmének szabályozása azonban a GDPR elfogadásával nem állt meg az uniós határok mentén, hanem az extraterritoriális hatály és a nemzetközi adattovábbítás szabályainak alkalmazásával rendkívül szélesre terjesztette ki az európai jog, amennyiben a személyes adatok kezeléséről van szó.

A harmadik országokba történő adattovábbításra vonatkozó szabályok következetes alkalmazásával és számonkérésével az elmúlt mintegy tíz évben sikerült elérni azt, hogy számos ország megpróbálja saját adatvédelmi jogi berendezkedését hozzáigazítani az uniós sztenderdekhez, amelyek leginkább a megfelelőségi határozatokban öltöttek testet. Mint láttuk, ez a legnehezebben éppen az Amerikai Egyesült Államokkal kapcsolatban ment, ahová a legtöbb európai érintett személyes adatai áramlanak át nap mint nap az online szolgáltatások igénybevétele miatt.

A kérdés, hogy vajon a GDPR nemzetközi adatáramlást megregulázó szabályai az USA-ba történő adattovábbítások kapcsán mennyire lesznek időtállók, hiszen már kétszer bebizonyosodott, hogy a két szereplő szabályozási felfogása közötti ellentétek mentén érvénytelenné lettek nyilvánítva a megfelelőségi határozatok. Felmerül a kérdés, hogy mi a garancia arra, hogy a legújabb megfelelőségi határozat, a DPF majd kiállja az EUB mércéjét, és nem lesz azt érvénytelenítő ítélet.

Véleményem szerint nem szabad letagadni, hogy az adattovábbítások kapcsán a megfelelő védelmi szint garantálására tett erőfeszítések látható eredményeket produkáltak az USA kapcsán. A Safe Harbor öntanúsítási, jogorvoslatot és érintetti

[107] Lásd EDPB (105. lj.) 52.
[108] Lásd EDPB (105. lj.) 59.

joggyakorlást szinte teljesen nélkülöző rendszere a mai napra átalakult egy kézzelfoghatóbb, eljárásában is sokkal kimunkáltabb jogorvoslati lehetőségeket és fórumokat tartalmazó rendszerré. A fejlődés jelei tehát látszanak, bár természetesen ezeket is lehet bőven kritizálni, mint ahogy az Európai Parlament is megtette azt határozatában.[109]

Véleményem szerint az EU és USA közötti adattovábbítási viszonyban a mai napig érzékelhető alapvető feszültséget a bizalom hiánya okozza, amelyet a 2013-as lehallgatási botrány óta nem sikerült helyreállítani. Mindig ugyanahhoz a kérdéshez térünk ugyanis vissza: mi garantálja majd azt, hogy az amerikai titkosszolgálatok nem gyűjtik majd tömegesen a kommunikációs adatokat, hogy így lehallgassák az európai érintetteket? Ez azonban alapvetően nem jogi kérdés. A szabályozás ugyanis lehet bármennyire is progresszív, előremutató és részletes, az elkártyázott bizalmat csak hosszú-hosszú idő után lehet visszanyerni, ha vissza lehet egyáltalán.

Az EU USA iránti bizalmának esetleges közeljövőben való visszanyerése kérdésében jelen sorok írója szkeptikus, a jogi szabályozás fejlődése terén azonban látja az előremutató jeleket. Vannak azonban olyan sebek és sérelmek, amiket a jogi szabályozás nem, csak az idő gyógyíthat be vagy feledtethet el végleg.

[109] Az Európai Parlament 2023. május 11-i állásfoglalása az EU–USA adatvédelmi keret által nyújtott védelem megfelelőségéről (2023/2501(RSP), *https://europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html*.