A Testület véleménye (a 70. cikk (1) bekezdésének s) pontja)

5/2023. sz. vélemény a személyes adatoknak az EU–USA adatvédelmi keret szerinti megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről

Elfogadás időpontja: 2023. február 28.

Összefoglaló

Az Európai Bizottság 2022. december 13-án megfelelőségi határozattervezetet (a továbbiakban: határozattervezet) tett közzé, amely olyan mellékleteket tartalmaz, melyek a transzatlanti személyesadat-csere egy új, az USA az Európai Unió Bírósága (a továbbiakban: EUB) által 2020. július 16-án, a Schrems II. ügyben érvénytelenített korább adatvédelmi pajzsának helyébe lépő keretét, az EU–USA adatvédelmi keretet (a továbbiakban: adatvédelmi keret) alkotják. Az adatvédelmi keret legfontosabb elemét az EU–USA adatvédelmi keret elvei alkotják, beleértve a kiegészítő elveket is (a továbbiakban együttesen: az adatvédelmi keret alapelvei).

A Bizottság az (EU) 2016/679 európai parlamenti és tanácsi rendelet[1] (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének s) pontjával összhangban kikérte az Európai Adatvédelmi Testület (a továbbiakban: EDPB) véleményét a határozattervezetről.

Az EDPB a határozattervezet vizsgálata alapján értékelte az USA-ban biztosított védelem szintjének megfelelőségét. Az EDPB mind a kereskedelmi vonatkozásokat, mind pedig az Egyesült Államok hatóságai által az EU-ból továbbított személyes adatokhoz való hozzáférést és azok felhasználását megvizsgálta.

Az EDPB figyelembe vette az általános adatvédelmi rendeletben meghatározott, alkalmazandó uniós adatvédelmi jogi keretet, valamint az Európai Unió Alapjogi Chartájának 7. és 8. cikkében ás az emberi jogok európai egyezményének 8. cikkében foglalt, a magánélethez és az adatvédelemhez való alapvető jogokat. Megvizsgálta továbbá a Charta 47. cikkében meghatározott, a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogot, valamint a különböző alapvető jogokkal kapcsolatos ítélkezési gyakorlatot.

Emellett az EDPB figyelembe vette az Európai Adatvédelmi Testület által elfogadott Megfelelőségi referenciában foglalt követelményeket is[2].

Az EDPB fő célja, hogy véleményt adjon az Európai Bizottságnak az azon természetes személyeknek nyújtott védelem szintjének megfelelőségéről, akiknek személyes adatai továbbításra kerülnek az Amerikai Egyesült Államokba. Fontos annak felismerése, hogy az Európai Adatvédelmi Testület nem várja el azt, hogy az amerikai egyesült államokbeli adatvédelmi keret reprodukálja az európai adatvédelmi jogot.

Az EDPB azonban emlékeztet arra, hogy ahhoz, hogy a harmadik ország jogszabályai megfelelő adatvédelmi szintet nyújtónak minősüljenek, azoknak az általános adatvédelmi rendelet 45. cikke és az Európai Unió Bíróságának ítélkezési gyakorlata által megkövetelteknek szerint, az EU-ban garantálttal lényegében egyenértékű védelmi szintet kell biztosítaniuk az érintettek számára.

1.1. Általános adatvédelmi szempontok

Az adatvédelmi keret úgy rendelkezik, hogy az adatvédelmi keret elveinek az adatvédelmi keret szervezetei általi betartása bizonyos esetekben korlátozható (pl. bírósági végzésnek vagy a közérdeknek való megfeleléshez szükséges mértékben). Annak érdekében, hogy jobban meg lehessen

[1] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1 o.).

[2] A 29. cikk szerinti munkacsoport, Megfelelőségi referencia, WP 254 rev.01, 2017. november 28., amely legutóbb 2018. február 6-án került felülvizsgálatra és elfogadásra, és amelyet az EDPB 2018. május 25-én hagyott jóvá (a továbbiakban: megfelelőségi referencia).

határozni ezeknek a mentességeknek az érintettek védelmi szintjére gyakorolt hatását, az EDPB azt javasolja, hogy a Bizottság a határozattervezetben egyértelműsítse a mentességek hatályát, beleértve az Egyesült Államok jogszabályainak értelmében alkalmazandó biztosítékokat is.

Az EDPB megjegyzi, hogy a mellékletek szerkezete és számozása meglehetősen megnehezíti az információk megtalálását és az azokra való hivatkozást. Ez hozzájárul az új keret átfogó, összetett megjelenítéséhez, amely mellékleteiben különböző jogi kötőerejű dokumentumokat egyesít, és amely esetlegesen nehezíti az adatvédelmi keret elveinek az érintettek, az adatvédelmi keret szervezetei és az uniós adatvédelmi hatóságok általi megfelelő megértését. Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy a terminológiát az egész adatvédelmi keretben következetesen kellene használni. Ehhez hasonlóan hiányzik néhány alapvető fogalom meghatározása is[3].

Az EDPB üdvözli az adatvédelmi keret elveinek aktualizálását[4], amely kötelező jogi keretet teremt majd az adatvédelmi keret szervezetei számára, ugyanakkor megjegyzi, hogy a határozattervezet preambulumbekezdéseiben szereplő számos módosítás és kiegészítő magyarázat ellenére az adatvédelmi keret elvei, amelyeket az adatvédelmi keret szervezeteinek be kell tartaniuk, az adatvédelmi pajzs értelmében alkalmazandó elvekhez viszonyítva (amelyeken a 29. cikk szerinti munkacsoport [a továbbiakban: WP29] és az Európai Adatvédelmi Testület éves közös felülvizsgálatai alapultak) lényegében változatlanok maradtak. Az adatvédelmi keret elvei nagymértékben megegyeznek az adatvédelmi pajzs tervezetében szereplő azon elvekkel is, amelyre a 29. cikk szerinti munkacsoport 2016-os véleményét alapozta[5]. Az adatvédelmi keret lényegében változatlanul hagyott elveinek vonatkozásában az Európai Adatvédelmi Testület nem tartja szükségesnek a 29. cikk szerinti munkacsoport által korábban tett valamennyi észrevétel megismétlését. Az EDPB úgy határozott, hogy olyan konkrét szempontokra összpontosít, amelyeket a jogi és technológiai környezet fejlődésének tükrében napjainkban még relevánsabbnak tart.

Az EDPB például megjegyzi, hogy egyes, a 29. cikk szerinti munkacsoport és az EDPB által az adatvédelmi pajzs elveivel kapcsolatban korábban felvetett, aggodalomra okot adó kérdések továbbra is fennállnak. Ezek különösen az érintettek jogaihoz (például a tájékoztatáshoz való jog alóli néhány kivételhez, valamint a kifogásolási jog időzítéséhez és módozataihoz), a kulcsfontosságú fogalommeghatározások hiányához, az adatvédelmi keret adatfeldolgozókra való alkalmazásával kapcsolatos egyértelműség hiányához, valamint a nyilvánosan hozzáférhető információkra vonatkozó széles körű mentességhez kapcsolódnak[6].

Az EDPB továbbá ismételten hangsúlyozni kívánja , hogy azon természetes személyek védelmének szintjét, akiknek az adatait továbbítják, nem áshatják alá a továbbított adatok eredeti címzettjétől történő újbóli továbbítások[7]. Az EDPB ismételten felkéri a Bizottságot annak tisztázására, hogy az eredeti címzett által a harmadik országbeli átvevővel szemben előírt biztosítékoknak a harmadik ország jogszabályainak fényében az adatvédelmi keret értelmében történő adattovábbítást megelőzően érvényesnek kell lenniük.

---

[3] Ez a helyzet áll fenn a „megbízott" és az „adatfeldolgozó" kifejezések esetében. A „humánerőforrás (HR)-adatok" fogalmát továbbá még meg kell vitatni az Egyesült Államok hatóságaival.

[4] Például annak tisztázását, hogy a kódolt adatok személyes adatok.

[5] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről, az elfogadási időpontja: 2016. április 13. (a továbbiakban: a 29. cikk szerinti munkacsoport 01/2016. sz. véleménye).

[6] EU–USA adatvédelmi pajzs – Harmadik éves közös felülvizsgálat, az Európai Adatvédelmi Testület 2019. november 12-én elfogadott jelentése, 11. pont.

[7] Általános adatvédelmi rendelet – Megfelelőségi referencia, 3. fejezet A. pont 9. alpont.

Különös figyelmet kell fordítani az automatizált döntéshozatal és profilalkotás gyors fejlődésére, amely egyre inkább a mesterségesintelligencia-technológiák révén valósul meg. Az EDPB üdvözli a Bizottság hivatkozásait az Egyesült Államok vonatkozó jogszabályai által a különböző területeken nyújtott konkrét biztosítékokra[8]. Úgy tűnik azonban, hogy a természetes személyek védelmének szintje eltérő attól függően, hogy milyen ágazatspecifikus szabályok – ha vannak ilyenek – alkalmazandók a szóban forgó helyzetre. Az Európai Adatvédelmi Testület fenntartja, hogy a megfelelő biztosítékok nyújtásához az automatizált döntéshozatalra vonatkozó konkrét szabályokra van szükség, beleértve a természetes személy azon jogát, hogy megismerje az alkalmazott logikát, megtámadja a döntést és emberi beavatkozást kérjen, amennyiben a döntés őt jelentős mértékben érinti.

Az EDPB emlékeztet az adatvédelmi keret hatékony felügyeletének és érvényesítésének fontosságára, és alapvető fontosságúnak tartja az érdemibb követelményekkel kapcsolatos megfelelőség-ellenőrzések alkalmazását. Az EDPB szorosan nyomon követi majd ezeket a szempontokat, többek között az időszakos felülvizsgálatok keretében. Az EDPB tudomásul veszi a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission, a továbbiakban: FTC)[9] és a Közlekedési Minisztérium (Department of Transportation, a továbbiakban DOT)[10] leveleiben szereplő megújított kötelezettségvállalásokat a jogérvényesítés tekintetében (pl. az adatvédelmi keret feltételezett megsértésére irányuló vizsgálat prioritásként való kezelése).

Az EDPB megjegyzi, hogy az uniós érintettek számára hét jogorvoslati lehetőség biztosított, amennyiben személyes adataikat az adatvédelmi keretet megsértve kezelik. Ezek a jogorvoslati mechanizmusok megegyeznek a korábbi adatvédelmi pajzsban meghatározottakkal, amelyekkel kapcsolatban a 29. cikk szerinti munkacsoport észrevételeket fogalmazott meg[11]. Az EDPB szorosan nyomon követi majd ezeknek a jogorvoslati mechanizmusoknak a hatékonyságát, többek között az időszakos felülvizsgálatok keretében.

1.2. Az Európai Unióból továbbított személyes adatokhoz való hozzáférés és az ilyen adatok felhasználása az egyesült államokbeli közigazgatási szervek által

A határozattervezetben az Európai Bizottság rögzíti, hogy „az Egyesült Államok hatóságainak közérdekből – különösen bűnüldözési és nemzetbiztonsági célokból– történő beavatkozása azon természetes személyek alapvető jogaiba, akiknek személyes adatait az EU–USA adatvédelmi keret értelmében az Unióból az Egyesült Államokba továbbítják, a szóban forgó jogszerű cél eléréséhez feltétlenül szükséges mértékre korlátozódik, és az említett beavatkozással szemben hatékony jogvédelem áll fenn[12]”.

Az Európai Bizottság az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítéséről szóló 14086. sz. elnöki rendelet (EO 14086) széles körű értékelését követően jutott erre a következtetésre. A 14086. sz. elnöki rendeletet az Egyesült Államok elnöke 2022. október 7-én adta ki azon tárgyalásokat követően, amelyeket az Európai Bizottság az adatvédelmi pajzsnak nevezett korábbi megfelelőségi határozat az Európai Unió Bírósága (EUB) általi érvénytelenítésének nyomán az Amerikai Egyesült Államok kormányával folytatott.

Az EDPB üdvözölné, ha a határozat nemcsak hatálybalépésének, hanem elfogadásának is feltétele lenne többek között az, hogy az Egyesült Államok valamennyi hírszerző ügynöksége elfogadja a

[8] A határozattervezet (35) preambulumbekezdése.
[9] A határozattervezet IV. melléklete.
[10] A határozattervezet V. melléklete.
[11] Lásd különösen a 29. cikk szerinti munkacsoport 01/2016. sz. véleménye 2.2.6. szakaszának a) pontját.
[12] A határozattervezet (195) preambulumbekezdése.

14086. sz. elnöki rendelet végrehajtását célzó aktualizált szabályzatokat és eljárásokat. Az Európai Adatvédelmi Testület azt ajánlja a Bizottságnak, hogy értékelje ezeket az aktualizált szabályzatokat és eljárásokat, és az értékelést ossza meg az Európai Adatvédelmi Testülettel.

Ami az Egyesült Államokba továbbított személyes adatokhoz való kormányzati hozzáférést illeti, az EDPB elemzését az új 14086. sz. elnöki rendelet értékelésére összpontosította, mivel annak tényleges célja az EUB azon Schrems II. ítéletében azonosított hiányosságok kezelése és orvoslása, melyben az EUB a korábbi megfelelőségi határozatot érvénytelennek találta.

Az Európai Adatvédelmi Testület elismeri, hogy az Egyesült Államok jelfelderítési tevékenységekre vonatkozó jogi keretét a 14086. sz. elnöki rendelet elfogadásával módosították, és az ebben a rendeletben foglalt további biztosítékokat jelentős előrelépésnek tekinti. A 14086. sz. elnöki rendelet bevezeti a szükségesség és arányosság fogalmát az Egyesült Államok jelfelderítési jogi keretébe, és – amennyiben az EU minősített regionális gazdasági integrációs szervezetként kerül megjelölésre – új jogorvoslati mechanizmust is biztosít az uniós természetes személyek számára. Az EDPB úgy véli, hogy az új jogorvoslati mechanizmus jelentősen javult az adatvédelmi pajzs keretében működő korábbi, úgynevezett ombudsmani mechanizmushoz képest. A korábbi jogi kerettel ellentétben, amely nem teremtett jogokat az uniós természetes személyek számára, amint azt az EUB kifejezetten megállapította, az új 14086. sz. elnöki rendelet ilyen jogosultságokat teremt, és több biztosítékot nyújt az Adatvédelmi Felülvizsgálati Bíróság függetlenségére, valamint hatékonyabb hatáskört biztosít a jogsértések orvoslására.

A 14086. sz. elnöki rendeletben foglalt további biztosítékok az Európai Unió Bíróságának és az Emberi Jogok Európai Bíróságának (a továbbiakban: EJEB) ítélkezési gyakorlata alapján az EDPB által szabványként kidolgozott alapvető európai garanciákkal való összehasonlította során az EDPB értékelésében még mindig számos, további pontosításra szoruló, figyelmet igénylő vagy aggodalomra okot adó pontot azonosított. Ezek a pontok azt tükrözik, hogy bár az EDPB véleményét a Schrems II. ítéletre alapozta, értékelésének hatóköre szükségszerűen olyan megfontolásokat is magában foglal, amelyek túlmutatnak a Schrems II. ítélet konkrét megállapításain.

Az EDPB úgy véli, hogy az Egyesült Államok jogi keretén belül további pontosításra van szükség különösen az „átmeneti, nagy mennyiségben történő adatgyűjtéssel”, illetve a (nagy mennyiségben) gyűjtött adatok további megőrzésével és terjesztésével kapcsolatos kérdések tekintetében.

Mivel az alapvető egyenértékűség vizsgálata nem azonosításra irányuló vizsgálat, és mivel a jelfelderítésre vonatkozó új jogi keretben foglalt biztosítékok megerősítésre kerültek, az EDPB által meghatározott fő figyelmet érdemlő és aggodalomra okot adó pont a biztosítékok egészben történő értékelésére összpontosít, olyan holisztikus megközelítést követve, amely az adatkezelés teljes ciklusára vonatkozó biztosítékokra kiterjed az adatgyűjtéstől kezdve az adatok terjesztéséig, beleértve a felügyelet és a jogorvoslat elemeit is.

E tekintetben az EDPB a következő megállapításokat emeli ki:

Bár az EDPB elismeri, hogy a 14086. sz. elnöki rendelet bevezeti a jelfelderítésre vonatkozó jogi keretbe a szükségesség és az arányosság fogalmát, hangsúlyozza, hogy szorosan nyomon kell követni e módosítások gyakorlati hatásait, beleértve az elnöki rendelet által meghatározott biztosítékokat az ügynökségek szintjén végrehajtó belső szabályzatok és eljárások felülvizsgálatát is.

Az EDPB üdvözli továbbá, hogy a 14086. sz. elnöki rendelet felsorolja azokat a konkrét célokat, amelyek érdekében az adatgyűjtés megvalósulhat vagy nem valósulhat meg, ugyanakkor megjegyzi, hogy a

célkitűzések az új nemzetbiztonsági szükségletek fényében további – nem feltétlenül nyilvános – célkitűzésekkel bővíthetők.

A jelenlegi keret hiányosságaként az EDPB különösen azt állapította meg, hogy az Egyesült Államok jogi kerete az adatok nagy mennyiségben történő gyűjtésének a 12333. sz. elnöki rendelet értelmében való lehetővé tételekor nem írja elő a független hatóság általi előzetes engedélyezés követelményét, amint azt az EJEB legutóbbi ítélkezési gyakorlata előírja, és nem ír elő bíróság vagy azzal egyenértékű független szerv általi szisztematikus, független, utólagos felülvizsgálatot sem. Ami a megfigyelés a külföldi hírszerzői tevékenység megfigyeléséről szóló amerikai törvény (FISA) 702. szakasza szerinti előzetes, független engedélyezését illeti, az Európai Adatvédelmi Testület sajnálatát fejezi ki amiatt, hogy a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság (a továbbiakban: FISC) a nem egyesült államokbeli személyeket célzó program tanúsításakor nem vizsgálja felül a programkérelem 14086. sz. elnöki rendeletnek való megfelelését, annak ellenére, hogy az a programot végrehajtó hírszerző hatóságokra nézve kötelező érvényű. Az Európai Adatvédelmi Testület véleménye szerint mindazonáltal az e rendeletben foglalt további biztosítékokat figyelembe kell vennie többek között a FISC-nek is. Az EDPB emlékeztet arra, hogy az Adatvédelmi és Polgári Szabadságjogi Felügyelő Tanács (Privacy and Civil Liberties Oversight Board, a továbbiakban: PCLOB) jelentései különösen hasznosak lennének annak értékeléséhez, hogy a 14086. sz. elnöki rendelet biztosítékai hogyan kerülnek majd végrehajtásra, illetve azokat hogyan alkalmazzák azokban az esetekben, amikor a FISA 702. szakasza és a 12333. sz. elnöki rendelet értelmében történik adatgyűjtés.

A jogorvoslati mechanizmust illetően az EDPB elismeri, hogy jelentős előrelépések történtek az Adatvédelmi Felülvizsgálati Bíróság (Data Protection Review Court, a továbbiakban: DPRC) hatáskörével és annak az ombudsmanhoz viszonyítva megnövekedett függetlenségével kapcsolatban. Az EDPB továbbá elismeri az új jogorvoslati mechanizmusban előirányzott olyan további biztosítékokat, mint a különleges ügyvédek szerepét, amely magában foglalja a panaszos érdekeit szolgáló képviseletet, valamint a jogorvoslati mechanizmus PCLOB általi felülvizsgálatát is. Bár az Európai Adatvédelmi Testület figyelembe veszi a nemzetbiztonság jellegét és a 14086. sz. elnöki rendelet által nyújtott biztosítékokat, aggodalmát fejezi ki a DPRC azon standard válaszának általános alkalmazása, amely arról értesíti a panaszost, hogy nem azonosítottak jogsértéseket, vagy hogy a megfelelő jóvátételt előíró határozatot adtak ki, és egyúttal amiatt, hogy a válasz ellen nem lehet fellebbezni. Tekintettel a jogorvoslati mechanizmus fontosságára, az EDPB felkéri a Bizottságot, hogy szorosan kövesse nyomon e mechanizmus gyakorlati működését.

Az Európai Adatvédelmi Testület elvárja, hogy a Bizottság eleget tegyen a megfelelőségi határozat sürgős esetben történő felfüggesztésére, hatályon kívül helyezésére vagy módosítására vonatkozó kötelezettségvállalásának, különösen abban az esetben, ha az Egyesült Államok kormányzata úgy döntene, hogy korlátozza az elnöki rendeletben foglalt biztosítékokat[13].

Összességében az EDPB pozitívan értékeli az elnöki rendelet által a korábbi jogi kerethez képest biztosított jelentős javulást, különösen a szükségesség és az arányosság elvének bevezetése, valamint az uniós érintettek egyéni jogorvoslati mechanizmusa tekintetében. Tekintettel a kifejtett aggályokra és a szükséges pontosításokra, az EDPB ezen aggályok kezelését, illetve azt javasolja, hogy a Bizottság bocsássa rendelkezésre a kért pontosításokat annak érdekében, hogy megszilárdítsa a határozattervezet alapjait, és biztosítsa ezen új jogi keret konkrét végrehajtásának szoros nyomon követését – különös tekintettel az abban foglalt biztosítékokra – a jövőbeli közös felülvizsgálatok során.

[13] A határozattervezet (212) preambulumbekezdése.

Tartalomjegyzék

Az Európai Adatvédelmi Testület,

Az Európai Adatvédelmi Testület a következő nyilatkozatot fogadta el:

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének s) pontjára[1],

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018. sz. határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[2],

tekintettel eljárási szabályzatának 12. és 22. cikkére,

A KÖVETKEZŐ VÉLEMÉNYT FOGADTA EL

1 BEVEZETÉS

1.1 Az Egyesült Államok adatvédelmi kerete

1. Az Egyesült Államok (a továbbiakban: USA) és az Európai Unió (a továbbiakban: EU) eltérő megközelítést alkalmaz a magánéletre és a személyes adatok védelmére vonatkozóan. Míg a magánélet és a személyes adatok Unión belüli védelme az Európai Unió Alapjogi Chartájának 7. és 8. cikkében biztosított alapvető jogok közé tartozik, az Egyesült Államokban az adatvédelmet általában a fogyasztóvédelem szempontjából közelítik meg. Ennek következtében az Egyesült Államokban és az EU-ban eltérőek a szabályozási megközelítések[3].

2. Az Egyesült Államokban – az általános adatvédelmi rendelet átfogó uniós megközelítésétől eltérően – szövetségi szinten nem létezik átfogó általános adatvédelmi jogszabály. A magánélet védelme az Egyesült Államokban inkább ágazati és állami megközelítéssel valósul meg. Egyes konkrét ágazatokra például olyan külön jogi aktusok vonatkoznak, mint:

   - az egészségbiztosítás hordozhatóságáról és elszámolási kötelezettségéről szóló törvény (HIPAA)[4],

[1] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) (HL L 119., 2016.5.4., 1. o.).

[2] Az e véleményben a „tagállamokra" való hivatkozásokat az „EGT-tagállamokra" való hivatkozásként kell értelmezni.

[3] Lásd még az (EU) 2016/679 európai parlamenti és tanácsi rendelet alapján a személyes adatok az EU–USA adatvédelmi keret értelmében biztosított megfelelő szintű védelméről szóló európai bizottsági végrehajtási határozat 2022. december 13-án közzétett tervezete (a továbbiakban: határozattervezet), I. mellékletének I. szakaszát.

[4] Az egészségbiztosítás hordozhatóságáról és elszámolási kötelezettségéről szóló 1996. évi törvény (HIPAA) az Egyesült Államok szövetségi törvénye. Nemzeti szabványokat határoz meg a betegek érzékeny egészségügyi

- a gyermekek online adatvédelmi törvénye (COPPA)[5],
- Gramm–Leach–Billey-törvény (GLBA)[6].

3. Az EU-ból az USA-ba továbbított személyes adatokhoz való kormányzati hozzáférés területén számos különböző jogalap, korlátozás és biztosíték alkalmazandó. Az információkhoz való bűnüldözési célú hozzáférésre vonatkozó jogi eljárások vagy közvetlenül az Egyesült Államok alkotmányából (negyedik módosítás), a tételes- és eljárási jogból, vagy az Igazságügyi Minisztérium szövetségi, illetve állami szintű irányelveiből és szabályzataiból erednek. Az információkhoz való nemzetbiztonsági célú hozzáférést több jogi eszköz szabályozza, különösen a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (Foreign Intelligence Surveillance Act , FISA), a 12333. sz. elnöki rendelet, a közelmúltban elfogadott 14086. sz. elnöki rendelet, valamint az adatvédelmi felülvizsgálati bíróságot (Data Protection Review Court, a továbbiakban: DPRC) létrehozó, az Egyesült Államok főügyésze által kiadott rendelet (a továbbiakban: főügyészi rendelet)[7].

4. A Bizottság 2022. december 13-án tette közzé az (EU) 2016/679 európai parlamenti és tanácsi rendelet alapján a személyes adatok az EU–USA adatvédelmi keret értelmében biztosított megfelelő szintű védelméről szóló európai bizottsági végrehajtási határozat tervezetét (a továbbiakban: határozattervezet), amelynek melléklete tartalmazza az EU–USA adatvédelmi keretet (a továbbiakban: adatvédelmi keret). A fent ismertetett okokból a határozattervezet nem egy konkrét és átfogó szövetségi jogi kereten, hanem az adatvédelmi kereten alapul.

5. Az adatvédelmi keret a következőképpen működik: *„Az Egyesült Államok Kereskedelmi Minisztériuma (a továbbiakban: Minisztérium) a nemzetközi kereskedelem támogatására, előmozdítására és fejlesztésére vonatkozó törvényes hatásköre értelmében (15 U.S.C., 1512. §) kiadja az EU–USA*

információinak védelme érdekében. A HIPAA célja, hogy kellően óvja a természetes személyek egészségügyi adatait, ugyanakkor lehetővé tegye az egészségügyi információk áramlását a magas színvonalú egészségügyi ellátás biztosítása és előmozdítása érdekében. A HIPAA szabályozza az egészségügyi információk az adatvédelmi szabály hatálya alá tartozó szervezetek általi felhasználását és közzétételét. Emellett előírásokat tartalmaz a természetes személyek azon jogára vonatkozóan, hogy megismerjék és felügyeljék egészségügyi adataik felhasználásának módját.
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974

[5] A COPPA elsődleges célja, hogy a szülők ellenőrzést gyakorolhassanak afelett, hogy 13 év alatti gyermekeiktől milyen személyes információkat gyűjtenek a gyermekeket célzó honlapok és online szolgáltatások (beleértve a mobilalkalmazásokat és a dolgok internetéhez tartozó eszközöket, például az intelligens játékokat), illetve az általános közönségnek szánt oldalak üzemeltetői. A COPPA előírja az ilyen üzemeltetők számára, hogy biztosítsanak szülői figyelmeztetést, és kérjenek ellenőrizhető szülői hozzájárulást. Ez a külföldi gyermekektől származó adatok esetében is érvényes, amennyiben a weboldalakat vagy szolgáltatásokat az Egyesült Államokban üzemeltetik, és azok a COPPA hatálya alá tartoznak. A rendeletek ugyanakkor a külföldi székhelyű weboldalakra és szolgáltatásokra is érvényesek, amennyiben azok az Egyesült Államokban élő gyermekeket célozzák meg. Lásd: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions és a határozattervezet IV. mellékletének 3. oldalát.

[6] A Gramm-Leach-Bliley törvény egyik célja a fogyasztók adatvédelme a pénzügyi ágazatban. A GLB-törvény előírja a pénzügyi intézmények számára, hogy tájékoztassák ügyfeleiket információmegosztási gyakorlataikról, és hozzanak létre biztosítékokat az ügyfelek adatainak védelme érdekében (pl. az FTC által az FTC biztosítékokra vonatkozó szabálya értelmében szabályozott vállalatok számára). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[7] A főügyész 5517-2022. sz. rendelete, amely módosítja az Egyesült Államok Igazságügyi Minisztériumának rendeleteit a 14086. sz. elnöki rendelet felhatalmazása és utasítása szerint.

adatvédelmi keret elveit, beleértve a kiegészítő elveket is (a továbbiakban együttesen: elvek). és az elvek I. mellékletét (a továbbiakban: I. melléklet)[8]."

6. Az „elvek" (a továbbiakban: az adatvédelmi keret elvei) kidolgozására az Európai Bizottsággal (a továbbiakban: Bizottság), az ágazattal és más érdekelt felekkel konzultálva került sor az EU és az USA közötti kereskedelem megkönnyítésére irányuló cél elérése érdekében[9], egyúttal biztosítva, hogy az érintettek az EU-ban biztosítottal lényegében azonos szintű védelemben részesüljenek.

7. Az adatvédelmi keret elvei az adatvédelmi keret „kulcsfontosságú elemeiként" kerülnek meghatározásra. Egyrészt „használatra kész mechanizmust" biztosítanak az EU-ból az USA-ba irányuló adattovábbításhoz, másrészt pedig az EU-ból az USA-ba továbbított személyes adatokat az uniós jog által előírtaknak megfelelően óvják és védik.

8. Az adatvédelmi keret kizárólag azokra az egyesült államokbeli szervezetekre alkalmazandó, amelyek a keret követelményeinek megfelelő öntanúsítással rendelkeznek (a továbbiakban: az adatvédelmi keret szervezetei). Ez egyelőre csak abban az esetben lehetséges, ha a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission, a továbbiakban: FTC) vagy a Közlekedési Minisztérium (Department of Transportation, a továbbiakban: DoT) hatáskörébe tartoznak. A jövőben az adatvédelmi keret elveinek végrehajtásának felügyeletére hatáskörrel rendelkező egyéb hatósági szerveket is rögzíteni lehetne egy későbbi mellékletben.

