DOI 10.26521/profuturo/2024/1/15320

Joggyakorlat

Kis Kelemen Bence*

Schrems III, avagy mi lesz veled, transzatlanti adattovábbítás? Gondolatkísérlet az EU–USA Adatvédelmi Keretrendszer Határozat érvényességéről

Schrems III or What Will Happen with Transatlantic Data Transfers? – A Thought Experiment on the Validity of the EU-USA Data Privacy Framework Decision

Absztrakt

Az Amerikai Egyesült Államok és Európa egymás legfontosabb együttműködő partnerei. Ebbe természetesen beletartozik a személyes adatok továbbítására épülő gazdasági kapcsolat is. A transzatlanti adattovábbítás az elmúlt közel egy évtizedben csak folyamatos jogi bizonytalanságok között működhetett az Európai Bizottság megfelelőségi határozatainak sorozatos érvénytelenítése és az általános szerződési feltételek alkalmazhatóságának problémái miatt. Ezek a kihívások jelenleg látszólag megoldódtak az EU–USA Adatvédelmi Keretrendszer Határozatnak köszönhetően, azonban már e bizottsági határozatot is megtámadták, illetve várhatóan az idei évben indul egy újabb eljárás is. A tanulmány célja, hogy gondolatkísérletként elvégezze az említett határozat érvényességének vizsgálatát, amely iránymutató lehet a későbbi joggyakorlat számára, illetve előrejelzést adhat a gazdaság szereplőinek a jövőben várható fejleményekről. A dolgozat végkövetkeztetése, hogy az alapvető jogok változatlan sérelme okán az EU–USA Adatvédelmi Keretrendszer Határozat valószínűleg érvénytelen.

Kulcsszavak: *adattovábbítás, GDPR, USA, Schrems, Adatvédelmi Keretrendszer Határozat, Európai Unió*

* Dr. Kis Kelemen Bence, egyetemi adjunktus, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Nemzetközi- és Európajogi Tanszék. E-mail: kis.kelemen.bence@ajk.pte.hu. A Kulturális és Innovációs Minisztérium ÚNKP-23-4 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült. Köszönettel tartozom Kiss Mátyásnak a tanulmányhoz nyújtott kutatástámogatási tevékenységéért.

Abstract

The United States of America and Europe are each other's most important cooperative partners. This naturally includes the economic relationship based on the transfer of personal data. Over the past nearly decade, this transatlantic data transfer has operated amid continuous legal uncertainties due to the repeated invalidation of the European Commission's adequacy decisions and issues related to the applicability of standard contractual clauses. The problem appears to be currently resolved thanks to the EU-US Data Privacy Framework Decision. However, this Commission decision has already been challenged, and a new procedure is expected to begin this year. The purpose of this study is to conduct a thought experiment to examine the validity of the mentioned decision, which could serve as guidance for future legal practice and provide forecasts for economic actors about expected developments. The paper's conclusion is that due to the unchanged violation of fundamental rights, the EU-US Data Privacy Framework Decision is likely invalid.

Keywords: *data transfer, GDPR, USA, Schrems, Data Privacy Framework Decision*

2023-ban a transzatlanti gazdaság értéke 7100 milliárd amerikai dollár volt. Az Amerikai Egyesült Államok és Európa egymás legfontosabb piacai és geoökonómiai partnerei.[1] A transzatlanti adattovábbítás pedig kritikus az előbb említett gazdasági együttműködés eléréséhez. Ez az adattovábbítás teszi ki Európa és az Egyesült Államok adattovábbításainak körülbelül felét, továbbá az EU-ban letelepedett vállalkozások 90%-a továbbít adatokat az Egyesült Államokba, vagy fogad adatokat innen.[2] Ennek ellenére nehéz megbecsülni ennek az adattovábbításnak a pontos értékét.[3]

Mindezek alapján nem meglepő, hogy az Európai Unió adatvédelmi szabályrendszere is különös figyelmet szentel ennek a gazdasági együttműködésnek. Az Általános Adatvédelmi Rendelet, azaz a GDPR[4] például már a (101)-es preambulumbekezdésében kiemeli, hogy *„[a] nemzetközi kereskedelem és a nemzetközi együttműködés bővítéséhez szükség van a személyes adatoknak az Unión kívüli országok és a nemzetközi szervezetek viszonylatában megvalósuló forgalmára".*[5] Az adatforgalom növekedésével természetesen előtérbe kerülnek az ehhez kapcsolódó adatvédelmi jogi kihívások is, amelyek középpontjában az a követelmény áll, hogy az adattovábbítások nem csorbíthatják az érintetteket egyébként megillető jogosultságokat.[6] A GDPR a fenti célok biztosítása érdekében szigorú szabályok betartása mellett teszi

[1] Hamilton, Daniel S.–Quinlan, Joseph P.: *The Transatlantic Economy 2023. Annual Survey of Jobs, Trade and Investment between the United States and Europe.* Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network, Washington, DC, 2023. ii.

[2] Hamilton–Quinlan: i. m., viii.

[3] Hamilton–Quinlan: i. m., 72.

[4] 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). HL L 119., 2016.5.4., 1–88.

[5] GDPR (101) preambulumbek.

[6] GDPR (101) preambulumbek.

csak lehetővé a hatálya alá tartozó adatkezelők számára, hogy személyes adatot továbbítsanak az Európai Unió területén kívülre, azaz harmadik országba, így tehát mások mellett az USA-ba is.

Az Egyesült Államokba történő adattovábbítás ténye, illetve az adattovábbításra épülő gazdasági modell az elmúlt közel egy évtizedben folyamatos jogi kockázatot jelentett az érintett vállalkozásoknak. Elegendő utalni arra, hogy sajtóértesülések szerint a Facebook és Instagram szolgáltatásokat működtető *Meta Platforms* 2022-ben arra figyelmeztetett, hogy ha nem oldódik meg az adattovábbítás körüli jogi bizonytalanság, valószínűleg el kell hagynia az öreg kontinenst.[7] Ugyan a *Meta Platforms* később cáfolta ezeket a híreket, jelezte, hogy a vállalkozásoknak szükségük van arra, hogy tisztán lássanak az ilyen és ehhez hasonló szabályozási kérdésekben.[8]

A fentiekben vázolt jogi bizonytalanság az adattovábbítás körül arra vezethető vissza, hogy az Európai Unió Bírósága (a továbbiakban: EUB vagy Bíróság) már két alkalommal nyilvánította érvénytelennek az Európai Bizottság azon határozatait, amelyek alapján az USA az Európai Unióhoz hasonló, azzal egyenértékű védelmet biztosít a személyes adatoknak. Ez képezi ugyanis az adattovábbítás uniós jogi megfelelőségének mércéjét: az, hogy az adattovábbítás címzett állama az uniós joggal lényegében megegyező védelmi szintet biztosítson a személyes adatoknak.

Az Európai Bizottság elsőként még a GDPR-t megelőző uniós szabályozás, az úgynevezett Adatvédelmi Irányelv[9] alapján adta ki a Biztonságos Kikötő Határozatot,[10] amely lehetőséget biztosított a keretrendszerben részt vevő szervezetek számára a további garanciák nélküli transzatlanti adattovábbításra. E határozat érvénytelenségét mondta ki az EUB 2015. október 6-án az azóta adatvédelmi aktivistává váló jogász és Facebook-felhasználó *Maximillian Schrems* keresete alapján, amelyet az ír adatvédelmi hatósághoz benyújtott panaszának elutasítása miatt indított (a továbbiakban: *Schrems I ítélet*). Az ítélet lényege dióhéjban az volt, hogy a Bíróság kifogásolta az Egyesült Államok hatóságainak általános, valódi korlátozásoktól mentes hozzáférési lehetőségét az európaiak személyes adataihoz, és azt is, hogy ehhez a magánszférába történő beavatkozáshoz nem kapcsolódik hatékony jogorvoslati lehetőség.[11]

[7] Davies, Pascale: Meta warns it may shut Facebook in Europe but EU leaders say life would be 'very good' without it. *Euronews,* 2022. február 7. https://www.euronews.com/next/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe-over-data-transfer-issues (2024. 07. 16.).

[8] Reinisch, Markus: Meta is Absolutely Not Threatening to Leave Europe. *Meta,* 2022. február 8. https://about.fb.com/news/2022/02/meta-is-absolutely-not-threatening-to-leave-europe/ (2024. 07. 16.).

[9] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. HL L 281., 1995.11.23., 31–50.

[10] A Bizottság 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. HL L 215., 2000.8.25., 7–47.

[11] C-362/14. sz. *Maximillian Schrems kontra Data Protection Commissioner* ügyben 2015. október 6-án hozott ítélet (ECLI:EU:C:2015:650). Az ügy azért az ír hatóság, illetve ír bíróság előtt indult, mert a Facebook szolgáltatásaival volt kapcsolatos, az Európai Unióban pedig az akkori Facebook a *Facebook Ireland Ltd.*-n keresztül nyújtotta szolgáltatásait. Ma ezt a szerepet a *Meta Platforms Ireland Ltd.* tölti be. https://www.facebook.com/privacy/policy/?entry_point=comet_dropdown (2024. 07. 16.). Az ügyet részletesen elemzi az 1.2. alpont.

Az Európai Bizottság viszonylag gyorsan reagált a kialakult helyzetre, és 2016-ban, még mindig az Adatvédelmi Irányelv hatálya alatt, elfogadta az Adatvédelmi Pajzs Határozatot,[12] figyelemmel a *Schrems I ítélet* megállapításaira és az USA jogrendszerével kapcsolatos elvárásokra. Az Adatvédelmi Pajzs Határozat egyik legnagyobb újítása a korábbi keretrendszerhez képest, hogy nagyban épít az Egyesült Államok által létrehozott új, a nemzetbiztonsági beavatkozásokkal foglalkozó felügyeleti mechanizmusra, az adatvédelmi ombudsmanra.[13] Végül az Adatvédelmi Pajzs Határozat sem bizonyult hosszú életűnek, hiszen szintén Schrems úr kezdeményezésére a Bíróság megállapította a bizottsági határozat érvénytelenségét (a továbbiakban: *Schrems II ítélet*). A döntés háttérében ismét az állt, hogy az USA nem biztosít megfelelő jogorvoslati lehetőséget az érintettek számára az állami beavatkozásokkal szemben, amely beavatkozások a kisebb amerikai jogi változások ellenére valódi korlátozástól mentesek maradtak.[14]

A *Schrems II ítéletet* egy viszonylag hosszú reflexiós periódus követte, amely során az USA és az Európai Unió tárgyalások sorával próbálta tető alá hozni az új adattovábbítási keretrendszert. A több mint egyéves tárgyalások eredményeképpen 2022. március 25-én az Európai Bizottság és az Egyesült Államok bejelentette, hogy elvi szinten megállapodtak az új transzatlanti adattovábbítási keretrendszerről.[15] E megállapodásból több mint egy évvel később, 2023. július 10-én született megfelelőségi határozat EU–USA Adatvédelmi Keretrendszer Határozat néven.[16]

Az EU–USA Adatvédelmi Keretrendszer Határozat hírére a Schrems úr nevével fémjelzett NOYB adatvédelmi aktivista civil szervezet már 2022 végén bejelentette, hogy az USA jogrendszerében bekövetkezett változások valószínűleg nem felelnének meg az EUB elvárásainak.[17] A szervezet a tanulmány írásának időpontjában még nem indította el az eljárást, ugyanakkor reményeik szerint 2024-ben még sort kerítenek rá.[18] Egy másik eljárás azonban folyamatban van: *Philippe Latombe,* a francia Nemzetgyűlés tagja 2023. szeptember 6-án nyújtott be keresetet a Törvényszéken az Európai Bizottság ellen, az EU–USA Adatvédelmi Keretrendszer Határozat megsemmisítése érdekében.[19] Az ügyben egyelőre egy ideiglenes intézkedés iránti kérelmet elutasító végzés született.[20]

[12] A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről. HL L 207., 2016.8.1., 1–112.

[13] Adatvédelmi Pajzs Határozat (65) preambulumbek.

[14] C-311/18. sz. *Data Protection Commissioner kontra Facebook Ireland Limited, Maximillian Schrems* ügyben 2020. július 16-án hozott ítélet (ECLI:EU:C:2020:559). Az ügyet részletesen elemzi az 1.2. alpont.

[15] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. Európai Bizottság, 2022. március 25. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (2024. 07. 16.).

[16] A Bizottság (EU) 2023/1795 végrehajtási határozata (2023. július 10.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatoknak az EU–USA adatvédelmi keret által biztosított megfelelő szintű védelméről. HL L 231., 2023.9.20., 118–229.

[17] Statement on EU Commission adequacy decision on US. NOYB, 2022. december 13. https://noyb.eu/en/statement-eu-comission-adequacy-decision-us (2024. 07. 16.).

[18] Elektronikus levelezés a NOYB szervezettel. Fellelhető a Szerzőnél.

[19] T-553/23. sz. *Latombe kontra Bizottság* ügyben 2023. szeptember 6-án benyújtott kereset (ECLI:EU:T:2023:621).

[20] T-553/23. R. sz. *Latombe kontra Bizottság* ügyben a Törvényszék elnökének 2023. október 12-i végzése (ECLI:EU:T:2023:621).

