YVES BOT
FŐTANÁCSNOK INDÍTVÁNYA
Az ismertetés napja: 2015. szeptember 23.[1]

C-362/14. sz. ügy

Maximillian Schrems
kontra
Data Protection Commissioner

(a High Court of Ireland [Írország] által benyújtott előzetes döntéshozatal iránti kérelem)

„Előzetes döntéshozatal iránti kérelem — Személyes adatok — Az egyének védelme az ilyen adatok kezelése vonatkozásában — Az Európai Unió Alapjogi Chartája — 7., 8. és 47. cikk — 95/46/EK irányelv — 25. cikk — 2000/520/EK határozat — Személyes adatok továbbítása az Egyesült Államokba — A védelmi szint megfelelőségének megítélése — Olyan természetes személy által benyújtott panasz, akinek a személyes adatait harmadik országba továbbították — Nemzeti felügyelő hatóság — Hatáskörök”

I – **Bevezetés**

1. Amint az Európai Bizottság 2013. november 27-i közleményében[2] megállapította, „[a] személyes adatok továbbítása a transzatlanti kapcsolatok fontos és szükséges eleme. Szerves részét képezi az Atlanti-óceánon átnyúló kereskedelmi forgalomnak, ideértve az egyre növekvő olyan digitális vállalkozásokat, mint például a közösségi média vagy a számítási felhők, amelyek révén nagy mennyiségű adat áramlik az EU-ból az Egyesült Államokba”[3].

2. A kereskedelmi forgalommal foglalkozik a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő” adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló, 2000. július 26-i 2000/520/EK bizottsági határozat.[4] Ez a határozat jogalapot biztosít a személyes adatoknak az Unióból az Egyesült Államokban székhellyel rendelkező azon vállalatok számára történő továbbításához, amelyek betartják a védett adatkikötőre vonatkozó elveket.

3. Az említett határozatnak napjainkban azzal a kihívással is szembe kell néznie, hogy az Unió és az Egyesült Államok közötti adatforgalmat az ezen adatok magas szintű védelmének biztosítása mellett tegye lehetővé, amint azt az uniós jog megköveteli.

1 — Eredeti nyelv: francia.

2 — A Bizottságnak az Európai Parlamenthez és a Tanácshoz intézett, „A bizalom helyreállítása az EU-USA adatáramlások tekintetében” című közleménye (COM(2013) 846 final).

3 — 2. o.

4 — HL L 215., 7. o.; magyar nyelvű különkiadás 16. fejezet, 1. kötet, 119. o.

4. Nemrég ugyanis néhány kiszivárogtatott információ jelentős méretű amerikai hírszerzési programok létére derített fényt. Ezek a kiszivárogtatások vitát indítottak a személyes adatoknak az Egyesült Államokban székhellyel rendelkező vállalatok számára történő továbbítására vonatkozó uniós jogi normák tiszteletben tartására és a biztonságos kikötő rendszerének gyengeségeire vonatkozóan.

5. A jelen előzetes döntéshozatal iránti kérelemben annak pontosítására kérték fel a Bíróságot, hogy milyen eljárást kövessenek a nemzeti felügyelő hatóságok és a Bizottság, amikor a 2000/520 határozat alkalmazása során működési zavarokkal találkoznak.

6. A személyes adatok feldolgozása [helyesen: kezelése] vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv [5] IV. fejezete meghatározza a személyes adatok harmadik országokba irányuló továbbítására vonatkozó szabályokat.

7. Ebben a fejezetben, az ezen irányelv 25. cikkének (1) bekezdésében felállított alapelv szerint a [helyesen: kezelésre] kerülő vagy továbbítás után feldolgozásra szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha az adott harmadik ország ezeknek az adatoknak megfelelő védelmi szintet tud biztosítani [helyesen: biztosít].

8. Ezzel szemben, amint arra az uniós jogalkotó az említett irányelv (57) preambulumbekezdésében rámutat, a személyes adatoknak a megfelelő védelmi szintet biztosítani nem tudó harmadik országokba irányuló továbbítását meg kell tiltani.

9. A 95/46 irányelv 25. cikkének (2) bekezdése értelmében „[a] harmadik ország által nyújtott védelem szintjének megfelelő mivoltát az adattovábbítási művelet vagy adattovábbítási műveletsorozat feltételeinek figyelembevételével kell értékelni; különös figyelmet kell fordítani az adatok jellegére, a tervezett adatfeldolgozási művelet vagy műveletek céljára és időtartamára, a kiindulási és a célországra, az adott harmadik országban hatályos, általános és ágazati jogrendre, valamint az adott országban érvényesülő szakmai szabályokra és biztonsági intézkedésekre”.