9. Az adatvédelmi keret elvei rögzítik, hogy a keret feltételei i. az FTC által a Szövetségi Kereskedelmi Bizottságról szóló törvény (FTC-törvény) a tisztességtelen és megtévesztő cselekmények a kereskedelemben való vagy a kereskedelmet érintő végrehajtásának tilalmáról szóló 5. szakasza értelmében[10], ii. a DoT által a 49 U.S.C a fuvarozók és a jegyértékesítők számára a tisztességtelen vagy megtévesztő gyakorlat folytatását vagy tisztességtelen versenymódszerek alkalmazását a légi közlekedés értékesítése során megtiltó 41712. §-a értelmében, illetve iii. az ilyen cselekedeteket megtiltó egyéb törvények vagy rendeletek értelmében hajtható végre.

10. Az adatvédelmi keret elveiben rögzítésre került, hogy azok nem érintik az általános adatvédelmi rendelet alkalmazását, és az Egyesült Államok joga szerint egyébként alkalmazott, meglévő adatvédelmi kötelezettségeket sem korlátozzák.

1.2 Az Európai Adatvédelmi Testület általi értékelés terjedelme

11. A határozattervezet a Bizottság értékelését tükrözi az adatvédelmi keretről, amely az Egyesült Államok kormányával folytatott megbeszélések eredménye. Az Európai Adatvédelmi Testületnek az általános adatvédelmi rendelet 70. cikke (1) bekezdésének s) pontjával összhangban véleményt kell kibocsátania az Európai Bizottság megállapításairól a valamely harmadik országban biztosított védelmi szint megfelelőségének vonatkozásában, és szükség esetén javaslatokat kell tennie a problémák kezelésére.

12. Az Európai Adatvédelmi Testület üdvözli az adatvédelmi keret elveinek aktualizálását[11], amely kötelező jogi keretet alkot majd az adatvédelmi keret szervezeteinek számára. Az Európai Adatvédelmi Testület ugyanakkor megjegyzi, hogy adatvédelmi keret elvei lényegében megegyeznek az adatvédelmi

[8] A határozattervezet I. mellékletének I. szakasza.
[9] *Ugyanott.*
[10] 15 U.S.C. 45. § a) pont.
[11] Például annak tisztázását, hogy a kódolt adatok személyes adatok.

pajzsban[12] szereplőkkel (amelyeken a 29. cikk szerinti munkacsoport [a továbbiakban: WP29] és az Európai Adatvédelmi Testület éves közös felülvizsgálatai alapultak). Az adatvédelmi keret elvei szintén nagymértékben megegyeznek az adatvédelmi pajzs tervezetében szereplő azon elvekkel is, amelyekre a 29. cikk szerinti munkacsoport 2016-os véleményét alapozta[13] (a továbbiakban: a WP29 01/2016. sz. véleménye). Az adatvédelmi keret lényegében változatlanul hagyott elveinek vonatkozásában az Európai Adatvédelmi Testület nem tartja szükségesnek a 29. cikk szerinti munkacsoport által korábban tett valamennyi észrevétel megismétlését. Az EDPB úgy határozott, hogy olyan konkrét szempontokra összpontosít, amelyeket a jogi és technológiai környezet fejlődésének tükrében napjainkban még relevánsabbnak tart.

13. Emellett az EUB ítélkezési gyakorlatával[14] összhangban az elemzés egy igen fontos része az Egyesült Államokba továbbított személyes adatokhoz való kormányzati hozzáférés jogi rendszerére terjed ki.

14. Értékelésében az EDPB figyelembe vette az alkalmazandó európai adatvédelmi keretet, beleértve az Európai Unió Alapjogi Chartájának (a továbbiakban: Charta) a magán- és a családi élethez való jogot védő 7., a személyes adatok védelméhez való jogot óvó 8., valamint a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogot védő 47. cikkét, illetve az emberi jogok európai egyezményének (a továbbiakban: EJEE) a magán- és a családi élethez való jogot védő 8. cikkét. A fentieken túlmenően az Európai Adatvédelmi Testület figyelembe vette az általános adatvédelmi rendelet követelményeit, a vonatkozó ítélkezési gyakorlatot és az Európai Adatvédelmi Testület által elfogadott megfelelőségi referenciát (a továbbiakban: az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referencia)[15].

15. A dokumentum célja, hogy véleményt adjon a Bizottságnak az adatvédelmi keret által biztosított védelmi szint megfelelőségének értékeléséről. A „megfelelő védelmi szint' már a 95/46/EK irányelv értelmében is létező fogalmát az EUB továbbfejlesztette. Ezért fontos emlékeztetni az EUB Schrems I.[16] (a „biztonságos kikötőt" érvénytelenítő) és Schrems II.[17] (az adatvédelmi pajzsot érvénytelenítő) ítéleteiben meghatározott normára.

16. Az EUB Schrems I. ítéletében rögzítette hogy bár a harmadik országban a „védelem szintjének" „lényegében azonosnak" kell lennie az EU-ban biztosított védelmi szinttel, „azok az eszközök, amelyeket a harmadik ország az ilyen védelmi szint biztosításához e tekintetben igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket […] az Unióban alkalmaznak[18]". Ennek értelmében

[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. o.).

[13] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye az EU–USA adatvédelmi pajzs megfelelőségéről szóló határozattervezetről, az elfogadás időpontja: 2016. április 13. (a továbbiakban: a 29. cikk alapján létrehozott munkacsoport 01/2016. sz. véleménye).

[14] Különösen az alábbiakkal: A Bíróság 2015. október 6-i ítélete, Maximilian Schrems kontra Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, valamint a Bíróság 2020. július 16-i ítélete, Data Protection Commissioner kontra Facebook Ireland Limited és Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] A 29. cikk szerinti munkacsoport, Megfelelőségi referencia, WP 254 rev.01, 2017. november 28., amely legutóbb 2018. február 6-án került felülvizsgálatra és elfogadásra, és amelyet az EDPB 2018. május 25-én hagyott jóvá (a továbbiakban: megfelelőségi referencia).

[16] A Bíróság 2015. október 6-i ítélete, Schrems I., Maximilian Schrems kontra Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650 (a továbbiakban: a Bíróság Schrems I. ügyben hozott ítélete).

[17] A Bíróság 2020. július 16-i ítélete, Data Protection Commissioner kontra Facebook Ireland Limited és Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (a továbbiakban: a Bíróság Schrems II. ügyben hozott ítélete).

[18] A Bíróság Schrems I. ügyben hozott ítélete, 73–74. pont.

a cél nem az uniós jogszabályok pontról pontra történő lemásolása, hanem a vizsgált jogszabályok lényegi és alapvető követelményeinek megállapítása. A megfelelőség az érintettek számára biztosított jogok és a személyes adatok kezelését végzők, illetve az ilyen adatkezelést ellenőrzők számára előírt kötelezettségek, valamint a független szervezetek általi felügyelet kombinációjával érhető el. Az adatvédelmi szabályok azonban csak akkor hatékonyak, ha azok a gyakorlatban is kikényszeríthetők és betarthatók. Ezért a szabályok hatékonyságának biztosítása érdekében nem csupán a harmadik országokba vagy nemzetközi szervezetek részére továbbított személyes adatokra vonatkozó szabályok tartalmát kell figyelembe venni, hanem a bevezetett rendszert is. Az eredményes végrehajtási mechanizmusok rendkívül fontosak az adatvédelmi szabályok hatékonysága tekintetében[19].

17. A Schrems II. ügyben hozott határozatában az EUB megállapította, hogy azok a jogszabályok, amelyeknek alapján az Egyesült Államok hírszerző hatóságai hozzáférhetnek az Egyesült Államokba továbbított személyes adatokhoz (a FISA 702. szakasza, 12333. sz. elnöki rendelet) aránytalan mértékben korlátozzák az Európai Unió Alapjogi Chartájának (a továbbiakban: Charta) 7. és 8. cikkében foglalt jogokat, és ezért nem olyan módon kerültek meghatározásra, hogy megfeleljenek a Charta 52. cikke (1) bekezdésének második mondata által az uniós jogban megkövetelt követelményekkel lényegében azonos követelményeknek[20].

18. Az EUB továbbá megállapította, hogy a korábbi jogi keret nem nyújtott a Charta 47. cikkében előírtakkal lényegében egyenértékű garanciákat, mivel az ombudsmani mechanizmus nem képes kompenzálni azt a tényt, hogy sem a PPD-28, sem a 12333. sz. elnöki rendelet nem biztosít hatékony jogorvoslatot a nem egyesült államokbeli személyek számára[21]. Az ombudsman nem volt független a végrehajtó hatalomtól és nem rendelkezett hatáskörrel arra, hogy kötelező erejű határozatokat fogadjon el az Egyesült Államok hírszerző szolgálataira vonatkozóan[22].

19. A 14086. sz. elnöki rendelet, amely általánosságban a PPD-28 helyébe lép, két új követelményt vezetett be az Egyesült Államok jogában, amelyek az EUB Schrems II. ítéletét tükrözik: egyrészről azt, hogy jelfelderítési tevékenységek csak abban az esetben végezhetők, amennyiben azok validált hírszerzési prioritásnak minősülő adatgyűjtés előmozdításához szükségesek, illetve csak a validált hírszerzési prioritással arányos mértékben, illetve módon; másrészről pedig egy jogorvoslati mechanizmust.

20. Ebben a véleményben az Európai Adatvédelmi Testület különösen azt értékeli, hogy az adatvédelmi keret, valamint a közelmúltban elfogadott 14086. sz. elnöki rendelet milyen mértékben kezeli hatékonyan az EUB ítéletében tett megállapításokat.

1.3 Általános észrevételek és aggályok

1.3.1 A nemzeti jog értékelése

21. Az Európai Adatvédelmi Testület úgy értelmezi, hogy a határozattervezetben foglalt értékelés az adatvédelmi keret elveire vonatkozik. Mindazonáltal az EDPB üdvözölné néhány információ feltüntetését az Egyesült Államok jogi környezetéről, amelyben az adatvédelmi keret szervezetei működnek. Ez lehetővé tenné az adatvédelmi keret és az Egyesült Államok joga közötti interakciók jobb megértését. Az I. melléklet I. szakaszában[23] például anélkül nyer megállapítást, hogy az adatvédelmi

[19] Általános adatvédelmi rendelet – Megfelelőségi referencia, 2. o.
[20] A Bíróság Schrems II. ügyben hozott ítélete, 184–185. pont.
[21] A Bíróság Schrems II. ügyben hozott ítélete, 192. pont.
[22] A Bíróság Schrems II. ügyben hozott ítélete, 195. pont.
[23] A határozattervezet I. melléklete I. szakaszának utolsó mondata.

keret elvei nem korlátozzák *„[…] az Egyesült Államok joga alapján egyébként alkalmazandó adatvédelmi kötelezettségeket*", hogy ezek a kötelezettségek ismertetésre kerültek volna.

1.3.2 Az Egyesült Államok nemzetközi kötelezettségvállalásai

22. Az általános adatvédelmi rendelet 45. cikke (2) bekezdésének c) pontja és az általános adatvédelmi rendelettel kapcsolatos megfelelőségi referencia szerint egy harmadik ország védelmi szintje megfelelőségének értékelésekor Bizottság figyelembe veszi többek között a harmadik ország által vállalt nemzetközi kötelezettségeket, vagy a harmadik országnak a többoldalú vagy regionális rendszerekben való részvételéből eredő egyéb kötelezettségeket, különösen a személyes adatok védelmével kapcsolatban, valamint e kötelezettségek végrehajtását.

23. Az Egyesült Államok részes fele több, a magánélet tiszteletben tartásához való jogot garantáló nemzetközi megállapodásnak, például a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának (17. cikk), a fogyatékossággal élő személyek jogairól szóló egyezménynek (22. cikk) és a Gyermekjogi egyezménynek (16. cikk). Ezen túlmenően az Egyesült Államokra az OECD-tagjaként az OECD adatvédelmi kerete vonatkozik, különös tekintettel a magánélet védelmét és a személyes adatok határokon átnyúló áramlását szabályozó iránymutatásokra. Az OECD-tagok és az Európai Unió minisztere, illetve magas szintű képviselői 2022. december 14-én elfogadták a magánszektorbeli szervezetek birtokában lévő személyes adatokhoz való kormányzati hozzáférésről szóló OECD-nyilatkozatot. Az Egyesült Államok részes fele a számítástechnikai bűnözésről szóló Budapesti Egyezménynek is.

24. Emellett az Egyesült Államok tagja az Ázsiai és Csendes-óceáni Gazdasági Együttműködés (Asia-Pacific Economic Cooperation, a továbbiakban: APEC) határokon átnyúló adatvédelmi szabályrendszerének (CBPR) is, amely egy kormány által támogatott olyan adatvédelmi tanúsítvány, amelyhez a vállalatok a nemzetközileg elismert adatvédelmi szabályoknak való megfelelés igazolása érdekében csatlakozhatnak. Az APEC vezetői jóváhagyták ezeket az adatvédelmi szabályokat.

25. Az EDPB egyúttal tudomásul veszi, hogy az Egyesült Államok megfigyelő államként részt vesz az Európa Tanács 108. egyezménye Tanácsadó Bizottságának munkájában.

26. Az EDPB továbbá tudomásul veszi és üdvözli , hogy az Egyesült Államok szervei folyamatosan részt vesznek a G7-ek adatvédelmi és a magánélet védelmével foglalkozó hatóságainak 2021-ben, újonnan létrehozott kerekasztalában (G7-ek adatvédelmi hatóságainak kerekasztala), amely a G7-országok független adatvédelmi és a magánélet védelmével foglalkozó hatóságait egyesíti. Ebben az összefüggésben támogatták például a G7-ek adatvédelmi hatóságai kerekasztalának legutóbbi, 2022. szeptember 8-án Bonnban (Németország) elfogadott közleményét[24], amely a bizalomra épülő szabad adatáramlás koncepciójára összpontosított.

[24] A G7-ek adatvédelmi és a magánélet védelmével foglalkozó hatóságainak kerekasztala, A bizalomra épülő szabad adatáramlás előmozdítása és a nemzetközi adatterek kilátásaira vonatkozó tudás megosztása, 2022. szeptember 8., https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1

1.3.3 Az Egyesült Államok adatvédelmi jogszabályai terén történt előrelépések

27. Az EDPB külön figyelmet fordít az Egyesült Államokban az adatvédelmi jogszabályok állami szintű fejlődésére. Az EDPB üdvözli az öt államban (Kalifornia, Colorado, Connecticut, Virginia és Utah)[25]. hatályba lépett vagy 2023-ig hatályba lépő adatvédelmi jogszabályok elfogadását.

28. Az EDPB egyúttal azt is megjegyzi, hogy az Egyesült Államok számos más államában indultak már el további, ezeknek megfelelő állami jogszabályokra vonatkozó kezdeményezések.

29. Az Európai Adatvédelmi Testület továbbá kifejezetten üdvözli a szövetségi adatvédelmi törvényre, az adatvédelemre és a magánélet védelmére vonatkozó amerikai törvényre (American Data Privacy and Protection Act, ADPPA) irányuló kétpárti kezdeményezéssel kapcsolatos erőfeszítéseket.

1.3.4 A határozattervezet hatóköre

30. A határozattervezet 1. cikke értelmében a Bizottság megállapítja, hogy az Egyesült Államok az I. melléklet I. szakaszának 3. pontjával összhangban, megfelelő szintű védelmet biztosít az EU-ból az Egyesült Államokban működő azon szervezetek számára továbbított személyes adatok tekintetében, amelyek az Egyesült Államok Kereskedelmi Minisztériuma (a továbbiakban: DoC) által kezelt és nyilvánosan hozzáférhetővé tett „adatvédelmi keret listáján" szerepelnek[26].

31. Az adatvédelmi keret az FTC vagy a DoT hatáskörébe tartozó vállalatok számára érhető el. Rögzítésre került, hogy a jövőben más, hasonló hatáskörrel rendelkező hatósági szervek is[27] bevonódhatnak.

1.3.5 Az adatvédelmi keret elveinek betartására vonatkozó kötelezettség korlátozása

32. Az I. melléklet I.5. pontja úgy rendelkezik, hogy az adatvédelmi keret elveinek az adatvédelmi keret szervezetei általi betartása többek között korlátozható i. a bírósági végzéseknek, közérdeknek, illetve a bűnüldözési[28] vagy nemzetbiztonsági követelményeknek[29] való megfeleléshez szükséges mértékben (beleértve azt az esetet is, amikor egy törvény vagy kormányrendelet ellentétes kötelezettségeket teremt), és ii. olyan törvény, bírósági végzés vagy kormányrendelet révén, amely kifejezett felhatalmazást hoz létre, feltéve, hogy az ilyen felhatalmazás gyakorlása során a adatvédelmi keret szervezete bizonyítani tudja, hogy az adatvédelmi keret elveinek nemteljesítése az ilyen felhatalmazás által támogatott törvényes érdekek teljesítéséhez szükséges mértékre korlátozódik.

33. Az Egyesült Államok jogának szövetségi és állami szintű teljes körű ismerete nélkül az EDPB nehezen tudja részletesen értékelni az e bekezdésben felsorolt mentességek hatályát. Az EDPB ezért azt

[25] Kaliforniai fogyasztói adatvédelmi törvény (2018; hatálybalépés: 2020. január 1.); Kaliforniai adatvédelemhez való jogról szóló törvény (2020; teljes körű alkalmazás: 2023. január 1.); Coloradói adatvédelmi törvény (2021; hatálybalépés: 2023. július 1.); Connecticuti adatvédelmi törvény (2022; hatályba lép: 2023. július 1.), Virginiai fogyasztói adatvédelmi törvény (2021; hatálybalépés: 2023. január 1.), Utahi fogyasztói adatvédelmi törvény (2022, hatálybalépés: 2023. december 31.).

[26] Határozattervezet, Záró megállapítások, 1. cikk, 57. o. Az Európai Adatvédelmi Testület úgy értelmezi, hogy a határozattervezet nem terjed ki az EU-n kívül található, de az általános adatvédelmi rendelet 3. cikkének (2) bekezdése értelmében az általános adatvédelmi rendelet hatálya alá tartozó szervezetektől az egyesült államokbeli, tanúsított szervezetek részére történő adattovábbításra.

[27] A határozattervezet, I. melléklete, I. szakaszának 2. pontja.

[28] Az EU–USA adatvédelmi keret hatálya alá tartozó személyes adatok bűnüldözési célú felhasználásával kapcsolatban lásd e vélemény 3.1. szakaszát.

[29] Az EU–USA adatvédelmi keret hatálya alá tartozó személyes adatok nemzetbiztonsági célú felhasználásával kapcsolatban lásd e vélemény 3.2. szakaszát. A kormányzat hozzáférése a személyes adatokhoz nemzetbiztonsági célból.

javasolja, hogy a Bizottság egyértelműsítse a mentességek hatályát a határozattervezetben, beleértve az Egyesült Államok joga szerint alkalmazandó biztosítékokat, annak érdekében, hogy jobban meg lehessen állapítani e mentességek az érintettek védelmi szintjére gyakorolt hatását. Az EDPB egyúttal azt is hangsúlyozza, hogy a Bizottságot tájékoztatni kell minden olyan törvény vagy kormányrendelet alkalmazásáról és elfogadásáról, amely érintené az adatvédelmi keret betartását, és a Bizottságnak ezeket nyomon kell követnie.

1.3.6 Az „adatvédelmi pajzsot" érintő változások

34. Az EDPB üdvözli a Schrems II. ítéletben foglalt követelmények teljesítése érdekében tett erőfeszítéseket. Mindazonáltal az Európai Adatvédelmi Testület üdvözölte volna, ha az adatvédelmi keretről szóló tárgyalások alkalmával több, i. a WP29 01/2016. sz. véleményében, és ii. a korábbi közös felülvizsgálatokban[30] azonosított kérdéssel is foglalkoztak volna.

35. Az EDPB azt is megjegyzi, hogy a határozattervezet preambulumbekezdéseiben szereplő számos módosítás és kiegészítő magyarázat ellenére az adatvédelmi keret azon alapelvei, amelyeket az adatvédelmi keret-szervezeteinek be kell tartaniuk, lényegében változatlanok maradnak az adatvédelmi pajzs keretében alkalmazandó elvekhez képest.

1.3.7 Az egyértelműség hiánya az adatvédelmi keret dokumentumaiban

36. Az EDPB megjegyzi, hogy a mellékletek szerkezete és számozása meglehetősen megnehezíti az információk megtalálását és az azokra való hivatkozást. Ez hozzájárul az új keret átfogó, összetett megjelenítéséhez, amely mellékleteiben különböző jogi kötőerejű dokumentumokat egyesít, és amely esetlegesen nehezíti az adatvédelmi keret elveinek az érintettek, az adatvédelmi keret szervezetei és az EU adatvédelmi hatóságai (a továbbiakban: uniós adatvédelmi hatóságok) általi megfelelő megértését.

37. Az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy a terminológiát az egész adatvédelmi keretben következetesen kellene használni. Jelenleg nem ez a helyzet például az „adatkezelés" fogalma esetében. Az adatvédelmi keret egyes részei ugyanis az „adatkezelés" kifejezés használata helyett bizonyos típusú feldolgozási műveleteket sorolnak fel. Ez jogbizonytalanságot és esetleges joghézagokat eredményezhet a védelem terén[31].

38. Az EDPB üdvözli, hogy egyes használt fogalmak meghatározásai szerepelnek a adatvédelmi keretben[32]. Nem ez a helyzet azonban néhány más olyan alapvető kifejezés esetében, mint legalábbis például a „megbízott" vagy az „adatfeldolgozó", amelyek az Európai Adatvédelmi Testület véleménye szerint indokolttá teszik az adatvédelmi keret. I. melléklete I. szakaszának 8. pontjában szereplő egyértelmű

[30] Éves felülvizsgálatok: „EU–USA adatvédelmi pajzs – Első éves közös felülvizsgálat", WP 255, a WP29 jelentése elfogadásának időpontja: 2017. november 28.(a továbbiakban: első közös felülvizsgálati jelentés); „EU–USA adatvédelmi pajzs – Második éves közös felülvizsgálat", az Európai Adatvédelmi Testület jelentése elfogadásának időpontja: 2019. január 22., (a továbbiakban: második közös felülvizsgálati jelentés); „EU–USA adatvédelmi pajzs – Harmadik éves közös felülvizsgálat", az Európai Adatvédelmi Testület jelentése elfogadásának időpontja: 2019. november 12., (a továbbiakban: harmadik közös felülvizsgálati jelentés).

[31] Például i. a határozattervezet I. melléklete III. szakasza 6. pontjának f) alpontja szerint az adatvédelmi keret elvei csak akkor alkalmazandók, ha a szervezet a kapott adatokat „tárolja, felhasználja vagy nyilvánosságra hozza" (azaz nem az „adatkezelés" fogalmába tartozó egyéb műveletek, például gyűjtés, rögzítés, módosítás, lekérdezés vagy betekintés vonatkozásában), valamint ii. a határozattervezet I. melléklete II. szakasza 4. pontjának a) alpontja szerint az adatbiztonságot csak a személyes adatok „létrehozása, fenntartása, felhasználása vagy terjesztése" tekintetében írnák elő.

[32] A határozattervezet I. melléklete I. szakaszának 8. pontja.

és konkrét fogalommeghatározásokat, és amelyeket illetően az USA és az EU egyetért, annak érdekében, hogy a későbbi szakaszban elkerülhetőek legyenek az adatvédelmi keret a keretre támaszkodó szervezetei, a felügyeleti hatóságok és a nyilvánosság félreértése.

39. Ami a humánerőforrás-adatok az EU-ban és az USA-ban való eltérő értelmezését illeti, az EDPB egyetért a Bizottság harmadik felülvizsgálati jelentésében szereplő azon célkitűzéssel, amely szerint folytatni kell a megbeszéléseket az Egyesült Államok hatóságaival[33].

2 ÁLTALÁNOS ADATVÉDELMI SZEMPONTOK

2.1 Tartalmi elvek

2.1.1 Fogalmak

40. Az általános adatvédelmi rendelet megfelelőségi referenciája értelmében a harmadik ország jogi keretének rendelkeznie kell az alapvető adatvédelmi fogalmakkal és/vagy elvekkel. Habár ezeknek nem kell az általános adatvédelmi rendelet terminológiáját tükrözniük, meg kell felelniük az európai adatvédelmi jogszabályokban megfogalmazott kifejezéseknek, és összhangban kell állniuk azokkal. Az általános adatvédelmi rendelet például az alábbi fontos kifejezéseket használja: „személyes adatok", „a személyes adatok kezelése", „adatkezelő", „adatfeldolgozó", „címzett" és „érzékeny adatok". Az EDPB üdvözli, hogy a „személyes adatok", az „adatkezelés" és az „adatkezelő" fogalmak meghatározása ugyanúgy szerepel a adatvédelmi keretben, ahogyan az adatvédelmi pajzs esetében.

41. Az EDPB megjegyzi, hogy továbbra sem egyértelmű, hogy az adatvédelmi keret elvei milyen mértékben alkalmazandók az adatvédelmi keret azon szervezeteire, amelyeknek részére az EU-ból a személyes adatok „pusztán adatkezelés" céljából kerülnek továbbításra (a továbbiakban: megbízottak vagy adatfeldolgozók). Az adatvédelmi keret nem tesz különbséget a megbízottakra és az adatkezelőkre alkalmazandó elvek között, ugyanakkor az azokban foglalt kötelezettségek közül számos nem megfelelő a megbízottak/feldolgozók számára. Például a megbízott/adatfeldolgozó nem lehet képes arra, hogy a természetes személy rendelkezésére bocsássa a teljes tájékoztatás a tájékoztatás elve által előírt valamennyi elemét (pl. azokat a célokat, amelyekre vonatkozóan személyes adatokat gyűjt és használ fel)[34], mivel a megbízott/adatfeldolgozó egyedül nem tudja meghatározni az adatkezelés eszközeit és céljait[35].

2.1.2 A célhoz kötöttség elve

42. Az általános adatvédelmi rendelet megfelelőségi referenciája az általános adatvédelmi rendelettel összhangban úgy rendelkezik, hogy az adatokat konkrét célból kell kezelni, és később csak olyan mértékben lehet használni, amely nem inkompatibilis az adatkezelés céljával.

43. Az adatok sértetlensége és a célhoz kötöttség elve kimondja, hogy a szervezet nem kezelhet személyes információkat a gyűjtés céljaival vagy az egyén által a későbbiekben engedélyezett célokkal

[33] Harmadik közös felülvizsgálati jelentés 5., 15., 16. és 30. oldal; Lásd még „A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak az EU–USA adatvédelmi pajzs működésének harmadik éves felülvizsgálatáról" című dokumentumot kísérő bizottsági szolgálati munkadokumentumot, 17–18. o.

[34] A határozattervezet I. melléklete II. szakasza 1. pontjának a) pontja.

[35] Lásd még a 29. cikk szerinti munkacsoport 01/2016. sz. véleményének 16. oldalát.

összeegyeztethetetlen módon[36]. Az Európai Adatvédelmi Testület megjegyzi, hogy a tájékoztatás, a választási lehetőség, valamint a sértetlenség és a célhoz kötöttség elvének tekintetében eltérő terminológiát használtak. Amint azt a 29. cikk szerinti munkacsoport megjegyezte, és a határozattervezet preambulumbekezdéseiben szereplő hasznos pontosítások ellenére, az olyan fogalmak, mint a „különböző célok", a „lényegesen eltérő" célok vagy az „összeegyeztethetetlen használat" az adatvédelmi keretben a dokumentumban való egyértelmű meghatározásuk nélkül kerültek felhasználásra, és jogbizonytalansághoz vezethetnek.

2.1.3 A hozzáféréshez, helyesbítéshez, törléshez és tiltakozáshoz való jog

44. Az adatvédelmi keretben az érintettek hozzáférésre, helyesbítésre és törlésre vonatkozó jogával a hozzáférés elve foglalkozik[37].

45. A hozzáférési elv az adatvédelmi pajzshoz viszonyítva változatlan maradt. Következésképpen a 29. cikk szerinti munkacsoport 01/2016. sz. véleményében megfogalmazott egyes aggályok továbbra is érvényesek az alábbiak szerint.

46. Ami a természetes személyek hozzáféréshez való jogát illeti, az EDPB szükségesnek tartja megismételni, hogy a természetes személy kéréseire vonatkozó válaszadás kötelezettségének részleteit jobban bele kellene foglalni az elv fő szövegébe (még mindig csak az [38]). lábjegyzetben kerül ismertetésre. Azt is egyértelművé kell tenni, hogy a hozzáférést a személyes adatok az adatvédelmi keret szervezete általi kezelésének megfelelő mértékben kell biztosítani, és nemcsak akkor, amikor a szervezet „tárolja" azokat[39]. Az EDPB véleménye szerint a jelenlegi megfogalmazás a hozzáférési jog szűk értelmezéséhez vezethet.

47. Ami a hozzáférési jog alóli kivételek listáját illeti[40], néhány továbbra is az adatvédelmi keret szervezeteinek érdekei felé billen. Az EDPB továbbra is aggályosnak tartja, hogy ezekben az esetekben látszólag nem áll fenn az természetes személyek jogainak és érdekeinek figyelembevételére vonatkozó követelmény[41].

48. Egy másik kivétel, amelyet a 29. cikk szerinti munkacsoport korábban is aggályosnak ítélt[42], és amely az EDPB számára túlzottan tágnak tűnik, a nyilvánosan elérhető információkhoz és a nyilvános nyilvántartásokból származó információkhoz való hozzáférés joga alóli kivétel[43]. Az EDPB több alkalommal kijelentette, hogy az uniós jog szerint az érintettek mindig jogosultak hozzáférni adataikhoz, függetlenül attól, hogy a személyes adatok közzétételre kerültek-e vagy sem. Ha a hozzáférés iránti kérelmeket azon az alapon utasítanák el, hogy az adatok nyilvános forrásokból, vagy nyilvánosan elérhető nyilvántartásokból származnak, a természetes személy nem lenne képes az adatok pontosságának, valamint annak ellenőrzésére, hogy azok közzététele jogszerű volt-e egyáltalán.