E tanulmány célja tehát, hogy egy gondolatkísérletként szolgáljon. A tanulmányban arra a kérdésre keresem a választ, hogy hogyan döntene az EUB a jelenleg hatályos Adatvédelmi Keretrendszer Határozat érvényességi vizsgálata során. Ennek érdekében elsőként bemutatom a GDPR harmadik országba és nemzetközi szervezet részére történő adattovábbításra vonatkozó szabályrendszerét és az úgynevezett „Schrems-tesztet", amelyet a Bíróság *Schrems I* és *Schrems II ítéleteinek* fényében állapíthatunk meg. E teszt arra szolgál, hogy vizsgálhatóvá váljon az adattovábbítás egyik jogalapjaként[21] azonosítható, az Európai Bizottság által elfogadott megfelelőségi határozat,[22] miszerint egy harmadik ország az EU-val lényegében egyenértékű védelmet biztosít a személyes adatok számára (1. pont).[23] Ezt követően rátérek az Adatvédelmi Keretrendszer – mint a fentiekben bemutatott bizottsági megfelelőségi határozat – érvényességi vizsgálatának szempontjából releváns elemekre, kiegészítve azt az Egyesült Államok jogának új, az Adatvédelmi Keretrendszer elfogadásához kapcsolódó forrásaival (2. pont). Ezek alapján lehetőség nyílik elvégezni a Schrems-tesztet az Adatvédelmi Keretrendszerrel létrehozott új adattovábbítási szabályozási rendszeren (3. pont), majd levonom a következtetéseket (4. pont).

A tanulmány végkövetkeztetése az, hogy az Európai Bizottság által elfogadott harmadik megfelelőségi határozat valószínűleg azonos sorsra fog jutni, mint elődei, azaz az EUB végül az érvénytelenség kimondása mellett dönt majd (a továbbiakban ezt a lehetséges döntést *Schrems III*-ként említem). Mindez azt jelenti, hogy a vállalkozásoknak tanácsos alternatív, alapvetően technikai és üzleti megoldásokat keresni az adattovábbításból származó jogi kockázatok kezelése érdekében. Kiemelem ugyanakkor, hogy a tanulmánynak nem célja az EU és USA közötti adattovábbítási rendszerekhez kapcsolódó eddigi kudarc okainak vizsgálata, ez ugyanis szétfeszítené a dolgozat fenti gondolatkísérletre fókuszáló kereteit.

1. Adattovábbítás harmadik országba a GDPR alapján és a Schrems-teszt

Ebben a pontban elsőként felvázolom a harmadik országba történő személyes adattovábbítás jogszabályi hátterét, kiegészítve a vonatkozó hatósági gyakorlattal és alapvető kommentárirodalommal (1.1. alpont). Ezt követően az EUB esetjoga, illetve a szakirodalom alapján bemutatom a Schrems-tesztet, amely alapján megítélhető az Európai Bizottság által elfogadott megfelelőségi határozatok érvényessége vagy érvénytelensége (1.2. alpont).

[21] GDPR 44. cikk.

[22] GDPR 45. cikk (1) bek.

[23] A fentiek bizonyos mélységig történő ismertetése elengedhetetlen ahhoz, hogy képet kapjunk arról a kontextusról, amiben a Bíróságnak döntenie kell az érvényességről vagy érvénytelenségről, illetve enélkül nem határozható meg az a mérce sem, ami alapján az EUB elvégzi saját értékelését. A tanulmánynak ennélfogva nem célja az adattovábbítási jogi keretrendszer fejlődésének részletes, minden elemre kiterjedő bemutatása, ugyanakkor az ezekre való kitérést a jelen mélységig indokoltnak tartja.

1.1. Az adattovábbítás jogszabályi háttere

A GDPR komoly garanciákhoz köti a kezelt személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítását. A szabályozás előzményeként foghatjuk fel az Adatvédelmi Irányelv által alkalmazott megoldást, amely a GDPR jelenlegi rendszeréhez hasonlóan alapvetően akkor tette lehetővé a harmadik országba történő személyesadat-továbbítást, ha az Európai Bizottság megállapította, hogy a kérdéses állam megfelelő védelmi szintet biztosít.[24] Ennek hiányában az adatkezelőnek valamilyen, az Adatvédelmi Irányelvben meghatározott jogalapot kellett felmutatnia a tervezett adattovábbításhoz, példának okáért az érintett egyértelmű hozzájárulását.[25] Emellett azonban lehetőség volt arra, hogy a tagállamok megfelelő garanciák mellett szintén engedélyezzék az adattovábbítást. Ilyen garanciák az Adatvédelmi Irányelv szerint elsősorban a megfelelő szerződési feltételek voltak.[26] A hazai kommentárirodalom megjegyzi, hogy a fenti szabályozás csak kiegészítő jellegű ahhoz az általános rendszerhez képest, amely a személyes adatok kezelésének általános feltételrendszere.[27] Az is megjegyzendő ugyanakkor, hogy az Adatvédelmi Irányelv, uniós irányelv lévén, nemzeti átültetést igényelt. Ezt Magyarországon az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) valósította meg. Az Infotv. a fentiektől némiképp eltérő megközelítésben, de végső soron azonos szabályok alkalmazásával tette lehetővé a harmadik országba történő adattovábbítást.[28]

A GDPR az Adatvédelmi Irányelvhez képest jóval részletesebb és szofisztikáltabb szabályrendszert alkalmaz. A GDPR egyfelől kiterjeszti szabályozása hatályát a harmadik országok mellett a nemzetközi szervezetek részére történő adattovábbításra, másfelől pedig egy önálló fejezetet (V. fejezet) szentel a kérdésnek, amelynek betartása minden adatkezelő és adatfeldolgozó számára kötelező, amennyiben személyes adatokat kívánnak továbbítani harmadik országba vagy nemzetközi szervezet részére.[29]

Az Adatvédelmi Irányelvhez hasonlóan a harmadik országba (és nemzetközi szervezet részére – ez utóbbi esetet ezt követően beleértem a harmadik országba történő adattovábbításba) történő adattovábbítás elsősorban az Európai Bizottság megfelelőségi határozatán alapulhat, azaz az adattovábbításhoz akkor nem szükséges külön engedély, *„ha a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít”.*[30] A GDPR azt is meghatározza, hogy a Bizottság mely szempontok mérlegelésével határoz, úgy mint a jogállamiság, általános és ágazati jogszabályok, nemzetbiztonsági szabályok,

[24] Adatvédelmi Irányelv 25. cikk (1) és (6) bek.
[25] Adatvédelmi Irányelv 26. cikk (1) bek. *a)* pont.
[26] Adatvédelmi Irányelv 26. cikk (2) bek.
[27] Az általános feltételrendszert lásd Adatvédelmi Irányelv II. fejezet. Péterfalvi Attila–Révész Balázs–Buzás Péter (szerk.): *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2021, 358.
[28] Péterfalvi–Révész–Buzás: i. m., 359–360.
[29] GDPR 44. cikk.
[30] GDPR 45. cikk (1) bek.

létezik-e független és hatékony felügyeleti hatóság, illetve milyen nemzetközi kötelezettségei vannak az adott harmadik államnak a személyes adatok védelmével kapcsolatban.[31] Az ez alapján elfogadott bizottsági megfelelőségi határozatokat legalább negyedévente felül kell vizsgálni, és folyamatosan figyelemmel kell kísérni a harmadik országban zajló fejleményeket, szükség esetén pedig hatályon kívül kell helyezni, módosítani kell, vagy fel kell függeszteni a megfelelőségi határozatot.[32]

A Bizottság eddig számos megfelelőségi határozatot fogadott el. Jelenleg a megfelelő védelmi szintet biztosító államok listája a következő: Andorra, Argentína, Kanada (a kereskedelmi szervezetek tekintetében),[33] Feröer-szigetek, Guernsey, Izrael, Man-sziget, Japán, Jersey, Új-Zéland, Dél-Korea, Svájc, Egyesült Királyság, Egyesült Államok (a 2. pontban foglaltak szerint) és Uruguay.[34]

A GDPR a bizottsági megfelelőségi határozat hiánya esetén akkor engedélyezi a személyes adatok harmadik országba történő továbbítását, ha *(i)* az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott és *(ii)* az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.[35] Mindez a gyakorlatban azt jelenti, hogy önmagában a megfelelő garanciák nyújtása szükséges, de nem elégséges feltétel a jogszerű adattovábbításhoz – a harmadik ország jogrendszerének továbbra is kompatibilisnek kell lennie az Unió jogrendjével, legalább ami a jogérvényesítést és a hatékony jogorvoslatot illeti.

A GDPR két kategóriában nevesíti a fent említett megfelelő garanciákat: egyfelől szól a felügyeleti hatóság engedélye nélküli garanciákról, másfelől a felügyeleti hatóság engedélyéhez kötött garanciákról. Az első csoportba az alábbi garanciák tartoznak: a közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszközök; a kötelező erejű vállalati szabályok; a Bizottság vagy a felügyeleti hatóság által elfogadott általános szerződési feltételek;[36] jóváhagyott magatartási kódex vagy tanúsítási mechanizmus az érintetti jogok alkalmazására vonatkozó, kikényszeríthető adatkezelői vagy adatfeldolgozói kötelezettségvállalással. A második csoportba tartozik például a továbbítás alanyai közötti szerződés.[37] Az Európai Adatvédelmi Testület (a továbbiakban: EDPB) 2021-ben ajánlást fogadott el azon intézkedésekről, amelyek kiegészítik az adattovábbítási

[31] GDPR 45. cikk (2) bek.

[32] GDPR 45. cikk (3)–(5) bek.

[33] Kanada csak abban az esetben biztosít megfelelő védelmet, ha az adattovábbítás címzettje a *Personal Information Protection and Electronic Documents Act* hatálya alá tartozik. Ez az egyike azon államoknak, amelyek nem általánosságban, hanem bizonyos többletfeltételek fennállása esetén biztosítanak megfelelő védelmet. A másik ilyen állam az Egyesült Államok. Lásd Jóri Andárs (szerk.): *A GDPR magyarázata.* HVG-ORAC, Budapest, 2018, 245.

[34] Adequacy decisions. Európai Bizottság. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (2024. 07. 18.).

[35] GDPR 46. cikk (1) bek.

[36] A Bizottság (EU) 2021/914 végrehajtási határozata (2021. június 4.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerinti, harmadik országok részére történő személyesadat-továbbításra vonatkozó általános szerződési feltételekről. HL L 199., 2021.6.7., 31–61.

[37] GDPR 46. cikk (2)–(3) bek.

eszközöket (jogalapokat)[38] a személyes adatoknak biztosítandó uniós védelmi szint lényegi elérése érdekében. Az EDPB ajánlásában egy folyamatot azonosított, amit az adatexportőrök követhetnek harmadik országok értékelése tekintetében. Az ajánlás alapján első lépésként tényszerűen fel kell térképezni az adattovábbításokat, majd második lépésként azonosítani kell a GDPR V. fejezete szerinti adattovábbítási jogalapot. Ezt követően harmadik lépésként – amelyet csak abban az esetben szükséges elvégezni, ha nem a GDPR 45. vagy 49. cikkén alapul az adattovábbítás – vizsgálni szükséges, hogy milyen hatást gyakorol az adattovábbítási művelet az alkalmazott garanciák hatékonyságára, tehát el kell végezni a harmadik ország jogszabályainak és hatósági gyakorlatának értékelését, és szükséges esetben megfelelő intézkedést kell hozni (például az adattovábbítás felfüggesztése vagy kiegészítő lépések). Ez utóbbiak azonosítása és elfogadása képezi az ajánlott negyedik lépést. Ötödikként meg kell tenni azokat a hivatalos eljárási lépéseket, amelyek szükségesek lehetnek a GDPR 46. cikke szerinti adattovábbításhoz (például általános szerződési feltételek módosítása esetén ki kell kérni a felügyeleti hatóság engedélyét).[39] Végül, de nem utolsósorban megfelelő időközönként újraértékelést szükséges végezni, valamint folyamatosan nyomon kell követni a személyes adatok védelmi szintjére hatással járó fejleményeket.[40]

Ha az adattovábbításra sem megfelelőségi határozat, sem pedig megfelelő garanciák alapján nem kerülhet sor, úgy a GDPR szerinti „különös helyzetben" további jogalapok biztosítottak az adattovábbításra. Ilyen jogalap lehet például az érintett kifejezett hozzájárulása, de csak abban az esetben, ha tájékoztatták az adattovábbítás kockázatairól, amely egyszeri vagy többszöri továbbításra is megfelelő.[41] A felügyeleti hatóság értesítése, illetve az adatvédelmi nyilvántartásban való dokumentálás mellett nem ismétlődő jellegű továbbításra sor kerülhet még kényszerítő erejű jogos érdek alapján is.[42]

A Nemzeti Adatvédelmi és Információszabadság Hatósággal (a továbbiakban: NAIH) 2020-ban folytatott, eljárási kereteket nélkülöző konzultáció során a NAIH felhívta a figyelmet arra, hogy a fenti különös helyzetekben alkalmazható jogalapok csak abban az esetben vehetők igénybe, ha az adatkezelő az adattovábbítást

[38] E tanulmány keretei között az „adattovábbítási eszköz" kifejezés helyett az „adattovábbítási jogalap" formulát használom. Helyesebb ugyanis egy konkrét adatkezelési művelet jogszerűségét lehetővé tevő jogi konstrukció esetében jogalapról (tehát a műveletet lehetővé tevő jogszabályi rendelkezésről) beszélni, mint valamilyen adattovábbítási eszközről, amely inkább azokat a technikai berendezéseket, megoldásokat jelenti, amely segítségével valósul meg az adattovábbítás. A Magyar Értelmező Kéziszótár is ezt a szóhasználatot támasztja alá. A szótár az eszközt a következőként definiálja: *„[vala]mely művelet elvégzését lehetővé tevő [vagy] megkönnyítő tárgy, szerszám, gép".* Lásd Pusztai Ferenc (szerk.): *Magyar Értelmező Kéziszótár.* Akadémiai Kiadó, Budapest, 2003, 327. Ezzel szemben a jogalapot azonos szótár úgy határozza meg, mint *„[vala]mely eljárást jogossá tevő szabály, törvény, rendelet".* Lásd Pusztai: i. m., 602.

[39] EDPB 01/2020. számú ajánlás azon intézkedésekről, amelyek kiegészítik az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében. https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_hu_0.pdf (2024. 07. 18.) 61. bek.

[40] 01/2020. sz. EDPB Ajánlás 3–5.