10. Ezen irányelv 25. cikkének (6) bekezdése értelmében a Bizottság megállapíthatja, hogy a harmadik ország biztosítja-e a személyes adatok megfelelő védelmi szintjét belföldi joga, vagy a vállalt nemzetközi kötelezettségei alapján. Amennyiben a Bizottság ilyen értelmű határozatot hoz, sor kerülhet a személyes adatoknak az érintett harmadik országba való továbbítására.

11. E rendelkezés végrehajtása érdekében a Bizottság elfogadta a 2000/520 határozatot. E határozat 1. cikkének (1) bekezdése szerint a „gyakran felvetődő kérdések” [6] által biztosított útmutatással összhangban bevezetett „»biztonságos kikötő« adatvédelmi elvek” úgy tekintendők, mint amelyek biztosítják az Unióból az Egyesült Államokban letelepedett vállalkozások számára továbbított személyes adatok megfelelő védelmi szintjét.

12. Következésképpen a 2000/520 határozat engedélyezi a személyes adatok továbbítását a tagállamokból az Egyesült Államokban letelepedett olyan vállalkozások számára, amelyek vállalják a biztonságos kikötő elveinek betartását.

13. A 2000/520 határozat I. mellékletében meghatároz néhány alapelvet, amelyekhez a vállalkozások önkéntes alapon csatlakozhatnak, korlátozások és különleges felügyeleti rendszer vállalása mellett. A „magatartási kódexnek” tekinthető elvekhez csatlakozó vállalkozások száma 2013-ban meghaladta a 3200-at.

5 — HL L 281., 31. o.; magyar nyelvű különkiadás 13. fejezet, 15. kötet, 355. o.

6 — Frequently asked questions (gyakran felvetődő kérdések), a továbbiakban: GYFK.

14. A biztonságos kikötő rendszere egy olyan megoldáson alapul, amely ötvözi a magánvállalkozások által végzett öntanúsítást és önértékelést, valamint a közhatalmi szervezetek beavatkozását.

15. A biztonságos kikötő elveit az „iparral és a nyilvánossággal konzultálva a kereskedelem, illetve az Egyesült Államok és az […] Unió közötti nemzetközi kereskedelem megkönnyítése érdekében dolgozták ki. Az elveket csak az Egyesült Államok olyan szervezeteinek használatára szánták, amelyek az […] Unióból személyes adatokat fogadnak, a »biztonságos kikötő« és az általa létrehozott »megfelelőségi« minősítés elnyerése céljából”[7].

16. A biztonságos kikötő elvei, amelyeket a 2000/520 határozat I. melléklete tartalmaz, többek között az alábbiakat írják elő:

– tájékoztatási kötelezettséget, mely szerint „[a] szervezetnek tájékoztatnia kell az egyéneket azokról a célokról, amelyek érdekében a rájuk vonatkozó információt gyűjti és használja; arról, hogy kérdéseikkel vagy panaszukkal hogyan léphetnek kapcsolatba a szervezettel; a harmadik felek típusairól, amelyeknek átadja az adatokat; valamint a választási lehetőségekről és eszközökről, amelyeket a szervezet az egyéneknek az adatok felhasználásának és nyilvánosságra hozatalának korlátozására felkínál. Ezt a tájékoztatást […] az első alkalommal akkor [kell megadni], amikor az egyéneket felkérik a személyes információ szolgáltatására a szervezetnek, vagy azt követően a lehető leghamarabb, de minden esetben azt megelőzően, hogy a szervezet az ilyen információt más célra használná fel, mint amelyre az adatokat átadó szervezet eredetileg gyűjtötte vagy kezelte, vagy mielőtt harmadik félnek azokat először átadná”;[8]

– a szervezetek arra vonatkozó kötelezettségét, hogy választási lehetőséget kínáljanak fel az egyéneknek, hogy személyes adataikat a) átadják-e harmadik félnek; vagy b) felhasználják-e olyan célra, amely nem összeegyeztethető azzal (azokkal) a céllal (célokkal), amelyre eredetileg gyűjtötték az adatokat, vagy amelyet az egyén a későbbiekben engedélyezett. Különleges adatok esetén „megerősítő vagy kifejezett választási lehetőséget (a kívánt lehetőség kiválasztásával) kell kapniuk, ha az információt harmadik fél számára átadják, vagy a gyűjtés eredeti céljától, illetve az egyén által a választási lehetőségével élve a későbbiekben engedélyezett céltól eltérő célra használják fel.”[9];