49. Az Európai Adatvédelmi Testület emlékeztet arra, hogy a hozzáférési jogot a Charta 8. cikkének (2) bekezdése rögzíti. Bár nem abszolút jog, alapvető fontosságú a személyes adatok védelméhez való

[36] A határozattervezet, I. melléklete II. szakaszának 5. pontja.
[37] A határozattervezet I. melléklete II. szakaszának 6. pontja és III. szakasza 8. pontja a) alpontjának i. pontja.
[38] A határozattervezet I. melléklete III. szakasza 8. pontja a) pontja i. alpontjának 1. pontja.– 14. lábjegyzet.
[39] A határozattervezet I. melléklete, III. szakasza 8. pontja d) pontjának ii. alpontja.
[40] A határozattervezet I. melléklete III. szakasza 8. pontjának e) pontja.
[41] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 2.2.5. pont.
[42] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 2.2.9. pont.
[43] A határozattervezet I. melléklete III. szakasza 15. pontjának d)–e) pontja.

jog szempontjából, mivel megkönnyíti az érintett egyéb jogainak, például a helyesbítéshez és törléshez, valamint a tiltakozáshoz való jognak a gyakorlását[44].

50. A hozzáféréshez, illetve eltávolításhoz és törléshez való jogon túlmenően az érintett számára biztosítani kell azt a jogot is, hogy a személyes helyzetéből eredő, kényszerítő erejű, jogos indokok apján bármikor tiltakozni tudjon a személyes adatai kezelése ellen a harmadik ország jogi keretében meghatározott feltételek függvényében[45].

51. A választási lehetőség elvével az adatvédelmi keret tiltakozáshoz való jogot (kívülmaradási jogot –„opt-out") biztosít a személyes adatok harmadik fél részére történő átadása vagy lényegesen eltérő célra történő felhasználása tekintetében[46]. Ezenkívül a természetes személyek bármikor élhetnek a kívülmaradási joggal személyes adataik közvetlen üzletszerzés céljából történő felhasználásával szemben[47]. A közvetlen üzletszerzési céloktól eltekintve a tiltakozáshoz való jog gyakorlásának módozatai – különösen az időzítés – nem kerültek részletes kifejtésre. Az EDPB ezért felkéri a Bizottságot annak tisztázására, hogy a természetes személyek hogyan élhetnek a tiltakozáshoz való jogukkal.

52. Ahogyan a 29. cikk alapján létrehozott munkacsoport 01/2016. sz. véleményében rögzíti, az EDPB úgy véli, hogy nem elegendő pusztán hivatkozni e jog meglétére az adatvédelmi politikában. Személyre szabott lehetőséget kell biztosítani e jog gyakorlására, és nemcsak a személyes adatok közzététele vagy újbóli felhasználása esetében. Az Európai Adatvédelmi Testület hangsúlyozza, hogy az adatvédelmi kereten belül biztosítani kell az érintett személyes helyzetéből eredő, kényszerítő erejű ,jogos indokok alapján történő tiltakozáshoz való általános jogot. Az Európai Adatvédelmi Testület azt ajánlja, hogy ez a tiltakozáshoz való jog mindenkor biztosított legyen, valamint, hogy az ne korlátozódjon az adatok közvetlen üzletszerzési célú felhasználására[48].

53. A humánerőforrás-adatokkal kapcsolatban az Európai Adatvédelmi Testület nagyra értékeli, hogy a Bizottság egyértelműsítette a tájékoztatás és a választási lehetőség elvének alkalmazását abban az esetben, ha egy tanúsított egyesült államokbeli szervezet a humánerőforrás-adatokat nem munkaviszonnyal összefüggő célokra – például marketingértesítésekre – szándékozik felhasználni[49]. Az EDPB ugyanakkor fenntartja, hogy a humánerőforrás-adatok munkaviszonyhoz nem kapcsolódó célokból történő további kezelése a legtöbb esetben összeegyeztethetetlennek minősül az eredeti céllal, és a hozzájárulás ritkán lesz teljesen szabad, ha azt foglalkoztatással összefüggésben adják meg.

54. Az EDPB megismétli továbbá a 29. cikk szerinti munkacsoport aggályait annak kapcsán, hogy a humánerőforrás-adatokra vonatkozóan kivétel lehetséges a tájékoztatás és választási lehetőség elvek alól „*olyan mértékben és arra az időtartamra, amely annak érdekében szükséges, hogy a szervezet lehetőségei ne csorbuljanak az előléptetések, kinevezések vagy más hasonló foglalkoztatási döntések meghozatala során*[50]", mely kivételt az EDPB tágnak és pontatlannak találja[51].

[44] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 2.2.5. pont.
[45] Általános adatvédelmi rendelet – Megfelelőségi referencia, 3. fejezet, A. pont 8. alpont.
[46] A határozattervezet I. melléklete II. szakasza 2. pontjának a) pontja.
[47] A határozattervezet I. melléklete III. szakasza 12. pontjának a) pontja.
[48] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 2.2.2. pont.
[49] A határozattervezet I. melléklete III. szakasza 9. pontja b) pontjának i. alpontja, valamint a (15) preambulumbekezdés és a 27. lábjegyzet.
[50] A határozattervezet I. melléklete III. szakasza 9. pontja b) pontjának iv. alpontja.
[51] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 2.2.7. pont.

2.1.4 Az újbóli adattovábbítás korlátozása

55. A személyes adatoknak az eredeti adattovábbítás elsődleges címzettje általi újbóli továbbítása kizárólag akkor lehet engedélyezett, ha a további címzettekre (azaz az újbóli adattovábbítás címzettjeire) olyan szabályok (beleértve a szerződéses szabályokat) vonatkoznak, amelyek megfelelő adatvédelmi szintet biztosítanak, és követik az adatkezelő nevében végzett adatkezelésre vonatkozó utasításokat. Az adattovábbítással érintett személyek védelmének szintjét az újbóli adattovábbítás nem csökkentheti. Az EU-ból továbbított adatok első címzettje felelős azért, hogy megfelelőségi határozat hiányában meggyőződjön az újbóli adattovábbításra vonatkozó megfelelő garanciák előírásáról. Ezekre az újbóli adattovábbításokra kizárólag korlátozott és meghatározott célokból kerülhet sor, és kizárólag abban az esetben, ha az adatkezelésnek van jogalapja[52].

56. Az adattovábbításért való elszámoltathatóság elve szerint az újbóli adattovábbításra csak korlátozott és meghatározott célokból kerülhet sor az adatvédelmi keret szervezete és a harmadik fél közötti szerződés (vagy vállalatcsoporton belüli hasonló megállapodás) alapján, és csak akkor, ha a szerződés előírja, hogy a harmadik félnek ugyanolyan szintű védelmet kell nyújtania, mint amelyet az adatvédelmi keret elvei garantálnak[53].

57. Az Európai Adatvédelmi Testület ismételten hangsúlyozni kívánja a 29. cikk szerinti munkacsoport 01/2016. sz. véleményében megfogalmazott aggályokat az adatkezelők közötti, csoporton belüli adattovábbításokra vonatkozó szerződések megléte alóli mentességgel kapcsolatban[54]. A humánerőforrás-adatokkal kapcsolatban az EDPB még mindig nem érti a harmadik fél adatkezelővel való szerződéskötési kötelezettség alóli mentesség indokát az „alkalmi, a foglalkoztatással összefüggő operatív intézkedések" esetében megvalósuló adattovábbítás esetén[55].

58. Az Európai Adatvédelmi Testület megismétli továbbá a 29. cikk szerinti munkacsoport azon kérését[56], hogy a keret hatálya alá tartozó szervezeteknek az újbóli adattovábbítás előtt értékelniük kell, hogy a harmadik ország címzettre alkalmazandó nemzeti jogszabályainak kötelező követelményei nem ásnak-e alá azon érintettek védelmének folytonosságát, akiknek az adatait továbbítják[57].

59. Az EDPB fenntartja, hogy a személyes adatok harmadik országokba történő újbóli továbbítása a természetes személyek alapvető jogaiba való beavatkozáshoz vezethet, és felkéri a Bizottságot annak

[52] Általános adatvédelmi rendelet – Megfelelőségi referencia, 3. fejezet A. pont 9. alpont.
[53] A határozattervezet I. melléklete II. szakaszának 3. pontja.
[54] A határozattervezet I. melléklet, III. szakasza 10. pontja b) pontjának i. alpontja, amely a „más csoporton belüli eszközök (pl. megfelelőségi vagy ellenőrzési programok)" esetére hivatkozik, amelyeknek láthatólag nem kell kötelező erejűnek lenniük.
[55] A határozattervezet I. melléklete III. szakasza 9. pontja e) pontjának i. alpontja, amely olyan példákat említ, mint a biztosításkötés.
[56] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 2.2.3. pont, 21. o.
[57] A Schrems II. ügyben hozott ítélet fényében az Európai Adatvédelmi Testület számos iránymutatásban és ajánlásban tovább pontosította az adatátadók és adatátvevők újbóli továbbítással kapcsolatos kötelezettségeit: lásd az Európai Adatvédelmi Testület 01/2020. számú ajánlását azon intézkedésekről, amelyek kiegészítik az adattovábbítási eszközöket a személyes adatok uniós védelmi szintjének való megfelelés biztosítása érdekében (2.0. változat, elfogadás időpontja: 2021. június 18.); Az Európai Adatvédelmi Testület 02/2020. számú ajánlása a megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról (elfogadás időpontja: 2020. november 10.); 04/2021. sz. iránymutatás az adattovábbítások eszközéül szolgáló magatartási kódexekről (2.0. változat, elfogadás időpontja: 2022. február 22.); 1/2022. sz. ajánlás a jóváhagyás iránti kérelemről és az adatkezelőre vonatkozó kötelező erejű vállalati szabályok elemeiről és elveiről (elfogadás időpontja: 2022. november 14.); 07/2022. sz. iránymutatás a tanúsításról mint az adattovábbítás eszközéről (a nyilvános konzultációt követő elfogadás időpontja: 2023. február 14.).

tisztázására, hogy az adatvédelmi keret összefüggésben történő újbóli adattovábbítás előtt az eredeti címzett által a harmadik országbeli átvevő számára előírt biztosítékoknak a harmadik országbeli jogszabályok tükrében hatékonynak kell lenniük[58].

2.1.5 Automatizált döntéshozatal és profilalkotás

60. A kizárólag automatizált adatkezelésen (egyedi ügyekben történő automatizált döntéshozatal), beleértve a profilalkotást is, alapuló döntésekre, amelyek joghatással vagy az érintettre nézve egyéb jelentős következménnyel járnak, kizárólag a harmadik ország jogi keretében meghatározott, bizonyos körülmények között kerülhet sor. Az európai jogi keretben ezen feltételek közé tartozik például az érintett kifejezett hozzájárulásának megléte vagy egy ilyen döntés szükségessége a szerződés megkötéséhez. Ha a döntés nem felel meg a harmadik ország jogi keretében lefektetett feltételeknek, az érintettnek joga van ahhoz, hogy kivonja magát az automatizált döntéshozatal alól. A harmadik ország jogszabályainak minden esetben biztosítania kell a szükséges garanciákat, beleértve a döntés alapjául szolgáló konkrét okokról és az alkalmazott logikáról szóló tájékoztatáshoz, a pontatlan vagy nem teljes információk helyesbítéséhez, valamint a helytelen tényálláson alapuló döntéshozatal elleni kifogás emeléséhez való jogot[59].

61. Az adatvédelmi keret nem ír elő konkrét jogi garanciákat arra az esetre, ha a természetes személyre olyan döntések vonatkoznak, amelyek joghatással járnak vagy jelentős mértékben érintik őket, és amelyek kizárólag olyan automatizált adatkezelésen alapulnak, amelynek célja a rájuk vonatkozó bizonyos személyes szempontok – például a munkahelyi teljesítményük, a hitelképességük, a megbízhatóságuk vagy a magatartásuk – értékelése.

62. Amint azt a 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, valamint az EDPB a Japánra és Dél-Koreára vonatkozó megfelelőségi határozatokról szóló korábbi véleményeiben[60] már kifejtette, az Európai Adatvédelmi Testület úgy véli, hogy az automatizált döntéshozatal és profilalkotás – egyre inkább mesterségesintelligencia-technológiák révén történő – gyors fejlődése különös figyelmet igényel e tekintetben[61].

63. Az Európai Adatvédelmi Testület tudomásul veszi a Bizottság érveit, amelyek szerint az automatizált döntéshozatalra vonatkozó konkrét szabályok hiánya az adatvédelmi kereten belül valószínűleg nem befolyásolja az Unióban gyűjtött személyes adatok védelmének szintjét (mivel az automatizált adatkezelésen alapuló döntéseket jellemzően az érintettel közvetlen kapcsolatban álló uniós adatkezelő hozza meg)[62]. Az EDPB véleménye szerint azonban nem zárható ki, hogy egy egyesült államokbeli székhelyű adatkezelő automatizált döntéshozatalt alkalmazzon a határozattervezet alapján továbbított adatok tekintetében (pl. a foglalkoztatással összefüggésben a munkahelyi teljesítmény, a biztosítás, a lakhatás értékelése céljából).

---

[58] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 2.2.3. pont, 21. o.

[59] Általános adatvédelmi rendelet – Megfelelőségi referencia, 3. fejezet B. pont 3. alpont.

[60] Az Európai Adatvédelmi Testület 28/2018. sz. véleménye a személyes adatok Japánban való megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről (elfogadás időpontja: 2018. december 5.); Az Európai Adatvédelmi Testület 32/2021. sz. véleménye a személyes adatok Koreai Köztársaságban biztosított megfelelő védelméről szóló európai bizottsági végrehajtási határozat tervezetéről (elfogadás időpontja: 2021. szeptember 24.).

[61] Lásd többek között: OQ kontra Land Hesse (SCHUFA Holding és társai), C-634/21, előzetes döntéshozatal iránti kérelem (folyamatban).

[62] A határozattervezet (33) és (34) preambulumbekezdése.

64. Az EDPB üdvözli a Bizottság hivatkozásait az Egyesült Államok vonatkozó jogszabályai által a különböző területeken nyújtott konkrét biztosítékokra[63]. Az EDPB számára ugyanakkor úgy tűnik, hogy a természetes személyek védelmének szintje eltérő attól függően, hogy milyen ágazatspecifikus szabályok – ha vannak ilyenek – alkalmazandók a szóban forgó helyzetre. Fennáll annak a kockázata, hogy egyes helyzetek azért nem kerülnek lefedésre, mert nem tartoznak az említett jogi aktusok hatálya alá. Ezenkívül az automatizált döntéshozatallal kapcsolatos egyéni jogok tartalmát a különböző jogi aktusok eltérően írják le.

65. Ennek alapján az EDPB úgy véli, hogy az automatizált döntéshozatalra vonatkozó konkrét szabályok lefektetésére van szükség az adatvédelmi keretben a megfelelő biztosítékok nyújtásához, beleértve az egyén azon jogát, hogy megismerhesse az alkalmazott logikát, megtámadhassa a döntést és emberi beavatkozást kérhessen, amennyiben a döntés őt jelentős mértékben érinti [64].

2.2 Eljárási és végrehajtási mechanizmusok

66. Az EDPB megjegyzi, hogy az adatvédelmi keret továbbra is egy öntanúsítási rendszerre támaszkodik, még akkor is, ha a Bizottság arra „tanúsítási" rendszerként hivatkozik.

67. Az EDPB emlékeztet a korábbi közös felülvizsgálatok során elért eredményekre. Ilyen például a DoC szerepe, az öntanúsítási/(újra)tanúsítási folyamat […], a vállalatok az adatvédelmi keret elveinek való megfelelésének nyomon követése (pl. szúrópróbaszerű ellenőrzések, megfelelésre vonatkozó kérdőívek használata), valamint a részvételre vonatkozó hamis állítások azonosítása és kezelése (pl. internetes keresések révén) vonatkozásában.

68. Ugyanakkor a 29. cikk szerinti munkacsoport és az Európai Adatvédelmi Testület aggodalmát fejezte ki az adatvédelmi pajzs követelményeinek való megfelelés felügyeletének bizonyos hiánya miatt[65]. Az EDPB különösen egyetért a Bizottságnak az adatvédelmi pajzs harmadik éves felülvizsgálatát követő megállapításaival, amelyek szerint az adatvédelmi pajzs értelmében a DoC által végzett szúrópróbaszerű ellenőrzések általában a formai követelményekre korlátozódtak (pl. a kijelölt kapcsolattartók válaszadásának hiánya vagy a vállalat adatvédelmi politikája online elérhetőségének hiánya)[66]. The EDPB considers that . Az Európai Adatvédelmi Testület úgy véli, hogy a lényegesebb követelményekkel kapcsolatos megfelelőségi ellenőrzések kulcsfontosságúak.

69. Az EDPB továbbá emlékeztet az adatvédelmi keret hatékony felügyeletének (ideértve a lényegi követelményeknek való megfelelést is) és végrehajtásának fontosságára. Az EDPB szorosan nyomon követi majd ezt a szempontot, többek között az időszakos felülvizsgálatok keretében.

70. Ami a végrehajtást illeti, az EDPB tudomásul veszi az FTC[67] és a DoT[68] leveleiben foglalt megújított kötelezettségvállalásokat, amelyek szerint prioritásként kell kezelni az adatvédelmi keret feltételezett megsértésére irányuló vizsgálatokat, megfelelő végrehajtási intézkedéseket kell hozni a részvételre vonatkozó hamis vagy megtévesztő állításokat benyújtó szervezetekkel szemben, nyomon kell követni az adatvédelmi keret megsértésére vonatkozó végrehajtási végzéseket, és együtt kell működni az uniós

[63] A határozattervezet (35) preambulumbekezdése.
[64] Lásd még a harmadik közös felülvizsgálati jelentés 76. pontját.
[65] Harmadik közös felülvizsgálati jelentés, 7. pont.
[66] A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak az EU–USA adatvédelmi pajzs működésének harmadik éves felülvizsgálatáról, 2019.10.23., COM(2019) 495 final, 4. o.
[67] A határozattervezet IV. melléklete.
[68] A határozattervezet V. melléklete.

adatvédelmi hatóságokkal. E tekintetben az EDPB azt is elismeri, hogy az FTC jelezte, miszerint jogérvényesítési erőfeszítéseit várhatóan még inkább az adatvédelmi keret jelentős mértékű megsértésére összpontosítja, és saját kezdeményezésre (is) vizsgálatokat kíván folytatni. Az EDPB szorosan nyomon követi majd ezeket a szempontokat többek között az időszakos felülvizsgálatok keretében.

2.3 Jogorvoslati mechanizmusok

71. Az EDPB üdvözli, hogy a határozattervezet egyértelműen bemutatja az uniós érintettek számára biztosított hét jogorvoslati lehetőséget, amennyiben személyes adataikat az adatvédelmi keret megsértésével kezelnék[69].

72. Ezek a különböző jogorvoslati mechanizmusok a jogorvoslat, végrehajtás és felelősség elvével, valamint a DoC által kiadott és a határozattervezet I. mellékletében említett, a vitarendezésről és végrehajtásról szóló 11. kiegészítő elv követelményeivel összhangban kerültek kialakításra[70].

73. Amint azt a Bizottság a határozattervezetében hangsúlyozta, *„az érintettet hatékony közigazgatási és bírósági jogorvoslatban kell részesíteni”*[71]. Ez megfelel a GDPR 45. cikke (2) bekezdésének a) pontjában rögzített követelménynek, miszerint a Bizottságnak a harmadik ország által biztosított védelmi szint megfelelőségének értékelésekor figyelembe kell vennie többek között azt is, hogy „az érintettek, akiknek a személyes adatait továbbítják, rendelkeznek-e hatékonyan érvényesíthető – a hatékony közigazgatási és bírósági jogorvoslatot is magukban foglaló – jogokkal”[72]. Erre a követelményre az általános adatvédelmi rendelet megfelelőségi referenciája is emlékeztet[73].

74. Az EDPB megjegyzi , hogy ezek a jogorvoslati mechanizmusok megegyeznek a korábbi adatvédelmi pajzsban meghatározottakkal, amelyekkel kapcsolatban a 29. cikk szerinti munkacsoport észrevételeket fogalmazott meg[74].

75. A választottbírósági mechanizmust illetően az Európai Adatvédelmi Testület megjegyzi, hogy ez a lehetőség az adatvédelmi keret alapelvei[75] alóli kivételek tekintetében nem áll rendelkezésre, ezért a 33. bekezdésben tett észrevételére hivatkozik.

76. Az Egyesült Államok joga alapján rendelkezésre álló további jogorvoslati lehetőségeket illetően az EDPB szintén üdvözölné az említett jogszabályokkal kapcsolatos további részletek ismertetését[76], és a 21. bekezdésben foglalt észrevételére hivatkozik.

77. Emellett az Európai Adatvédelmi Testület üdvözli az FTC azon levelét, amelyben az uniós adatvédelmi hatóságokkal való szoros együttműködésre irányuló szándékát fejezi ki[77]. Az Európai Adatvédelmi

[69] A határozattervezet (67) preambulumbekezdése.
[70] A határozattervezet I. melléklete II. szakaszának 7. pontja és III. szakaszának 11. pontja, valamint I. mellékletének I. melléklete.
[71] A határozattervezet (64) preambulumbekezdése.
[72] Lásd még az általános adatvédelmi rendelet (141) preambulumbekezdését, amely az Alapjogi Charta 47. cikkére hivatkozik az EU-ban a hatékony bírósági jogorvoslathoz való jog tekintetében.
[73] Általános adatvédelmi rendelet – Megfelelőségi referencia, 8. o.
[74] Lásd különösen a 29. cikk szerinti munkacsoport 01/2016. sz. véleménye 2.2.6. szakaszának a) pontját.
[75] A határozattervezet I. melléklete I. mellékletének A. pontja.
[76] A határozattervezet (85) preambulumbekezdése.
[77] A határozattervezet IV. melléklete.

Testület üdvözli továbbá, hogy az FTC prioritásként kezeli a panaszokat, bár lehetséges, hogy ez nem biztosítja az érintett számára, hogy panaszaival a szervezet minden esetben foglalkozni fog.

78. Azt a lehetőséget illetően, hogy bizonyos esetekben a természetes személyek panaszt nyújthatnak be valamely uniós adatvédelmi hatósághoz, az EDPB üdvözölné a további információkat i. arra vonatkozóan, hogy az uniós adatvédelmi hatóság azon lehetősége, hogy a korrekciós vagy kompenzációs intézkedésekkel kapcsolatban tanácsot adjon, magában foglalhat-e a bírságokra vagy a vizsgálati hatáskörök alkalmazására vonatkozó ajánlást, és ii. azt illetően, hogy az uniós adatvédelmi hatóság fellépései az FTC vagy a DoT végrehajtási intézkedéseinek bizonyítékaként milyen mértékben kerülnek figyelembevételre[78].

79. Az EDPB szorosan nyomon követi majd a jogorvoslati mechanizmusok hatékonyságát többek között az időszakos felülvizsgálatok keretében.

3 AZ EURÓPAI UNIÓBÓL TOVÁBBÍTOTT SZEMÉLYES ADATOKHOZ VALÓ HOZZÁFÉRÉS ÉS AZ ILYEN ADATOK FELHASZNÁLÁSA AZ EGYESÜLT ÁLLAMOK HATÓSÁGAI ÁLTAL

3.1 Bűnüldözési célú hozzáférés és felhasználás

3.1.1 A bűnüldöző hatóságok személyes adatokhoz való hozzáférésének egyértelmű, pontos és hozzáférhető szabályokon kell alapulnia

80. Az EDPB üdvözli a határozattervezetben szereplő, a korábbi megfelelőségi határozathoz képest részletesebb információkat és magyarázatokat a személyes adatokhoz az Egyesült Államok hatóságai általi, bűnüldözési célból történő hozzáférésre és azok felhasználására vonatkozóan. A határozattervezet VI. melléklete továbbá az Egyesült Államok Igazságügyi Minisztériuma bűnügyi osztályának levelét is tartalmazza, amely „rövid áttekintést nyújt az Egyesült Államokban a kereskedelmi adatok és más vállalati információk bűnüldözési vagy közérdekű (polgári és közigazgatási) célú beszerzésére használt elsődleges nyomozati eszközökről, ideértve az ezekben a hatáskörökben meghatározott betekintési korlátokat”. A levél szerint az abban leírt valamennyi jogi eljárást az egyesült államokbeli vállalatoktól való információszerzésre használják fel, tekintet nélkül az érintett állampolgárságára vagy tartózkodási helyére, és ezek az eljárások közvetlenül az Egyesült Államok alkotmányából (negyedik módosítás), a tételes és eljárási jogból, vagy az Igazságügyi Minisztérium irányelveiből és szabályzataiból erednek. Ez az áttekintés nem terjed ki a bűnüldözés által a terrorizmus és más nemzetbiztonsági nyomozások során használt nemzetbiztonsági nyomozati eszközökre[79].

81. Az EDPB megjegyzi, hogy a határozattervezet és annak VI. melléklete elsősorban a szövetségi bűnüldöző és szabályozó hatóságokat[80] tárgyalja, és nem hivatkozik kifejezetten azokra az állami törvényekre, amelyek előírják ezeket az információszerzésre irányuló eljárásokat. A VI. melléklet azt is megemlíti, hogy „vannak más, az adott ágazaton és a birtokukban lévő adatok típusán alapuló jogalapok is a közigazgatási hivatalok adatkéréseinek vitatására”, és több nem kimerítő példát sorol

[78] A határozattervezet I. melléklete III. szakasza 5. pontja b) pontjának iii. alpontja.
[79] A határozattervezet VI. mellékletének 1. lábjegyzete.
[80] Lásd a határozattervezet (90)–(93) preambulumbekezdését.

fel, így a banktitokról szóló törvényt és annak végrehajtási rendeleteit[81], a méltányos hitelminősítésről szóló törvényt[82] és a pénzügyi adatok védelméről szóló törvényt[83]. Az EDPB megjegyzi, hogy egy adott hozzáférés iránti kérelemre alkalmazandó jogalap a kért adatok jellegétől, a vállalat jellegétől, a jogi eljárások jellegétől (büntetőjogi, közigazgatási, egyéb közérdekhez kapcsolódó) és a hozzáférést kérő szervezet jellegétől függ. Mivel a bűnüldöző hatóságoknak az Egyesült Államokba továbbított adatokhoz való hozzáférését korlátozó valamennyi alkalmazandó szabály az alkotmányon, a tételes jogon és az Igazságügyi Minisztérium átlátható szakpolitikáin alapul, az EDPB elismeri e szabályok hozzáférhetőségét, és felkéri a Bizottságot, hogy ezt az elemet vegye figyelembe a határozattervezetben. A VI. mellékletből következik, hogy ezek a törvények az érintett állampolgárságától vagy a tartózkodási helytől függetlenül alkalmazandók, és általánosságban magukban foglalják a negyedik alkotmánymódosítás követelményeit (bár gyakran túlmutatnak ezen, és további védelmet is rögzítenek).

82. Következésképpen az EDPB tudomásul veszi a határozattervezetben foglalt, a szövetségi bűnüldöző hatóságok hozzáférésére vonatkozó és a korábbi megfelelőségi határozathoz képest részletesebb értékelést. Ami az állami bűnüldöző hatóságok hozzáférését illeti, az EDPB azt is tudomásul veszi, hogy a VI. melléklet szerint az állami jogi védelemnek az Egyesült Államok alkotmánya által biztosított védelemmel legalább egyenértékűnek kell lennie, beleértve többek között az alkotmány negyedik módosítását is. Az EDPB felkéri a Bizottságot, hogy a jövőbeli felülvizsgálatok során az állami jog által előírt védelem elemét további értékelésnek vesse alá.

3.1.2 Bizonyítani kell az intézkedés szükségességét és arányosságát az elérni kívánt jogszerű célokra tekintettel

83. Az EDPB megjegyzi, hogy az adatokhoz bűnüldözési céljából való hozzáférésre irányuló kérelem általánosságban jogszerű célt szolgálónak tekinthető. Ugyanakkor az ilyen beavatkozások csak akkor fogadhatók el, ha azok szükségesek és arányosak[84].

84. Az EUB állandó ítélkezési gyakorlatának megfelelően az arányosság elve a magánélethez és a személyes adatok védelméhez való jogokba való beavatkozást bevezető jogalkotási intézkedésektől elvárja, hogy azok „alkalmasak legyenek a szóban forgó szabályozás által kitűzött jogszerű célok elérésére, és ne haladják meg az e célok eléréséhez szükséges mértéket[85]”. Ezért a szükségesség és arányosság értékelése főszabály szerint mindig a jogalkotás által tervezett konkrét intézkedésekkel kapcsolatosan végzendő el.

85. Az Egyesült Államok hatóságai a VI. mellékletben meghatározzák, hogy a szövetségi ügyészek és a szövetségi nyomozó ügynökök „többféle típusú kötelező bírósági eljáráson keresztül kérhetik vállalati dokumentumok és más adatok kiadását, beleértve a vádesküdtszéki idézéseket, a

[81] 31 U.S.C. 5318. §; 31 C.F.R. X. fejezet.
[82] 15 U.S.C. 1681b. §.
[83] 12 U.S.C. 3401–3423. §.
[84] Lásd: a Bíróság 2020. október 6-i ítélete, La Quadrature du Net és társai egyesített ügyek, C-511/18, C-512/18 és C-520/18, ECLI:EU:C:2020:791 (a továbbiakban: a Bíróság La Quadrature du Net ügyben hozott ítélete), 140. pont. Lásd még: EDPS: Eszköztár: A személyes adatok védelmére való alapvető jogot korlátozó intézkedések szükségességének értékelése, 2017. április 11. , és EDPS: Az európai adatvédelmi biztos iránymutatása az adatvédelemhez és a személyes adatok védelméhez fűződő alapvető jogokat korlátozó intézkedések arányosságának értékeléséről, 2019. december 19.
[85] Lásd: a Bíróság 2014. április 8-i ítélete, Digital Rights Ireland egyesített ügyek, C-293/12 és C-594/12, ECLI:EU:C:2014:238 (a továbbiakban: a Bíróság Digital Rights Ireland ügyben hozott ítélete), 46. pont és az ott hivatkozott ítélkezési gyakorlat.

bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat, valamint a házkutatási parancsokat", és a „szövetségi bűnügyi lehallgatási és hívásrögzítési hatáskörök szerint" más kommunikációkhoz is hozzáférhetnek[86]. Ezen túlmenően a polgári és szabályozó feladatkörrel felruházott hivatalok bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat adhatnak ki vállalatoknak „üzleti adatok, elektronikusan tárolt információk vagy más ingóságok tárgyában"[87]. Magukat a folyamatokat a határozattervezet (90)–(93) preambulumbekezdése is kifejti. Az EDPB e tekintetben megjegyzi az Egyesült Államok elektronikusan tárolt információkkal kapcsolatos ítélkezési gyakorlatában tapasztalható, a határozattervezetben említett pozitív változást[88].