[41] GDPR 49. cikk (1) bek. *a)* pont.

[42] GDPR 49. cikk második albek.

megelőzően az adattovábbítás minden körülményére kiterjedő vizsgálatot folytatott le.[43] A NAIH álláspontja szerint ez összhangban áll az EDPB 2/2018-as iránymutatásával, amely szerint többszintű megközelítést szükséges alkalmazni, tehát először vizsgálni szükséges, hogy megfelelő védelmi szintet biztosít-e a harmadik ország, ha pedig nem, akkor megfelelő garanciák biztosítását szükséges előnyben részesíteni.[44] Álláspontom szerint ugyanakkor itt nem arról van szó, hogy az adatkezelőnek vagy adatfeldolgozónak kellene elvégeznie azt az elemzést, amit egyébként az Európai Bizottság tesz meg a megfelelőség vizsgálatakor, hanem egyszerűen azt szükséges vizsgálni, hogy ezt megtette-e a Bizottság, és van-e egyáltalán lehetőség arra, hogy megfelelő garanciák adása mellett jogszerűen sor kerülhessen az adattovábbításra (azaz léteznek-e érvényesíthető érintetti jogok, valamint hozzá tartozó jogorvoslati lehetőségek). Az ellenkező értelmezés olyan pénzügyi többletterhet róna az adatkezelőkre/adatfeldolgozókra, ami nem áll arányban az elérendő céllal.

Mindez véleményem szerint igaz a 01/2020. sz. EDPB ajánlás által taglalt eljárás vonatkozásában is. Az adatkezelőkre/adatfeldolgozókra rótt kötelezettségek már-már riasztó mértéket öltenek, ha figyelemmel vagyunk az ajánlás negyedik lépéséhez fűződő kommentárirodalom álláspontjára. Eszerint szükséges vizsgálni a célország jogszabályait, referenciaként felhasználni ehhez az Európai Unió Alapjogi Chartájának 47. és 52. cikkeit, valamint értékelni, hogy a hatóságok általi potenciális hozzáférés szükséges és arányos mértékű-e egy demokratikus társadalomban, az érintettek számára van-e hatékony jogorvoslati lehetőség, illetve milyen a jogállamiság helyzete.[45] Hogyan várható el egy adatkezelőtől (adott esetben mondjuk egy egyéni vállalkozótól) mindezen kérdések vizsgálata, ha az Európai Bizottság hosszú évek munkájával, immáron két alkalommal is pontosan a fentiek tekintetében jutott helytelen jogkövetkeztetésre?[46] Álláspontom szerint az ilyen és ehhez hasonló puha vizsgálati kötelezettségek indokolatlan, sőt a gyakorlatban gyakran kivitelezhetetlen kötelezettséget és felelősséget telepítenek az adatkezelőkre.

Végül, de nem utolsósorban ki kell emelni azt is, hogy a GDPR bizonyos esetekben megtiltja a harmadik országba történő adattovábbítást. Ilyennek tekinthetők főszabály szerint azok az esetek, amikor harmadik ország bírósága vagy hatósága az adatkezelőt vagy adatfeldolgozót személyes adatok továbbítására vagy közlésére kötelezi. Kivételt képez a tilalom alól az, ha e döntések az EU vagy egy tagállam között nemzetközi szerződésen (például kölcsönös jogsegélyszerződésen) alapulnak, feltéve, hogy nem sértik a GDPR egyéb rendelkezéseit.[47]

A kommentárirodalom szerint a GDPR V. fejezetének célja az, hogy a személyes adatok védelmének szintje folyamatos, azaz lényegében azonos legyen, függetlenül attól, hogy ezeket az adatokat az Európai Unióban vagy azon kívül kezelik. Ez alól

[43] NAIH/2020/6367/2.

[44] EDPB 2/2018. sz. iránymutatás az (EU) 2016/679 rendelet 49. cikke szerinti eltérésekről. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_hu.pdf (2024. 07. 18.) 4. Vö. NAIH/2020/6367/2.

[45] Péterfalvi–Révész–Buzás: i. m., 364.

[46] Lásd a Biztonságos Kikötő Határozatot és az Adatvédelmi Pajzs Határozatot, valamint az azokat érvénytelenítő *Schrems I és Schrems II ítéletet.*

[47] GDPR 48. cikk.

kivételt csak a GDPR 49. cikkének „különös helyzetben" alkalmazható szabályai jelentenek. Ugyanakkor ezek csak a többi adattovábbítási jogalap hiánya esetén jöhetnek szóba, továbbá általában alkalomszerű adattovábbításokra használhatók, azzal, hogy mindenképpen elkerülendő, hogy a kivételszabály főszabállyá váljon.[48]

A nagyvállalati *compliance* világában azonban nem kizárólag az Európai Unió létezik, így utalni szükséges arra a tényre is, hogy más államok, úgymint Argentína, Ausztrália, Brazília, Kolumbia, India, Japán és Oroszország is alkalmaznak hasonló megoldásokat, azaz előírják a joghatóságuk alá tartozó jogalanyoknak, hogy legalább azonos vagy erősebb védelmi szinttel rendelkező államba továbbíthatnak csak személyes adatokat. Megjegyzendő ugyanakkor, hogy a gyakorlatban az ezeknek való megfelelés általában az uniós *compliance*-et követő lépés, hiszen ennek elemei gyakorta máshol is felhasználhatók.[49]

Kiemelést érdemel az is, hogy az adattovábbítások esetében nem elegendő csupán a GDPR-nak való alapvető megfelelésre koncentrálni az alapul fekvő adatkezelés tekintetében, és biztosítani, hogy a címzett megfelelő védelmi szintet biztosít, hanem igazolni kell tudni azt az indokot is, hogy miért szükséges az adattovábbítás – ezt nevezzük a „három küszöb-tesztnek". Ez utóbbi lépés az, amely a gyakorlatban általában elmarad.[50]

További, a gyakorlatból levonható következtetés, hogy a nagyvállalatok többsége az általános szerződési feltételek alkalmazását részesíti előnyben a megfelelőség biztosítása érdekében, amelyek így nemzetközi standardokká is váltak.[51] Az általános szerződési feltételekre való támaszkodás ugyanakkor szintén kockázatos, tekintettel arra, hogy a nemzeti felügyeleti hatóságok vizsgálhatják az adatok továbbítását ilyen esetekben is, ahogy azt tette például az osztrák adatvédelmi hatóság a *Google Analytics* szolgáltatásai tekintetében, ahol a hatóság azt állapította meg, hogy az általános szerződési feltételek nem nyújtanak megfelelő védelmet.[52] Szintén a Google Analytics használata vonatkozásában hasonló megállapításra jutott a francia[53] és az olasz[54] adatvédelmi hatóság is.

[48] Péterfalvi–Révész–Buzás: i. m., 361–362., 386–387.

[49] Determann, Lothar: *Determann Adatvédelmi Jogi Útmutatója. Nemzetközi vállalati compliance.* HVG-ORAC, Budapest, 2020. 64–65.

[50] Determann: i. m., 65–67.

[51] Determann: i. m., 73. Például a *Meta Platforms* adatkezelési tájékoztatója szerint a vállalat mind a mai napig az általános szerződési feltételekre alapozza a személyes adatok Egyesült Államokba történő továbbítását. Lásd Egan, Erin: Steps We Take to Transfer Data Securely. *Meta,* 2021. március 11. https://about.fb.com/news/2021/03/steps-we-take-to-transfer-data-securely/ (2024. 07. 19.). Erre a cikkre közvetlen link vezet a tájékoztatóból. A *Google* ezzel szemben csak ott alkalmazza az általános szerződési feltételeket, ahol nem áll rendelkezésre megfelelőségi határozat. Lásd Google Adatvédelmi és Általános Szerződési Feltételek, 2023. szeptember 1. https://policies.google.com/privacy/frameworks?hl=hu (2024. 07. 19.).

[52] GZ: D155.027. 2021-0.586.257. https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf (2024. 07. 19.). Rendelkező rész 2. pont *b)* alpont.

[53] https://www.cnil.fr/sites/cnil/files/atoms/files/med_google_analytics_anonymisee.pdf (2024. 07. 19.). 6. pont.

[54] Provvedimento del 9 giugno 2022 [9782890]. https://www.easyteam.org/wp-content/uploads/2022/06/Garante-Privacy-9782890-1.0.pdf (2024. 07. 19.).

1.2. A Schrems-teszt

Az adattovábbításra vonatkozó uniós jogszabályi környezet és hatósági gyakorlat ismertetését követően ebben az alpontban a Bíróság esetjoga által kialakított úgynevezett Schrems-tesztet mutatom be, ennek alapján vizsgálható ugyanis az EU–USA Adatvédelmi Keretrendszer Határozat érvényessége.

A Schrems-teszt a *Schrems I ítéletben* születetett meg 2015-ben. Elöljáróban rögzítendő, hogy a konkrét ügyben az EUB kimondta, hogy az Unió voltaképpen lefoglalja a megfelelőségi döntés hatáskörét, azaz a tagállamok nem fogadhatnak el a Bizottság által hozott határozattal ellentétes intézkedést, ennek felülvizsgálatára pedig csak a Bíróság jogosult.[55] Ettől függetlenül az érintettek az Alapjogi Charta rendelkezései alapján továbbra is kérelemmel fordulhatnak a nemzeti felügyeleti hatóságokhoz, amelyet lényegében úgy kell értelmezni, hogy az a határozat alapjogi megfelelőségére vonatkozik.[56] Ez pedig végső soron egy nemzeti bírósági, majd EUB felülvizsgálatot kell hogy eredményezzen, függetlenül attól, hogy a nemzeti adatvédelmi hatóság egyetért-e az érintett kérelmével, vagy sem.[57] Végeredményben ez képezi a mindenkori megfelelőségi határozat eljárási kereteit. Az érintett tehát ennek alapján jogosult a felügyeleti hatósághoz fordulni, amely vagy maga kezdeményez bírósági eljárást, vagy az érintettre kedvezőtlen döntés után ő maga tud nemzeti bírósághoz fordulni, ami pedig előzetes döntéshozatali eljárás keretében az EUB elé utalhatja majd a kérdést. Természetesen lehetőség van ennél egyszerűbb eljárási keretek között, megsemmisítési eljárás során is megtámadni a döntést, ez azonban időben korlátozott lehetőség,[58] és a Bíróság (a folyamatban lévő ügyben a Törvényszék) nem is mindig fogadja be az ilyen jellegű kereseteket.[59]

Az eljárás időpontjában még az Adatvédelmi Irányelv volt hatályban, így a Bíróság ennek alapján vizsgálta felül a Biztonságos Kikötő Határozatot. Az EUB rögzítette, hogy az Adatvédelmi Irányelv nem határozza meg a megfelelő védelmi szint fogalmát, ugyanakkor álláspontja szerint azt az egyén magánélete, alapvető jogai és szabadságainak védelme alapján lehet értékelni. Ennek alapján a Bíróság úgy határozott, hogy az uniós joggal *lényegében azonos* védelmi szintet követel meg az adattovábbítás címzett államának jogrendjétől, tehát nem várja el az unióssal teljesen megegyező védelmi szintet.[60]

A Bizottságnak a megfelelőségi határozat kiadása során az alábbi szempontokat kell figyelembe vennie: *(i)* a fogadó államban alkalmazandó szabályok tartalma (belső jog és nemzetközi kötelezettségek egyaránt) és *(ii)* e szabályok tiszteletben tartására irányuló gyakorlat.[61]

[55] *Schrems I ítélet* 52. bek.
[56] *Schrems I ítélet* 53. és 59. bek.
[57] *Schrems I ítélet* 64–65. bek.
[58] EUMSZ 263. cikk.
[59] Lásd az Adatvédelmi Pajzs Határozat megtámadása vonatkozásában: T-670/16. sz. *Digital Rights Ireland kontra Bizottság* ügyben a Törvényszék 2017. november 22-i végzése (ECLI:EU:T:2017:838) 53–54. bek.
[60] *Schrems I ítélet* 70–74. bek.
[61] *Schrems I ítélet* 75. bek.

A Bíróság a Biztonságos Kikötő Határozat vonatkozásában elvégezte ezt a vizsgálatot, amelynek kapcsán rögzítette, hogy a megfelelőségi határozat szerint a programban részt vevő szervezetekre alkalmazandó elvek bizonyos helyzetekben korlátozhatók, ilyen például, ha az adatokhoz való hozzáférés nemzetbiztonsági okból, közérdekből vagy a bűnüldözés érdekében szükséges. Ezek a célok elsőbbséget élveznek a Biztonságos Kikötő Határozatban foglalt elvekkel szemben. Továbbá az is megállapítható volt, hogy a beavatkozás általános jellegű, korlátozásoktól mentes, és nem kapcsolódik hozzá hatékony bírói védelem.[62]

Mindezek alapján az EUB megállapította, hogy a Biztonságos Kikötő Határozat ellentétes az Alapjogi Charta 7. és 47. cikkével, tehát érvénytelen.[63]

A fentiek alapján a Schrems-teszt úgy foglalható össze, hogy a Bizottság által elfogadott megfelelőségi határozat akkor tekinthető érvényesnek, ha az tiszteletben tartja az Alapjogi Chartában meghatározott alapvető emberi jogokat és szabadságokat, ezt pedig az adott állam belső joga, valamint nemzetközi kötelezettségei, illetve az ezek végrehajtására irányuló gyakorlat alapján szükséges vizsgálni. A Schrems-teszt tételes jogi megerősítést is nyert a GDPR elfogadásával, ugyanis a 44. cikk (2) bekezdése részletesen kifejti, hogy a Bizottságnak milyen szempontok szerint kell értékelnie egy adott harmadik országot.