– az adatok későbbi továbbítására vonatkozó szabályokat. Így „[a]hhoz, hogy az információt harmadik fél számára átadhassák, a szervezeteknek alkalmazniuk kell az értesítés és a választási lehetőség elveit”[10];

– az adatok biztonságával kapcsolatosan azon kötelezettséget, mely szerint „[a] személyes információt létrehozó, fenntartó, felhasználó vagy terjesztő szervezeteknek megfelelő intézkedéseket kell tenniük, hogy megóvják az információt az elvesztéstől, a hibás felhasználástól és a jogtalan hozzáféréstől, a nyilvánosságra hozataltól, a megváltoztatástól és a megsemmisítéstől”[11];

– az adatok integritásával összefüggésben a szervezetek kötelezettségét, mely szerint „megfelelő lépéseket kell tenni[ük] annak biztosítására, hogy az adatok a tervezett felhasználás szempontjából megbízhatók, pontosak, teljesek és időszerűek legyenek”[12];

7 — A 2000/520 határozat I. mellékletének második bekezdése.

8 — Lásd: I. melléklet „Értesítés” alcíme.

9 — Lásd: I. melléklet „Választási lehetőség” alcíme.

10 — Lásd az I. melléklet „Adattovábbítás harmadik fél részére” alcímét.

11 — Lásd az I. melléklet „Biztonság” alcímét.

12 — Lásd az I. melléklet „Adatintegritás” alcímét.

– azt, hogy azok a személyek, akiknek vagy amelyeknek az adatai valamely szervezet birtokában vannak, általános szabályként „hozzáféréssel rendelkez[zenek] [ezekhez az] információhoz, és lehetőségük kell, hogy legyen a pontatlan információk javítására, módosítására vagy törlésére” [13];

– kötelezettséget arra, hogy biztosítsák „az elvek teljesítését biztosító mechanizmusokat, a jogorvoslati jogot az elvek nem teljesítése által érintett egyének számára, valamint a szervezetre vonatkozó következményeket, amikor az elveket nem követik” [14].

17. Annak az amerikai szervezetnek, amely csatlakozni kíván a biztonságos kikötő elveihez, adatvédelmi politikájában fel kell tüntetnie, hogy az elvek elfogadását nyilvánosan közzéteszi, ezeknek ténylegesen megfelel, és ezt önmaga tanúsítja az Egyesült Államok Kereskedelmi Minisztériuma felé. [15]

18. A szervezeteknek több eszköz is rendelkezésükre áll ahhoz, hogy megfeleljenek a biztonságos kikötő elveinek. Így például „csatlakoz[hatnak] egy olyan önszabályozó adatvédelmi programhoz, amely elfogadja az elveket, [vagy] saját önszabályozó adatvédelmi politikájuk kidolgozásával, feltéve hogy politikájuk megfelel az elveknek. […] Ezen túlmenően, a hatósági, szabályozó, közigazgatási vagy más jogi szerv (vagy szabályok) hatálya alá tartozó szervezetek, amelyek hatékonyan védik a személyes adatokat, szintén jogot szerezhetnek a »biztonságos kikötő« cím előnyeire.” [16]

19. A választottbíróság és az állami hatóságok által ellátott felügyelet intézményét ötvöző többféle eszköz létezik annak ellenőrzésére, hogy betartják-e a biztonságos kikötő elveit. A felügyeletet így biztosítható a jogviták független harmadik fél által bírósági eljáráson kívül történő rendezésére szolgáló rendszer révén. Másfelől a vállalkozások vállalhatják, hogy együttműködnek az európai adatvédelmi bizottsággal. Végezetül a panaszok elintézésére a Szövetségi Kereskedelmi Bizottságról szóló törvény (Federal Trade Commission Act) 5. szakaszában ráruházott jogkörében a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission, a továbbiakban: FTC) és az Egyesült Államok Szövetségi Törvénykönyvének (United States Code) 49. címében szereplő 41 712. szakaszában ráruházott jogkörében a Közlekedési Minisztérium (Department of Transportation) rendelkezik hatáskörrel.