86. A VI. melléklet rögzíti továbbá, hogy ezek a jogi eljárások mentesek a hátrányos megkülönböztetéstől, és azokat általában az egyesült államokbeli „vállalatoktól" való információszerzésre használják fel, függetlenül attól, hogy azok az Egyesült Államok–EU adatvédelmi kereten belül rendelkeznek-e tanúsítvánnyal vagy sem, illetve függetlenül „az érintett állampolgárságától vagy lakóhelyétől".

87. Emellett a VI. melléklet az Egyesült Államok alkotmányának negyedik módosítása szerinti biztosítékokra vonatkozó megállapításokat is tartalmaz, amelyeknek értelmében a bűnüldöző hatóságok által végrehajtott átkutatáshoz és lefoglalásokhoz – amennyiben alapos ok áll fenn és teljesül az egyediség követelménye – elsődlegesen bírósági végzésre van szükség, valamint hivatkozik arra a tényre, hogy kivételes esetekben, amikor a végzésre vonatkozó követelmény nem alkalmazandó, a bűnüldözés folyamatát a negyedik módosítás szerinti „észszerűségi" vizsgálat alá kell vetni[89]. Az a személy, akinek vonatkozásában kutatást folytatnak, vagy akinek személyes vagyonát átkutatják, indítványozhatja a jogellenes átkutatás során szerzett vagy abból származó bizonyítékok kizárását, amennyiben e bizonyítékot egy büntetőeljárás során ellene hozzák fel[90].

88. Következésképpen az EDPB megjegyzi, hogy az Egyesült Államokban a kereskedelmi adatok és egyéb nyilvántartási információk a vállalatoktól bűnüldözési vagy közérdekű célokból – ideértve a hozzáférési korlátozásokat és biztosítékokat is – történő megszerzésére használt nyomozati eszközök rendszere átfogó, de egyben összetett intézkedésrendszert is biztosít, amely tükrözi többek között az Egyesült Államok kormányának szövetségi jellegét.

89. Ezért az Egyesült Államok bűnüldözési nyomozati intézkedéseinek rendszere általában véve megfelelőnek tekinthető a szükségesség és arányosság követelményeinek vonatkozásában a magánélethez és az adatvédelemhez való alapvető jogok tekintetében.

3.1.3 Független felügyeleti mechanizmus kialakítása

90. Az EDPB megjegyzi, hogy a határozattervezet és a VI. melléklet által leírt legtöbb eljárás előfeltételezi egy bírósági határozat meglétét a hatóságoknak az adatokhoz való hozzáférését megelőzően (pl. hívásrögzítésre és lehallgatásra vonatkozó bírósági végzések[91], a szövetségi lehallgatási törvény szerinti

[86] A határozattervezet VI. mellékletének 2. oldala.
[87] A határozattervezet VI. mellékletének 4. oldala.
[88] Lásd a határozattervezet 146. lábjegyzetét. Egy 2018-as ítéletében az Egyesült Államok Legfelsőbb Bírósága megerősítette, hogy a bűnüldöző hatóságok számára a kutatási parancsra vagy a kutatási alóli kivételt elrendelő határozatra is szükség van ahhoz, hogy hozzáférhessenek azokhoz a múltbeli, cellainformációkon alapuló helymeghatározó adatokhoz, amelyek átfogó áttekintést nyújtanak a felhasználó mozgásairól, illetve, hogy a felhasználó az ilyen információk tekintetében méltányosan várhatja el adatainak védelmét (Timothy Ivory Carpenter kontra Amerikai Egyesült Államok, 16-402. sz. ítélet, 585 U.S. [2018]).
[89] Lásd a határozattervezet VI. mellékletének 2. oldalát.
[90] Lásd a határozattervezet (90) preambulumbekezdését.
[91] Lásd a határozattervezet (92) preambulumbekezdését.

megfigyelésre szóló bírósági végzések[92], házkutatási parancsok – a szövetségi büntetőeljárási szabályok 41. szabálya[93]). Ugyanakkor úgy tűnik, hogy nem mindegyikhez szükséges a bíróság előzetes részvétele. Például polgári és szabályozó feladatkörrel felruházott hivatalok „bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat adhatnak ki"[94]. Ilyen esetekben fennáll az idézés észszerűségével kapcsolatos utólagos bírósági ellenőrzés lehetősége, mivel a bizonyításfelvételben való közreműködésre kötelező hatósági határozatokat címzettje bíróságon vitathatja az adott határozat végrehajtását[95].

91. A határozattervezet emellett leírja a szövetségi bűnüldöző szervek különböző szervezetek általi felügyeletét az adatvédelmi és polgári szabadságjogi tisztségviselők által végzett belső ellenőrzéstől kezdve a főfelügyelő és az Egyesült Államok kongresszusának különbizottságai által végzett külső ellenőrzésekig[96]. Az Európai Bizottság árnyalt és részletes információkkal szolgál, és általában véve érthető következtetéseket fogalmaz meg. Az EDPB ezért tartózkodik attól, hogy a véleményben szereplő ténymegállapításokat és értékeléseket megismételje ebben a véleményben.

92. A rendelkezésre álló információk alapján a EDPB megjegyzi, hogy a bűnüldöző hatóságok az egyesült államokbeli cégek által tárolt adatokhoz való hozzáférésének vonatkozásában egy meglehetősen erős, független felügyeleti mechanizmus van érvényben.

3.1.4 A magánszemélyek számára hatékony jogorvoslati lehetőségeket kell biztosítani

93. Az EUB ítélkezési gyakorlata értelmében a természetes személynek hatékony jogorvoslattal kell rendelkeznie jogainak érvényesítéséhez abban az esetben, ha úgy ítéli meg, hogy azokat nem tartják vagy nem tartották tiszteletben. Az EUB a Schrems I. ügyben kifejtette, 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 töröltesse, nem tartja tiszteletben a hatékony bírói jogvédelemhez való jog lényegét, amelyet az Európai Unió Alapjogi Chartája 47. cikke mond ki. E cikk első bekezdése ugyanis megköveteli, hogy mindenkinek, akinek az Unió joga által biztosított jogait és szabadságait megsértették, a hivatkozott cikkben megállapított feltételek mellett joga van a bíróság előtti hatékony jogorvoslathoz"[97].

94. A határozattervezet[98] és annak VI. melléklete további információkat tartalmaz a törvényi szabályozásból eredő lehetséges jogorvoslati lehetőségekről, amelyek az természetes személyek rendelkezésére állnak abban az esetben, ha a hatóságok jogellenesen férnek hozzá adataikhoz.

95. E tekintetben a Bizottság szerint[99] az 5 U.S.C. 702. §-a (A közigazgatási eljárásról szóló törvény [Administrative Procedure Act – APA]) úgy rendelkezik, hogy az a személy, akit egy ügynökség tevékenysége miatt jogsérelem ér, vagy aki valamely vonatkozó törvény értelmében az ügynökségi eljárás miatt hátrányos helyzetbe kerül vagy sérelmet szenved, az üggyel kapcsolatosan bírósági felülvizsgálatra jogosult.

[92] Lásd a határozattervezet VI. mellékletének 3. oldalát.
[93] Lásd a határozattervezet (90) preambulumbekezdését és VI. mellékletének 3. oldalát.
[94] Lásd a határozattervezet VI. mellékletének 4. oldalát, valamint (91) preambulumbekezdését.
[95] Lásd a határozattervezet VI. mellékletének 4. oldalát, valamint (91) preambulumbekezdését.
[96] Lásd a határozattervezet (103)–(106) preambulumbekezdését.
[97] A Bíróság Schrems I. ügyben hozott ítélete, 95. pont.
[98] Lásd a határozattervezet (107)–(112) preambulumbekezdését.
[99] Lásd a határozattervezet (109) preambulumbekezdését.

96. Ezen túlmenően a tárolt kommunikációról szóló törvény (Stored Communications Act – [SCA]) (amelyet az elektronikus hírközlési adatvédelmi törvény II. címe alatt iktattak be) úgy rendelkezik, hogy az említett fejezet bármely olyan megsértése által sérelmet szenvedett személy, amelynek során a jogsértést megvalósító magatartás tudatos vagy szándékolt volt, az Egyesült Államoktól eltérő, az adott jogsértésben részt vevő személytől vagy szervezettől polgári per keretében megfelelő jogorvoslatot követelhet[100]. Ezen túlmenően bármely olyan személy, akit az említett fejezet vagy a 119. fejezet szándékos megsértése miatti sérelem ért, az Egyesült Államok Kerületi Bíróságán pénzbeli kártérítés iránti keresetet nyújthat be az Egyesült Államokkal szemben[101].

97. Emellett a határozattervezet tartalmaz információkat a szövetségi ügynökségi nyilvántartáshoz az információkhoz való szabad hozzáférésről szóló törvény (Freedom of Information Act– FOIA)[102] és számos más olyan jogszabály értelmében történő hozzáférés jogáról is, amelyek feljogosítják a természetes személyeket arra, hogy keresetet indítsanak valamely egyesült államokbeli hatóság vagy tisztviselő ellen személyes adataik kezelése kapcsán (például a lehallgatásról szóló törvény, a számítógépes csalásról és visszaélésről szóló törvény, a kártérítési követelésekről szóló szövetségi törvény, a pénzügyi adatok védelméről szóló törvény, valamint a méltányos hitelminősítésről szóló törvény)[103].

98. Az Európai Adatvédelmi Testület ezért üdvözli a Bizottság által a magánszemélyek számára igénybe vehető jogorvoslati lehetőségek számára vonatkozóan nyújtott pontosításokat. Az Európai Adatvédelmi Testület továbbá felkéri a Bizottságot annak további tisztázására, hogy ezek a jogorvoslatok az EUB kérésének megfelelően lehetővé teszik-e az érintett számára, hogy „a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse”.

3.1.5 A gyűjtött adatok további felhasználása

3.1.5.1 Az Egyesült Államok bűnüldöző hatóságai által hozzáférhető adatok további felhasználása

99. Az Európai Adatvédelmi Testület pozitívnak véli, hogy a határozattervezet értékeli az Egyesült Államok bűnüldöző hatóságai által hozzáférhető adatok további felhasználását. Az EDPB azonban sajnálatát fejezi ki azt illetően, hogy csak egy olyan példa kerül ismertetésre, amelynek alapján az információk tovább terjeszthetők[104]. E tekintetben az Európai Adatvédelmi Testület azt ajánlja a Bizottságnak, hogy a határozattervezetbe foglaljon bele további pontosításokat az adatok további felhasználására alkalmazandó elvekről és biztosítékokról, például azokról, amelyek az adatvédelmi törvényben szerepelnek (5 U.S.C. 552a)[105].

3.1.5.2 Az Egyesült Államokon kívüli adattovábbítások

100. Az Európai Adatvédelmi Testület továbbá megjegyzi, hogy az Európai Bizottság utalt az Egyesült Államok bűnüldöző hatóságaitól harmadik országok hatóságai részére történő adattovábbításokra is, de csak a legfőbb ügyész belföldi FBI-műveletekre vonatkozó általános iránymutatásának vonatkozásában (AGG–DOM)[106]. Az EDPB megítélése szerint ezek az információk és értékelések

[100] 18 U.S.C. 2707. §.
[101] 18 U.S.C. 2712. §.
[102] Lásd a határozattervezet (111) preambulumbekezdését.
[103] Lásd a határozattervezet (112) preambulumbekezdését.
[104] Lásd a határozattervezet (102) preambulumbekezdését.
[105] Lásd a legfőbb ügyész belföldi FBI-műveletekre vonatkozó általános iránymutatását (Attorney General Guidelines for Domestic FBI Operations – AGG-DOM), 36. oldal, B. (1)(g).
[106] Lásd a határozattervezet (102) preambulumbekezdését.

elengedhetetlenek ahhoz, hogy elvégezhető legyen az Egyesült Államok jogszabályi kerete és gyakorlata által a nemzetközi közlésekkel és további felhasználással kapcsolatban nyújtott védelem szintjének átfogó értékelése. Tekintettel arra, hogy a Bizottság csak egy korlátozott példával szolgált az Egyesült Államokon kívüli további adattovábbítások kérdésének egészére vonatkozóan, az EDPB felkéri a Bizottságot, hogy pontosítsa az Egyesült Államokban bűnüldözési célból gyűjtött, majd – többek között nemzetközi megállapodások révén – harmadik országokba továbbított személyes adatok újbóli továbbítására, további felhasználására és közzétételére alkalmazandó szabályokat és biztosítékokat.

3.2 Nemzetbiztonsági célú hozzáférés és felhasználás

101. Általános megjegyzésként az Európai Adatvédelmi Testület elismeri, hogy az államok széles mérlegelési jogkörrel rendelkeznek nemzetbiztonsági kérdésekben, amit az EJEB is elismer. Az Európai Adatvédelmi Testület emlékeztet továbbá arra, hogy – amint azt a felügyeleti intézkedésekre vonatkozó alapvető európai garanciákról szóló aktualizált ajánlásai is kiemelik[107] –, az Európai Unióról szóló szerződés 6. cikkének (3) bekezdése kimondja, hogy az EJEE-ben rögzített alapvető jogok az uniós jog általános elveit képezik. Amint azonban az EUB ítélkezési gyakorlatában emlékeztet rá, ez utóbbi – mindaddig, amíg az EU nem csatlakozott hozzá – nem minősül olyan jogi eszköznek, amely hivatalosan be van építve az uniós jogba[108]. Így az alapvető jogoknak az általános adatvédelmi rendelet 45. cikkében előírt védelmi szintjét az e rendeletnek az Alapjogi Chartában rögzített alapvető jogokra tekintettel értelmezett rendelkezései alapján kell meghatározni. Mindemellett az EU Alapjogi Chartája 52. cikkének (3) bekezdése szerint az abban foglalt jogoknak, amelyek megfelelnek az EJEE által biztosított jogoknak, ugyanazzal a jelentéssel és hatállyal kell rendelkezniük, mint az EJEE-ben rögzített jogoknak. Következésképpen, amint arra az EUB emlékeztetett, az EJEB-nek az uniós Chartában is szereplő jogokra vonatkozó ítélkezési gyakorlatát az uniós Chartában foglalt megfelelő jogok értelmezéséhez szükséges minimális védelmi szintként kell figyelembe venni[109]. Az EU Alapjogi Chartája 52. cikke (3) bekezdésének utolsó mondata szerint azonban *„[e]z a rendelkezés nem akadályozza meg azt, hogy az Unió joga kiterjedtebb védelmet nyújtson*”.

102. Ezért a következő értékelés során az Európai Adatvédelmi Testület figyelembe vette az EJEB ítélkezési gyakorlatát, amennyiben az EU Chartája az EUB értelmezése szerint nem rendelkezik olyan magasabb szintű védelemről, amely az EJEB ítélkezési gyakorlatán kívül más követelményeket írna elő.

103. Több jogi eszköz is lehetővé teszi az Egyesült Államok jogi keretében működő amerikai hírszerző ügynökségek számára az adatok gyűjtését, az azokhoz való további hozzáférést és azok kezelését.

104. Amint arra az Európai Bizottság a határozattervezetében emlékeztetett, *„az egyesült államokbeli hírszerző ügynökségek nemzetbiztonsági célokból csak a törvény által engedélyezett módon kérhetnek hozzáférést az Egyesült Államokban található szervezeteknek továbbított személyes adatokhoz, különösen a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (Foreign Intelligence Surveillance Act – FISA) vagy a nemzetbiztonsági levél (National Security Letter – NSL) útján történő hozzáférést engedélyező jogszabályi rendelkezések alapján*”[110]. *„Az Egyesült Államok hírszerző ügynökségeinek lehetőségük van arra is, hogy az Egyesült Államokon kívül személyes adatokat*

[107] Lásd az Európai Adatvédelmi Testület megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. számú ajánlását.
[108] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 98. pontját.
[109] Lásd a Bíróság La Quadrature du Net ügyben hozott ítéletének 124. pontját.
[110] Lásd a határozattervezet (115) preambulumbekezdését.

gyűjtsenek, amelyek magukban foglalhatnak az Unió és az Egyesült Államok között átvitel alatt lévő személyes adatokat is" a 12333. sz. elnöki rendelet (EO 12333) értelmében[111].

105. A konkrét adatgyűjtési rendszerek – különösen a FISA 702. szakasza és a 12333. sz. elnöki rendelet – tekintetében a 14086. sz. elnöki rendelet új szabályokat ír elő az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítése érdekében. Ezeket az általános szabályokat horizontálisan kell alkalmazni, és „további végrehajtásuknak olyan ügynökségi szabályzatok és eljárások révén kell megvalósulnia, amelyek a napi működésre vonatkozó konkrét rendelkezésekbe ültetik át őket"[112]. A 14086. sz. elnöki rendelet többnyire a korábbi 28. elnöki politikai irányelv (PPD-28) helyébe lépett[113].

106. A nemzetbiztonsági célú adatgyűjtésre, -hozzáférésre és további adatfeldolgozására vonatkozó jogi keret értékelése érdekében ezért fontos megvizsgálni az Egyesült Államokon belüli és kívüli adatgyűjtést szabályozó konkrét jogi keretet, azaz a FISA 702. szakaszát és a 12333. sz. elnöki rendeletet, amelyek önmagukban nem változtak az adatvédelmi pajzs korábbi felülvizsgálata óta, figyelembe véve azt a tényt, hogy az új, 14086. sz. elnöki rendelet olyan biztosítékokat nyújt, amelyeket a konkrét szövegek, például a FISA 702. szakasza és a 12333. sz. elnöki rendelet alapján történő adatgyűjtés keretében is végre kell hajtani.

3.2.1 „A" garancia – Az adatkezelésnek összhangban kell állnia a jogszabályokkal, valamint egyértelmű, pontos és hozzáférhető szabályokon kell alapulnia

107. A nemzetbiztonsági célú adatgyűjtés általános felépítésének értékelése során az Európai Adatvédelmi Testület emlékeztetni kíván az úgynevezett „alapvető európai garanciák" közül az elsőre, amely szerint „az adatkezelésnek egyértelmű, pontos és hozzáférhető szabályokon kell alapulnia"[114].

108. Az EUB állandó ítélkezési gyakorlatának megfelelően a személyes adatok védelméhez való jog gyakorlása csak a törvény által korlátozható, és a beavatkozást lehetővé tevő jogalapnak magának kell meghatároznia az érintett jog gyakorlásával kapcsolatos korlátozás terjedelmét[115]. Emellett a Bíróság emlékeztetett arra is, hogy „e szabályozásnak a belső jogban jogilag kötelező erejűnek kell lennie"[116]. E tekintetben az EJEB ítélkezési gyakorlata egyértelművé teszi, hogy a „jog" fogalma anyagi, nem pedig alaki értelemben értendő. Ez magában foglalhatja a Parlament által rájuk ruházott független szabályalkotási hatáskörrel rendelkező szakmai szabályozó testületek által hozott alacsonyabb szintű jogszabályok és szabályozási intézkedések elfogadását, sőt, akár az íratlan jogot is. Ahhoz, hogy

[111] Lásd a határozattervezet (117) preambulumbekezdését.
[112] Lásd a határozattervezet (120) preambulumbekezdését.
[113] Ez az elnöki rendelet hatályon kívül helyezi a 28. elnöki politikai irányelvet, kivéve annak 3. és 6. szakaszát, valamint titkosított mellékletét, amelyek továbbra is hatályban maradnak. Lásd a 2022. október 7-i elnöki nemzetbiztonsági feljegyzést.
[114] A megfigyelési intézkedésekre vonatkozó alapvető európai garanciákról szóló 02/2020. számú ajánlás, elfogadás időpontja: 2020. november 10. Lásd a Schrems II. ügyben hozott ítélet 175. és 180. pontját, valamint a 2017. július 26-i 1/15. sz. vélemény (EU–Kanada PNR-megállapodás) 139. pontját, és a hivatkozott ítélkezési gyakorlatot.
[115] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 174–175. pontját és az ott hivatkozott ítélkezési gyakorlatot. Lásd még a tagállami hatóságok hozzáférését illetően: Privacy International, C-623/17, ECLI:EU:C:2020:790 (a továbbiakban: az EUB Privacy International ügyben hozott ítélete), 65. pont; és az EUB La Quadrature du Net ügyben hozott ítélete, 175. pont.
[116] Az EUB Privacy International ügyben hozott ítéletének 68. pontja.

„törvény” legyen, a normának legalább megfelelően hozzáférhetőnek és kellő pontossággal megfogalmazottnak kell lennie[117].

109. A megkövetelt pontossági fokot a jog korlátozásának mértékéhez viszonyítva kell mérni[118]. Továbbá, ami a törvény „előreláthatóságát” illeti, az EJEB a Zakharov-ügyben emlékeztetett arra, hogy a titkos megfigyelési intézkedésekkel, például a kommunikáció megfigyelésével összefüggésben „az előreláthatóság nem jelenti azt, hogy az egyénnek előre tudnia kell a hatóságok valószínű megfigyelési tevékenységéről, hogy így ehhez igazíthassa a viselkedését”. A titkos megfigyelési intézkedésekre vonatkozó egyértelmű és részletes szabályok azonban elengedhetetlenek az önkényesség kockázatának megelőzéséhez, amennyiben a végrehajtó hatalomra ruházott hatáskört titkosan gyakorolják. „A hazai jognak kellően világosnak kell lennie ahhoz, hogy az állampolgárok részére megfelelően jelezze, hogy milyen körülmények között és feltételek mellett jogosultak az állami hatóságok ilyen intézkedésekhez folyamodni”[119].

110. Emellett az EUB egyértelművé tette, hogy az alkalmazandó harmadik országbeli jog értékelésének arra kell összpontosítania, hogy a természetes személyek hivatkozhatnak-e rá és érvényesíthetik-e azt a bíróság előtt. Az érintettek számára biztosított jogoknak különösképpen érvényesíthetőknek kell lenniük, és az egyéneket a hatóságokkal szemben érvényesíthető jogokkal kell felruházni[120], ami az előző PPD-28 összefüggésében nem történt meg. A 14086. sz. elnöki rendelet, amely az EDPB értelmezése szerint ugyanazzal a joghatással bír az Egyesült Államok jogrendjében, mint a PPD-28 (azaz a végrehajtó hatalomra nézve kötelező érvényű), rendelkezik a hatóságokkal szemben érvényesíthető jogosultságokról. Az érintettek új érvényesíthető jogainak részletes értékelését a jogorvoslatról szóló szakasz tartalmazza.

111. A határozattervezet (114)–(152) preambulumbekezdése és a VII. melléklet összefoglalja az irányadó jogi keret egyes vonatkozásait, a gyűjtés korlátait, a megőrzési és terjesztési korlátozásokat, a megfelelést és a felügyeletet, az átláthatóságot és a jogorvoslatot. Az Egyesült Államok hírszerzési tevékenységekre vonatkozó jogrendszere számos különböző dokumentumból áll, beleértve az egyes ügynökségek jelentéseit, szabályzatait és eljárásait. E tekintetben az EDPB értékelése általa kulcsfontosságúnak ítélt, korlátozott számú kérdésre összpontosít.

112. A határozattervezet (115)–(119) preambulumbekezdése szerint az amerikai nemzetbiztonsági hatóságok csak a FISA alapján, más jogszabályi rendelkezések alapján (12 U.S.C. § 3414, 15 U.S.C. § 1681u–1681v és 18 U.S.C. § 2709), vagy az átvitel alatt álló személyes adatokkal kapcsolatban a 12333. sz. elnöki rendelet alapján férhetnek hozzá a továbbított személyes adatokhoz. A határozattervezet (116) és (118) preambulumbekezdéséből következik, hogy a Bizottság az Egyesült Államok nemzetbiztonsági hatóságainak a személyes adatokhoz való hozzáférésével kapcsolatos értékelését a legrelevánsabbnak tekintett rendelkezésekre, azaz a FISA 105., 302., 402., 501. és 702. szakaszára (az USA-n kívül tartózkodó nem amerikai személyeket célzó külföldi hírszerző tevékenységek) és a 12333. sz. elnöki rendeletre (átvitel alatt lévő személyes adatokra vonatkozó külföldi hírszerzési tevékenységek) összpontosítja. Az EDPB véleménye ezért e rendelkezések Bizottság

[117] Az EJEB 1979. április 26-i ítélete, Sunday Times kontra Egyesült Királyság (1. sz.), CE:ECHR:1979:0426JUD000653874 (a továbbiakban: az EJEB Sunday Times kontra Egyesült Királyság ügyben hozott 1. számú ítélete), 49. pont.

[118] EJEB, Sunday Times kontra Egyesült Királyság 1. sz. ítélet, 49. pont.

[119] Az EJEB 2015. december 4-i ítélete, Zakharov kontra Oroszország (a továbbiakban: az EJEB Zakharov ítélete), 229. pont.

[120] A Bíróság Schrems I. ügyben hozott ítélete, 181. pont.

általi értékelésére korlátozódik, figyelembe véve a 14086. sz. elnöki rendeletben meghatározott korlátozásokat és biztosítékokat[121].

113. E tekintetben meg kell jegyezni, hogy a határozattervezetben említett valamennyi jogi eszköz hozzáférhető a nyilvánosság számára (az Egyesült Államokban és azon kívül), és online is elérhető. Az elnöki rendeletben meghatározott követelmények továbbá az Egyesült Államok Hírszerző Közösségének[122] egészére nézve kötelező érvényűek, és horizontálisan alkalmazandók valamennyi külföldi hírszerzési célú tevékenységre vonatkozóan.

114. A „jelfelderítés" fogalmát a 14086. sz. elnöki rendelet nem határozza meg. Utóbbi dokumentum a külföldi hírszerzés és kémelhárítás hatályának meghatározásához a 12333. sz. elnöki rendeletben szereplő fogalommeghatározásokra hivatkozik, amelyek tágan értelmezettek. E tekintetben, még azon megfogalmazott érv ellenére is, miszerint a FISA bevezetése óta a 12333. sz. elnöki rendelet csak az Egyesült Államok területén kívüli adatgyűjtésre vonatkozóan használható fel, az EDPB emlékeztet arra, hogy maga a 12333. sz. elnöki rendelet, amely továbbra is változatlan, nem kellően részletezett a rendelet földrajzi hatálya, az adatok gyűjtésének, megőrzésének, és további terjesztésének mértéke, és a megfigyelés alapjául szolgáló bűncselekmények természete, valamint az összegyűjthető és felhasználható információk jellege tekintetében. Elviekben a 12333. sz. elnöki rendelet hatálya alá tartozó valamennyi külföldi hírszerzési adatgyűjtésre sor kerülhet az Egyesült Államok elnökének belátása szerint[123]. Ugyanakkor az Európai Adatvédelmi Testület értelmezése szerint a 14086. sz. elnöki rendelet fő célja a személyes adatok külföldi hírszerzéssel összefüggésben történő gyűjtésére és kezelésére vonatkozó korlátozások előírása, függetlenül attól, hogy melyik megfigyelési programot használják, valamint, hogy az adatokat honnan szerzik be. Ezért az EDPB úgy értelmezi, hogy a 14086. sz. elnöki rendeletben előírt további biztosítékok az átvitel alatt lévő személyes adatokra alkalmazandó, 12333. sz. elnöki rendelet értelmében zajló megfigyelési programokkal összefüggésben is alkalmazandók[124].

115. E tekintetben a 14086. sz. elnöki rendelet 12, a jelfelderítési adatgyűjtés során követendő, jogszerű célt sorol fel, 5 olyan célt, amelyek esetében tilos jelfelderítési adatgyűjtést végezni[125], valamint 6 jogszerű célt a tömegesen gyűjtött adatok felhasználására vonatkozóan[126]. Míg néhányuk meglehetősen részletes (pl. „túszok mentése"), mások általánosabbak (pl. „globális biztonság"). A 14086. sz elnöki rendelet a tiltott célok listáját is tartalmazza, amelyek közé tartozik nevezetesen a „jogos adatvédelmi érdekek" semmibevétele, illetve korlátozása[127]. A 14086. sz. elnöki rendelet arról is rendelkezik, hogy az Egyesült Államok elnöke további célokkal egészítheti ki azon célok listáját, melyeknek esetében a gyűjtés megengedett, és ez a lista az elnök döntése alapján nyilvánosságra nem hozhatónak is minősíthető, amennyiben az elnök úgy ítéli meg, hogy a nyilvánosságra hozatal

121 Ez az elnöki rendelet hatályon kívül helyezi a 28. elnöki politikai irányelvet, kivéve annak 3. és 6. szakaszát, valamint titkosított mellékletét, amelyek továbbra is hatályban maradnak. Lásd a 2022. október 7-i elnöki nemzetbiztonsági feljegyzést.

122 Lásd a határozattervezet (120) preambulumbekezdését.

123 Az Egyesült Államok alkotmányának II. cikke értelmében a nemzetbiztonság garantálásának felelőssége, beleértve különösen a külföldi hírszerzési információk gyűjtését, az elnök mint a fegyveres erők főparancsnoka hatáskörébe tartozik.