Az EUB ítélkezési gyakorlata szintén megerősítette a *Schrems I ítéletben* foglaltakat. A *Schrems II ítéletben* a Bíróság egyfelől megismételte a felülvizsgálat eljárási keretei kapcsán korábban írottakat,[64] másfelől azt, hogy az uniós védelmi szinttel lényegében megegyező védelmet szükséges biztosítani a személyes adatokat fogadó harmadik államban.[65] Az ügyben az Adatvédelmi Pajzs Határozat érvényességének kérdése merült fel. Az Adatvédelmi Pajzs Határozat terjedelemében ugyan többszöröse volt a Biztonságos Kikötő Határozatnak, az EUB megállapítása szerint ugyanakkor a személyes adatok védelme a korábbiakhoz hasonlóan a nemzetbiztonság, a közérdek és a bűnüldözés követelményeihez szükséges mértékben korlátozható, így tehát ezek ismét elsőbbséget élveznek a határozatban egyébként kötelező elvekkel szemben.[66] A Bíróság ítéletében konkrétan kiemelte a PRISM és az UPSTREAM megfigyelési programokat, és a 12333. sz. elnöki rendelet alapján történő beavatkozásokat, amelyeket ismételten általános jellegűnek minősített.[67]

A Bíróság által e körben használt standard – hasonlóan a *Schrems I ítéletben* foglaltakhoz – korábbi esetjogából származik. Eszerint személyes adatok állami hatósággal való közlése beavatkozásnak minősül, függetlenül az adatok későbbi felhasználásától, azok minőségétől (érzékeny jellegű vagy sem), illetve, hogy ez okozott-e kellemetlenséget az érintett számára.[68] Tekintettel azonban arra, hogy

[62] *Schrems I ítélet* 84., 86–87., 89–90. és 93. bek.

[63] *Schrems I ítélet* 94–95. és 105. bek.

[64] *Schrems II ítélet* 156–158. bek.

[65] *Schrems II ítélet* 162. bek.

[66] *Schrems II ítélet* 164. bek.

[67] *Schrems II ítélet* 165. bek.

[68] *Schrems II ítélet* 171. bek. Lásd még *Schrems I ítélet* 91. bek.; C-293/12. és C-594/12. sz. *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Írország és az Attorney General* (C-293/12), *Kärnt-*

az Alapjogi Charta 7. és 8. cikkeiben rögzített alapvető jogok (magán- és családi élet tiszteletben tartása és a személyes adatok védelme) nem abszolút jellegűek, korlátozásukra lehetőség van az Alapjogi Charta 52. cikk (1) bekezdése alapján, amely az EU által elismert általános érdekű célkitűzések vagy mások jogainak és szabadságainak védelme céljából elengedhetetlenül szükséges és arányos mértékben megengedett.[69]

E kérdések vizsgálata során az EUB értékelte az 1978-as *Foreign Intelligence Surveillance Act* 702. cikkén alapuló megfigyelési programokat, amelyek esetében azt a megállapítást tette, hogy a külföldi hírszerzési programok tekintetében nincs semmilyen korlátozás, a nem amerikai érintettek számára elérhető garanciák pedig nem léteznek, következésképpen e jogszabály nem alkalmas arra, hogy az unióssal lényegében azonos védelmi szintet biztosítson a személyes adatok védelmének.[70] Az amerikai jog az Adatvédelmi Pajzs Határozatban nevesített részei ezen felül nem biztosítanak az érintettek számára az amerikai hatóságokkal szemben a bíróságok előtt érvényesíthető jogokat sem, amely szintén alkalmatlanná teszi ezeket a lényegileg azonos védelmi szint megállapításához.[71]

A Bíróság ezen felül azt is vizsgálta, hogy az amerikai jog tartalmaz-e az Alapjogi Charta 47. cikkének megfeleltethető hatékony jogorvoslati mechanizmust, amelyet szintén a Schrems-teszt részeként fogalmazott meg olyan módon, hogy *„az olyan szabályozás, amely nem biztosít a jogalany számára semmilyen jogorvoslati lehetőséget abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltethesse, nem tartja tiszteletben a hatékony bírói jogvédelemhez való jog lényegét”.*[72]

Az Adatvédelmi Pajzs Határozat nagy újítása volt az úgynevezett ombudsmani rendszer létrehozása, amely a Bizottság szerint garantálja a független felügyeletet és az egyéni jogorvoslati lehetőséget.[73] Az EUB ehhez képest megállapította, hogy az ombudsmant az USA külügyminisztere nevezi ki, és az szerves részét képezi az Egyesült Államok külügyminisztériumának, valamint nincs utalás arra, hogy az ombudsman kinevezéséhez vagy visszahívásához kapcsolódna bármilyen jellegű garancia, megkérdőjelezve ezzel az intézmény függetlenségét.[74] A Bíróság ezen túlmenően azt is megállapította, hogy az ombudsman nem rendelkezik felhatalmazással kötelező erejű döntések meghozatalára, illetve nincsenek olyan jogszabályi garanciák sem, amelyek a kötelezettségvállalásokhoz társulnának. Mindezekből pedig az következik, hogy az ombudsmani rendszer sem biztosít az unióssal lényegében azonos védelmi szintet a személyes adatok védelméhez.[75] Ezek alapján pedig az

ner Landesregierung, Michael Seitlinger, Christof Tschohl és társai (C-594/12) egyesített ügyekben 2014. április 8-án hozott ítélet (ECLI:EU:C:2014:238) 33–36. bek.

[69] *Schrems II ítélet* 172. és 174. bek.

[70] *Schrems II ítélet* 180. bek.

[71] *Schrems II ítélet* 181–184. bek.

[72] *Schrems II ítélet* 187. bek.

[73] Adatvédelmi Pajzs határozat (117)–(123) preambulumbek.

[74] *Schrems II ítélet* 195. bek.

[75] *Schrems II ítélet* 196–197. bek.

is megállapítható volt, hogy az Adatvédelmi Pajzs Határozat érvénytelen.[76] Megjegyzendő ugyanakkor, hogy az EUB azonos döntésében érvényesnek ismerte el a Bizottság által elfogadott általános szerződési feltételek korábbi változatát.[77]

A *Schrems I ítélet* hivatkozási gyakorlatát vizsgálva megállapítható, hogy a 25 ügyből, amelyben a Bíróság érdemben hivatkozott az ítéletre, túlnyomó részben, összesen 14 esetben eljárási és előzetes döntéshozatali kontextusban került sor,[78] szemben a 6 adatvédelmi és 3 hatékony bírói jogvédelem jellegű hivatkozással.[79] Az ítélkezési gyakorlatban mindösszesen 2 esetben merült fel a harmadik ország által biztosított védelem lényegében azonos szintjének vizsgálata. Az egyik természetesen a *Schrems II ítélet* volt. A másik hasonló döntés a Kanada és az Európai Unió közötti, az utasnyilvántartási adatállomány adatainak továbbításáról és kezeléséről szóló megállapodástervezet EUB általi véleményezése során született, amiben a Bíróság több alkalommal hivatkozott a *Schrems I ítéletre*. Az ügyben az EUB részletesen vizsgálta a továbbított személyes adatokhoz való hozzáférés mint beavatkozás szükségességét és arányosságát, valamint sommásan kezelte a hatékony bírói jogvédelem kérdését is.[80] Ezzel szemben a *Schrems II ítélet* hivatkozási gyakorlatánál már más tendenciákat látunk. A 25 ügyben, ahol megjelenik a hivatkozás, 12 adatvédelmi tárgyú[81] és csak 8 eljárási jellegű.[82] Összesen pedig csak három olyan ügy volt, ahol mindkét Schrems ítéletre történt hivatkozás.[83]

---

[76] *Schrems II ítélet* 199. bek.

[77] *Schrems II ítélet* 149. bek. Vö. 2010/87/EU: A Bizottság határozata (2010. február 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről. HL L 39., 2010.2.12., 5–18.

[78] Lásd például C-415/20., C-419/20. és C-427/20. sz. *Gräfendorfer Geflügel- und Tiefkühlfeinkost Produktions GmbH* (C-415/20), *F. Reyher Nchfg. GmbH & Co. KG vertr. d. d. Komplementärin Verwaltungsgesellschaft F. Reyher Nchfg. mbH* (C-419/20), *Flexi Montagetechnik GmbH & Co. KG kontra Hauptzollamt Hamburg* (C-415/20 és C-419/20), *Hauptzollamt Kiel* (C-427/20) egyesített ügyekben 2022. április 28-án hozott ítélet (ECLI:EU:C:2022:306); C-212/19. sz. *Ministre de l'Agriculture et de l'Alimentation kontra Compagnie des pêches de Saint-Malo* ügyben 2020. szeptember 17-én hozott ítélet (ECLI:EU:C:2020:726); C-123/18. P. sz. *HTTS Hanseatic Trade Trust & Shipping GmbH kontra az Európai Unió Tanácsa, Európai Bizottság* ügyben 2019. szeptember 10-én hozott ítélet (ECLI:EU:C:2019:694).

[79] Lásd például adatvédelmi hivatkozásként C-458/22. P. sz. *Robert Roos és mások kontra Európai Parlament és mások* ügyben 2023. november 16-án hozott ítélet (ECLI:EU:C:2023:871) és C-210/16. sz. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein kontra Wirtschaftsakademie Schleswig-Holstein GmbH* ügyben 2018. június 5-én hozott ítélet (ECLI:EU:C:2018:388). A hatékony bírói védelem vonatkozásában lásd C-131/15. P. sz. *Club Hotel Loutraki kontra Európai Bizottság, Görög Köztársaság, Organismos Prognostikon Agonon Podosfairou AE* ügyben 2016. december 21-én hozott ítélet (ECLI:EU:C:2016:989). A statisztikai adatok alapját minden esetben a https://curia.europa.eu/ ítélkezési gyakorlat keresője képezte. Az ebből eredő technikai hibák miatt eltérések lehetségesek a közölt adatoktól.

[80] Lásd a Bíróság 1/15. sz. 2017. július 26-i véleménye [Az EUMSZ 218. cikk (11) bekezdése alapján adott vélemény] (ECLI:EU:C:2017:592) 119–231. bek.

[81] Lásd például C-458/22. sz. ítélet és C-26/22. és C-64/22. sz. *UF* (C-26/22), *AB* (C-64/22) *kontra Land Hessen* egyesített ügyekben 2023. december 7-én hozott ítélet (ECLI:EU:C:2023:958).

[82] Lásd például C-522/21. sz. *MS kontra Saatgut-Treuhandverwaltungs GmbH* ügyben 2023. március 16-án hozott ítélet (ECLI:EU:C:2023:218); C-77/21. sz. *Digi Távközlési és Szolgáltató Kft. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság* ügyben 2022. október 20-án hozott ítélet (ECLI:EU:C:2022:805).

[83] C-458/22. sz. ítélet; C-212/19. sz. ítélet; T-486/21. sz. *OE kontra Bizottság* ügyben 2022. szeptember 7-én hozott ítélet (ECLI:EU:T:2022:517).

1.3. Adattovábbítás és Schrems-teszt a szakirodalomban

Az adattovábbítások és a Schrems-teszt gazdag hazai[84] és nemzetközi szakirodalommal rendelkezik.[85] A szakirodalom szemlézése alapján megállapíthatjuk, hogy a *Schrems II ítélet* (és így természetesen beleértve a *Schrems I ítéletet* is) komolyan csökkentette a transzatlanti adattovábbításra használható jogalapokat,[86] különösen, ha figyelembe vesszük, hogy az általános szerződési feltételek sem jelentenek biztos megfelelést.[87] Olvashatunk olyan szakirodalmi véleményt is, amely a *Schrems II ítélet* alapján gyakorlatilag feleslegesnek tartja a megfelelőségi határozatokat, hiszen az EUB egyébként is alkalmazni rendelte az általános szerződési feltételek vonatkozásában a lényegében azonos védelem szintjét, e szerződések pedig lényegesen gyorsabban megköthetők, mint ahogy egy megfelelőségi határozat meghozható.[88] Mások úgy vélekednek, hogy a *Schrems II ítélet* által meghatározott nagyon szigorú szabályok, ahol az elszámoltathatóság elve gyakorlatilag kiterjed a harmadik állam megfelelőségének biztosítására, megtiltja az Egyesült Államokba történő adattovábbítást.[89] Egyes szerzők úgy gondolják, hogy a *Schrems II ítéletet* követő EUB esetjog árnyalta a Schrems-tesztet annyiban, hogy az államoknak valamilyen fokú rugalmassággal kell rendelkezniük a nemzetbiztonsági megfigyelési programok célpontjainak, illetve az alkalmazott módszereknek a kiválasztásában, tehát önmagában az egyéni vizsgálat hiánya nem jelent minden esetben problémát.[90] A szakirodalom azt is megállapította, hogy sokan jogosan kritizálták a *Schrems I ítéletet* annak hiányos érvelése miatt, főként ami az Egyesült Államok alapjog-korlátozó gyakorlatát illeti. Ezek a hiányosságok azonban a *Schrems II ítéletben* már nem merülnek fel a kérdések részletes elemzése okán.[91] Mások megjegyezték, hogy a

[84] Lásd például Kis Kelemen Bence–Hohmann Balázs: A Schrems ítélet hatásai az Európai Uniós és magyar adattovábbítási gyakorlatokra. *Infokommunikáció és Jog,* 2016/2, 64–70.; Kelemen Anna–Róna Bence: Adatvédelem az Európai Unióban és az USA-ban a Schrems-ügy következményei fényében. *Infokommunikáció és Jog,* 2016/2, 57–63.; Kaszián Ábel: Az Európai Unió Bíróságának Schrems II. ügyben hozott döntése [C-311/18]. *Jogesetek Magyarázata,* 2021/2–3, 91–107.; Bakó Beáta: Az Európai Bíróság ítélete a Schrems-ügyben: az USA nem biztonságos adatkikötő: C-362/14. *Jogesetek Magyarázata,* 2016/1–2, 85–99.; Turcsiné Czapári Dóra: Harmadik országba történő adattovábbítás aktuális kérdései. *Infokommunikáció és Jog,* 2021/1, 28–34.