20. A 2000/520 határozat I. mellékletének negyedik bekezdése alapján a biztonságos kikötő elveihez való csatlakozást korlátozhatják többek között „a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményei” és „törvény, kormányrendelet vagy precedensjog […], amelyek az elvekkel ellentétes kötelezettségeket vagy kifejezett felhatalmazásokat hoznak létre, feltéve hogy bármilyen ilyen felhatalmazás gyakorlása során a szervezet bizonyítani tudja, hogy az elvek nem teljesítése az ilyen felhatalmazás által támogatott törvényes érdekek teljesítéséhez szükséges mértékre korlátozódik” [17].

21. Továbbá a tagállamok illetékes hatóságainak az adatforgalom felfüggesztésére vonatkozó lehetősége több feltételhez kötött, amelyeket a 2000/520 határozat 3. cikkének (1) bekezdése szabályoz.

22. A jelen előzetes döntéshozatal iránti kérelem a 2000/520 határozat terjedelmének az Európai Unió Alapjogi Chartája (a továbbiakban: Charta), 7., 8. és 47. cikke, valamint a 95/46 irányelv 25. cikkének (6) bekezdése és 28. cikke alapján történő értelmezésére irányul. Ezt a kérelmet a M. Schrems és a Data Protection Commissioner (adatvédelmi biztos, a továbbiakban: Commissioner) között folyó jogvitában terjesztették elő, amelynek tárgya a M. Schrems által a Facebook Ireland Ltd. (a továbbiakban: Facebook Ireland) ellen, a felhasználók személyes adatainak az Egyesült Államokban található szervereken történő tárolása miatt benyújtott panasz kivizsgálásának elutasítása.

13 — Lásd az I. melléklet „Hozzáférés” alcímét.

14 — Lásd az I. melléklet „Végrehajtás” alcímét.

15 — A 2000/520 határozat 1. cikkének (2) és (3) bekezdése. Lásd még: II. melléklet, 6. GYFK.

16 — Az I. melléklet harmadik bekezdése.

17 — Lásd a IV. melléklet B. alcímét.

23. M. Schrems Ausztriában lakóhellyel rendelkező osztrák állampolgár. 2008 óta felhasználója a Facebook közösségi hálónak.

24. Az Unió területén lakó valamennyi Facebook-felhasználónak alá kell írnia egy szerződést a Facebook Irelanddel, az amerikai anyavállalat, a Facebook Inc. (a továbbiakban: Facebook USA) leányvállalatával. Az Facebook Ireland Unió területén lakóhellyel rendelkező felhasználóira vonatkozó adatokat részben vagy egészben a Facebook USA Egyesült Államokban található szervereire továbbítják és ott tárolják.

25. 2013. június 25-én M. Schrems panaszt nyújtott be a Commissionerhöz, amelyben lényegében azzal érvelt, hogy az Egyesült Államok joga és gyakorlata nem biztosít az Egyesült Államokban tárolt adatok számára valódi védelmet az állami felügyelettel szemben. Mindez az E. Snowden által 2013. májusától kezdődően az amerikai hírszerző szolgálatoknak, és különösen a National Security Agencynek (Nemzetbiztonsági Ügynökség, a továbbiakban: NSA) tevékenységére vonatkozóan kiszivárogtatott információkból derült ki.

26. E kiszivárogtatásokból többek között kiderül, hogy az NSA „PRISM” néven egy olyan programot hozott létre, amelynek keretében ezen ügynökség tömeges szabad hozzáférést kapott az Egyesült Államok szerverein tárolt adatokhoz, amelyeket számos, az internet és a technológia területén tevékenykedő, a Facebook USA-hoz hasonló vállalkozás birtokolt vagy felügyelt.

27. A Commissioner úgy ítélte meg, hogy a panaszt nem köteles kivizsgálni, mivel az jogilag megalapozatlan. Véleménye szerint nem volt bizonyíték arra, hogy az NSA hozzáférhetett M. Schrems adataihoz. Emellett a panaszt szerinte a 2000/520 határozat értelmében el kell utasítani, mivel ebben a Bizottság megállapította, hogy az Egyesült Államok a biztonságos kikötő rendszerének keretében megfelelő védelmi szintet biztosít a továbbított személyes adatok számára. Az Egyesült Államokban folytatott adatvédelem megfelelőségére vonatkozóan felmerülő bármilyen kérdést e határozattal összhangban kell megválaszolni, és ez kizárja a panaszban felvetett probléma kivizsgálását.