124 Lásd a határozattervezet (134) preambulumbekezdését.

125 Lásd a 14086. sz. elnöki rendelet („EO 14086") 2. szakasza b) pontja ii. alpontja A. pontjának 1–5. pontját.

126 Lásd a határozattervezet (134) preambulumbekezdését és a 14086. sz. elnöki rendelet. 2. szakasza c) pontjának ii. alpontját.

127 Lásd a 14086. sz. elnöki rendelet 2. szakasza b) pontja ii. alpontja A. pontjának 2. pontját.

veszélyeztetné az Egyesült Államok nemzetbiztonságát[128]. Az ilyen frissítések csak „az új nemzetbiztonsági követelmények fényében" engedélyezhetők.

116. A hírszerző ügynökségek a jelfelderítési adatgyűjtés igazolásához önmagukban nem hivatkozhatnak ezekre a célokra, hanem azokat operatív célból további, olyan konkrétabb prioritásokkal kell alátámasztani, amelyekre vonatkozóan jelfelderítés végezhető. A 14086. sz. elnöki rendelet részletesen ismerteti azon prioritások jóváhagyási eljárását, amelyekre vonatkozóan jelfelderítés végezhető[129]. Az EDPB úgy értelmezi, hogy a jóváhagyott hírszerzési prioritások meghatározásának folyamata elviekben az Egyesült Államok Hírszerző Közösségének igazgatójára hárul, és elismeri, hogy annak főszabályként magában kell foglalnia a nemzeti hírszerzés igazgatója irodája polgári szabadságjogok védelmével foglalkozó tisztviselőjének (Civil Liberties Protection Officer – CLPO) értékelését is, amellyel az igazgatónak jogában áll egyet nem érteni, mely esetben „a nemzeti hírszerzési prioritási keret (National Intelligence Priorities Framework – NIPF) az elnöknek való bemutatásakor a CLPO értékelését és az igazgató véleményét is fel kell tüntetni"[130].

117. Az Európai Adatvédelmi Testület ugyanakkor azt is megjegyzi, hogy a „jóváhagyott hírszerzési prioritás" fogalommeghatározása értelmében „az Egyesült Államok jelfelderítési adatgyűjtési tevékenységei legnagyobb részének"[131] vonatkozásában ezek a prioritások az (előző bekezdésben ismertetett) elnöki rendelet 2. szakasza b) pontjának iii. alpontja szerint jóváhagyott prioritásokat jelölnek. A jóváhagyás bizonyos esetekben „szigorú feltételek mellett" eltérhet ettől a folyamattól, amely esetben az elnök vagy a Hírszerző Közösség valamely egységének vezetője is meghatározhat prioritást „a lehetőségekhez mérten" az ugyanazon 2. szakasz b) pontja iii. alpontja A. pontjának 1–3. pontjában meghatározott kritériumokkal összhangban, amelyek magukban foglalják a személyek adatvédelme és polgári szabadságjogai megfelelő figyelembevételének követelményét, de mindezt a CLPO bevonása nélkül.

118. A 14086. sz. elnöki rendelet hangsúlyozza továbbá, hogy „a jelfelderítési adatok gyűjtésének a lehető legcélzottabbnak kell lennie" annak érdekében, hogy előmozdítsa a jóváhagyott hírszerzési prioritást, és, hogy „a Hírszerző Közösségnek mérlegelnie kell más, kisebb beavatkozással járó források elérhetőségét, megvalósíthatóságát és megfelelőségét is", valamint általános szükségességi és arányossági követelményeket ír elő[132].

119. Az 5. szakasz h) pontja szerint továbbá a 14086. sz. elnöki rendelet lehetőséget ad arra, hogy a CLPO-hoz jogszerű panaszt lehessen benyújtani, valamint, hogy kérelmezni lehessen a CLPO határozatainak az adatvédelmi felülvizsgálati bíróság általi, az említett rendelet 3. szakaszában meghatározott jogorvoslati mechanizmussal összhangban történő felülvizsgálatát.

120. A FISA szövege az elrendelhető hírszerzési műveletek tekintetében egyértelműbbnek és pontosabbnak tűnik, mint a 12333. sz. elnöki rendelet. A FISA-t és a 12333. sz. elnöki rendeletet jelenleg a 14086. sz. elnöki rendeletet tekintetbe véve kell alkalmazni, különös tekintettel többek között a szükségesség és az arányosság elvére.

121. A 14086. sz. elnöki rendeletben rögzített követelmények további végrehajtását olyan ügynökségi szabályzatok és eljárások révén kell megvalósítani, amelyek a napi működésre vonatkozó konkrét rendelkezésekbe ültetik át őket. E tekintetben a 14086. sz. elnöki rendelet az egyesült államokbeli

[128] Lásd a 14086. sz. elnöki rendelet 2. szakasza b) pontja i. alpontjának B. pontját.
[129] Lásd a határozattervezet (129) preambulumbekezdését.
[130] Lásd a 14086. sz. elnöki rendelet 2. szakasza b) pontja iii. alpontjának B. pontját.
[131] Lásd a 14086. sz. elnöki rendelet 4. szakaszának n) pontját.
[132] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja i. alpontjának A és B. pontját.

hírszerző ügynökségek számára legfeljebb egy évet biztosít (azaz 2023. október 7-ig ad lehetőséget) meglévő szabályzataik és eljárásaik aktualizálására oly módon, hogy azok összhangba kerüljenek az elnöki rendeletben foglalt követelményekkel. Ezeket az aktualizált szabályzatokat és eljárásokat a legfőbb ügyésszel, a CLPO-val, valamint az Adatvédelmi és Polgári Szabadságjogi Felügyelő Tanáccsal (Privacy and Civil Liberties Oversight Board – PCLOB) konzultálva kell kidolgozni, és a lehető legnagyobb mértékben nyilvánosan hozzáférhetővé kell tenni[133].

122. Az EDPB üdvözölné, ha a határozat nemcsak hatálybalépésének, hanem elfogadásának is feltétele lenne többek között az, hogy az Egyesült Államok valamennyi hírszerző ügynöksége elfogadja a 14086. sz. elnöki rendelet végrehajtását célzó aktualizált szabályzatokat és eljárásokat. Az Európai Adatvédelmi Testület azt ajánlja a Bizottságnak, hogy értékelje ezeket az aktualizált szabályzatokat és eljárásokat, és az értékelést ossza meg az Európai Adatvédelmi Testülettel.

123. Végezetül, az eredetileg nemzetbiztonsági célokból gyűjtött, továbbított adatok megőrzésével kapcsolatban az EDPB megjegyzi, hogy a 14086. sz. elnöki rendelet biztosítja, hogy az egyesült államokbeli személyek személyes adataira alkalmazandó szabályok a nem egyesült államokbeli személyek személyes adataira is alkalmazandók legyenek[134]. A határozattervezetből úgy tűnik, hogy ezeket a szabályokat a 2015-ös költségvetési évre vonatkozó hírszerzési engedélyezési törvény 309. szakasza írja elő[135], amely főszabály szerint legfeljebb 5 éves megőrzési időszakot állapít meg a személy beleegyezése nélkül beszerzett nem nyilvános telefonos vagy elektronikus kommunikáció esetében. Az EDPB e tekintetben azt ajánlja, hogy a Bizottság tegye egyértelműbbé az egyesült államokbeli személyek személyes adataira alkalmazandó megőrzési szabályok értékelését a határozatban.

3.2.2 „B" garancia – Bizonyítani kell a szükségességet és az arányosságot a követett jogszerű célra tekintettel

3.2.2.1 Az új 14086. sz. elnöki rendelet által biztosított horizontális biztosítékok – szükségesség és arányosság

124. Az új 14086. sz. elnöki rendelet, amely általánosságban véve a PPD-28 helyébe lép, célja, hogy olyan szabályokat állapítson meg az Egyesült Államok jelfelderítési tevékenységeire vonatkozó biztosítékok megerősítésére, amelyeket a Hírszerző Közösség egységei a továbbiakban a belső szabályzataikban és eljárásaikban végrehajtanak.

125. A 14086. sz. elnöki rendelet két olyan új követelményt vezet be az Egyesült Államok jogában, amelyek tükrözik az EUB Schrems II. ügyben hozott ítéletben felidézett követelményeket, nevezetesen azt, hogy jelfelderítési tevékenységeket csak a jóváhagyott hírszerzési prioritásnak minősül adatgyűjtéshez szükséges mértékben, valamint csak a jóváhagyott hírszerzési prioritással arányos mértékben és módon lehet végezni[136].

126. Az EDPB értelmezése szerint ezek az elemek azért kerültek beépítésre, hogy tükrözzék a szükségesség és az arányossági az uniós jogban, valamint az EUB és az EJEB ítélkezési gyakorlatában előírt elveit, amelyeknek célja annak biztosítása, hogy az adatgyűjtés és -kezelés a szükséges és arányos mértékre korlátozódjon.

[133] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja iv. alpontjának B és C. pontját.
[134] A határozattervezet (150) preambulumbekezdése.
[135] A határozattervezet 272. lábjegyzete.
[136] Lásd a 14086. sz. elnöki rendelet 2. szakasza a) pontja ii. alpontjának A. és B. pontját.

127. E tekintetben az EDPB emlékeztet a hírszerzési prioritások jóváhagyására irányuló folyamatra, valamint az esetleges eltérésre (lásd a 116. és a 117. bekezdést).

128. Az EDPB megjegyzi továbbá, hogy a szükségesség és arányosság az elnöki rendelet által előírt elvét egy éven belül működőképessé kell tenni és végre kell hajtani a Hírszerző Közösség egyes egységei szabályzataiban és eljárásaiban[137].

3.2.2.2 A jelfelderítési adatok gyűjtésére vonatkozó különleges biztosítékok

129. Az EDPB megjegyzi továbbá, hogy a 14086 sz. elnöki rendelet korlátozásokat ír elő azon célokat illetően, amelyekre vonatkozóan a személyes adatok gyűjtése engedélyezett, illetve nem engedélyezett a jelfelderítési adatok gyűjtésével összefüggésben[138].

130. Az EDPB üdvözli, hogy az elnöki rendelet rendelkezései értelmében a célzott gyűjtést előnyben kell részesíteni a tömeges gyűjtéssel szemben[139]. A jelfelderítési adatgyűjtéssel összefüggésben az elnöki rendelet egy 12 olyan célkitűzésből álló listát rögzít, amelyekre vonatkozóan lehet adatokat gyűjteni – és amelyeket hírszerzési prioritásokra kell váltani (lásd a 117. bekezdést) –, valamint egy 5 olyan célkitűzést tartalmazó listát, amelyek tekintetében jelfelderítési adatgyűjtési tevékenységek nem végezhetők[140]. Ezek a rendelkezések elvben garanciát jelentenek az adatgyűjtés szükségességének biztosítására.

131. Az EDPB azonban emlékeztet arra, hogy a 14086. sz. elnöki rendelet szintén lehetőséget biztosít az Egyesült Államok elnökének arra, hogy a listát további célkitűzésekkel egészítse ki (lásd a 114. és a 115. bekezdést)[141].

3.2.2.3 A tömeges gyűjtésre vonatkozó különleges biztosítékok

132. Az EUB a Schrems I. ügyben hozott ítéletében hangsúlyozta, hogy „*a magánélet tiszteletben tartásához való alapvető jog védelme uniós szinten megköveteli, hogy a személyes adatok védelme alóli kivételek és e védelem korlátozásai a feltétlenül szükséges határokon belül maradjanak*”[142], és kimondta, hogy az „*olyan szabályozást, amely lehetővé teszi a hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, úgy kell tekinteni, hogy az a magánélet tiszteletben tartásához való, az Európai Unió Alapjogi Chartája 7. cikkében biztosított alapvető jog lényegét sérti*”.

133. A Schrems II. ügyben[143] a tömeges adatgyűjtés a 12333. sz. elnöki rendelet és a PPD-28 korrelatív értelmezésével kapcsolatos elemzését, és különösen annak 183–185. pontját illetően a Bíróság a fentiek szerint hangsúlyozta, hogy a tömeges adatgyűjtés lehetősége, „*amely az EO 12333-on alapuló megfigyelési programok keretében megengedi az Egyesült Államokba továbbított adatokhoz való hozzáférést anélkül, hogy e hozzáférés bármiféle bírósági felügyelet alá tartozna, semmi esetre sem szabályozza kellőképpen egyértelműen és pontosan a személyes adatok ilyen tömeges gyűjtésének terjedelmét*”.

[137] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja iv. alpontjának B. pontját.
[138] Lásd a 14086. sz. elnöki rendelet 2. szakasza b) pontja i. alpontja A. pontjának 1–12. pontját.
[139] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja ii. alpontjának A. pontját.
[140] Lásd a 14086. sz. elnöki rendelet 2. szakasza b) pontja ii. alpontja A. pontjának 1–5. pontját.
[141] Lásd a 14086. sz. elnöki rendelet 2. szakasza b) pontja i. alpontjának B. pontját.
[142] A Bíróság Schrems I. ügyben hozott ítélete, 92. pont.
[143] Lásd a Bíróság Schrems II. ügyben hozott ítéletét.

134. Az EDPB ezért megjegyzi, hogy az EUB alapelvként nem zárta ki a tömeges gyűjtést, de a Schrems II. határozatában úgy ítélte meg, hogy ahhoz, hogy az ilyen tömeges gyűjtésre jogszerűen kerüljön sor, kellően egyértelmű és pontos korlátokat kell megállapítani az ilyen tömeges gyűjtés hatályának körülhatárolásához.

135. Az EDPB azt is elismeri, hogy a PPD-28 felváltása mellett a 14086. sz. elnöki rendelet új biztosítékokat és korlátozásokat rögzít az Egyesült Államokon kívül gyűjtött adatok gyűjtésére és felhasználására vonatkozóan, mivel a FISA vagy más konkrétabb egyesült államokbeli jogszabályok korlátozásai nem alkalmazandók.

136. A tömeges adatgyűjtést illetően az EDPB tudomásul veszi, hogy a 14086. sz. elnöki rendelet rögzíti, miszerint a tömeges adatgyűjtés továbbra is megengedett. Az EDPB hangsúlyozza, hogy a tömeges gyűjtés fogalommeghatározása ugyanaz maradt, mint az előző PPD-28-ban: *„jelfelderítési adatok tömeges gyűjtése": nagy mennyiségű jelfelderítési adat engedélyezett gyűjtése, amely műszaki vagy operatív megfontolások miatt diszkriminánsok (pl. konkrét azonosítók, kiválasztási feltételek stb.) használata nélkül történik*[144]*".*

137. A Schrems II. ügyben hozott ítélete óta a Bíróság nem részletezte pontosan a tömeges adatgyűjtéshez szükséges biztosítékokat. Az EDPB azonban emlékeztet arra, hogy az EJEB fontos határozatokat hozott a tömeges adatgyűjtésről és ezzel összefüggésben a vonatkozó biztosítékokról.

138. Az Európai Adatvédelmi Testület emlékeztet arra, hogy a tömeges adatgyűjtés azáltal, hogy nagy mennyiségű adat diszkriminánsok nélküli gyűjtését teszi lehetővé, nagyobb kockázatot jelent a természetes személyek számára[145], mint a célzott gyűjtés, és ezért további biztosítékok nyújtását teszi szükségessé.

139. Az EDPB azt is megjegyzi, hogy az EUB a forgalmi és helymeghatározó adatok megőrzésével, valamint a távközlési szolgáltatók által megőrzött adatokhoz való későbbi hozzáféréssel – beleértve nemzetbiztonsági célból való hozzáférést is – kapcsolatos további ítélkezési gyakorlatot is kialakított, ami, bár ebben az összefüggésben nem tekinthető közvetlenül alkalmazandónak, bizonyos mértékben releváns lehet a tömeges adatgyűjtés a 12333. sz. elnöki rendelet keretében történő jelenlegi értékelése szempontjából.

1) <u>Célhoz kötöttség</u>

140. Az elnöki rendelet úgy rendelkezik, hogy a tömeges adatgyűjtésre csak annak megállapítását követően kerülhet sor, hogy *„a jóváhagyott hírszerzési prioritás előmozdításához szükséges információk célzott gyűjtéssel észszerű módon nem szerezhetők meg"*[146], valamint, hogy *„a Hírszerző Közösség adott egységének észszerű módszereket és technikai intézkedéseket kell alkalmaznia annak érdekében, hogy az összegyűjtött adatokat a jóváhagyott hírszerzési prioritás előmozdításához szükséges mértékre korlátozza, ugyanakkor minimalizálja a nem releváns információk gyűjtését"*[147]. E biztosítékok mellett az EDPB azt is elismeri, hogy a tömegesen gyűjtött adatokat a felsorolt hat célkitűzés közül egynek vagy

[144] Lásd a 14086. sz. elnöki rendelet 4. szakasza b) pontját.

[145] Lásd például: az EJEB (nagytanács) 2021. május 25-i ítélete, Big Brother Watch és társai kontra Egyesült Királyság (a továbbiakban: az EJEB Big Brother Watch ügyben hozott ítélete), (363) preambulumbekezdés, amelyben a Bíróság megállapítja, hogy *„nincs meggyőződve arról, hogy a kapcsolódó kommunikációs adatok tömeges lehallgatás útján történő megszerzése szükségszerűen kevésbé beavatkozó jellegű, mint a tartalom megszerzése*".

[146] A 14086. sz. elnöki rendelet 2. szakasza c) pontja ii. alpontjának A. pontja.

[147] A 14086. sz. elnöki rendelet 2. szakasza c) pontja ii. alpontjának A. pontja.

többnek az elérésére kell felhasználni[148]. Az EDPB hangsúlyozza továbbá, hogy bár ezek a célkitűzések részletesebbek, mint az előző PPD-28-ban meghatározottak, amelynek a helyébe általánosságban véve a 14086. sz. elnöki rendelet lépett, az ilyen adatgyűjtési lehetőségek nagyságrendje továbbra is potenciálisan széles körű maradt, azaz nagy mennyiségű adatot foglal magában.

141. Az EDPB ismételten emlékeztet arra, hogy a 14086. sz. elnöki rendelet szintén lehetőséget biztosít az Egyesült Államok elnökének arra, hogy a listát további célkitűzésekkel egészítse ki (lásd a 115. bekezdést)[149].

2) Előzetes független engedélyezés

142. Az EDPB hangsúlyozza, hogy az EJEB a nemzetbiztonsági célú tömeges adatgyűjtéssel összefüggésben nagy jelentőséget tulajdonít az előzetes független engedélyezésnek. A Bíróság ugyanis kifejezetten kimondta, hogy „*a tömeges lehallgatási hatáskörrel való visszaélés kockázatának minimalizálása érdekében a Bíróság úgy véli, hogy az eljárást »végponttól végpontig terjedő« biztosítékokkal kell óvni, ami azt jelenti, hogy nemzeti szinten a folyamat minden szakaszában értékelni kell a meghozott intézkedések szükségességét és arányosságát; a tömeges lehallgatást már kezdettől fogva, a művelet tárgyának és hatókörének meghatározásakor független engedélyhez kell kötni; valamint hogy a műveletet ellenőrzésnek és független utólagos felülvizsgálatnak kell alávetni. A Bíróság véleménye szerint ezek olyan alapvető biztosítékok, amelyek a 8. cikknek megfelelő tömeges lehallgatási rendszer sarokkövét képezik*”[150].

143. Az EDPB megjegyzi továbbá a nagytanácsban hozott ítélet következő pontját, amelyben a strasbourgi bíróság azt is kiemeli, hogy „*egyetért a nagytanáccsal abban, hogy bár a bírósági engedély »fontos biztosíték az önkényességgel szemben«, nem »szükséges követelmény« (lásd a nagytanács ítéletének 318–320. pontját). Mindazonáltal a tömeges lehallgatást független szervnek kell engedélyeznie; azaz egy olyan szervnek, amely független a végrehajtó hatalomtól*“[151].

144. Ebben az összefüggésben az EDPB megjegyzi, hogy az elnöki rendelet nem ír elő ilyen független előzetes engedélyt a tömeges gyűjtésre vonatkozóan, valamint, hogy ezt a 12333. sz. elnöki rendelet sem irányozza elő (lásd a 12333. sz. elnöki rendeletről szóló szakaszt).

3) A megőrzésre vonatkozó szabályok

145. Az Európai Adatvédelmi Testület emlékeztet arra, hogy a biztosítékok egy másik fontos készletét az adatgyűjtés és -megőrzés időtartamára vonatkozó szabályok alkotják. E tekintetben az EJEB hangsúlyozta, hogy „*a nemzeti jognak korlátoznia kell a lehallgatás időtartamát, a megszerzett adatok vizsgálata, felhasználása és tárolása során követendő eljárást, az adatok más felekkel való közlése során alkalmazandó óvintézkedéseket, valamint azokat a körülményeket, amelyek között a lehallgatott adatokat törölhetik vagy megsemmisíthetik, illetve azokat törölni kell vagy meg kell semmisíteni*[152]”, mivel ezek a biztosítékok „*ugyanolyan fontosak a tömeges lehallgatás szempontjából*”[153].

146. E vonatkozásban az Európai Adatvédelmi Testület értelmezése szerint az elnöki rendelet szabályokat ír elő a jelfelderítés útján gyűjtött személyes adatok megőrzésére vonatkozóan, beleértve a tömegesen

[148] A 14086. sz. elnöki rendelet 2. szakasza c) pontja ii. alpontjának B. pontja.
[149] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja ii. alpontjának C. pontját.
[150] Lásd az EJEB Big Brother Watch ügyben hozott ítéletének 350. pontját.
[151] Lásd az EJEB Big Brother Watch ügyben hozott ítéletének 351. pontját.
[152] Lásd az EJEB Big Brother Watch ügyben hozott ítéletének 348. pontját.
[153] Lásd az EJEB Big Brother Watch ügyben hozott ítéletének 348. pontját.

gyűjtött adatokat is[154]. Az EDPB megjegyzi, hogy a 14086. sz. elnöki rendelet 2. szakasza c) pontja iii. alpontjának A. pontja szerint a Hírszerző Közösség minden egyes, a jelfelderítés útján gyűjtött személyes információkat kezelő egységének olyan szabályzatokat és eljárásokat kell kidolgoznia és alkalmaznia, amelyeknek célja a jelfelderítés útján gyűjtött személyes információk terjesztésének és megőrzésének minimalizálása. Ezek a szabályok azonban nem írnak elő konkrét megőrzési időszakot, hanem általában ugyanazokra az alkalmazandó szabályokra hivatkoznak az egyesült államokbeli személyekre vonatkozó adatok megőrzése, valamint azon helyzetek tekintetében, amelyekben nem került sor a megőrzés végleges megállapítására. Az Európai Adatvédelmi Testület ezért aggodalmát fejezi ki amiatt, hogy a célzott adatgyűjtés tekintetében a jelen elnöki rendelet nem határozza meg egyértelműen ezeket az adatmegőrzési időszakokat (lásd: 122. bekezdés) a tömegesen gyűjtött adatok vonatkozásában. Felkéri a Bizottságot, hogy ossza meg az egyesült államokbeli személyekre alkalmazandó megőrzési időszakok szükségességére és arányosságára vonatkozó értékelését, valamint a megőrzési időszakokra vonatkozóan a gyakorlatban rendelkezésre álló információkat, azokban az esetekben, amikor az Egyesült Államok jogának értelmében nem születik végleges, a megőrzésre vonatkozó döntés, mivel a határozattervezet jelenlegi állapotában csupán egyetlen rövid bekezdésben[155] és egy lábjegyzetben[156] emlékeztet erre az általános szabályra, ami nem teszi lehetővé annak megállapítását, hogy ezek a megőrzési időszakok szükségesek és arányosak-e. Mivel – amint azt az EJEB is hangsúlyozta – ez alapvető biztosíték ahhoz, hogy az érintettek gyakorolhassák jogaikat egy olyan helyzetben, amikor az adataik gyűjtése érdekében különösen beavatkozó jellegű intézkedést hoznak, az Európai Adatvédelmi Testület felkéri az Európai Bizottságot, hogy adjon további felvilágosítást a gyakorlatban alkalmazott különböző megőrzési időszakokról.

4) A „terjesztésre" vonatkozó biztosítékok

147. Az EDPB emlékeztet továbbá arra, hogy a szükségesség és az arányosság , valamint a célhoz kötöttség elve hatékonyságának biztosítása érdekében az EJEB elismerte az összegyűjtött adatok további terjesztésére vonatkozó, a jogban előírt szabályok fontosságát többek között a tömeges gyűjtéssel összefüggésben is[157].

148. A 14086 sz. elnöki rendelet 2. szakasza c) pontja iii. alpontja A. pontja 1. pontjának c) pontja úgy rendelkezik, hogy a jelfelderítési tevékenységek során gyűjtött, nem egyesült államokbeli személyekre vonatkozó információk csak akkor terjeszthetők, ha egy felhatalmazott és megfelelően képzett személy megalapozottan feltételezi, hogy a személyes adatok megfelelő védelemben részesülnek, valamint, hogy a címzettnek ismernie kell az információt.

149. Ezt figyelembe véve az EDPB úgy értelmezi, hogy a 14086. sz. elnöki rendelet szerinti terjesztésre vonatkozó rendelkezések nem írják elő a nemzetbiztonsági célokon kívüli célból történő terjesztés kifejezett tilalmát sem az Egyesült Államok illetékes hatóságai részére történő terjesztés esetében[158]. Az Európai Adatvédelmi Testület felkéri a Bizottságot, hogy pontosítsa az ebben az esetben alkalmazandó szabályokat és biztosítékokat.

150. Az Európai Adatvédelmi Testület ezért aggodalmát fejezi ki amiatt, hogy a Hírszerző Közösség illetékes hatóságai által megszerzett adatokat ezt követően továbbítani lehet az Egyesült Államok illetékes

[154] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja iii. alpontja A. pontja 2. pontjának (a)–(c) pontját.
[155] Lásd a határozattervezet (150) preambulumbekezdését.
[156] Lásd a határozattervezet 271. lábjegyzetét.
[157] Lásd az EJEB Big Brother Watch ügyben hozott ítéletének 348. pontját.
[158] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja iii. alpontja A. pontjának 1. pontját.

hatóságainak a bűnözés elleni küzdelem – ideértve a súlyos bűncselekmények elleni küzdelmet is – céljából a bűnügyi nyomozások keretében, ezáltal további konkrét korlátozások nélkül lehetőséget biztosítva a bűnüldöző hatóságoknak arra, hogy olyan adatokat szerezzenek be, amelyek közvetlen gyűjtése számukra egyébként tiltott lett volna, és felkéri a Bizottságot, hogy vizsgálja meg ezt a pontot.

151. Az újbóli adattovábbítás konkrét összefüggésében (az Egyesült Államok kormányán kívüli címzettek, többek között külföldi kormány vagy nemzetközi szervezet részére[159] történő terjesztés vonatkozásában) az Európai Adatvédelmi Testület emlékeztet arra, hogy véleménye szerint az adatok számára biztosított védelmet az újbóli adattovábbítással összefüggésben is fenn kell tartani, többek között a nemzetbiztonság területén is[160].

152. E tekintetben az elnöki rendelet előír bizonyos biztosítékokat, nevezetesen azt a követelményt, hogy az adatok terjesztése előtt kellően figyelembe kell venni a terjesztés célját – habár azt nem írja elő kifejezetten, hogy a terjesztés célja a nemzetbiztonság védelme is kell, hogy legyen –, a terjesztett személyes információk jellegét és mértékét, valamint az érintett személyre vagy személyekre gyakorolt lehetséges káros hatást.

153. Bár az EDPB elismeri, hogy e biztosítékok némelyike – különösen az érintett(ek)re gyakorolt „*esetleges káros hatás*"[161] figyelembevétele – tükrözi az EJEB bizonyos követelményeit, azt is hangsúlyozza, hogy a strasbourgi bíróság szintén előírja, miszerint jogilag kötelező erejű kötelezettséget kell előírni „*annak elemzésére és meghatározására, hogy a hírszerzési információ külföldi címzettje elfogadható minimális szintű biztosítékokat nyújt-e*"[162], amit az Európai Adatvédelmi Testület nem tudott kifejezetten azonosítani az elnöki rendelet külföldi címzettek részére történő terjesztésre vonatkozó rendelkezéseiben. Az EDPB ezért felkéri a Bizottságot, hogy folytassa ezen elem értékelését.

154. Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy az Európai Bizottság a megfelelőség értékelésének részeként nem vette figyelembe a harmadik országokkal vagy nemzetközi szervezetekkel kötött olyan meglévő nemzetközi megállapodásokat, amelyek konkrét rendelkezéseket írhatnak elő a személyes adatok hírszerző szolgálatok által harmadik országokba történő nemzetközi továbbítására vonatkozóan. Az EDPB úgy véli, hogy a hírszerzési együttműködés céljából harmadik országokkal kötött két- vagy többoldalú megállapodások valószínűleg hatással lesznek az értékelt adatvédelmi jogi keretre.

155. Az Európai Adatvédelmi Testület ezért felkéri az Európai Bizottságot annak tisztázására, hogy léteznek-e ilyen megállapodások, illetve, hogy milyen feltételek mellett köthetők meg, valamint annak értékelésére, hogy a nemzetközi megállapodások rendelkezései hatással lehetnek-e az EGT-ből továbbított személyes adatok a nemzetbiztonsági célú adattovábbítással kapcsolatos jogszabályi keret és gyakorlatok által biztosított védelmi szintjére.