[85] Lásd például Chander, Anupam: Is Data Localization a Solution for Schrems II? *Journal of International Economic Law,* 2020/3. 771–784. (DOI: 10.1093/jiel/jgaa024); Murphy, Maria Helen: Assessing the implications of Schrems II for EU-US data flow. *International Comparative Law Quarterly*, 2021/1. 245–262. (DOI: 10.1017/S0020589321000348); Kuner, Christopher: Schrems II Re-Examined. *Verfassungsblog*, 25 August 2020. https://verfassungsblog.de/schrems-ii-re-examined/ (2024. 07. 22.); Voss, W. Gregory: Transatlantic Data Transfer Compliance. *Boston Journal of Science and Technology Law,* 2022/2, 158–214.

[86] Chander: i. m., 773.

[87] Murphy: i. m., 254.

[88] Kuner: i. m.

[89] Bradford, Laura–Aboy, Mateo–Liddell, Kathleen: Standard contractual clauses for cross-border transfers of health data after Schrems II. *Journal of Law and the Biosciences,* 2021/1. (DOI: 10.1093/jlb/lsab007) 11.

[90] Rubinstein, Ira–Margulies, Peter: Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground. *Connecticut Law Review,* 2022/2. 410.

[91] Tzanou, Maria: Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights. Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (Forthcoming, Hart Publishing 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3710539 (2024. 07. 22.) 8–10; 16–17.

Schrems I ítéletnek való megfelelés soha nem volt egy valós lehetőség az Egyesült Államok számára, tekintettel az EU és az USA között fennálló adatvédelmi „szakadékra", továbbá a fentebb, illetve lentebb is említett gazdasági hatások miatt az Európai Bizottság is a *status quo* fenntartásában érdekelt.[92] Van olyan szakirodalmi álláspont is, amely szerint a *Schrems ítéletek* az úgynevezett „Brüsszel-effektus" részét képezik, aminek keretei között az EU exportálja saját jogi követelményeit a világ más pontjaira.[93]

Gyakorta jelenik meg az a nézet az irodalomban, hogy az adatlokalizáció, azaz a személyes adatok Európán belüli tárolása megoldást jelenthetne, vagy legalábbis a vállalatok úgy érzik, hogy ez a helyes irány a *Schrems ítéletek* által megfogalmazott jogszerűségi aggályokra.[94] Ez azonban gyakorta több problémát okozna, mint amennyit megoldana. Utalunk itt egyfelől arra, hogy az USA nemzetbiztonsági tevékenysége ritkán korlátozódik az Egyesült Államok területére; másfelől az adatlokalizáció költséges, ami a kisebb vállalkozások számára aránytalan pénzügyi terhet jelenthet: óriási *compliance* költségről beszélünk egy mini megfelelési teszt elvégzése keretében, vagy pedig költséges helyi infrastruktúra kiépítésének formájában.[95] Az adatlokalizáció ezen felül nem járul hozzá a transzatlanti kereskedelem erősödéséhez, továbbá ellenintézkedésekkel is találkozhatunk más államoktól, a több helyi rendszer nagyobb kiberbiztonsági kitettséggel rendelkezik, végül pedig versenytorzító hatással is jár.[96] Ezen felül hangsúlyosan jelenik meg az adatszuverenitás vagy digitális szuverenitás kérdésköre[97] is, amely szerint már az adatlokalizáció mint megoldás sem megoldás, hanem helyi szolgáltatók szükségesek, tehát meg kell gátolni a személyes adatokhoz való hozzáférést az amerikai cégek számára.[98] Álláspontom szerint az adatlokalizáció ellen megfogalmazott kritikák közül az első, tudniillik az USA által itt is megvalósítható megfigyelési tevékenység a legerősebb, tekintve, hogy az egész adattovábbítási rendszer jogi problémaköre ebből származik. Ha a megoldás nem valódi, tehát a kitettség oka továbbra is jelen van, akkor teljességgel értelmetlen egy alapvető jog gyakorlatban meg nem valósuló védelme érdekében emelni az adatkezelők megfelelési költségeit. Az adatlokalizáció az adatszuverenitással kombinálva azonban legalább ezt a problémát megoldaná. Ilyen esetben sem mentesülünk azonban a káros gazdasági hatásoktól, ami egy 2021-es becslés alapján az EU-s export 4%-os csökkenéséhez vezetne, ami 2030-ig összesen 1500 milliárd dollár veszteséggel, valamint 1,3 millió elveszített munkahellyel járna.[99]

[92] Terpan, Fabian: EU-USA Data Transfer from *Safe Harbour* to *Privacy Shield*: Back to Square One? *European Papers,* 2018/3. (DOI: 10.15166/2499-8249/261) 1057–1058.

[93] Costello, Róisín Áine: Schrems II: Everything Is Illuminated? *European Papers,* 2020/2, 1054. (DOI: 10.15166/2499-8249/396)

[94] Chander: i. m., 777.; Turcsiné Czapári: i. m., 33.; Cory, Nigel: How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime. *ITIF,* 8 July 2021. https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data/ (2024. 08. 22.).

[95] Chander: i. m., 778, 782.

[96] Chander: i. m., 782–783.

[97] Fahey, Elaine: Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses? *European Papers,* 2023/2, 503–5112. (DOI: 10.15166/2499-8249/670)

[98] Cory: i. m.

[99] Cory: i. m.

A szakirodalom az egyesült államokbeli jog kompatibilitási gondjainak megoldása kapcsán azt is kiemeli, hogy a helyzet megoldása elnöki rendeletek formájában – ahogy ez történt az EU–USA Adatvédelmi Keretrendszer Határozat esetében – ingoványos, tekintve, hogy ennek módosítása vagy hatályon kívül helyezése rendkívül egyszerű, kizárólag az elnök hatáskörébe tartozó kérdés.[100]

1.4. Részkövetkeztetések

Részkövetkeztetésként a fentiek alapján rögzíthető, hogy a Bizottság által elfogadott megfelelőségi határozatokat meg lehet támadni megsemmisítési eljárás keretében, illetve érvényteleníthetőek a felügyeleti hatóságokon keresztül indított eljárások során is. Ez utóbbiak természetesen előzetes döntéshozatali eljárásban kell hogy végződjenek. A Schrems-teszt alapján a Bizottság akkor határozhat megfelelőségi határozat kiadása mellett, ha bizonyítani tudja, hogy a harmadik ország az unióssal lényegében azonos védelmi szintet biztosít a személyes adatoknak, amelyet különösen az adott ország belső joga és nemzetközi kötelezettségei, valamint a GDPR által meghatározott egyéb szempontok alapján szükséges mérlegelni. A Schrems-teszt valamennyi harmadik ország megfelelő védelmi szintjének biztosítására alkalmazható, ugyanakkor az EUB esetjoga eddig csak az Egyesült Államokkal és Kanadával foglalkozott részletesen.

Az Egyesült Államok vonatkozásában a problémát a nemzetbiztonsági, közérdekű, illetve bűnüldözési célzatú állami beavatkozások jelentik, amelyek alapján az USA hatóságai hozzáférhetnek európaiak személyes adataihoz. E beavatkozások ezek általános jellege, valamint az ezekkel szembeni hatékony bírói jogorvoslat hiánya miatt nem felelt meg az uniós jog elvárásainak. Az EU–USA Adatvédelmi Keretrendszer Határozat tehát a Schrems-teszt alapján vizsgálható felül, különösen a hatékony bírói jogvédelem, illetve a beavatkozások korlátozására tett amerikai lépések fényében.

A szakirodalom felhívja a figyelmet arra, hogy az adattovábbítás a GDPR, illetve EUB által meghatározott keretrendszere rendkívül szigorú, és egy biztos alapokon nyugvó megfelelőségi határozat hiányában az adattovábbítás – legalábbis az Egyesült Államok irányába – valószínűleg jogellenes lenne. A problémára alkalmazható technikai/szervezési/gazdasági megoldások pedig gyakorta több problémát okozhatnak, mint amennyit megoldanak, az Európai Bizottság új megfelelőségi határozata pedig vélhetően ismét elvérzik majd a Schrems-teszten.

2. Az EU–USA Adatvédelmi Keretrendszer Határozat és az amerikai jog

Ebben a pontban röviden bemutatom a Bizottság határozatát, illetve a mögöttes amerikai jogot annak érdekében, hogy ez alapján elvégezhető legyen a megfelelőségi határozat érvényességi vizsgálata. Elöljáróban rögzítem, hogy a tanulmánynak nem lehet célja a több mint 100 oldalas EU–USA Adatvédelmi Keretrendszer Ha-

[100] Voss: i. m., 177–178.

tározat részletes ismertetése, illetve az sem, hogy mindenre kiterjedően elemezze az érvényesség kérdését. Ebből adódóan kizárólag azokra a pontokra fókuszálok, amelyek a *Schrems I és Schrems II ítéletek* fényében problémásak lehetnek, így érvényesnek és megfelelőnek fogadok el minden olyan elemet, amelyet a korábbi határozatok kapcsán az EUB már ilyenként értékelt.

Az Európai Bizottság 2023. július 10-én fogadta el az Egyesült Államok vonatkozásában legújabb megfelelőségi határozatát, az EU–USA Adatvédelmi Keretrendszer Határozatot. E döntés alapvetően három pilléren nyugszik. Egyfelől az Egyesült Államok kiadta a 14086. sz. elnöki rendeletet, amely az USA jelfelderítési tevékenységei kapcsán érvényesülő biztosítékokról és korlátokról szól. Másfelől az Egyesült Államok főügyésze is kiadott egy rendeletet, amely létrehozott egy adatvédelmi felülvizsgálati bíróságot. Ez egészül ki harmadik pillérként az EU-ból személyes adatokat fogadó kereskedelemi szervezetekre vonatkozó szabályok aktualizálásával.[101]

Mindezek alapján jutott arra a következtetésre a Bizottság, hogy az Egyesült Államok megfelelő védelmi szintet biztosít az Unión belüli adatkezelőtől vagy adatfeldolgozótól a fenti harmadik pillérben részt vevő tanúsított amerikai szervezetek részére továbbított személyes adatok tekintetében.[102] Látszólag egyet is érthetünk ezekkel a következtetésekkel, hiszen a *Schrems I és II ítéletekben* foglalt kihívásokat papíron minden további nélkül kezelik a megfigyelési tevékenységet korlátozó, illetve az ahhoz kapcsolódó felülvizsgálatot megteremtő amerikai jogszabályok. De vajon valóban így van?

Sorrendben haladva elsőként a 14086. sz., 2022. október 7-én kiadott elnöki rendelettel foglalkozom. Az elnöki rendelet rögzíti a jelfelderítési tevékenységre vonatkozó alapelveket, úgymint, hogy milyen formában rendelhetők el, illetve hajthatók végre ezek a műveletek, milyen megfelelő biztosítékoknak kell megfelelni, hogy az alapvető jogok biztosítottak legyenek a jelfelderítés tervezése és végrehajtása során, illetve hogy szigorú felügyeletnek kell alávetni az ilyen jellegű tevékenységeket.[103] Jelfelderítési tevékenységre csak akkor kerülhet sor, ha megerősített hírszerzési prioritás[104] előmozdítása érdekében szükséges,[105] és a tevékenység csak e célhoz arányos mértékben valósulhat meg.[106] Az elnöki rendelet meghatározza azokat a legitim célokat is, amelyek elérése érdekében jelfelderítési tevékenység végezhető (összesen 12), úgymint a terrorizmussal szembeni védelem, külföldi kormányok képességeinek és szándékainak kifürkészése, a választások integritásának megőrzése stb.[107] Tekintve, hogy majdnem minden formula fenyegetésként vagy

[101] EU–USA Adatvédelmi Keretrendszer Határozat (6) preambulumbek.

[102] EU–USA Adatvédelmi Keretrendszer Határozat (7) preambulumbek.

[103] Executive Order 14086: Enhancing Safeguards for United States Signals Intelligence Activities, 7 October 2022. Federal Register, Vol. 87, No. 198. (a továbbiakban: Executive Order 14086) Sec. 2.

[104] Az elnöki rendelet a megerősített hírszerzési prioritások meghatározását is szabályozza, lásd Executive Order 14086 Sec. 2. (b) (iii).

[105] A szükségesség nem abszolút, tehát akkor is alkalmazható, ha nem ez az egyetlen módja a legitim cél elérésének, ugyanakkor a kevésbé beavatkozó folyamatokat kell előnyben részesíteni, lásd Executive Order 14086 Sec. 2. (c) (i) (A). Itt alapvetően egy *soft law* kötelezettségről beszélünk, mert nincs jogkövetkezmény rendelve ahhoz, ha a kevésbé korlátozó intézkedések helyett más megoldást választ a jogalkalmazó.

[106] Executive Order 14086 Sec. 2. (a) (ii).