28. A Commissioner a panaszt az alábbi nemzeti jogszabályok alapján utasította el.

29. Az adatvédelemről szóló 2003. évi adatvédelmi törvénnyel (Data Protection Act 2003) módosított, 1988. évi adatvédelmi törvény (Data Protection [Amendment] Act 1988, a továbbiakban adatvédelmi törvény) 10. cikkének (1) bekezdése, amely felhatalmazza a Commissionert a panaszok kivizsgálására, kimondja:

„a) A Commissioner megvizsgálhatja vagy megvizsgáltathatja, hogy sérülnek-e vagy sérülhetnek-e a jelen törvény rendelkezései egy adott személlyel kapcsolatban, akár azért, mert ez a személy panaszt nyújtott be hozzá e rendelkezések valamelyikének megsértése miatt, akár azért, mert a Commissioner úgy ítéli meg, hogy fennállhat ilyen jogsértés.

b) A Commissioner, amennyiben valaki panaszt nyújt be előtte a jelen bekezdés a) pontja értelmében,

i. kivizsgálja, vagy kivizsgáltatja a panaszt, kivéve ha az jelentéktelen vagy zaklató, és

ii. ha észszerű időn belül az érintett felek alternatív vitarendezéssel nem oldják meg a panaszt, írásban értesíti a panaszost az e tárgyban hozott határozatáról, egyben tájékoztatja, hogy ha e határozatot sérelmesnek tartja, a jelen törvény 26. cikke alapján fellebbezést nyújthat be e határozattal szemben a kézhezvételétől számított 21 napon belül”.

30. A jelen ügyben a Commissioner arra a következtetésre jutott, hogy M. Schrems panasza „jelentéktelen és zaklató”, mivel jogi megalapozottság hiányában el kell utasítani. Ezért megtagadta e panasz kivizsgálását.

31. Az adatvédelmi törvény 11. cikke szabályozza a személyes adatok nemzeti területen kívülre történő továbbítását. E törvény 11. cikke (2) bekezdésének a) pontja előírja, hogy:

„Amikor a jelen törvény hatálya alá tartozó eljárás során kérdés merül fel,

i. annak meghatározása érdekében, hogy a jelen cikk (1) bekezdésében meghatározott megfelelő védelmi szintet biztosítja-e az Európai Gazdasági Térség [(EGT)] területén kívüli ország vagy terület, ahová a személyes adatok továbbításra kerülnek, és

ii. uniós megállapításra került sor a szóban forgó továbbítás típusát illetően,

a kérdést e megállapítással összhangban kell kezelni”.

32. Az adatvédelmi törvény 11. cikke (2) bekezdésének b) pontja az uniós megállapítás fogalmát az alábbiakban határozza meg

„A jelen bekezdés a) pontjában szereplő »uniós megállapítás« azon megállapítást jelenti, amelyet a […] Bizottság a [95/46] irányelv 25. cikkének (4) vagy (6) bekezdése céljából [az ezen irányelv] 31. cikkének (2) bekezdésében foglalt eljárás keretében annak meghatározása érdekében tett, hogy a jelen cikk (1) bekezdésében meghatározott megfelelő védelmi szintet biztosítja-e valamely [EGT]-n kívüli ország vagy terület.”

33. A Commissioner megállapította, hogy a 2000/520 határozat az adatvédelmi törvény 11. cikke (2) bekezdésének a) pontja értelmében vett „uniós megállapítás”, így e törvény alapján e megállapítással összhangban kell megválaszolni minden, a továbbítás helye szerinti harmadik országban biztosított adatvédelem megfelelőségére vonatkozóan felmerülő kérdést. Mivel M. Schrems panaszának ez volt a lényege – nevezetesen az, hogy a személyes adatokat olyan harmadik országba továbbították, amely a gyakorlatban nem biztosít megfelelő védelmi szintet – a Commissioner úgy vélte, hogy e kérdés vizsgálata a biztonságos kikötőről szóló határozat jellegénél és léténél fogva kizárt.

34. M. Schrems a Commissioner által hozott, panaszát elutasító határozattal szemben keresetet nyújtott be a High Court of Ireland előtt. E bíróság, miután megvizsgálta az alapeljárásban benyújtott bizonyítékokat, megállapította, hogy a személyes adatok elektronikus megfigyelése és lehallgatása szükségszerű és alapvető közérdekű célokat szolgál, nevezetesen a nemzetbiztonság védelmét és a súlyos bűncselekmények megelőzését. A High Court of Ireland e tekintetben megjegyezte, hogy az Unióból az Egyesült Államokba továbbított személyes adatok megfigyelése és lehallgatása jogszerű terrorizmusellenes célokat követ.