5) <u>Ideiglenes tömeges gyűjtés a célzott gyűjtés kezdeti technikai szakaszának támogatására</u>

156. Az Európai Adatvédelmi Testület emlékeztet arra, hogy az adatvédelmi pajzs legutóbbi közös felülvizsgálatával összefüggésben zajlott megbeszélések főként a tömeges adatgyűjtés azon további jogalapjainak (helyzeteinek/forgatókönyveinek) alkalmazására és értelmezésére összpontosítottak,

[159] Lásd különösen a 14086. sz. elnöki rendelet 2. szakasza c) pontja iii. alpontja A. pontja 1. pontjának (d) pontját.
[160] Lásd például az EDPB 14/2021. sz. véleményét a személyes adatoknak az Egyesült Királyságban történő megfelelő védelméről szóló, az (EU) 2016/679 rendelet szerinti európai bizottsági végrehajtási határozat tervezetéről. Elfogadás időpontja: 2021. április 13., 4.3.2.1. és 4.3.2.2. szakasz.
[161] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja iii. alpontja A. pontja 1. pontjának d) pontját.
[162] Lásd: az EJEB (nagytanács) 2021. május 25-i ítélete, Centrum För Rättvisa kontra Svédország, 326. pont.

amelyet a PPD-28 2. szakasza 5. lábjegyzetének első mondata ír elő, miszerint „*az e szakaszban foglalt korlátozások nem vonatkoznak az olyan jelfelderítési adatokra, amelyeket a célzott gyűjtés megkönnyítése érdekében ideiglenesen szereztek meg*". Az Egyesült Államok hatóságai akkoriban kifejtették, hogy mit jelentenek „*a célzott gyűjtés megkönnyítése érdekében ideiglenesen megszerzett jelfelderítési adatok*". Az EDPB e megbeszélésekből azt a következtetést vonta le, hogy a lábjegyzet jelentése értelmében az adatok gyűjtése tömegesen – és a kijelölt hat céltól függetlenül – is történhet, amennyiben a gyűjtésre ideiglenesen, egy meghatározott célpont azonosítójának megállapítása céljából kerül sor. Ez tehát további jogalapot jelentene a tömeges adatgyűjtéshez, mely esetben már csak a PPD-28 1. szakaszának általános elvei kerülnének alkalmazásra. A fent említetteknek megfelelően a Schrems II. ügyben hozott ítéletben az EUB úgy vélte, hogy a tömeges adatgyűjtés tekintetében a 12333. sz. elnöki rendelet és a PPD-28 együttesen nem szabályozzák „*kellőképpen egyértelműen és pontosan a személyes adatok ilyen tömeges gyűjtésének terjedelmét*"[163].

157. Az EDPB megjegyzi, hogy a 14086. sz. elnöki rendelet továbbra is lehetőséget ad egy, az ilyen tömeges gyűjtést lehetővé tevő eltérésre[164]; az Európai Adatvédelmi Testület ugyanakkor üdvözli, hogy ez az eltérés korlátozottabbá vált a PPD-28-hoz képest, és a 14086. sz. elnöki rendelet keretében további biztosítékok is bevezetésre kerültek.

158. Az EDPB úgy értelmezi, hogy az új 14086. sz. elnöki rendelet olyan biztosítékokat ír elő, amelyek továbbra is alkalmazandók az ilyen típusú ideiglenes technikai tömeges adatgyűjtésre, különös tekintettel a szükségesség és az arányosság általános elveire a jóváhagyott hírszerzési prioritással kapcsolatban, amennyiben az adatokat diszkriminánsok nélkül kerülnek megszerzésre a célzott adatgyűjtést megelőzően (14086. sz. elnöki rendelet, 2. szakasz a)–b) pont, 2. szakasz c) pont i. alpont). Az EDPB egyúttal úgy is értelmezi, hogy a későbbi célzott jelfelderítési adatgyűjtést támogató tömeges adatgyűjtésre a (2) bekezdés c) pontjának iii. alpontjától kezdődően megfogalmazott további biztosítékok is vonatkoznak[165].

159. Az EDPB azonban arra is emlékeztet – lásd a fenti 117. pontot –, hogy a „*jóváhagyott hírszerzési prioritás*" meghatározása egy olyan, a szokásostól eltérő eljárást biztosít, amely nem foglalja magában a nemzeti hírszerzési igazgató hivatalának polgári szabadságjogok védelmével foglalkozó tisztviselőjét.

160. Az EDPB azonban továbbra is megjegyzi, hogy a tömeges gyűjtésre vonatkozó alszakaszban foglalt biztosítékok nem alkalmazandók a 14086. sz. elnöki rendelet 2. szakasza c) pontjának ii. alpontjának D. pontjában vázolt, a célzott jelfelderítési tevékenység kezdeti technikai szakaszának támogatására használt ideiglenes tömeges adatgyűjtésre, ami pedig azt jelenti, hogy ebben az összefüggésben a tömegesen gyűjtött adatok a 2. alszakasz c) pontjának ii. alpontjában felsoroltaktól eltérő célokra is felhasználhatók. Az EDPB üdvözölné a határozattervezet pontosítását az ebben az összefüggésben tömegesen gyűjtött adatok lehetséges felhasználási céljait, valamint a (2) bekezdés c) pontjának i. alpontjában meghatározott korlátozásoknak általánosságban a jelfelderítési adatgyűjtésre (azaz csak az ott felsorolt jogszerű célokra) vonatkozó, a határozattervezetben szereplő, ideiglenes tömeges adatgyűjtéssel összefüggésben történő alkalmazását illetően.

161. Végezetül az Európai Adatvédelmi Testület azt is hangsúlyozza, hogy ez az ideiglenes, tömeges adatgyűjtésre vonatkozó eltérés a célzott gyűjtés és a fennmaradó alkalmazandó biztosítékok tekintetében továbbra sem egyértelmű, különösen annak vonatkozásában, hogy a 14086. sz. elnöki

[163] A Bíróság Schrems II. ügyben hozott ítélete, 183. pont.

[164] Lásd a 14086. sz. elnöki rendelet 2. szakasza c) pontja ii. alpontjának D. pontját és a határozattervezet 226. lábjegyzetét.

[165] Az e rendelkezésekkel kapcsolatos további elemeket lásd az előző szakaszokban.

rendelet mely biztosítékai alkalmazandók az adott szakaszokra (tömeges adatgyűjtés, további célzott gyűjtés), és felkéri a Bizottságot, hogy értékelje tovább ezeket elemeket, valamint értékelje ezeket a szempontokat a gyakorlatban is a jövőbeli közös felülvizsgálatok során.

162. Bár az EDPB továbbá sajnálatát fejezi ki amiatt, hogy még ha az „átmeneti" fogalma az elnöki rendeletben valamivel részletesebb is, mint a PPD-28-ban, az Európai Adatvédelmi Testület értelmezése szerint továbbra is azt jelenti, hogy mindaddig, amíg a célpontot nem azonosították, a tömeges gyűjtés folytatódhat. E tekintetben az EDPB emlékeztet arra, hogy egyértelmű és pontos szabályokra van szükség, és ismét hangsúlyozza azt a kulcsfontosságú biztosítékot, amelyet ezek a szabályok jelentenek az érintettek számára.

163. Következésképpen a tömeges adatgyűjtésre alkalmazandó biztosítékokat illetően az EDPB továbbra is aggályát fejezi ki amiatt, hogy a 14086. sz. elnöki rendelet keretében nyújtott további biztosítékok ellenére még mindig lehetőség nyílik a tömeges, azaz diszkriminánsokat nélkülöző és olyan kulcsfontosságú biztosítékok nélkül adatgyűjtésre, mint az ilyen adatok gyűjtésének előzetes engedélyezése – többek között ideértve az ideiglenes technikai tömeges adatgyűjtés eltérő esetét is – , egyúttal figyelembe véve a további pontosítások szükségességét és az adatokhoz való későbbi hozzáférés szigorú célhoz kötöttségére, az egyértelmű és szigorú adatmegőrzési szabályokra, valamint a tömegesen gyűjtött adatok terjesztésére vonatkozó szigorúbb biztosítékokra vonatkozóan kifejezett aggályokat, többek között az újbóli adattovábbítással összefüggésben is.

164. Az EDPB általánosságban kiemeli, hogy az EJEB fent említett határozata ismét rámutat a független felügyeleti hatóságok átfogó felügyeletének fontosságára. Az EDPB hangsúlyozza, hogy a független felügyelet a nemzetbiztonsági célú kormányzati hozzáférési folyamat valamennyi szintjén fontos biztosíték az önkényes megfigyelési intézkedésekkel szemben, és ennélfogva az adatvédelem megfelelő szintjének értékeléséhez is. A felügyeleti hatóságok Charta 8. cikkének (3) bekezdésében előírt függetlenségére vonatkozó garancia célja, hogy biztosítsa a személyes adatok kezelése tekintetében a természetes személyek védelmére vonatkozó szabályok betartásának hatékony és megbízható ellenőrzését. Ez különösen azokra az esetekre vonatkozik, amikor a megfigyelés titkos jellegéből adódóan az egyénnek nincs lehetősége arra, hogy a megfigyelési intézkedés végrehajtása előtt vagy közben jogorvoslatot keressen, vagy bármilyen jogorvoslati eljárásban közvetlenül vegyen részt.

165. Az EDPB emlékeztet arra, hogy véleménye szerint a megfelelőség értékeléséhez az adott eset valamennyi körülményét figyelembe kell venni, különös tekintettel az utólagos felügyelet és a jogi keretben előírt jogorvoslat hatékonyságára.

3.2.2.4 Az Egyesült Államok területén belüli és kívüli hírszerző közösségi szervezeti egységek nemzetbiztonsági célú gyűjtésének jogi kerete

166. A Schrems II. ügyben hozott ítéletében az EUB a FISA 702. szakaszával kapcsolatban hangsúlyozta, hogy a szövegből „*semmilyen módon nem következik az abban foglalt, a megfigyelési programok külföldi hírszerzés céljából történő végrehajtására vonatkozó felhatalmazás korlátozásának létezése, sem pedig az e programok által esetlegesen érintett, nem amerikai személyek számára szóló garanciák fennállása*"[166]. Ennek alapján a Bíróság úgy ítélte meg, hogy „*e körülmények között […] e cikk nem alkalmas arra, hogy a Charta által biztosított […] védelmi szinttel lényegében azonos védelmi szintet biztosítson, […] amely szerint az alapvető jogokba való beavatkozást lehetővé tevő jogalapnak az*

[166] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 180. pontját.

arányosság elvének való megfelelés érdekében magának kell meghatároznia az érintett jog gyakorlása korlátozásának terjedelmét, és egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása tekintetében, valamint minimumkövetelményeket kell előírnia"[167].

167. A 12333. sz. elnöki rendelet kapcsán a bíróság megjegyezte, hogy „*e rendelet sem biztosít az amerikai hatóságokkal szemben a bíróságok előtt érvényesíthető jogokat*"[168], és, miután a PPD-28-cal összefüggésben elemezte azokat a feltételeket, amelyek mellett a rendelet értelmében a tömeges adatgyűjtésre sor kerülhet. arra a következtetésre is jutott, hogy a lehetőség, „*amely a 12333. sz. elnöki rendeleten alapuló megfigyelési programok keretében megengedi az Egyesült Államokba továbbított adatokhoz való hozzáférést anélkül, hogy e hozzáférés bármiféle bírósági felügyelet alá tartozna, semmi esetre sem szabályozza kellőképpen egyértelműen és pontosan a személyes adatok ilyen tömeges gyűjtésének terjedelmét*"[169].

168. E konkrét adatgyűjtési rendszerek tekintetében a 14086. sz. elnöki rendelet új szabályokat ír elő.

3.2.2.4.1 A 702. szakasz szerinti nemzetbiztonsági célú adatgyűjtés

169. Az EDPB emlékeztet arra, hogy a PCLOB legutóbbi jelentésében üdvözölte a FISA 702. szakaszára[170] vonatkozó megállapításokat, miszerint „*a gyakorlatban a »nem egyesült államokbeli személyek« is részesülnek a különböző ügynökségek minimalizációs és/vagy célzási eljárásai által előírt hozzáférési és megőrzési korlátozások előnyeiből, mivel az egyesült államokbeli személyekre vonatkozó információk nagy adathalmaz vonatkozásában történő azonosításának és eltávolításának költsége és bonyolultsága azt eredményezi, hogy jellemzően a teljes adatkészletet a magasabb szintű egyesült államokbeli adatszabványoknak megfelelően kezelik*".

170. E megállapítások szerint „a program nem tömegesen gyűjtött kommunikációs adatok útján működik". A nemzeti hírszerzés igazgatójának irodája által kiadott 2014. és 2021. évi statisztikai átláthatósági jelentések megerősítették ezt a megállapítást. Emellett a PCLOB jelentése szerint a megfigyelés célzására „kiválasztási kritériumokat", például e-mail-címet vagy telefonszámot használnak.

171. Az EDPB azonban arra is emlékeztet, hogy a 702. szakasz összefüggésében az adatvédelmi pajzs legutóbbi felülvizsgálata során egyértelművé vált, hogy a célpontként azonosított „személy" több olyan személyt is jelölhet, akik ugyanazt az azonosítót használják, feltéve, hogy ezek a személyek nem egyesült államokbeli személyek, és a célzáshoz alkalmazandó kritériumok teljesülnek az esetükben. Az EDPB emlékeztet továbbá arra is, hogy az adatvédelmi pajzs 2019. évi harmadik éves közös felülvizsgálata során az UPSTREAM programmal összefüggésben további pontosításra szólítottak fel annak kizárására, hogy a nem egyesült államokbeli személyek személyes adataihoz tömeges szintű, különbségtétel nélküli hozzáférésre kerülhessen sor[171].

172. Emellett az EDPB emlékeztet arra, hogy az a tény, hogy a FISA 702. szakasza szerinti adatgyűjtést az támasztja alá, miszerint „az adatszerzés jelentős célja külföldi hírszerzési információk megszerzése", továbbra is hagy némi bizonytalanságot maga után a célhoz kötöttség és szükségessége tekintetében. Ugyanakkor az Európai Adatvédelmi Testület azt is megjegyzi, hogy a 14086. sz. elnöki rendelet 2. szakasza a) pontjának A. és B. pontja szerint a jelfelderítési tevékenységeket csak annak megállapítását követően lehet folytatni, hogy a tevékenységek egy jóváhagyott prioritás

[167] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 180. pontját.
[168] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 182. pontját.
[169] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 183. pontját.
[170] Lásd a PCLOB jelentését a FISA 702. szakasza alapján működtetett megfigyelési programról, 100. o.
[171] Lásd a harmadik közös felülvizsgálati jelentés 17. oldalának 83. pontját.

előmozdításához szükségesek, és kizárólag az adott prioritással arányos mértékben és módon, valamint, hogy a tevékenységet a lehető legnagyobb mértékben a jóváhagyott prioritás előbbre viteléhez kell igazítani, kellően figyelembe véve az olyan releváns tényezőket, mint az adatgyűjtés beavatkozó jellege, az adatok érzékenysége, és az, hogy nem befolyásolja aránytalanul a magánéletet és a polgári szabadságjogokat. Az Európai Adatvédelmi Testület azonban további pontosításokat vár arra vonatkozóan, hogy ezek az előírások konkrétan hogyan kerülnek végrehajtásra és működtetésre többek között a FISA 702. szakasza tekintetében.

173. E tekintetben, az információkhoz való közvetlen hozzáférés hiányában, az EDPB független értékelést kért a „célszemélyek" és a „külföldi hírszerzés" a FISA 702. szakasza szerinti definíciója, illetve fogalma szükségességéről és arányosságáról (többek között az UPSTREAM programmal összefüggésben) annak megújítását követően. Az Európai Adatvédelmi Testület úgy véli, hogy a kiválasztási kritériumok bizonyos esetekben való alkalmazási folyamatának (a továbbiakban: a kiválasztási kritériumok meghatározása) további független értékelésére irányuló korábbi felhívása, valamint a további pontosításra irányuló kérése.az UPSTREAM programmal összefüggésben relevánsnak tekinthető. Ezért, figyelembe véve az új 14086. sz. elnöki rendeletet, az EDPB további információkat kér annak értékeléséhez és nyomon követéséhez, hogy az újonnan bevezetett szükségességi és arányossági elvek hogyan és milyen mértékben kerülnek alkalmazásra a gyakorlatban ebben az összefüggésben, és várakozásai szerint ez a jövőbeli közös felülvizsgálatok keretében is értékelésre kerül.

174. Az EDPB üdvözli, hogy a teljeskörűen működő Adatvédelmi és Polgári Szabadságjogi Felügyelő Tanács (Privacy and Civil Liberties Oversight Board – PCLOB) független felügyeleti ügynökségként úgy határozott, hogy egy „olyan felügyeleti projektet hajt végre, amelynek célja, hogy megvizsgálja a külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (FISA) 702. szakasza alapján a végrehajtó hatalmi ág által működtetett megfigyelési programot, készülve a 702. szakasz 2023. decemberi lejárati dátumára, valamint újraengedélyezésének közelgő nyilvános és kongresszusi megvitatására"[172]. Az Európai Adatvédelmi Testület üdvözli továbbá, hogy „a felülvizsgálat a vizsgálat kijelölt, kiemelt területeire terjed ki, beleértve többek között, de nem kizárólag, a 702. szakasz értelmében gyűjtött információk egyesült államokbeli személyek általi lekérdezéseit és a 702. szakasz szerint végrehajtott »upstream« adatgyűjtést"[173], és „egyúttal magába foglalja a program múltbeli és előre jelzett értékének és hatékonyságának, valamint a magánélet védelmére és a polgári szabadságjogokra vonatkozó meglévő biztosítékok megfelelőségének felülvizsgálatát is"[174]. Az EDPB következésképpen hangsúlyozza, hogy a megfigyelési program keretében nyújtott és alkalmazott adatvédelmi biztosítékok megfelelő és átfogó értékeléséhez hozzá kell férni a PCLOB a jelentésben a 702. szakaszra vonatkozóan tett megállapításaihoz.

175. Az új 14086. sz. elnöki rendeletre figyelemmel az EDPB további információkat kér annak értékeléséhez és nyomon követéséhez, hogy az újonnan bevezetett szükségességi és arányossági elvek, valamint a szövegben rögzített egyéb biztosítékok hogyan és milyen mértékben kerülnek alkalmazásra a gyakorlatban ebben az összefüggésben.

3.2.2.4.2 A 12333. sz. elnöki rendelet szerinti nemzetbiztonsági célú adatgyűjtés

176. Amint azt az EUB a Schrems II. ügyben hozott ítéletében elismerte, azon harmadik ország jogszabályainak elemzése, amelynek megfelelőségét mérlegelik, nem korlátozódhat az adott ország

[172] Lásd a PCLOB A KÜLFÖLDI HÍRSZERZŐI TEVÉKENYSÉG MEGFIGYELÉSÉRŐL SZÓLÓ TÖRVÉNY (FISA) 702. SZAKASZÁT VIZSGÁLÓ FELÜGYELETI PROJEKTJÉNEK KÖZLEMÉNYÉT.
[173] Lásd fent.
[174] Lásd fent.

fizikai határain belüli megfigyelést lehetővé tevő jogszabályokra és gyakorlatokra, hanem magában kell foglalnia az adott harmadik ország jogszabályaiban szereplő azon jogalapok elemzését is, amelyek lehetővé teszik számára, hogy az uniós adatok tekintetében a területén kívül megfigyelést végezzen. Az adatokhoz való kormányzati hozzáférés szükséges korlátozásainak ki kell terjedniük az azon országba irányuló „átmenő" személyes adatokra is, amelynek megfelelőségét elismerték.

177. Az EDPB üdvözli a PCLOB által a 12333. sz. elnöki rendeletre vonatkozóan kiadott és 2021 áprilisában közzétett általános, nyilvános jelentést, de megjegyzi, hogy ez a jelentés továbbra is általános jellegű, mivel a megállapítások többségét titkosították.

178. Ebben az összefüggésben az EDPB ismételten hangsúlyozza a PCLOB e szövegről szóló, várt jelentéseinek fontosságát, tekintettel a bizonytalanságra és az egyértelműség hiányára azzal kapcsolatban, hogy a 12333. sz. elnöki rendeletet hogyan alkalmazták korábban, valamint annak tisztázásának fontosságára, hogy az új 14086. sz. elnöki rendelet fényében azt hogyan alkalmazzák majd[175]. Az EDPB ugyanakkor tisztában van vele, hogy a dokumentumok tartalmának nagy része valószínűleg továbbra is titkosított marad, így sem a nyilvánosság, sem pedig az Európai Adatvédelmi Testület számára nem áll majd rendelkezésre további információ a 12333. sz. elnöki rendelet konkrét megvalósulásáról, valamint annak szükségességéről és arányosságáról.

179. Az EDPB ezért különösen üdvözölné, ha a PCLOB a 14086. sz. elnöki rendelet alkalmazásáról szóló jelentése annak elkészülte után nem titkosított, hanem teljes mértékben hozzáférhető lenne, beleértve azokat a részeket is, amelyek azt hivatottak értékelni, hogy a 14086 sz. elnöki rendelet biztosítékai hogyan kerülnek majd alkalmazásra a 12333 sz. elnöki rendelet értelmében történő adatgyűjtés során. Az EDPB továbbá felkéri a Bizottságot, hogy a jövőbeli közös felülvizsgálatokkal összefüggésben fordítson különös figyelmet erre a kérdésre.

180. Általánosságban véve, azon különböző jogi eszközök tekintetében, amelyek lehetővé teszik az egyesült államokbeli hírszerző ügynökségek számára az adatok gyűjtését, valamint az azokhoz való további hozzáférést és azoknak további feldolgozását az Egyesült Államok jogi keretén belül, az EDPB üdvözölné az ezen jogi eszközöknek az új, 14086. sz. elnöki rendelettel való kölcsönhatására vonatkozó pontosításokat, és biztosítékokat vár arra vonatkozóan, hogy a korábbi véleményeiben megfogalmazott korábbi aggályok e tekintetben ezen új biztosítékok elfogadásával megoldásra kerülnek.

181. Az EDPB felkéri továbbá a Bizottságot, hogy a jövőbeli közös felülvizsgálatokkal összefüggésben fordítson különös figyelmet ezekre a szempontokra.

3.2.2.4.3 PCLOB-jelentés

182. Az Európai Adatvédelmi Testület üdvözli, hogy a 14086 sz. elnöki rendelet értelmében a PCLOB-nak jelentést kell készítenie az elnöki rendelet végrehajtásáról. Az EDPB hangsúlyozza, hogy a jelentésnek tartalmaznia kell az elnöki rendelet által biztosított azon konkrét lehetőség értékelését is, amelynek értelmében adatok gyűjthetők a célzott adatgyűjtés vonatkozásában felsorolt célokból, valamint tömegesen is, többek között technikai okokból, annak érdekében, hogy jobban lehessen értelmezni a

[175] A 12333. sz. elnöki rendeletről szóló általános jelentés többnyire továbbra is titkosított maradt – csak egy rövid nyilvános változat, valamint a CIA a 12333 sz. elnöki rendeletnek megfelelően folytatott, terrorizmus elleni tevékenységeiről szóló jelentés és ajánlások kerültek közzétételre, amelyeknek titkosítását szintén csak részben oldották fel.

14086. sz. elnöki rendelet legfontosabb fogalmait, valamint azt, hogy ezeket hogyan értelmezik és alkalmazzák a különböző megfigyelési programokban a gyakorlatban. Ez a jelentés annak értékeléséhez is szükséges, hogy az elnöki rendelet hogyan kerül majd végrehajtásra a hírszerző közösségi szervezeti egységek belső eljárásaiban és szabályzataiban.

3.2.3 „C" garancia – Felügyelet

3.2.3.1 Bevezetés

183. Az Egyesült Államok hírszerzési tevékenységei többszintű felügyeleti eljárás hatálya alá tartoznak. A felügyeleti struktúra az Egyesült Államokban belső és külső felügyeletre osztható. A hírszerző közösség valamennyi szervezeti egysége rendelkezik olyan felügyeleti és megfelelési tisztviselőkkel, akik rendszeres időszakonként felülvizsgálják a jelfelderítési tevékenységeket, ideértve az adatvédelmi és polgári szabadságjogi tisztségviselőket és a főfelügyelőket is. Emellett léteznek külső felügyeleti szervek is, például az Adatvédelmi és Polgári Szabadságjogi Felügyelő Tanács (Privacy and Civil Liberties Oversight Board – PCLOB) és a Hírszerzési Felügyeleti Testület.

184. Az EDPB emlékeztet arra, hogy a beavatkozásra az adatgyűjtés időpontjában, de akkor is sor kerül, amikor a hatóság további feldolgozás céljából hozzáfér az adatokhoz. Emellett az EJEB ítélkezési gyakorlatában több alkalommal kimondta, hogy a magánélethez és az adatvédelemhez való jogba való bármiféle beavatkozásra hatékony, független és pártatlan felügyeleti rendszernek kell vonatkoznia, amelyet bírónak vagy más független testületnek[176] (pl. közigazgatási hatóságnak vagy parlamenti szervnek) kell biztosítania.

185. Bár az EJEB kifejezésre juttatta, hogy a bíró általi felügyeletet részesíti előnyben, nem zárta ki egy másik szerv felelősségi körét sem, *„feltéve, hogy az adott hatóság kellően független a végrehajtó hatalomtól"*[177] és *„a felügyeletet végző hatóságoktól, és megfelelő hatáskörrel és illetékességgel rendelkezik ahhoz, hogy hatékony és folyamatos ellenőrzést gyakoroljon"*[178].

186. Az EJEB hozzátette, hogy a függetlenség értékelésekor figyelembe kell venni *„a felügyeleti szerv tagjai kinevezésének módját és a tagok jogállását"*[179].

187. Az EJEB azt is megállapította, hogy meg kell vizsgálni, hogy a felügyeleti szerv tevékenysége nyitva áll-e a nyilvános vizsgálatok előtt. Ez például úgy valósulhat meg, ha a felügyelet évente jelentést tesz a kormánynak, a nyilvános jelentéseket pedig a Parlament elé terjesztik, és azokat a Parlament megvitatja[180].

188. A megfigyelési intézkedések végrehajtásának független felügyeletét az EUB a Schrems II. ítéletben is figyelembe vette, mivel *„[…] a FISC által végzett ellenőrzés így annak vizsgálatára irányul, hogy e megfigyelési programok megfelelnek-e a külföldi hírszerzési információk megszerzésére irányuló*

[176] Az EJEB 1978. szeptember 6-i ítélete, Klass és társai kontra Németország. (a továbbiakban: EJEB Klass ügyben hozott ítélet), 17. és 51. pont.
[177] Az EJEB Zakharov ügyben hozott ítéletének 258. pontja; az EJEB 2009. február 10-i ítélete, Iordachi és társai kontra Moldova, 40. és 51. pont; az EJEB 2007. április 26-i ítélete, Dumitru Popescu kontra Románia, 70–73. pont.
[178] Az EJEB Klass ügyben hozott ítéletének 56. pontja.
[179] Az EJEB Zakharov ügyben hozott ítéletének 278. pontja.
[180] Az EJEB Zakharov ügyben hozott ítéletének 283. pontja; az EJEB 1990. június 9-i ítélete, L. kontra Norvégia; az EJEB 2010. május 18-i ítélete, Kennedy kontra Egyesült Királyság, 166. pont.

célnak, de nem terjed ki arra a kérdésre, hogy „az egyéneket megfelelően veszik-e célba a külföldi hírszerzési információk megszerzéséhez”[181].

3.2.3.2 Belső felügyelet

3.2.3.2.1 Főfelügyelők

189. Az EDPB elismeri, hogy a főfelügyelőket a hírszerzési tevékenységek nyomon követéséhez szükséges engedélyezések széles körével bízzák meg. Kiemelendő, hogy a főfelügyelők hozzáférnek minden annak értékeléséhez szükséges információhoz, hogy az ügynökségek munkája összességében megfelel-e a jogszabályoknak, ideértve többek között a magánélet védelmére és az adatvédelemre vonatkozó jogszabályokat, továbbá a bizonyításfelvételben való közreműködésre kötelező határozatokat adhatnak ki, és eskü letételét kérhetik bármely személytől a főfelügyelők által folytatott vizsgálattal kapcsolatban.

190. A fentiek alapján az EDPB úgy véli, hogy a főfelügyelők általában széles körű vizsgálati hatáskörrel rendelkeznek. Nem rendelkeznek azonban kötelező erejű jogorvoslati hatáskörrel, és csak nem kötelező erejű ajánlásokat adnak ki[182].

191. Az EDPB elismeri, hogy a főfelügyelők főszabály szerint nem akadályozhatók meg abban, illetve számukra nem tiltható meg az, hogy bármilyen ellenőrzést vagy vizsgálatot kezdeményezzenek, végezzenek vagy folytassanak le, illetve, hogy az ellenőrzés vagy a vizsgálat során a bizonyításfelvételben való közreműködésre kötelező határozatokat adjanak ki[183]. Ezzel összefüggésben azonban az EDPB megjegyzi, hogy a főfelügyelők az adott szervezeti egység vezetőjének felügyelete, irányítása és ellenőrzése alatt állnak, akik megtilthatják számukra az információkhoz való hozzáférést, a nyomozás lefolytatását és többek között a bizonyításfelvételben való közreműködésre kötelező határozatok kiadását olyan esetekben, amikor a szervezeti egység vezetője megállapítja, hogy az ilyen tilalom a nemzeti érdekek védelme érdekében szükséges. A szervezeti egység vezetőjének e hatáskörének gyakorlásáról azonban tájékoztatnia kell az Egyesült Államok Kongresszusának illetékes bizottságait[184].

192. Az EDBP megjegyzi, hogy a főfelügyelőket csak az Egyesült Államok elnöke távolíthatja el pozíciójukból, akinek tájékoztatnia kell a Kongresszust az eltávolítás okairól.

193. Az Európai Adatvédelmi Testület megjegyzi, hogy a 29. cikk szerinti munkacsoport véleménye, illetve az Európai Adatvédelmi Testület későbbi véleménye óta nem történt jelentős módosítás a belső felügyeleti mechanizmus tekintetében. Az EDPB ezért a 29. cikk szerinti munkacsoport 01/2016. sz. véleményével[185] összhangban azt a következtetést vonja le, hogy általánosságban véve elegendő belső felügyeleti mechanizmus van érvényben.