[107] Executive Order 14086 Sec. 2. (b) (i) (A).

potenciális fenyegetésként van jellemezve, így ebbe a körbe gyakorlatilag minden fajta jelfelderítési tevékenység legitim módon beleérthető. Bizonyos célok elérése érdekében végzett hírszerzési tevékenység *expressis verbis* tiltott az elnöki rendelet szerint, ilyen például a magánszférához fűződő legitim érdekek elnyomása vagy korlátozása.[108]

Az elnöki rendelet szerint a célzott adatgyűjtést kell előnyben részesíteni. A tömeges megfigyelést csak akkor lehet engedélyezni, ha a megerősített hírszerzési prioritás másként nem mozdítható elő, és ilyen esetben is intézkedéseket kell hozni az adatminimalizálás érdekében.[109] Ezen felül meghatározza azokat a legitim célokat (itt már csak 6-ot), amelyek elérése érdekében alkalmazható tömeges megfigyelés, úgymint a terrorizmus elleni védelem, kémkedés elleni védelem stb.[110] További biztosítékok kerültek be a „diszkriminánsok", azaz például meghatározott azonosítók vagy kiválasztási kifejezések nélküli célzott adatgyűjtés esetében.[111]

A személyes adatok kezelése vonatkozásában érvényesül az adatminimalizálás (amerikai értelemben vett) elve, amely szerint csak korlátozott körben lehet megosztani a gyűjtött személyes adatokat, illetve korlátozott ideig lehet tárolni őket.[112] Alkalmaznak egyfajta adatbiztonsági, illetve adatminőségi, valamint elszámoltathatósági (dokumentációs) elveket is.[113]

Az elnöki rendelet egy három lábon álló felügyeleti rendszert is létrehoz, amely jelenti egyfelől az olyan hivatalnokokat, akik jogi és megfelelőségi felügyeletet látnak el a jelfelderítési tevékenység keretei között, másfelől jelenti a hírszerzésben dolgozók képzését, és a jelentős meg nem felelési incidensek jelentését és kezelését is.[114]

Az EU–USA Adatvédelmi Keretrendszer Határozat második pilléreként az adatvédelmi felülvizsgálati bíróság azonosítható, ennek az eljárása azonban kiegészül egy megelőző eljárással, amelyet, valamint a bíróság legalapvetőbb szabályait szintén a 14086. sz. elnöki rendelet rendezi. Ennek alapján a nemzeti hírszerzési igazgató polgári szabadságjogok védelmével foglalkozó tisztviselője (a továbbiakban: CLPO – *Civil Liberties Protection Officer of the Director of the National Security*) megvizsgál minden megfelelő panaszt[115] és amennyiben szükséges, orvosolja a jogellenes helyzetet, de úgy, hogy közben védi a titkosított, valamint egyébként privilegizált és

[108] Executive Order 14086 Sec. 2. (b) (ii) (A).
[109] Executive Order 14086 Sec. 2. (c) (ii) (A).
[110] Executive Order 14086 Sec. 2. (c) (ii) (B).
[111] Executive Order 14086 Sec. 2. (c) (ii) (D).
[112] Executive Order 14086 Sec. 2. (c) (iii) (A). Ezek nem minden esetben jelentenek valódi korlátozást, például az Egyesült Államok kormányán belül úgy lehet megosztani személyes adatokat, ha egy *felhatalmazott* és *megfelelően képzett* egyén *megalapozottan hiheti,* hogy a személyes adatot majd *megfelelően* fogják védeni és a *címzettnek tudnia kell* az információról. A magam részéről az ilyen és ehhez hasonló korlátozásokat nem tekintem érdemi korlátozó faktornak, lásd Executive Order 14086 Sec. 2. (c) (iii) (A) (1) (c).
[113] Executive Order 14086 Sec. 2. (c) (iii) (B)–(E). A dokumentációs kötelezettség is szokatlan módon került meghatározásra (legalábbis európai szemmel), amikor az nem konkrétan, hanem a helyzet körülményeihez igazodó észszerű dokumentációt kíván meg. Az, hogy ez pontosan mit takar, a bírósági felülvizsgálatig valószínűleg nem derül ki.
[114] Executive Order 14086 Sec. 2. (d).
[115] Executive Order 14086 Sec. 4. (k).

védett információkat.[116] A CLPO feladatai az alábbiakra terjednek ki: *(i)* megvizsgálja a panasz kivizsgálásához szükséges információkat, *(ii)* megvizsgálja, hogy volt-e olyan jogsértés, amire hatásköre kiterjed,[117] *(iii)* titkosított jelentést készít a jogsértésről, amennyiben ilyenre sor került, *(iv)* tájékoztatja a panaszost anélkül, hogy megerősítené vagy cáfolná, hogy az érintett jelfelderítési tevékenység tárgya volt, és *(v)* titkosított, indokolással ellátott döntést hoz.[118] A CLPO döntései kötelező erejűek,[119] és a hatóság független.[120]

Az elnöki rendelet felhatalmazást ad az Egyesült Államok főügyészének, hogy létrehozzon egy adatvédelmi felülvizsgálati bíróságot (a továbbiakban: DPRC – *Data Protection Review Court*), és meghatározza a DPRC eljárásnak alapjait is.[121] Ehhez a bírói fórumhoz lehet fordulni a CLPO döntéseivel szembeni fellebbezéssel.[122] A DPRC tagjait a főügyész nevezi ki, akik megfelelő tapasztalattal rendelkező gyakorló jogászok lehetnek, és akik függetlenek az Egyesült Államok kormányától.[123] A DPRC három bíróból álló tanácsokban vizsgálja felül a CLPO döntéseit,[124] munkáját pedig különleges főtanácsnokok *(special advocates)* segítik.[125]

A DPRC döntéseit a CLPO titkosított és *ex parte,* tehát csak a bíróság számára elérhető dokumentumai, illetve a panaszos, a titkosszolgálatok és a különleges főtanácsnok által előadottak alapján hozza meg.[126] A DPRC a CLPO-hoz hasonlóan egy titkosított jelentést készít, majd tájékoztatja az érintettet a döntésről.[127] A bíróság döntése kötelező erővel rendelkezik, ami vagy nem állapít meg jogsértést, vagy rendelkezik a jogsértés megfelelő orvoslásáról.[128] Az Egyesült Államok kereskedelmi minisztere nyilvántartást vezet a panaszosokról, valamint legkorábban öt évvel a döntés után, majd azt követően ötévente megkeresi az illetékes titkosszolgálatot, hogy a döntések alapjául szolgáló adatok titkosítását megszüntették-e. Amennyiben igen, úgy erről a tényről tájékoztatja az érintettet.[129]

Az Egyesült Államok főügyésze a 14086. sz. elnöki rendelettel azonos napon megalkotta a DPRC-vel kapcsolatos rendeletét. Ebben megismételte és részint kiegészítette a DPRC bírói, illetve a különleges főtanácsnokok megválasztására vonatkozó szabályokat, rendelkezett a bíróság részére nyújtott adminisztratív támogatásról, valamint a bíróság eljárásáról.[130] Kiemelést érdemel az a rendelkezés,

[116] Executive Order 14086 Sec. 3. (c) (i).
[117] Executive Order 14086 Sec. 4. (d).
[118] Executive Order 14086 Sec. 3. (c) (i).
[119] Executive Order 14086 Sec. 3. (c) (ii).
[120] Executive Order 14086 Sec. 3. (c) (iv).
[121] Executive Order 14086 Sec. 3. (d) (i).
[122] Executive Order 14086 Sec. 3. (c) (i) (E) (2).
[123] Executive Order 14086 Sec. 3. (d) (i) (A) és (d) (iv).
[124] Executive Order 14086 Sec. 3. (d) (i) (B).
[125] Executive Order 14086 Sec. 3. (d) (i) (C).
[126] Executive Order 14086 Sec. 3. (d) (i) (D).
[127] Executive Order 14086 Sec. 3. (d) (i) (F)–(G).
[128] Executive Order 14086 Sec. 3. (d) (ii).
[129] Executive Order 14086 Sec. 3. (d) (v).
[130] 28 CFR Part 201. Docke No. NSD 103; Attorney General Order No. 5517-2022. Data Protection Review Court. Federal Register Vol. 87, No. 198. (a továbbiakban: Attorney General Order No. 5517-2022).

amely értelmében e rendelet nem hoz létre semmilyen kikényszeríthető anyagi vagy eljárásjogi jogosultságot az Egyesült Államok ellen, vagy bárki más ellen, és kizárólag a létrehozott jogorvoslati rendszerben meghozott hatósági döntések felülvizsgálatára szolgál, ugyanakkor nem is módosítja a jogorvoslati eljárásban meghozott döntések bírói felülvizsgálatának lehetőségét vagy terjedelmét.[131] Jelenleg a bíróság nyolc bíróval és két különleges főtanácsnokkal működik.[132] Az amerikai hatóságokkal és a bírósággal való kommunikáció az uniós felügyeleti hatóságokon keresztül működik.[133]

Végül, de nem utolsósorban az EU–USA Adatvédelmi Keretrendszer Határozat harmadik pillére egy tanúsítási rendszeren nyugszik. Az ebben részt vevő entitások kötelezettséget vállalnak bizonyos elvek betartására,[134] úgymint a tájékoztatás, a biztonság, a hozzáférés, az adatok sértetlensége és célhoz kötöttsége stb.[135] Az előző határozatok is hasonló mechanizmusokat követtek,[136] amelyet az EUB nem talált problémásnak, így ezek részletesebb kifejtésétől itt eltekintek.

Összefoglalóan megállapíthatjuk, hogy a *Schrems II ítéletet* követően lényeges változások következtek be az amerikai jogban, a Bizottság pedig fenntartotta azt a korábban is működőképesnek vélt öntanúsításon alapuló konstrukciót, amire (részben) alapította az adattovábbítást. Az amerikai jog változásai papíron mindenképpen számottevőek, hiszen biztosítékokat és korlátokat állapítanak meg a hírszerző hatóságok számára, amikor azok személyes adatokhoz férnek hozzá, illetve létrehoztak egy önálló új bíróságot is, amely függetlenül képes elbírálni a hozzá beérkező panaszokat. A lényegében azonos védelmi szint azonban csak látszólagos, hiszen az alkalmazandó szabályok nem minden esetben jelentenek valódi, kikényszeríthető korlátokat a magánszférába való beavatkozással szemben, továbbá azok felülvizsgálata is egy alapjaiban egyenlőtlen eljárásban, titkosított keretek között történik, amin az sem javít, hogy az érintett ötévente lehetőséget kap arra, hogy esetleg megismerhesse az ügyében született döntéseket. Ez is azonban az amerikai hatóságok diszkréciójától függ.

3. A Schrems-teszt és az EU–USA Adatvédelmi Keretrendszer Határozat

Ebben a pontban a GDPR 45. cikk (2) bekezdése, valamint a Schrems-teszt és az EUB további ítélkezési gyakorlata alapján válaszolok arra a kérdésre, hogy érvényesnek tekinthető-e az EU–USA Adatvédelmi Keretrendszer Határozat.

Elöljáróban rögzítendő, hogy a határozat harmadik pillérét képező tanúsítási rendszert nem vizsgálom, tekintettel arra, hogy ezzel kapcsolatban a Bíróság korábban sem fogalmazott meg problémákat, így azt a lényegében azonos védelmi szint szem-

[131] Attorney General Order No. 5517-2022 § 201.12. Álláspontom szerint az utóbbi bírói felülvizsgálat a DPRC eljárására utalhat, nem pedig e bíróság döntésének felülvizsgálatára.

[132] https://www.justice.gov/opcl/redress-data-protection-review-court (2024. 07. 23.).

[133] EU–USA Adatvédelmi Keretrendszer Határozat (177) preambulumbek.

[134] EU–USA Adatvédelmi Keretrendszer Határozat (9) preambulumbek.

[135] EU–USA Adatvédelmi Keretrendszer Határozat I. Melléklet II. pont.

[136] Biztonságos Kikötő Határozat I. Melléklet; Adatvédelmi Pajzs Határozat II. Melléklet.

pontjából megfelelőnek fogadom el. Ezt az álláspontot a szakirodalom is megerősíteni látszik,[137] továbbá egybecseng a határozattervezetről adott EDPB véleménnyel is, amely szerint az elvek nagy vonalakban azonosak az Adatvédelmi Pajzs Határozatban rögzítettekkel.[138] A vizsgálódásom alapját így az Alapjogi Charta 7–8., 47. és 52. cikkei, azaz a magánélethez, a személyes adatok védelméhez, illetve a hatékony jogorvoslathoz való jogok, valamint ezek korlátozhatósága képezik.

3.1. A magánélethez való jog és a személyes adatok védelméhez való jog

Elsőként rögzítendő, hogy a 14086. sz. elnöki rendelettel és más jogszabályokkal szabályozott amerikai jelfelderítési tevékenységek, amennyiben azok személyes adatokra irányulnak[139] és ennek eredményeképpen az Egyesült Államok hatóságai hozzáférnek, illetve megőriznek európai személyes adatokat, érintik a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez való jogot. Ilyen esetben harmadik személlyel, állami hatósággal történik az adatok közlése, amely beavatkozásnak minősül, függetlenül attól, hogy utóbb ezeket az adatokat mire használják fel.[140]

Az Alapjogi Charta 7–8. cikkeiben rögzített jogosultságok azonban nem korlátlan jogosultságok,[141] azok a Charta 52. cikk (1) bekezdése alapján *„törvény által, és e jogok lényeges tartalmának tiszteletben tartásával korlátozhatók. Az arányosság elvére figyelemmel, korlátozásukra csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja."* A korlátozást lehetővé tevő jogszabályi rendelkezésnek meg kell határoznia a korlátozás terjedelmét,[142] továbbá a szigorúan szükséges határokon belül kell maradnia, azaz arányosnak kell lennie.[143] *Maria Giacalone* ezzel kapcsolatban kétségesnek tartja, hogy az USA joga kellően világos és precíz a korlátozások megfogalmazása tekintetében.[144]

Ezzel kapcsolatban rögzítendő, hogy a 14086. sz. elnöki rendelet olyan jogszabály, amely ugyan nem kongresszusi, tehát törvényi szinttel összemérhető, de mégis jogi keretrendszert ad a korlátozásnak, és véleményem szerint minősülhet ennek

[137] Batlle, Sergi–van Waeyenberge, Arnaud: EU–US Data Privacy Framework: A First Legal Assessment. *European Journal of Risk Regulation,* 2023/1, 196. (DOI: 10.1017/err.2023.67)

[138] Ennek alapján az EDPB azonos kritikákat is megfogalmazott az elvekkel kapcsolatban. Lásd 5/2023. sz. vélemény a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről. https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_hu.pdf (2024. 07. 23.) 3–4.

[139] EU–USA Adatvédelmi Keretrendszer Határozat (120)–(126) preambulumbek.; Executive Order 14086. Sec. 2. (c) (iii).