---

[181] A Bíróság Schrems I. ügyben hozott ítéletének 179. pontja.
[182] A határozattervezet (105) preambulumbekezdése.
[183] A főfelügyelőről szóló 1978. évi törvény 3. §-ának a) pontja.
[184] Lásd pl. a főfelügyelőről szóló 1978. évi törvény 8. §-át (a Védelmi Minisztérium vonatkozásában); 8E. § (az Igazságügyi Minisztérium vonatkozásában), 8G. §-a d) pontjának (2) pontjának A. és B. pontját (a Nemzetbiztonsági Ügynökség vonatkozásában); az Egyesült Államok Szövetségi Törvénykönyve 50. címe 403q. §-ának b) pontját (a Központi Hírszerző Ügynökség vonatkozásában); a 2010-es költségvetési évre vonatkozó hírszerzési engedélyezési törvény 405. szakaszának (f) pontja (a Hírszerző Közösség vonatkozásában).
[185] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye.

3.2.3.3 Külső felügyelet

194. Az EDPB megjegyzi, hogy az alábbiakban említett szerveken kívül az Egyesült Államok kormányának olyan különböző egyéb szervei felügyelik az Egyesült Államok hírszerző ügynökségeinek tevékenységét, mint például a Hírszerzési Felügyeleti Testület (Intelligence Oversight Board – IOB) vagy a kongresszusi bizottságok. Ez utóbbiak saját vizsgálatokat végezhetnek és jelentéseket készíthetnek.

3.2.3.3.1 Adatvédelmi és polgári szabadságjogi felügyeleti tanács (Privacy and Civil Liberties Oversight Board, PCLOB)

195. Az EDPB elismeri a PCLOB átfogó felügyeleti szerepét az új jogorvoslati mechanizmus és a 14086. sz. elnöki rendelet végrehajtása tekintetében.

196. Először is, új feladatai közé tartozik a legfőbb ügyésszel folytatott konzultáció a DPRC bíráinak és a különleges ügyvédeknek a kinevezéséről. Másodszor, a PCLOB évente felülvizsgálja a jogorvoslati eljárást, azaz a jogszerű panaszoknak a jogorvoslati mechanizmus általi feldolgozását. Ez magában foglalja annak vizsgálatát is, hogy a CLPO és az Adatvédelmi Felülvizsgálati Bíróság időben feldolgozta-e a jogszerű panaszokat, teljes körű hozzáférést kap-e a szükséges információkhoz, és a 14086. sz. elnöki rendeletnek megfelelően működik-e, valamint, hogy a Hírszerző Közösség megfelel-e a CLPO és a DPRC határozatainak.

197. Ezenkívül a PCLOB-vel való konzultáció akkor is kötelező, amikor a hírszerző ügynökségek a 14086. sz. elnöki rendelet végrehajtása érdekében aktualizálják belső szabályzataikat és eljárásaikat. Emellett a PCLOB felülvizsgálja az aktualizált szabályzatokat és eljárásokat, és értékeli, hogy azok megfelelnek-e a 14086. sz. elnöki rendeletnek[186]. Bár a PCLOB megállapításai szigorú értelemben nem kötelező erejűek, a Hírszerző Közösség minden egyes szervezeti egységének vezetője köteles gondosan mérlegelni és végrehajtani vagy más módon figyelembe venni az ilyen felülvizsgálatokban foglalt valamennyi ajánlást az alkalmazandó joggal összhangban[187]. Az EDPB felkéri a Bizottságot, hogy a határozattervezet elfogadása esetén a jövőbeli felülvizsgálatok során fordítson különös figyelmet arra, hogy a PCLOB ajánlásait az ügynökségek szintjén végrehajtották-e, és amennyiben igen, hogyan.

198. Az EDPB emlékeztet arra, hogy a PCLOB, mivel független, ösztönözhető, de nem kötelezhető annak felülvizsgálatára, hogy a 14086. sz. elnöki rendeletben meghatározott biztosítékokat megfelelően figyelembe veszi-e, valamint, hogy a Hírszerző Közösség teljes mértékben eleget tesz-e a jogorvoslati eljárás követelményeinek. Az EDPB értelmezése szerint azonban a PCLOB az Európai Adatvédelmi Testületnek adott kiegészítő magyarázatában és nyilvánosan is kijelentette[188], hogy el fogja látni a 14086. sz. elnöki rendeletben előirányzott szerepet.

199. Az EDPB továbbá üdvözli, hogy a PCLOB-jelentések eredményeit nyilvánossá kívánják tenni. Figyelembe véve, hogy a jogorvoslati mechanizmusban részt vevő szerveknek és a Hírszerző Közösség szerveinek alapszabályként végre kell hajtaniuk vagy más módon figyelembe kell venniük a PCLOB jelentéseiben foglalt ajánlásokat, az EDPB elismeri, hogy ezek az ajánlások fontos szerepet játszanak az adatvédelmi biztosítékok vonatkozásában.

[186] A 14086. sz. elnöki rendelet 2. szakasza c) pontjának i. v. alpontja és 2. szakasza c) pontjának v. alpontja.
[187] A 14086. sz. elnöki rendelet 2. szakasza c) pontja v. alpontjának B. pontja.
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf

200. Az EDPB megjegyzi, hogy amennyiben az Egyesült Államok elnöke engedélyezi, hogy az Egyesült Államok kormányának minisztériumai, ügynökségei vagy szervezeti egységei „fedett műveleteket”[189] hajtsanak végre, a PCLOB információkhoz való hozzáférése korlátozott[190].

201. Korábbi véleményeit követően az EDPB a felügyeleti struktúra alapvető elemének tekinti a PCLOB-t mint olyan független szervet, amelynek ajánlásai jelentős mértékben hozzájárultak az egyesült államokbeli reformokhoz, és amelynek jelentései különösen hasznos forrásként szolgáltak a különböző felügyeleti programok működésének megismeréséhez.

202. Az EDPB azonban sajnálatát fejezte ki a korábbi EU–USA adatvédelmi pajzs harmadik éves közös felülvizsgálata során azt illetően, hogy a PCLOB csak ugyanazokat az információkat bocsátotta az EDPB rendelkezésére, mint a nyilvánosság számára. Sajnálatos továbbá, hogy a PCLOB nem adott ki további, az első jelentését nyomon követő jelentéseket a PPD-28-ról annak érdekében, hogy további információkat biztosítson a PPD-28 biztosítékainak alkalmazására vonatkozóan, és a FISA 702. szakaszáról szóló általános, aktualizált jelentést sem.

203. Az EDPB ezért üdvözli a PCLOB az Európai Adatvédelmi Testület felé tett bejelentését, amely szerint a közeljövőben várható a FISA 702. szakaszáról szóló nyomonkövetési jelentés elkészülte. Az EDPB továbbá elégedettségét fejezi ki azzal kapcsolatban, hogy a PCLOB tájékoztatta arról a kötelezettségvállalásáról, miszerint lehetővé teszi a 14086. sz. elnöki rendeletről szóló jelentéseinek nyilvánosságra hozatalát. Az EDPB ugyanakkor emlékeztet arra, hogy a nem titkosított jelentések közzétételét az Egyesült Államok joga szabályozza, és azt a Hírszerző Közösség ügynökségeivel összehangoltan kell végezni, a PCLOB-nak önálló döntési joga e tekintetben nincs.

204. Ezért az EDPB emlékeztet arra, hogy a határozattervezet elfogadása esetén az EU–USA adatvédelmi keret jövőbeli felülvizsgálatai során az Európai Adatvédelmi Testület átvilágított szakértőinek lehetőséget kell adni a további dokumentumok áttekintésére és a további titkosított elemek megvitatására annak biztosítása érdekében, hogy a jelentésekben szereplő információk megfelelően értékelhetők legyenek, ugyanakkor figyelembe véve a vonatkozó nemzetbiztonsági érdekeket és a magánélet védelmére vonatkozó, alkalmazandó szabályokat.

205. Az EDPB üdvözli a PCLOB függetlenségét és felügyeletét a nemzeti hírszerző közösség felett, melynek meg kell felelnie a PCLOB ajánlásainak vagy egyéb módon figyelembe kell vennie azokat, amit a PCLOB az Egyesült Államok Kongresszusának címzett jelentésében rögzít.

206. Figyelembe véve az EJEB nyilvános ellenőrzésre vonatkozó követelményeit[191], miszerint a felügyeleti szerv jelentéseit a Parlament elé kell terjeszteni és azt a Parlamentnek meg kell vitatnia, az Európai Adatvédelmi Testület kielégítőnek tartja, hogy a PCLOB jelentéseit legalább félévente benyújtja az

[189] Az Egyesült Államok Szövetségi Törvénykönyve 50. címe 3093. §-a e) pontjának 1. alpontja értelmében a „fedett művelet” az Amerikai Egyesült Államok kormányának külföldi politikai, gazdasági vagy katonai feltételek befolyásolására irányuló olyan tevékenységét vagy tevékenységeit jelenti, amelynek során az Egyesült Államok kormányának szerepe szándékoltan nem látható, illetve nyilvánosan el nem ismert, de nem foglalja magában 1. azokat a tevékenységeket, amelyek elsődleges célja a hírszerzés, a hagyományos kémelhárítási tevékenységeket […].

[190] Az Egyesült Államok Szövetségi Törvénykönyve 42. címe 2000ee. §-a g) pontjának 5. alpontja; az Egyesült Államok Szövetségi Törvénykönyve 50. címe 3093. §-ának a) pontja.

[191] Az EJEB Zakharov ügyben hozott ítéletének 283. pontja, az EJEB 1990. június 9-i ítélete, L. kontra Norvégia; az EJEB 2010. május 18-i ítélete, Kennedy kontra Egyesült Királyság, 166. pont.

Egyesült Államok elnökének és különösen a Szenátus és a Képviselőház kongresszusi bizottságainak[192], amelyek az Egyesült Államok parlamenti szervei.

3.2.3.3.2 A külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság (Foreign Intelligence Surveillance Court – FISC)

207. A FISA 702. szakasza értelmében[193] a személyes adatok gyűjtésének felügyeletéért a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó bíróság felel, és a FISC határozatai ellen pedig fellebbezéssel a külföldi hírszerzési tevékenységek megfigyelésével foglalkozó fellebbviteli bíróságnál (Foreign Intelligence Surveillance Court of Review – FISCR) lehet élni.

208. A FISC felügyeli a külföldi hírszerzési információk gyűjtésére vonatkozó, a FISA 702. szakasza szerinti tanúsítási eljárást, illetve engedélyezi az elektronikus megfigyelést, a fizikai átkutatást és a külföldi hírszerzési célokból végzett egyéb nyomozási intézkedéseket[194]. A FISC engedélyezi továbbá a célkiválasztásra, a minimalizálásra és a tanúsítványok lekérdezésére vonatkozó eljárásokat, amelyek jogilag kötelező erejűek az USA hírszerző ügynökségeinek vonatkozásában[195]. Amennyiben a FISC azt állapítja meg, hogy a követelmények nem teljesültek, részben vagy egészben megtagadhatja a tanúsítást, és kérheti az eljárások módosítását.

209. Amennyiben a célkiválasztási eljárások megsértése kerül megállapításra, a FISC korrekciós intézkedések alkalmazását rendelheti el az adott érintett hírszerző ügynökség számára[196]. Az ilyen korrekciók az egyedi intézkedésektől a strukturális intézkedésekig, például az adatszerzés leállításától a jogellenesen megszerzett adatok törlésén át az adatgyűjtési gyakorlat megváltoztatásáig – beleértve a személyzet részére biztosítandó iránymutatást és képzést – terjedhetnek.

210. Az EDPB elismeri, hogy a 14086. sz. elnöki rendelet előírja, miszerint a CLPO és DPRC a jogsértéseket köteles jelenteni a nemzetbiztonságért felelős helyettes legfőbb ügyésznek, aki ezeket jelenti a FISC-nek[197].

211. Amint azt az EUB a Schrems II. ügyben hozott ítéletében megjegyezte, a FISC nem egyéni megfigyelési intézkedéseket, hanem megfigyelési programokat engedélyez[198]. Az EDPB ezért továbbra is aggályosnak tartja, hogy a FISC nem biztosít hatékony bírósági felügyeletet a nem egyesült államokbeli személyek célszemélyként való kijelölése tekintetében, amire úgy tűnik, hogy az új 14086. sz. elnöki rendelet sem biztosít megoldást.

212. Ami a megfigyelés a FISA 702. szakasza szerinti előzetes független engedélyezését illeti[199], az EDPB sajnálatát fejezi ki amiatt, hogy – ahogyan azt az EDPB a határozattervezet[200] és az Egyesült Államok kormánya által adott magyarázatok alapján értelmezi – a FISC-et látszólag nem kötik a 14086. sz. elnöki rendelet további biztosítékai a nem egyesült államokbeli személyek célszemélyként való megjelölését

[192] Az Egyesült Államok Szövetségi Törvénykönyve, 42. cím, 2000ee. § e) pont.
[193] Az Egyesült Államok Szövetségi Törvénykönyve, 50. cím,1881. §, a) pont.
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court
[195] Az Egyesült Államok Szövetségi Törvénykönyve, 50. cím,1881a. §, i) pont.
[196] Az Egyesült Államok Szövetségi Törvénykönyve, 50. cím, 1803. §, h) pont.
[197] A 14086. sz. elnöki rendelet 3. szakasza c) pontja i. alpontjának D) pontja; A 14086. sz. elnöki rendelet 3. szakasza d) pontja i. alpontjának F) pontja.
[198] A Bíróság Schrems I. ügyben hozott ítéletének 179. pontja.
[199] Az EDPB aggodalmát fejezi ki amiatt, hogy abban az esetben, ha a FISC nem rendelkezik hatáskörrel a 12333. sz. elnöki rendelet szerinti tömeges adatgyűjtést illetően, nincs érvényben előzetes engedélyezési eljárás a tömeges adatgyűjtésre vonatkozóan (lásd még a „B" garanciát).
[200] A határozattervezet (165) preambulumbekezdése.

engedélyező programok tanúsítása során. Az EDPB véleménye szerint mindazonáltal az e rendleletben foglalt további biztosítékokat is figyelembe kell venni ebben az összefüggésben. Az EDPB emlékeztet arra, hogy a PCLOB jelentései különösen hasznosak lennének annak értékeléséhez, hogy a 14086. sz. elnöki rendelet biztosítékai hogyan kerülnek majd végrehajtásra, illetve azokat hogyan alkalmazzák azokban az esetekben, amikor a FISA 702. szakasza értelmében történik adatgyűjtés.

3.2.4 „D" garancia –A magánszemélyek számára hatékony jogorvoslati lehetőségeket kell biztosítani

213. Az EDPB emlékeztet arra, hogy a magánszemélyek tényleges és érvényesíthető jogai alapvető fontosságúak a megfelelő szintű adatvédelem harmadik országban való megállapításához. A természetes személynek hatékony jogorvoslattal kell rendelkeznie jogainak érvényesítéséhez abban az esetben, ha úgy ítéli meg, hogy azokat nem tartják vagy tartották tiszteletben. Az EUB Schrems I. és II. ügyben hozott ítéletében kifejtette, 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 töröltesse, nem tartja tiszteletben a hatékony bírói jogvédelemhez való jog lényegét, amelyet az Európai Unió Alapjogi Chartája 47. cikke mond ki"[201].

214. Az Egyesült Államok bírósági jogorvoslatra vonatkozó rendszere egy olyan fontos korlátozást tartalmaz, amely nagyon megnehezíti az Egyesült Államok kormánya által hozott megfigyelési intézkedésekkel szembeni bírósági eljárások rendes bíróságok előtti kezdeményezését. Az Egyesült Államok alkotmánya megköveteli az egyéntől, hogy bizonyítsa kereshetőségi jogát, azaz „bizonyítsa egy konkrét, részletezett, meglévő vagy hamarosan bekövetkező jogsérelem bekövetkezését"[202]. A megfigyeléssel kapcsolatos ügyekben ez a követelmény látszólag semmis, mivel a megfigyelés alá vont természetes személyeket még az intézkedések befejezése után sem értesítik azokról.

215. Ezzel összefüggésben az Európai Adatvédelmi Testület üdvözli, hogy a 14086. sz. elnöki rendelet konkrét jogorvoslati mechanizmust teremt a nem egyesült államokbeli természetes személyektől érkező, az USA jelfelderítési tevékenységeivel kapcsolatos panaszok kezelésére és rendezésére. Ezen új mechanizmus keretében a kereshetőségi jogra vonatkozó követelmény nem alkalmazandó: a 14086. sz. elnöki rendelet 4. szakasza k) pontjának ii. alpontja értelmében a felperesnek nem kell bizonyítania, hogy adatai ténylegesen egyesült államokbeli jelfelderítés tárgyát képezték. Az érintettek így hivatkozhatnak a 14086. sz. elnöki rendelet által előírt biztosítékokra, beleértve azokat is, amelyeket a 14086. sz. elnöki rendelet 4. szakasza d) pontjának iii. alpontjában említett egyéb vonatkozó jogszabályok és rendelkezések írnak elő[203]. E tekintetben az új mechanizmus olyan jogorvoslati lehetőséget teremt, amely egyébként nem létezne.

216. Az új mechanizmus két szintből áll: Az első szinten a természetes személyek panaszt nyújthatnak be a nemzeti hírszerzés igazgatója irodája polgári szabadságjogok védelmével foglalkozó tisztviselőjéhez (CLPO). A második szinten a természetes személyeknek lehetőségük van arra, hogy egy újonnan létrehozott szerv, az úgynevezett Adatvédelmi Felülvizsgálati Bíróság (DPRC) előtt fellebbezzenek a CLPO határozata ellen. A következő szakaszok elsősorban a jogorvoslati mechanizmus második szintjére összpontosítanak. Az EDPB úgy véli, hogy a CLPO mint megbízott kormánytisztviselő nem rendelkezik kellő mértékű függetlenséggel a végrehajtó hatalomtól, és így önmagában nem képes

[201] Az EUB Schrems I. ügyben hozott ítélete, 95. pont; az EUB Schrems II. ügyben hozott ítélete, 187. pont.
[202] Clapper kontra Amnesty International USA, 568 U.S. 398 (2013) II., 10. o.
[203] A 14086. sz. elnöki rendelet 5. szakaszának h) pontja kifejezetten feljogosítja az érintetteket arra, hogy a jogorvoslati mechanizmussal összhangban panaszt nyújtsanak be.

megfelelően teljesíteni a Charta 47. cikkéből eredő követelményeket. Ezt az álláspontot a Bizottság több alkalommal is megerősítette.

3.2.4.1 Önmagában elegendő-e a DPRC elnöki rendeleten alapuló létrehozása

217. A DPRC nem a Kongresszus által az Egyesült Államok alkotmányának III. cikke alapján létrehozott rendes bíróság, hanem az Egyesült Államok elnöke által kiadott elnöki rendeleten alapul. Bár az EDPB tisztában van a létrehozás alapjául szolgáló megfontolással – nevezetesen a kereshetőség bizonyítására vonatkozó követelmény elkerülésével (lásd még a 215. bekezdést), és általánosságban véve üdvözli azt, felvetődik egy alapvető kérdés: Egy ilyen jogorvoslati mechanizmus megfelelhet (egyáltalán) a Charta 47. cikkében foglalt követelményeknek? A rendelkezés értelmében mindenkinek, akinek az Unió joga által biztosított jogait és szabadságait megsértették, joga van a törvény által megelőzően létrehozott bíróság előtti hatékony jogorvoslathoz.

218. Míg a Charta 47. cikkének angol szövege „tribunal"-okra (törvényszékekre) hivatkozik, más nyelvi változatok a „court", azaz „bíróság" szót részesítik előnyben[204]. Az EUB Schrems II. ügyben hozott ítéletében ismételten leszögezte, hogy „az érintetteknek különösen rendelkezniük kell azzal a lehetőséggel, hogy független és pártatlan bíróság előtt éljenek jogorvoslati lehetőségekkel abból a célból, hogy a rájuk vonatkozó személyes adatokhoz hozzáférést kapjanak, vagy az ilyen adatokat helyesbíttetni vagy töröltetni tudják"[205]. Az EUB ugyanakkor az adatvédelmi szint megfelelőségének értékelésével összefüggésben úgy véli, hogy az ilyen beavatkozásokkal szembeni hatékony bírói jogvédelem nemcsak bíróság, hanem egy olyan szerv által is biztosítható, amely a Charta 47. cikkében előírtakkal lényegében egyenértékű garanciákat nyújt[206]. Az EJEB hasonlóképpen kimondja, hogy „mindenkinek, akinek jogait és szabadságait megsértették, hatékony jogorvoslattal kell rendelkeznie a nemzeti hatóság előtt"[207], amelynek – az EJEB állandó ítélkezési gyakorlata szerint – nem feltétlenül kell igazságügyi hatóságnak lennie[208]. A hatóság előtti jogorvoslat hatékonyságának értékelése szempontjából sokkal inkább a hatóság hatáskörei és eljárási garanciái relevánsak, különösen, hogy független-e a végrehajtó hatalomtól és biztosítja-e az eljárás tisztességes lefolytatását[209]. A két bíróság értékelését láthatóan nem tisztán formális kritériumokra alapozza, hanem az érdemi biztosítékokat tekinti meghatározónak.

219. A Schrems II. ügyben az EUB különös figyelmet fordított a hatékony jogorvoslatra a nemzetbiztonság területén a személyes adatokhoz való hozzáférés tekintetében. Az EDPB tudomásul veszi, hogy ennek során az EUB nem vitatta meg a Charta 47. cikkében szereplő, „a törvény által megelőzően létrehozott" feltételt, habár az adatvédelmi pajzs ombudsmani mechanizmusa sem az Egyesült Államok tételes jogán alapul. Az EUB e kérdés vizsgálata helyett a megfelelőségi teszt különböző szempontjait értékelte például a jogorvoslati hatáskörök hiányát. Így a Schrems II. ügyben hozott ítélet nem ad iránymutatást a Charta 47. cikke szerinti, „a törvény által megelőzően létrehozott" minősítés értékeléséhez. Léteznek azonban más olyan ítéletek is, amelyekben az EUB észrevételeket fogalmazott meg erre a kérdésre vonatkozóan. Az EJEB ezzel kapcsolatos állandó ítélkezési gyakorlatával összhangban az EUB a C-487/19. és a C-132/20. sz. ügyben emlékeztetett arra, hogy a „törvény által megelőzően létrehozott""

[204] Például „Gericht" a német nyelvi változatban.
[205] A Bíróság Schrems I. ügyben hozott ítélete, 194. pont.
[206] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 197. pontját.
[207] Az EJEE 13. cikke.
[208] Az EJEB Klass ügyben hozott ítéletének 67. pontja; az EJEB Big Brother Watch ügyben hozott ítéletének 359. pontja.
[209] Az EJEB Klass ügyben hozott ítéletének 67. pontja; az EJEB Big Brother Watch ügyben hozott ítéletének 359. pontja.

kifejezés bevezetésének oka annak biztosítása volt, hogy az igazságszolgáltatási rendszer kialakítása egy demokratikus társadalomban ne a végrehajtó hatalom mérlegelési jogkörétől függjön, hanem azt a törvényhozó hatalom által a hatáskörének gyakorlására vonatkozó szabályoknak megfelelően elfogadott törvény szabályozza[210]. Amint e megállapításból kitűnik, a törvény által megelőzően létrehozott bírósághoz való jog nagyon szorosan kapcsolódik a függetlenség biztosításához.

220. Mindezek alapján az EDPB arra a következtetésre jutott, hogy a védelmi szint megfelelősége értékelésének tekintetében a 14086. sz. elnöki rendelet értelmében létrehozott konkrét jogorvoslati mechanizmus a III. cikk szerinti bíróságok általi jogorvoslattal összehasonlítva önmagában véve nem tekintendő elégtelennek. E tekintetben a védelem szintjének értékelése attól függ, hogy a 14086. sz. elnöki rendeletben előírt és a főügyészi rendelettel kiegészített biztosítékok megfelelően biztosítják-e a DPRC függetlenségét a többi hatalmi ággal szemben.

221. A Bizottságnak folyamatosan nyomon kell követnie, hogy a 14086. sz. elnöki rendeletben meghatározott szabályokat és annak kiegészítő rendelkezéseit, különösen azokat, amelyek célja a DPRC függetlenségének előmozdítása, teljes mértékben végrehajtották-e, és a gyakorlatban hatékonyan működnek-e. Emellett a keret minden módosítását gondosan felül kell vizsgálni a határozattervezet szerinti bizottsági értékelésre gyakorolt hatás szempontjából. E tekintetben az EDPB megjegyzi, hogy a 14086. sz. elnöki rendelet és a főügyészi rendelet módosítása olyan azonnal alkalmazandó végrehajtási jogi aktusok elfogadását vonhatja maga után, amelyek felfüggesztik, hatályon kívül helyezik vagy módosítják a megfelelőségi határozatot[211].

3.2.4.2 Kellő függetlenség a végrehajtó hatalomtól

222. A Schrems II. ügyben hozott ítéletében az EUB hangsúlyozta, hogy a bíróság vagy szerv – különösen a végrehajtó hatalomtól való – függetlenségét minden szükséges garanciával biztosítani kell, többek között a visszahívás vagy a kinevezés megszüntetése feltételeinek tekintetében is. Konkrétabb értelemben véve az EUB bírálta azt a tényt, hogy az ombudsmant a külügyminiszter nevezi ki, és közvetlenül neki tartozik felelősséggel. Az ombudsmant az Egyesült Államok külügyminisztériumának szerves részeként tartják számon. Az EUB megállapította továbbá, hogy nincsenek konkrét garanciák az ombudsman visszahívására vagy a kinevezésének megszüntetésére vonatkozóan, ami aláássa az ombudsman végrehajtó hatalomtól való függetlenségét.

223. Az EDPB tudomásul veszi, hogy a 14086. sz. elnöki rendelet és a kiegészítő főügyészi rendelet rendelkezései nem írnak elő beszámolási kötelezettséget a DPRC számára a legfőbb ügyész felé, mivel az alá-fölérendeltségi viszonyt jelentene. A DPRC azonban nem tartozik a legfőbb ügyész „napi szintű felügyelete" alá sem[212]. Ezek a biztosítékok jelentős előrelépést jelentenek az adatvédelmi pajzshoz képest. A DPRC ugyanakkor a végrehajtó hatalmi ágon, nevezetesen az Igazságügyi Minisztériumon belül jött létre. Éppen ezért a biztosítékok gyakorlati végrehajtása és hatékony működése lesz döntő fontosságú annak meghatározásában, hogy a DPRC – mint nem az Igazságügyi Minisztérium szerves részét képező, ugyanakkor a végrehajtó hatalomban helyet kapó szervezet – a gyakorlatban kellően függetlennek tekinthető-e. Az EDPB felkéri a Bizottságot annak gondos nyomon követésére, hogy ezek a biztosítékok teljes mértékben tükröződnek-e a gyakorlatban. Emellett az EDPB a „napi szintű felügyelet" fogalmának pontosítását is javasolja annak érdekében, hogy a DPRC „bírái" semmilyen

[210] Lásd: a Bíróság 2021. október 6-i ítélete, W.Ż, C-487/19, ECLI:EU:C:2021:798 és 2022. március 29-i ítélete, Getin Noble Bank S.A., C-132/20, ECLI:EU:C:2022:235, 129. és 121. pont.
[211] A határozattervezet (212) preambulumbekezdése.
[212] A főügyészi rendelet 201.7. §-ának d) pontja.

felügyelet alá ne tartozzanak. A Bizottság megerősítette, hogy a „napi szintű felügyelet” kifejezést ebben az értelemben kell értelmezni.

224. A fenti biztosítékok mellett az EU–USA adatvédelmi keret bizonyos garanciákat irányoz elő a DPRC „bíráinak” kinevezésére és felmentésére vonatkozóan. A „bírákat” a legfőbb ügyész nevezi ki, kinevezésük azonban a szövetségi bírói jelöltek értékelésére használt kritériumokon alapul, és egy, a PCLOB-val folytatott konzultációt is magában foglal. A „bírák” felmentésére hivatali idejük lejárta előtt vagy egy folyamatban lévő eljárás vonatkozásában csak olyan szigorúan meghatározott körülmények között van lehetőség, amelyek – az Európai Adatvédelmi Testület értelmezése szerint – a szövetségi bírákra alkalmazandó rendelkezések mintáján alapulnak[213]. E szabályok alkalmazása további előrelépést jelent a DPRC független pozíciójának megerősítése felé, amelynek tekintetében a gyakorlati végrehajtás szintén döntő fontosságú lesz. Magából a határozattervezetből azonban nem derül ki egyértelműen, hogy az Egyesült Államokban felügyelik-e az említett követelményeknek való megfelelést, és amennyiben igen, hogyan. A Bizottság és az Egyesült Államok kormánya által adott kiegészítő magyarázatok alapján az EDPB úgy értelmezi, hogy a PCLOB a jogorvoslati eljárás éves felülvizsgálata során foglalkozhat a fent említett rendelkezésekkel, valamint, hogy az Igazságügyi Minisztériumon belüli főfelügyelő által meghatározott jogi követelményeknek való maradéktalan megfelelés nyomon követésével és biztosításával kapcsolatos felelősség magában foglalja a 14086. sz. elnöki rendelet és a DPRC-t létrehozó rendeletek által előírt követelményeket is. Az EDPB felkéri a Bizottságot, hogy tisztázza ezt a kérdést a határozattervezetben. Mindemellett a Bizottságnak a személyes adatok határozattervezetben értékelt kezelése tényleges gyakorlatának nyomon követése során figyelembe kell vennie ezeket a biztosítékokat.

225. A határozattervezet nem foglalkozik azzal a kérdéssel, hogy az Egyesült Államok elnöke jogosult-e „bírákat” felmenteni vagy eltávolítani a DPRC-ből, és ha igen, milyen feltételek mellett. Az EDPB tudomása szerint az elnöknek erre nincs jogosultsága, amint azt az Európai Bizottság kifejtette és az Egyesült Államok kormányának képviselői is megerősítették. Az EDPB azt javasolja, hogy e kérdést egyértelműsítsék a megfelelőségi határozatban.

226. A DPRC „bíráit” megújítható, négyéves hivatali időre nevezik ki, és feltétel, hogy az eredeti kinevezésük időpontját megelőző két évben nem állhattak alkalmazásban a végrehajtó hatalmi ágon belül[214]. A DPRC „bírájaként” való kinevezésük ideje alatt nem tölthetnek be semmilyen más hivatali feladatot vagy állást az Egyesült Államok kormányán belül[215]. Az Egyesült Államok szövetségi bíráitól eltérően azonban részt vállalhatnak az olyan bíróságon kívüli tevékenységekben, mint az üzleti tevékenységek, a pénzügyi tevékenységek, a nonprofit adománygyűjtési tevékenységek, a vagyonkezelői tevékenységek és az ügyvédi praxis, amennyiben ezek a tevékenységek nem befolyásolják feladataik pártatlan ellátását, illetve a DPRC hatékonyságát vagy függetlenségét[216]. A bírói függetlenség nemcsak az utasíthatatlanságból ered, hanem a személyes függetlenségből is. Ebben a vonatkozásban az olyan tényezők relevánsak, mint a hivatali idő, az újbóli kinevezés lehetősége, valamint az esetleges összeférhetetlenség. A 14086. sz. elnöki rendeletben, illetve a főügyészi rendeletben előirányzott négyéves hivatali idő, amely bár például rövidebb, mint az EUB és az EJEB bíráinak hivatali ideje (előbbi esetében hat év az ismételt kinevezés lehetőségével, míg utóbbinál kilenc év az ismételt kinevezés lehetősége nélkül), önmagában nem vet fel komoly aggályokat. Az EDPB-nek nincs tudomása olyan

[213] A 14086. sz. elnöki rendelet 3. szakasza d) pontjának iv. alpontja; a főügyészi rendelet 201.7. §-a.
[214] A főügyészi rendelet 201.3. §-ának a) pontja.
[215] A főügyészi rendelet 201.3. §-ának c) pontja.
[216] A főügyészi rendelet 201.7. §-ának c) pontja.

ítélkezési gyakorlatról, amely e tekintetben minimális hivatali időt írna elő[217]. Az EDPB azt is elismeri, hogy a bíróságon kívüli tevékenységek végzésének lehetősége attól a feltételtől függ, hogy azok – egyszerűen megfogalmazva – ne vezessenek olyan összeférhetetlenséghez, amely veszélyeztetné a DPRC kötelezettségeit. Az EDPB az Egyesült Államok kormányának kiegészítő magyarázatai alapján úgy értelmezi, hogy ezeket a követelményeket is felülvizsgálja és nyomon követi a PCLOB és az Igazságügyi Minisztérium főfelügyelője (lásd a fenti 226. pontot). A közös felülvizsgálatok részeként foglalkozni kell azzal is, hogy ezt a követelmény hogyan alkalmazzák és demonstrálják majd a gyakorlatban.

227. A 14086. sz. elnöki rendelet 3. szakasza d) pontja i. alpontjának B. pontja értelmében a DPRC valamennyi „bírájának" rendelkeznie kell olyan személyes biztonsági tanúsítvánnyal, amely lehetővé teszi számukra a titkosított adatokhoz való hozzáférést, azaz a nemzetbiztonsági ügyek elbírálására irányuló feladat ellátását[218]. Ezzel szemben a személyi biztonsági tanúsítványokról szóló egyes európai törvények és rendeletek a bírákat – amennyiben igazságszolgáltatási feladatokat látnak el – mentesítik a biztonsági ellenőrzés követelménye alól, mivel az ilyen részletes ellenőrzést a bírói függetlenséggel esetlegesen ellentétes gyakorlatnak ítélik[219]. Az Egyesült Államok kormányának magyarázata szerint, míg az egyesült államokbeli bíróságok tekintetében a bírói kinevezésre jelölt személyt alapos átvilágításnak vetik alá, miután az adott személyt szövetségi bíróvá nevezték ki egy egyesült államokbeli bíróságon, ebben a szerepében már nincs szükség személyi biztonsági tanúsítvány megszerzésére az adott ügy szempontjából releváns, titkosított dokumentumokhoz való hozzáféréshez.

228. Az EDPB véleménye szerint a fent vázolt körülmények részben különbségeket tárnak fel az Egyesült Államok szövetségi bíráinak és a DPRC „bíráinak" helyzete és jogállása között. A nyújtott biztosítékok azonban nem adnak okot a DPRC függetlenségének megkérdőjelezésére. Az Európai Adatvédelmi Testület arra kéri a Bizottságot, hogy amennyiben a határozattervezetet elfogadják, a fent említett biztosítékokat kezeljék prioritásként az EU–USA adatvédelmi keret első közös felülvizsgálata során. Ezen túlmenően az Európai Adatvédelmi Testület elvárja, hogy a Bizottság eleget tegyen az elfogadott megfelelőségi határozat felfüggesztésére, hatályon kívül helyezésére vagy módosítására vonatkozó kötelezettségvállalásának abban az esetben, ha az Egyesült Államok kormányzata úgy döntene, hogy korlátozza az elnöki rendeletben foglalt biztosítékokat[220].

3.2.4.3 A DPRC hatáskörei

3.2.4.3.1 Az információkhoz való hozzáférés

229. A hatékony jogvédelem megköveteli, hogy a bíróság elegendő vizsgálati hatáskörrel rendelkezzen a vitatott intézkedés felülvizsgálatához. A Kadi II. ügyben az EUB a Charta 47. cikke kapcsán úgy ítélte meg, hogy az európai uniós bíróságoknak biztosítaniuk kell, hogy a határozatokat kellően biztos ténybeli alapon hozzák meg[221]. Az EUB kijelenti, hogy „az uniós bíróság feladata e vizsgálat elvégzése úgy, hogy adott esetben az Unió illetékes hatóságát az ilyen vizsgálathoz releváns – bizalmas vagy nem

[217] Lásd még értelemszerűen: az EJEB (nagytanács) 2021. május 25-i ítélete, Centrum För Rättvisa kontra Svédország, 346. pont.
[218] Lásd még a főügyészi rendelet 201.11. §-ának b) pontját és a határozattervezet (177) preambulumbekezdését.
[219] Pl. a személyi biztonsági tanúsítványról szóló német törvény 2. §-ának (3) bekezdése.
[220] A határozattervezet (212) preambulumbekezdése.
[221] A Bíróság 2013. július 18-i ítélete, Európai Bizottság és társai kontra Yassin Abdullah Kadi, C-584/10 P., C-593/10 P. és C-595/10 P. számú egyesített ügyek (a továbbiakban: az EUB Kadi II. ügyben hozott ítélete), 119. pont.

bizalmas jellegű – információk vagy bizonyítékok szolgáltatására kéri”[222], ami azt jelenti, hogy „nem lehet […] információk vagy bizonyítékok titkos vagy bizalmas jellegére hivatkozni”[223].

230. A határozattervezet (181) preambulumbekezdése értelmében a DPRC felülvizsgálja a CLPO által tett, – legalább – a CLPO vizsgálatának jegyzőkönyvén alapuló megállapításokat, valamint a panaszos, a különleges ügyvéd vagy a hírszerző ügynökség által szolgáltatott információkat és beadványokat. A határozattervezet továbbá kimondja, hogy a DPRC hozzáféréssel rendelkezik minden szükséges információhoz, amelyeket esetlegesen a CLPO-n keresztül szerez meg. Ez a főügyészi rendelet 201.9. §-ának b) pontja alapján valósul meg, amely felhatalmazza a DPRC-t, hogy „kérelmezze, hogy az ODNI CLPO a jegyzőkönyvet konkrét magyarázó vagy pontosító információkkal egészítse ki, valamint, hogy az ODNI CLPO szükség esetén további ténymegállapításokat tegyen annak érdekében, hogy a DPRC testület elvégezhessük a felülvizsgálatot”. Az EDPB értelmezése szerint a DPRC által végzett értékelés tehát semmilyen módon nem korlátozódik a CLPO által az új jogorvoslati mechanizmus első szintjén tett megállapításokra. Éppen ellenkezőleg, a DPRC további jogi információk és – ami még fontosabb – ténybeli részletek megadását is kérheti annak elemzéséhez, hogy történt-e jogsértés. Az EDPB ugyanakkor azt is megjegyzi, hogy ezek az általában széles körű vizsgálati hatáskörök nem terjednek ki a természetes személyek birtokában lévő adatokhoz való közvetlen hozzáférésre. A Bizottság kifejtette, hogy a CLPO mindig közvetítői szerepet tölt majd be, amikor a DPRC-nek további információkra lesz szüksége. Következésképpen a DPRC-nek a felülvizsgálati kérelem független elbírálásához szükséges információkhoz való hozzáférése bizonyos mértékben a szükséges információk CLPO általi rendelkezésre bocsátásán alapul. Az EDPB elismeri, hogy a CLPO köteles „minden szükséges támogatást” megadni a DPRC-nek, és a hírszerző ügynökségek kötelesek biztosítani a CLPO számára a DPRC felülvizsgálatának elvégzéséhez szükséges információkhoz való hozzáférést [224]. Ugyanakkor azt is megjegyzi, hogy maga a CLPO nem független, és a jogorvoslati eljárás első szakaszában ő folytatja le a panasz kezdeti vizsgálatát. Az EDPB ezért üdvözli, hogy a PCLOB a jogorvoslati mechanizmus éves felülvizsgálata során ellenőrizni fogja, hogy a DPRC teljes körű hozzáférést kapott-e az összes szükséges információhoz [225]. Emellett az EDPB felkéri a Bizottságot, hogy a határozattervezet elfogadása esetén foglalkozzon ezzel a kérdéssel a közös felülvizsgálatok során, megvizsgálva e rendszer hatásait.

3.2.4.3.2 Jogorvoslati hatáskörök

231. Az adatvédelmi pajzs egyik legfontosabb hiányossága, amely a Schrems II. ügyben az EUB általi érvénytelenítéséhez vezetett, az volt, hogy az ombudsman nem rendelkezik kötelező erejű jogorvoslati hatáskörrel. Az EUB megállapította, hogy „semmilyen […] utalás nincs arra vonatkozóan, hogy ezen ombudsmannak felhatalmazása lenne arra, hogy e szervezetekkel szemben kötelező erejű határozatokat hozzon”[226]. Az Egyesült Államok kormányának puszta (politikai) kötelezettségvállalása arra vonatkozóan, hogy a Hírszerző Közösség orvosolja az alkalmazandó szabályoknak az ombudsman által észlelt megsértését, nem elegendő a Charta 47. cikkében biztosítottal lényegében egyenértékű védelmi szint biztosításához.

232. Ezzel szemben az új jogorvoslati mechanizmus keretében a CLPO és a DPRC által hozott határozatok kötelező erővel bírnak[227]. Az EDPB egyrészt elismeri, hogy ez a felhatalmazás nem korlátozódik konkrét

[222] A Bíróság Kadi II. ügyben hozott ítélete, 120. pont.
[223] A Bíróság Kadi II. ügyben hozott ítélete, 125. pont.
[224] A 14086. sz. elnöki rendelet, 3 szakasza c) pontja i. alpontjának H. pontja és 3. szakasza d) pontjának iii. alpontja.
[225] A 14086. sz. elnöki rendelet, 3. szakasza e) pontjának i. alpontja.
[226] A Bíróság Schrems I. ügyben hozott ítélete, 196. pont.
[227] A 14086. sz. elnöki rendelet, 3. szakasza c) pontjának ii. alpontja és 3. szakasza d) pontjának ii. alpontja.

intézkedésekre, hanem lehetővé teszi az azonosított jogsértések „teljes körű jogorvoslatát” célzó, „megfelelő korrekciós intézkedések” alkalmazását. A 14086. sz. elnöki rendelet 4. szakaszának a) pontja kifejezetten megemlíti a jogellenesen gyűjtött adatok törlését. Másrészt az EDPB megjegyzi, hogy a 14086. sz. elnöki rendelet 4. szakasza a) pontjának megfogalmazása némi bizonytalanságot teremt az ilyen „megfelelő korrekciós intézkedések” meghatározásának folyamatát illetően. Bár az intézkedést úgy kell kialakítani, hogy teljes mértékben orvosolja a jogsértést, figyelembe kell venni azt is, hogy „az azonosított típusú jogsértéseket általában milyen módon kezelik”[228]. E követelmény jelentése és hatása nem egyértelmű. Az EDPB ezért felkéri a Bizottságot, hogy szorosan kövesse nyomon a gyakorlatban elfogadott korrekciós intézkedéseket.

3.2.4.4 Panasz benyújtása az új jogorvoslati mechanizmus keretében

233. A 14086. sz. elnöki rendelet alapján létrehozott jogorvoslati mechanizmus kizárólag az Egyesült Államok jelfelderítési tevékenységeivel kapcsolatos olyan jogszerű panaszokra alkalmazandó, amelyeket egy jogosult állam megfelelő hatósága továbbít egy jogsértéssel kapcsolatban[229]. Ezért e jogi védelem igénybevételéhez több feltételnek kell teljesülnie.

3.2.4.4.1 Jogosult államként való megjelölés

234. Először is, az az ország vagy regionális gazdasági integrációs szervezet, ahonnan az adatokat az Egyesült Államokba továbbították, a panasz alapjául szolgáló adattovábbítást megelőzően jogosult tagállami minősítést kellett, hogy kapjon[230]. Nyilvánvalóan alapvető fontosságú, hogy a biztosított jogorvoslati mechanizmus a megfelelőségi határozat hatálybalépésekor rendelkezésre álljon. Ennek megfelelően a határozattervezet (196) preambulumbekezdése úgy rendelkezik, hogy a határozat hatálybalépésének feltétele többek között az, hogy az Uniót a jogorvoslati mechanizmus tekintetében jogosult entitásnak minősítsék. Úgy tűnik ugyanis, hogy a Bizottság feltételezi, hogy a jogosultnak minősítésre a határozat elfogadása előtt sor kerül, mivel a tervezet már tartalmaz egy, az EU legfőbb ügyész általi minősítésére szolgáló üres helyet[231] (szemben azzal, hogy a minősítést a határozattervezet rendelkező részében előzetes feltételként szabnák meg).

3.2.4.4.2 Az adatvédelem és a polgári szabadságjogok érdekeire, valamint a „kereshetőségre” gyakorolt hátrányos hatás

235. A „jogszerű panasznak” egy állítólagos „jogsértésen” kell alapulnia, ami viszont olyan jogsértést feltételez, mely hátrányosan érinti a panaszos adatvédelemhez és polgári szabadságjogokhoz fűződő érdekeit[232]. Az EDPB a Bizottságtól kapott kiegészítő magyarázatok alapján úgy értelmezi, hogy a „hátrányos hatás” a panasz elfogadhatóságának szempontjából semmilyen korlátozást nem jelent. Ehelyett, amint azt a Bizottság megállapította, az ilyen hátrányos hatás a 4. szakasz d) pontjának iii. alpontjában említett rendelkezéseket, például a 14086. sz. elnöki rendelet biztosítékait sértő, jelfelderítési tevékenységek céljából végzett személyesadat-kezeléssel kapcsolatos minden panaszra érvényes. Az EDPB sajnálatát fejezi ki amiatt, hogy ez nem szerepel a határozattervezet szövegében, és felkéri a Bizottságot, hogy pontosítsa a „hátrányos érintettség” fogalmát annak biztosítása érdekében, hogy az érintettek jogainak bármilyen megsértése értékelésre és orvoslásra kerüljön,

[228] A 14086. sz. elnöki rendelet 4. szakaszának a) pontja.
[229] A 14086. sz. elnöki rendelet 3. szakaszának a) pontja.
[230] A 14086. sz. elnöki rendelet, 4. szakasza d) pontjának i. alpontja és 4. szakasza k) pontjának i. alpontja.
[231] A határozattervezet 320. lábjegyzete.
[232] A 14086. sz. elnöki rendelet, 4. szakasza k) pontjának i. alpontja és 4. szakasza d) pontjának ii. alpontja.

valamint, hogy ne legyen olyan „súlyossági” szint, amelyet bizonyítani kellene a jogorvoslathoz és a megfelelő jóvátételhez való hozzáféréshez.

236. Amint az már említésre került, a 14086. sz. elnöki rendelet szerinti panasz nem követeli meg a panaszostól a kereshetőségi jog bizonyítását (lásd:. 215. bekezdés)[233]. Az Európai Adatvédelmi Testület üdvözli a 14086. sz. elnöki rendelet 4. szakaszának k) pontjában szereplő pontosítást, amely szerint „meggyőződési tesztet” alkalmaznak majd, és nem szükséges bizonyítani, hogy a panaszos adataihoz valóban hozzáfértek jelfelderítési tevékenységek révén. A jogorvoslati mechanizmus létrehozása fontos lépés, mivel a kereshetőség követelménye nagyon megnehezíti a megfigyelési intézkedések megtámadását az Egyesült Államok rendes bíróságai előtt.

237. A fentiek alapján az EDPB úgy véli, hogy a határozattervezetben is említett[234] rendes bíróságokhoz fordulás nem nyújtana megfelelő szintű védelmet[235]. E tekintetben az Európai Adatvédelmi Testület emlékeztet a rendes bíróságok előtti kereshetőségi joggal kapcsolatban már többször kifejezett aggályaira[236]. Ezenkívül az Európai Adatvédelmi Testület az Egyesült Államok kormányának további nyilatkozatai alapján úgy értelmezi, hogy bár a 14086. sz. elnöki rendelet nem zárja ki a rendes bíróságokhoz fordulást, bizonytalan, hogy egy ilyen bíróság hogyan alkalmazná ezt a rendeletet. A határozattervezet elfogadása esetén ezt a kérdést a jövőbeli felülvizsgálatok során tovább lehetne vizsgálni.

3.2.4.4.3 Panasztételi eljárás

238. Az EDPB alapelvként támogatja a panaszok a tagállamok felügyeleti hatóságain keresztül történő továbbítására vonatkozó eljárást, és továbbra is úgy véli, hogy a panaszos azonosításának az EU területén kell megtörténnie. Az adatvédelmi pajzs ombudsmani mechanizmusához hasonlóan azonban a határozattervezet előírja, hogy az ilyen panaszt benyújtani kívánó érintettnek a panaszt egy uniós tagállam olyan felügyeleti hatóságához kell benyújtania, amely felügyeleti hatáskörrel rendelkezik a nemzetbiztonsági szolgálatok és/vagy a személyes adatok hatóságok általi kezelése tekintetében[237]. E tekintetben az Európai Adatvédelmi Testület emlékeztet a 29. cikk szerinti munkacsoport adatvédelmi pajzsról szóló véleményében már kifejtett aggályaira, például arra, hogy nemzetbiztonsági szolgálatok felügyeletére létrehozott tagállami mechanizmusok sokfélesége miatt a természetes személyek nehézségekbe ütközhetnek az illetékes hatóság azonosításában[238]. Figyelembe véve a nemzeti adatvédelmi hatóságok szerepét az EU-USA adatvédelmi keretének alkalmazásában és felügyeletében, helyénvalóbb e panaszokat rajtuk keresztül továbbítani.

3.2.4.5 A DPRC határozata

239. A panaszos kérelmének felülvizsgálatát követően a DPRC nem fedheti fel, hogy a panaszos egyesült államokbeli jelfelderítési tevékenységek tárgyát képezte-e vagy sem. Ehelyett a panaszost arról tájékoztathatják, hogy „a felülvizsgálat nem tárt fel jogsértést, vagy az Adatvédelmi Felülvizsgálati Bíróság olyan határozatot hozott, amely megfelelő jogorvoslatot tesz szükségessé”[239]. Ez a szabványos válasz az Egyesült Államok hírszerzési tevékenységeivel kapcsolatos érzékeny információk védelmének

[233] Clapper kontra Amnesty International USA, 568 U.S. 398 (2013) II., 10. o.
[234] A határozattervezet (187) és azt követő preambulumbekezdései.
[235] Lásd a Bíróság Schrems II. ügyben hozott ítéletének 191. és 192. pontját.
[236] Lásd a 29. cikk szerinti munkacsoport 01/2016. sz. véleményét, 43. o.
[237] A határozattervezet (169) preambulumbekezdése.
[238] A 29. cikk szerinti munkacsoport 01/2016. sz. véleménye, 48–49. o.
[239] A 14086. sz. elnöki rendelet, 3. szakasza d) pontja i. alpontjának H. pontja. A 14086. sz. elnöki rendelet ezt a választ a CLPO-ra is meghatározza.

általánosan törvényes célját szolgálja. Az EDPB azonban aggodalmát fejezi ki amiatt, hogy a 14086. sz. elnöki rendelet semmilyen mentességet nem biztosít a DPRC szabványos válasza alól.

240. A Kadi II. ügyben az EUB-nak egyrészt az államtitok összeférhetetlenségével, másrészt a tisztességes és lehetőségekhez mérten kontradiktórius eljárásokkal kellett foglalkoznia. Az EUB kimondta, hogy olyan körülmények között, amikor a nemzetbiztonsággal összefüggő kényszerítő megfontolások kizárják az információknak vagy bizonyítékoknak az érintett személlyel való közlését, a bíróságok feladata, hogy a bírósági felülvizsgálat során olyan technikákat alkalmazzanak, amelyek figyelembe veszik az információ jellegére és forrásaira vonatkozó jogszerű biztonsági megfontolásokat, valamint azt a szükségletet, hogy a jogalanynak kellően biztosítsák az eljárási jogai – mint a meghallgatáshoz való jog és a kontradiktórius eljárás elve – tiszteletben tartását[240]. Az EUB továbbá pontosította, hogy az Európai Unió illetékes hatósága által szolgáltatott jogi és ténybeli bizonyítékok összességének vizsgálata során a bíróságok feladata annak meghatározása, hogy megalapozottak-e az e hatóság által a adatközlés megtagadásának indokaként felhozott okok[241]. Ha bebizonyosodik, hogy az Európai Unió illetékes hatósága által hivatkozott okok valóban kizárják az információk vagy bizonyítékok az érintett személlyel való közlését, akkor is megfelelő egyensúlyt kell teremteni a hatékony bírói jogvédelemhez való joghoz kapcsolódó, valamint a nemzetbiztonságból eredő követelmények között[242]. Ilyen mérlegelés céljából olyan lehetőségekhez lehet fordulni, mint a szóban forgó információk vagy bizonyítékok tartalmáról szóló összefoglaló közlése[243]. Habár a Bíróság megállapításai nem írnak elő követelményeket a bíróságok által hozott határozat vonatkozásában, hanem inkább az illetékes hatóság határozatára és a bírósági eljárás lefolytatására vonatkoznak, utalnak a fent említett érdekeknek a hatékony bírói jogvédelemhez való joggal összefüggésben történő mérlegelésére. További iránymutatásként hivatkozni lehet a Big Brother Watch-ügyre is, amelyben az EJEB az eljárás tisztességességére és különösen a kontradiktórius eljárás elvére hivatkozva megállapította, hogy a bírósági vagy más módon független szerv döntéseit indokolni kell[244].

241. Az Európai Adatvédelmi Testület elismeri, hogy a DPRC határozatai valóban indokoltak. A DPRC kifejezetten köteles olyan írásbeli határozatot kiadni, amely tartalmazza a megállapításait és a megfelelő jogorvoslat pontos leírását[245]. Emellett az Európai Adatvédelmi Testület megjegyzi, hogy az egyént értesítik, ha a DPRC általi felülvizsgálattal kapcsolatos információk titkosítását feloldják[246]. Az EDPB elismeri továbbá az új jogorvoslati mechanizmusban szereplő különleges ügyvédek szerepét, amely magában foglalja a panaszos ügyhöz fűződő érdekének előmozdítását is[247]. Az EUB és az EJEB fent ismertetett ítélkezési gyakorlatának következményeire tekintettel, valamint figyelembe véve, hogy a DPRC határozata végleges, és az ellen fellebbezni nem lehet[248], az Európai Adatvédelmi Testületnek aggályai vannak a DPRC szabványos válaszának általános alkalmazásával kapcsolatban. Az EDPB emlékeztet arra, hogy a PCLOB független módon fogja felülvizsgálni az új jogorvoslati mechanizmus működését, és felkéri a Bizottságot, hogy a határozat elfogadása esetén a jövőbeli felülvizsgálatok során fordítson különös figyelmet erre a kérdésre, beleértve a PCLOB e szempontra vonatkozó értékelését is.

[240] A Bíróság Kadi II. ügyben hozott ítélete, 125. pont.
[241] A Bíróság Kadi II. ügyben hozott ítélete, 126. pont.
[242] A Bíróság Kadi II. ügyben hozott ítélete, 128. pont.
[243] A Bíróság Kadi II. ügyben hozott ítélete, 129. pont.
[244] Az EJEB Big Brother Watch ügyben hozott ítéletének 359. pontja.
[245] A főügyészi rendelet 201.9. §-ának g) pontja.
[246] A 14086. sz. elnöki rendelet 3. szakasza d) pontjának v. alpontja.
[247] A főügyészi rendelet 201.8. §-ának g) pontja.
[248] A főügyészi rendelet 201.9. §-ának g) pontja.

4 A HATÁROZATTERVEZET VÉGREHAJTÁSA ÉS NYOMON KÖVETÉSE

242. A határozattervezet nyomon követését és felülvizsgálatát illetően az EDPB megjegyzi, hogy az EUB ítélkezési gyakorlata szerint „tekintettel arra, hogy a harmadik ország által biztosított védelmi szint változhat, a Bizottságnak, azt követően, hogy az [általános adatvédelmi rendelet 45. cikke] alapján megfelelőségi határozatot fogadott el, rendszeresen meg kell vizsgálnia, hogy a szóban forgó harmadik ország által biztosított védelem megfelelő szintjére vonatkozó megállapítás továbbra is ténybelileg és jogilag igazolt-e. Ezen vizsgálat minden esetben szükséges, amikor a valószínűsítő körülmények alapján kétségek merülhetnek fel e tekintetben”[249].

243. Emellett az Európai Adatvédelmi Testület megjegyzi, hogy a DoC nyilatkozata értelmében a DoC és adott esetben más amerikai ügynökségek rendszeres üléseket tartanak a Bizottsággal, az érdekelt uniós adatvédelmi hatóságokkal és az Európai Adatvédelmi Testület megfelelő képviselőivel[250].

244. Az Európai Adatvédelmi Testület úgy véli, hogy az állami jog védelme a bűnüldöző hatóságok adatokhoz való hozzáférésével összefüggésben, az Egyesült Államok nemzetbiztonsági hatóságai általi célzott adatgyűjtés okán történő ideiglenes tömeges adatgyűjtésre vonatkozó eltérés, a szükségesség és arányosság újonnan bevezetett elveinek gyakorlati alkalmazása, többek között az UPSTREAM programmal összefüggésben, a 14086. sz. elnöki rendelet és az olyan különböző egyesült államokbeli jogi eszközök közötti kölcsönhatás, amelyek lehetővé teszik az amerikai hírszerző ügynökségek számára a személyes adatok gyűjtését és további feldolgozását, a belső szabályzatok és eljárások végrehajtása, az, hogy ezeket a biztosítékokat hogyan veszik figyelembe a FISC által irányított felügyelet keretében, és a jogorvoslati mechanizmus hatékonyan működési módjai, valamint az újbóli adattovábbítást, az automatizált döntéshozatalt, a adatvédelmi keret elveinek érdemi és hatékony felügyeletét és érvényesítését, illetve a hatékony jogorvoslatot érintő kérdések különleges figyelmet érdemelnek a következő időszakos felülvizsgálatok során.

245. Az EDPB megjegyzi, hogy a megfelelőségre vonatkozó megállapítások felülvizsgálatára a megfelelőségi határozatról szóló tagállami értesítés időpontjától számított egy év elteltével, majd azt követően legalább négyévente kerül sor[251]. A megfelelőségi határozat folyamatos nyomon követésének további megerősítése érdekében az Európai Adatvédelmi Testület felkéri a Bizottságot, hogy legalább háromévente végezze el a későbbi felülvizsgálatokat.

246. Ami az EDPB-nek és képviselőinek a jövőbeli időszakos felülvizsgálatok előkészítésében és lefolytatásában való gyakorlati részvételét illeti, az Európai Adatvédelmi Testület megismétli, hogy a releváns dokumentumokat – a levélváltásokat is beleértve – a felülvizsgálatok előtt kellő időben, írásban meg kell osztani az Európai Adatvédelmi Testülettel. Az adatvédelmi pajzs keretében végzett felülvizsgálatokhoz hasonlóan az Európai Adatvédelmi Testület azt javasolja, hogy legkésőbb három hónappal a felülvizsgálat megkezdése előtt a Bizottság, az Egyesült Államok kormánya és az Európai Adatvédelmi Testület határozza meg és fogadja el a felülvizsgálat módozatait.

247. Az Európai Adatvédelmi Testület továbbá megjegyzi és üdvözli, hogy a határozattervezet (212) preambulumbekezdése példákat hoz a védelem szintjét aláásó olyan módosításokra, amelyek indokolhatják egy olyan „sürgősségi hatályon kívül helyezési eljárás” megindítását, amely a 14086. sz.

[249] A Bíróság Schrems I. ügyben hozott ítélete, 76. pont. Lásd még a határozattervezet 3. cikkének (4) bekezdését.
[250] A határozattervezet III. melléklete.
[251] A határozattervezet 3. cikkének (4) bekezdése.

elnöki rendelettel és a kapcsolódó főügyészi rendelettel kapcsolatos esetleges módosításokra összpontosít.

Az Európai Adatvédelmi Testület részéről

az Elnök

(Andrea Jelinek)