[140] *Schrems I ítélet* 86–87. bek.; 1/15. sz. vélemény 122–124. és 126. bek.; *Schrems II ítélet* 164. és 171. bek.

[141] 1/15. sz. vélemény 136–138. bek.; *Schrems II ítélet* 172–174. bek.

[142] 1/15. sz. vélemény 139. bek.; *Schrems II ítélet* 175. bek.

[143] 1/15. sz. vélemény 140. bek.; *Schrems II ítélet* 176. bek.

[144] Giacalone, Maria: Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework. *European Papers,* 2023/1, 152–154. (DOI: 10.15166/2499-8249/644)

alapján „jogalkotási aktusnak", ami az EUB esetjogának elvárása a „törvényi szint" vonatkozásában.[145] A szakirodalomban ezzel szemben találunk olyan álláspontot, amely szerint az elnöki rendelet már jogforrási formája miatt alkalmatlan lehet céljának elérésére, ugyanis nem módosítja a FISA nem amerikai állampolgárok célzott megfigyelését lehetővé tevő kongresszusi, tehát felsőbb szintű normákat.[146] A rendelet részletesen szabályozza, hogy milyen célokból és milyen korlátozások keretei között van lehetőség az érintettek magánszférájába történő beavatkozásra. Álláspontom szerint ugyanakkor az Egyesült Államok túlzottan tág körben határozta meg az alapvető jogokba való beavatkozás legitim céljait, és a korlátozások egy része sem jelent a látszatra való törekvésnél többet.

Elsőként érdemes kiemelni, hogy természetesen az elnöki rendelet által meghatározott bizonyos legitim beavatkozási célok megfeleltethetőek az EU általános érdekű céljainak, úgymint a terrorizmusból, a túszok szedéséből, a merényletekből (asszaszináció), tömegpusztító fegyverek birtoklásából és nemzetközi bűncselekményekből stb. eredő fenyegetésekkel szembeni védelem.[147] Más célok ugyanakkor minden bizonnyal nem tekinthetők ilyennek, úgymint külföldi kormányok vagy külföldi szervezetek képességeinek, szándékainak és tevékenységeinek megértése az Egyesült Államok nemzetbiztonságának védelme érdekében.[148] E célok túl általánosak és homályosak a világosság és egyértelműség általánosságban érvényesülő követelményeinek betartásához.[149]

Szükséges utalni arra a rendelkezésre is, ami szerint a hozzáférés megengedhető, ha a megfelelően képzett hivatalnok *véleménye* szerint valakinek meg kell ismernie a személyes adatot, és ennek során *megalapozottan hiheti,* hogy a személyes adatok megfelelő védelemben részesülnek majd, amely véleményem szerint csak egy látszat korlátozást jelent.[150]

Nagyobb problémát jelent ugyanakkor az, hogy az elnöki rendelet szó szerint rögzíti, hogy a beavatkozás olyankor is lehetséges, ha az nem szigorúan szükséges az elérendő megerősített hírszerzési prioritás előmozdítása érdekében. Ugyan ebben az esetben is a kevésbé beavatkozó intézkedéseket kell előnyben részesíteni,[151] ez azonban semmilyen módon nem kikényszeríthető.

A tömeges megfigyelés, valamint az adatmegőrzési idők meghatározásának módja szintén felveti a megfelelőség kérdését. Az elnöki rendelet ugyan rögzíti, hogy a célzott adatgyűjtést kell előnyben részesíteni, ugyanakkor szűken meghatározott keretek között lehetővé teszi a tömeges megfigyelést bizonyos célok elérése érdekében, ha a megerősített nemzetbiztonsági prioritás észszerűen más módon nem érhető el.[152] Ha mindezt összevetjük az irányadó EUB gyakorlattal, akkor láthatjuk,

[145] 1/15. sz. vélemény 145–146. bek.

[146] Batlle–van Waeyenberge: i. m., 195–196.

[147] Executive Order 14086 Sec 2. (b) (i) (A) (5)–(7), (10). Az EU általános érdekű céljaihoz vö. 1/15. sz. vélemény 148–149. bek.

[148] Executive Order 14086 Sec 2. (b) (i) (A) (1)–(2).

[149] 1/15. sz. vélemény 181. bek.

[150] Executive Order 14086 Sec 2. (c) (iii) (A) (1) (c).

[151] Executive Order 14086 Sec 2. (c) (i) (A).

[152] Executive Order 14086 Sec 2. (c) (ii).

hogy a személyes adatokhoz való általános, megkülönböztetés nélküli (tehát a jelen helyzetben tömeges) hozzáférés állami hatóságok részéről ellentétes az uniós joggal, tekintve, hogy olyan személyek esetében is sor kerül erre, akik esetében semmilyen jel nem utal arra, hogy fenyegetést jelentenének a nemzetbiztonságra.[153] Ugyanakkor nem ellentétes az uniós joggal az általános és megkülönböztetés nélküli adatgyűjtés valós, közvetlen és előre látható súlyos nemzetbiztonsági fenyegetés esetén, mégpedig olyan módon, hogy a tömeges megfigyelést elrendelő határozat bíróság vagy független hatóság által tényleges ellenőrzésnek vethető alá, az adatmegőrzési idő pedig a feltétlenül szükséges mértékre korlátozódik.[154] Álláspontom szerint az elnöki rendelet szabályozása már a valós, közvetlen és előre látható súlyos nemzetbiztonsági fenyegetés tesztjén elbukik, tekintve, hogy az amerikai szabályozás távolibb fenyegetések esetén is hozzáférési jogalapot biztosít, amelyek egyértelműen nem közvetlenek vagy előre láthatóak, az elnöki rendelet ugyanis kizárólag annyit emel ki, hogy a tömeges megfigyelés célja lehet például a terrorizmus elleni védelem. Tekintve, hogy itt semmilyen korlátozást nem találunk az ebből eredő fenyegetés mértékére, így az semmiképpen sem lehet azonos az uniós jog által megkívánt szinttel.[155] *Maria Giacalone* osztja ezt a következtetést, azzal, hogy megjegyzi, a tömeges megfigyelés általánosságban nem tartja tiszteletben a kérdéses alapvető jogok lényegi tartalmát.[156] Az amerikai jog tekintetében említést érdemel, hogy a tömeges megfigyelésre azután már nincs jogi lehetőség, hogy az adatok továbbítása megtörtént az Egyesült Államokba.[157] A bírósági és hatósági felülvizsgálat ugyan megvan, de ennek hatékonysága kérdéseket vet fel, amire a 3.2. alpontban visszatérek.

Az adatmegőrzési idő kérdése nemcsak a tömeges megfigyelés esetében merül fel kérdésként – tudniillik csak a feltétlenül szükséges mértékűre korlátozódik-e –, hanem általánosságban is. Az elnöki rendelet ugyanis az adatmegőrzéssel kapcsolatban rögzíti, hogy a nem amerikai személyek személyes adatait annyi ideig lehet kezelni, mint az amerikaiakét, ezt követően pedig törölni kell az adatokat.[158] Nem határozza meg tehát pontosan az adatmegőrzési időket, a megfelelőségi határozatban pedig az Európai Bizottság is jótékony homályban tartja a kérdést.[159] Az amerikai szakirodalom azonban rávilágít, hogy valójában egy ötéves adatmegőrzési periódusról beszélhetünk, amely viszont nem vet fel megfelelőségi aggályokat.[160]

Szintén az amerikai szakirodalom emeli ki, hogy az elnöki rendelet tiszteletben tartja a szükségesség és arányosság uniós jogi elveit, azzal, hogy azokat a megfe-

[153] C-623/17. sz. *Privacy International kontra Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* ügyben 2020. október 6-án hozott ítélet (ECLI:EU:C:2020:790) 80–82. bek.

[154] C-511/18., C-512/18. és C-520/18. sz. *La Quadrature du Net és mások kontra Premier ministre és mások* egyesített ügyekben 2020. október 6-án hozott ítélet (ECLI:EU:C:2020:791) 137–139. bek.

[155] Executive Order 14086 Sec 2. (c) (ii) (B).

[156] Giacalone: i. m., 152–154.

[157] Joel, Axel: Necessity, Proportionality, and Executive Order 14086. *Joint PIJIP/TLS Research Paper Series,* 2023/5.

[158] Executive Order 14086 Sec 2. (c) (iii) (A) (2).

[159] EU–USA Adatvédelmi Keretrendszer Határozat (157) preambulumbek.

[160] Joel: i. m., 31.

lelő amerikai jogi környezetbe, illetve terminológiába ülteti. Kiemelendő az is, hogy e szerint a nézet szerint az amerikai intézményrendszer, beleértve a Kongresszust, az uniós jognak megfelelő, végpontok közötti *(„end-to-end")* ellenőrzést valósít meg a megfigyelési programok tekintetében.[161] A szükségesség és arányosság elvének beépülésére az EDPB is pozitív újdonságként tekint.[162]

Mindebből véleményem szerint az a következtetés vonható le, hogy az EUB vélhetően megállapítaná, hogy az Egyesült Államok jelfelderítési tevékenysége az új amerikai jogszabályok fényében összeegyeztethetetlen az Alapjogi Charta 7–8., illetve 52. cikkeivel. Ebből pedig az a következtetés adódik, hogy az Egyesült Államok nem biztosítja az Unióval lényegében azonos védelmi szintet a személyes adatok védelmének.

3.2. A hatékony jogorvoslathoz való jog

Járulékos, azonban nem kevésbé fontos kérdésként kell megemlíteni az Alapjogi Charta 47. cikke szerinti hatékony jogorvoslathoz való jogot is, amely alapján az érintetteknek tényleges jogorvoslati lehetőségük kell hogy legyen a rájuk vonatkozó személyes adatokhoz való hozzáférés, azok helyesbítése, illetve törlése tekintetében.[163] Kétségtelen, hogy az elnöki rendelet és a rá épülő főügyészi rendelet létrehoz egy jogorvoslati mechanizmust, amelynek keretei között a CLPO hatóságként végez egy elsődleges felülvizsgálatot, majd ezt követi esetlegesen a DPRC általi konkrét bírói felülvizsgálat. Zárójelben megjegyzendő az is, hogy még a bírósági eljárást megelőzően a CLPO mint hatóság előtti eljárás vonatkozásában felmerülhet az állami beavatkozás alapjául szolgáló dokumentumokhoz való hozzáférés az Alapjogi Charta 41. cikke alapján is.

Az Alapjogi Charta 47. cikk (2) bekezdésében meghatározott követelmények alapján *„[m]indenkinek joga van arra, hogy ügyét a törvény által megelőzően létrehozott független és pártatlan bíróság tisztességesen, nyilvánosan és ésszerű időn belül tárgyalja".* Az irányadó kommentárirodalom szerint ahhoz, hogy egy jogorvoslati mechanizmus megfeleljen az uniós jognak, az szükséges, hogy *(i)* bíróságról beszéljünk, és hogy ez *(ii)* függetlenül és pártatlanul működjön, tisztességes és nyilvános eljárás során.[164]

E kontextusban azzal érdemes kezdeni, hogy létezik olyan szakirodalmi álláspont is, ami a DPRC-t nem tekinti bíróságnak, ezt azonban nem támasztja alá semmivel.[165] Ennek alapján tehát elsőként rögzítendő, hogy a szakirodalom és az alapjául szolgáló ítélkezési gyakorlat szerint a „bíróság" önálló fogalommal rendelkezik az EU-jogban, amely leginkább az előzetes döntéshozatali eljárásokkal kapcsolatos

[161] Joel: i. m., 4., 6–12., 15., 30.

[162] 5/2023. sz. EDPB vélemény 5.

[163] *Schrems I ítélet* 95. bek.; *Schrems II ítélet* 187–189. bek.

[164] Természetesen egyéb követelményeket is megállapíthatunk, azonban a konkrét elemzés tekintetében ezek vizsgálata szükséges és egyben elegendő.

[165] Batlle–van Waeyenberge: i. m., 198.

EUB döntések során kristályosodott ki.[166] Akkor beszélhetünk uniós jogi értelemben bíróságról, ha azt jog hozta létre, állandó jelleggel működik, kötelező joghatósággal rendelkezik, jogot alkalmaz és független, illetve pártatlan.[167]

A DPRC esetében vitán felül áll, hogy azt jog, nevezetesen a 14086. sz. elnöki rendelet felhatalmazása alapján a főügyész 5517-2022-es számú rendelete hozta létre. A DPRC működése állandó, döntései kötelezők. A függetlenség tekintetében először érdemes röviden visszakanyarodni a *La Quadrature du Net and Others*-ügyben fentebb hivatkozott követelményre, miszerint legalább a tömeges megfigyelés esetén független hatósági kontrollra vagy bírói felülvizsgálatra van szükség.[168] Tekintve azonban, hogy a CLPO a nemzeti hírszerzés igazgatójának hivatala, valamint a Nemzeti Terrorelhárítási Központ alá tartozik mint megosztott szolgálat,[169] ennek függetlensége megkérdőjelezhető, annak ellenére, hogy az elnöki rendelet szerint a nemzeti hírszerzés igazgatója nem szólhat bele a hatóság eljárásába, illetve visszahívására sem kerülhet sor az eljárás során meghozott döntései miatt, kivéve valóban indokolt esetekben.[170]

Nem ez a helyzet azonban a DPRC esetében. Véleményem szerint a DPRC bíráinak jogállása esetében kellően komoly garanciák érvényesülnek a kiválasztás kritériumai, az eljárás, illetve a visszahívhatóság tekintetében,[171] így függetlenségükhöz ezen a ponton nem férhet kétség. Itt is ki kell emelni, hogy létezik olyan szakirodalmi álláspont, amely a DPRC bíráinak függetlenségét kétségbe vonja azok kormányzati szintről történő kinevezése miatt.[172] Álláspontom szerint ez utóbbi ugyanakkor a működésüket érintő garanciák, illetve a kiválasztásuk során érvényesülő elvek tekintetében kevésbé jelentős aggály lehet. A CLPO és a DPRC vonatkozásában az EUB által megfogalmazott azon elvárás is teljesül, hogy eljárásuk végén kötelező erejű határozatot hoznak.[173]

Más következtetést szükséges levonni azonban, ha a tisztességes és nyilvános eljárás követelményeit vizsgáljuk. A kommentárirodalom itt szintén meghatároz olyan követelményeket, amelyeknek teljesülniük kell az alapjog lényeges tartalmának tiszteletben tartásához. Ilyen a kontradiktórius eljárás (amennyiben ez értelmezhető), a fegyverek egyenlőségének elve, a döntések indokolási kötelezettsége és a nyil-

[166] Sayers, Debbie: VI. Article 47(2)—A Fair and Public Hearing within Reasonable Time. In: Peers, Steve–Hervey, Tamara–Kenner, Jeff–Ward, Angela (eds.): *The EU Charter of Fundamental Rights.* Beck–Hart–Nomos, Oxford–New York–Dublin, 2021, 1339–1341.

[167] Sayers: i. m., 1342.

[168] C-511/18., C-512/18. és C-520/18. sz. egyesített ügyek, 137–139. bek.

[169] https://www.dni.gov/index.php/nctc-who-we-are/organization (2024. 08. 22.).

[170] Executive Order 14086 Sec 3. (c) (iv). Felvethető még az a kérdés is, hogy a CLPO mint hatóság teljesíti-e az uniós jogból fakadó függetlenség követelményét, mert nem biztos, hogy kívül esik a hagyományos közigazgatási struktúrán. Kinevezésére ugyanis a nemzeti hírszerzés igazgatója jogosult, akit pedig az elnök nevez ki. Vö. Csatlós Erzsébet: Az Európai Bíróság ítélete az adatvédelmi ombudsman tisztségének megszüntetéséről. *Jogesetek Magyarázata,* 2015/3, 71–72.; Csatlós Erzsébet: Fejezetek az EU magyar közigazgatásra gyakorolt hatásából: Hogyan legyen egy közigazgatási szerv független. *Közjogi Szemle,* 2014/4, 13. 50 USC 401 Section 102(1).

[171] Executive Order 14086 Sec 3. (d) (i) (A) és (iv).

[172] Batlle–van Waeyenberge: i. m., 198.

[173] Executive Order 14086 Sec 3. (c) (ii) és (d) (ii). Vö. *Schrems II ítélet* 196. bek.

vános tárgyalás.[174] E követelmények megkívánják, hogy a felek hatékonyan részt vehessenek az eljárásban, megismerhessék és megérthessék az ügyet, és legyen lehetőségük észrevételek, valamint kifogások megtételére. Ez magában foglalja a jogot arra, hogy megvizsgálhassák az összes dokumentumot, ami alapján a bíróság eljár. Információ visszatartására csak nemzetbiztonsági okból és szigorúan szükséges keretek között van lehetőség.[175] A bíróság döntését indokolni köteles, amiben legalább az alapvető felmerült kérdéseket szükséges érinteni.[176] Ezen túlmenően a nyilvános tárgyalás tartása is követelmény, amennyiben arra a felek igényt tartanak, amely egyfokú eljárásban kötelező. A nyilvánosság a tárgyalásról kizárható, de a tárgyalás megtartásától ilyen esetbe sem lehet eltekinteni.[177]

Egyfelől rögzítendő, hogy a DPRC döntéseinek alapját a CLPO által készített titkosított *ex parte* dokumentum, valamint a panaszos, a különleges főtanácsnok és a hírszerzés által nyújtott információk és észrevételek képezik.[178] Másfelől a DPRC döntése szintén titkosított, az érintett csak arról kap tájékoztatást, hogy történt-e jogsértés, arról nem, hogy az Egyesült Államok jelfelderítési tevékenysége kiterjedt-e rá avagy sem.[179] Látszólag tehát a DPRC eljárása nem egyeztethető össze az uniós joggal, tekintve, hogy az érintett nem ismerheti meg a döntés alapjául szolgáló iratokat, azokra érdemben nem tud reagálni, illetve a bíróság döntésének indokait sem. Ezt a problémát nem orvosolja az a lehetőség, hogy öt évet követően eshetőlegesen megismerheti ezeket az információkat más eljárás keretei között. Fontos kiemelni azt is, hogy az érintettnek nincs lehetősége sem nyilvános, sem pedig zárt tárgyalást kérni az eljárás során.

Felvetődik ugyanakkor, hogy a fenti korlátozások összeegyeztethetőek-e az uniós joggal a nemzetbiztonsági érdekre való hivatkozás esetén, ami ebben a helyzetben nyilvánvalóan megállja a helyét. Az EUB ezt a kérdést részletesen vizsgálta a *Kadi-ügyekben*. A Bíróság egyik fontos megállapítása volt, hogy ha az érintett nem tudja megismerni a terhére rótt körülményeket, úgy nem is tudja megfelelően ismertetni álláspontját, ezzel pedig sérül a hatékony bírói védelemhez való jog.[180] Az EUB a döntések indokolása kapcsán azt is megállapította, hogy bizonyos helyezetekben jogszerű lehet az információ ilyen értelemben vett visszatartása is, de ezeket a helyzeteket minden esetben egyénileg vizsgálni kell, és amennyiben lehetőség van rá, legalább a döntésre vezető indokok összefoglalását elérhetővé kell tenni.[181]

[174] Sayers: i. m., 1347–1350.; Pech, Laurent: V. Article 47(2)—An Independent and Impartial Tribunal Previously Established by Law. In: Peers, Steve–Hervey, Tamara–Kenner, Jeff–Ward, Angela (eds.): *The EU Charter of Fundamental Rights.* Beck–Hart–Nomos, Oxford–New York–Dublin, 2021. 1361–1370.

[175] Sayers: i. m., 1347.; Pech: i. m., 1361–1362.

[176] Sayers: i. m., 1347.; Pech: i. m., 1367.

[177] Sayers: i. m., 1347.; Pech: i. m., 1368–1369.

[178] Executive Order 14086 Sec 3. (d) (i) (D).

[179] Executive Order 14086 Sec 3. (d) (i) (F) és (H).

[180] C-402/05. P. és C-415/05. P. sz. *Yassin Abdullah Kadi, Al Barakaat International Foundation kontra az Európai Unió Tanácsa, az Európai Közösségek Bizottsága, Nagy-Britannia és Észak-Írország Egyesült Királysága* ügyben 2008. szeptember 3-án hozott ítélet (ECLI:EU:C:2008:461) 349. bek.

[181] C-584/10. P., C-593/10. P. és C-595/10. P. sz. *Európai Bizottság* (C-584/10. P.), *az Európai Unió Tanácsa* (C-593/10. P.), *Nagy-Britannia és Észak-Írország Egyesült Királysága* (C-595/10. P.) *kontra Yassin Abdul-*

Ezt a követelményt „kodifikálja" a Törvényszék Eljárási Szabályzatának 105. cikke is, ami az EU, illetve egy vagy több tagállam biztonságát és egyéb kérdéseket érintő tájékoztatások vagy mellékletek kezelésével foglalkozik. E szerint az ellenérdekű féllel közölni kell *„a tájékoztatások vagy mellékletek olyan nem bizalmas változatát vagy nem bizalmas összefoglalását, amelyben szerepel azok lényegi tartalma, és a lehető legszélesebb körben lehetővé teszi az ellenérdekű felperes vagy alperes számára, hogy előadja észrevételeit".*[182] Megjegyzendő ugyanakkor, hogy a szakirodalom így is kritikát fogalmaz meg a „zárt ajtók mögötti" eljárás kapcsán, különösen annak a Bíróság legitimációjára gyakorolt hatása tekintetében.[183] Ezt az álláspontot tükrözi a *GM-ügy* is, ahol az EUB megismételte, hogy a határozatot alátámasztó okok lényegét legalább az érintett rendelkezésére kell bocsátani.[184] E lényegi tartalom a *Kadi II ügyben* kapott pontosítást, mégpedig akként, hogy az indokok egyikének legalább kellően pontosnak, konkrétnak és alátámasztottnak kell lennie ahhoz, hogy önmagában igazolja a döntést.[185]

A témával foglalkozó szakirodalom a fentiek mellett a bírák újraválasztásával kapcsolatban fogalmaz meg függetlenségi aggályokat, felhívja a figyelmet az átláthatóság hiányára és arra is, hogy az érintettek a gyakorlatban a lehető legkevesebb esetben értesülnek arról bármilyen formában, hogy ők megfigyelés célpontjai lettek, így jogorvoslati lehetőséggel sem képesek élni.[186] Az EDPB előzetes véleménye a jogorvoslati rendszer tekintetében pozitív volt, ugyanakkor a fellebbezés hiányát és a döntések átláthatatlanságát e testület is kifogásolta.[187]

Tekintve, hogy a jelen helyzetben az érintett már a CLPO érdemi döntése esetében is csak egy bináris eredményt kap, megállapítható, hogy a DPRC előtti eljárás kiüresedik, hiszen a panaszosnak nem áll módjában ismertetni álláspontját, sőt azt sem tudja, hogy megfigyelés célpontja volt-e. A DPRC döntéseinek indokolása szintén ellentétes az uniós joggal, hiszen egyfelől nincs egyéni vizsgálat a titkosított döntés vonatkozásában, másfelől a bíróság az indokok összefoglalását sem teszi közzé.

Mindebből az következik, hogy az Alapjogi Charta 47. cikkének sérelme miatt az EUB szintén nem állapíthatja meg, hogy az USA az Unióval lényegében azonos védelmi szintet biztosít.

Iah Kadi, Francia Köztársaság egyesített ügyekben 2013. július 18-án hozott ítélet (ECLI:EU:C:2013:518) 128–129. bek.

[182] A Törvényszék eljárási szabályzata, HL L 105., 2015.4.23., 1–66. 105. cikk (6) bek.

[183] Leppävirta, Liisa: Procedural Rights in the Context of Restrictive Measures: Does the Adversarial Principle Survive the Necessities of Secrecy? *European Papers,* 2017/2. 668–669. (DOI: 10.15166/2499-8249/172)

[184] C-159/21. sz. *GM kontra Országos Idegenrendészeti Főigazgatóság, Alkotmányvédelmi Hivatal, Terrorelhárítási Központ* ügyben 2022. szeptember 22-én hozott ítélet (ECLI:EU:C:2022:708) 60. bek.

[185] C-584/10 P., C-593/10 P. és C-595/10 P. sz. ítélet, 130. bek. Vö. Csatlós Erzsébet: Az Európai Unió Bíróságának GM-ügyben hozott döntése. *Jogesetek Magyarázata,* 2023/4, 63.

[186] Dimović, Zoran: Analyising the EU Data Privacy Implications Resulting From Executive Order 14086: A Legal Perspective. *LeXonomica,* 2024/1. (DOI: 10.18690/lexonomica.16.1.85-110.2024) 97.

[187] 5/2023. sz. EDPB vélemény 6.

4. Következtetések

A fentiek alapján megállapítható, hogy ugyan számottevő és lényeges változások következtek be az amerikai jogban a megfigyelési programokat illetően, ezek az EU–USA Adatvédelmi Keretrendszer Határozat mint bizottsági megfelelőségi határozat ellenére sem felelnek meg a személyes adatok számára biztosítandó lényegében azonos védelmi szintnek, amely viszont a GDPR-ból és a Bíróság ítélkezési gyakorlatából következő követelmény.

A megfigyelési programok egyfelől sértik az Alapjogi Charta 7–8., illetve 52. cikkeit, amikor a feltétlenül szükséges mértéken átlépve férnek hozzá amerikai hatóságok európaiak személyes adataihoz. E személyek pedig nem rendelkeznek a Charta 47. cikke szerinti hatékony jogorvoslati joggal a hatóságok általi hozzáférések esetében, tekintve, hogy az eljárás titkosított adatokon alapul, mellőzi a tárgyalást és indokolást sem fűz a döntésekhez.

Ennek alapján az a következtetés vonható le, hogy *Latombe* képviselő úr keresete, illetve a NOYB által ebben az évben tervezett eljárás valószínűsíthetően azzal végződik majd, hogy az EUB érvénytelenné nyilvánítja az EU–USA Adatvédelmi Keretrendszer Határozatot. A Schrems III döntés jelen állás szerint beláthatatlan következményekkel járna a transzatlanti gazdasági kapcsolatokra, tekintettel arra, hogy az általános szerződési feltételeken, valamint a különös helyzetekben való adattovábbítások az USA hatóságai által megvalósított megfigyelési programok, valamint a kivételszabály főszabállyá változása miatt – a hatósági gyakorlat alapján – szintén alkalmatlanok a harmadik országba történő adattovábbítás megalapozására. Egy potenciális Schrems III döntéssel tehát a Bíróság effektíve megtilthatja az Egyesült Államokba történő személyes adattovábbítást, aminek az egyetlen reális alternatívája az adatlokalizáció lehet, ez azonban az adatszuverenitás vagy digitális szuverenitás elvének alkalmazása nélkül szintén alkalmatlan a probléma valódi megoldására, nem is beszélve a lehetséges gazdasági károkról.

A fentiek alapján az is látszik, hogy a probléma egyetlen reális megoldását az jelenthetné, ha az USA felhagyna a jelenlegi kiterjedt megfigyelési programjaival, és/vagy ha ez nem megvalósítható, úgy azt megfelelő felügyelettel és jogorvoslati lehetőségekkel látná el az alapjogsérelmek elkerülése érdekében. Voltaképpen tehát a problémát a jelenlegi helyzetben az oldhatná meg, ha az USA átvenné az EU adatvédelmi jogi szemléletmódját. Ezek azonban véleményem szerint legfeljebb illuzórikus megoldásnak tekinthetők.