35. Ugyanezen bíróság szerint az E. Snowden által kiszivárogtatott információk ugyanakkor az NSA és a hasonló hatóságok részéről fennálló jelentős túlkapásokat mutatnak. Bár az Egyesült Államokban a Foreign Intelligence Surveillance Court (a külföldi titkosszolgálatok felügyeleti ügyeiben eljáró bíróság, a továbbiakban: FISC) az 1978-as külföldi hírszerzői tevékenység megfigyeléséről szóló törvény (Foreign Intelligence Surveillance Act of 1978) [18] keretében felügyeli e területet, mindezt *ex parte* és titkos módon teszi. Ráadásul azon túl, hogy a személyes jogokhoz való hozzáférésre vonatkozó határozatokat az amerikai jog alapján hozzák meg, az uniós polgárok nem rendelkeznek tényleges meghallgatáshoz való joggal az adataik megfigyelésére és lehallgatására vonatkozó kérdésekkel kapcsolatban.

18 — Lásd ennek, a 2008. évi törvénnyel (Foreign Intelligence Surveillance Act of 2008) módosított törvénynek a702. szakaszát. E szakasz alkalmazásában működteti az NSA a „PRISM” néven ismert adatbázisát (lásd: Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 2013. november 27.).

36. A jelen eljárásban benyújtott, eskü alatt tett nyilatkozatokban szereplő részletes dokumentumokból egyértelmű, hogy nem vitatott az E. Snowden által kiszivárogtatott információk legtöbbjének helytállósága. A High Court of Ireland ennek megfelelően megállapította, hogy a személyes adatok Egyesült Államokba való továbbítását követően az NSA és más szövetségi ügynökségek, mint például a Federal Bureau of Investigation (Szövetségi Nyomozóiroda, FBI), hozzáférhetnek azokhoz ezen adatok tömeges és válogatás nélküli megfigyelése és lehallgatása útján.

37. A High Court of Ireland megállapítja, hogy az ír jogban a magánélethez és a magánlakás sérthetetlenségéhez való alkotmányos jogok fontossága mindenképpen megköveteli, hogy az ezen jogokba való valamennyi beavatkozás megfeleljen a törvény által előírt követelményeknek, és arányos legyen. A személyes adatokhoz való tömeges és válogatás nélküli hozzáférés nem tesz eleget az arányosság követelményének, és így az ír alkotmánnyal ellentétesnek kell tekinteni. [19]

38. A High Court of Ireland kifejti, hogy ahhoz, hogy az elektronikus kommunikáció lehallgatása alkotmányosnak tekinthető legyen, bizonyítani kell azt, hogy a kommunikáció meghatározott lehallgatása és bizonyos egyének vagy az egyének bizonyos csoportjának meghatározott megfigyelése objektív módon igazolt a nemzetbiztonság és a bűncselekmények szankcionálása érdekében, továbbá megfelelő és igazolható biztosítékok léteznek.

39. Ennélfogva a High Court of Ireland kifejtette, hogy ha a jelen ügyet kizárólag az ír jog alapján kellene kezelni, akkor felmerülne az a jelentős kérdés, hogy az Egyesült Államok „biztosítja[-e] a magánélet, valamint az alapvető jogok és szabadságok megfelelő szintű védelmét” az adatvédelmi törvény 11. cikke (1) bekezdésének a) pontja értelmében. Ebből következik, hogy az ír jog, és különösen az alkotmányjogi követelmények alapján a Commissioner nem utasíthatta volna el M. Schrems panaszát, ezt a kérdést vizsgálnia kellett volna.

40. Ugyanakkor a High Court of Ireland megállapítja, hogy az előtte folyamatban lévő ügy a Charta 51. cikkének (1) bekezdése értelmében az uniós jog végrehajtását érinti, ily módon a Commissioner határozatának jogszerűségét az uniós jog alapján kell megítélni.

41. A Commissioner előtt felmerült problémát a High Court of Ireland a következőképpen ismerteti. Az adatvédelmi törvény 11. cikke (2) bekezdésének b) pontja kimondja, hogy a Commissionernek a harmadik országbeli védelem megfelelőségére vonatkozó kérdést a Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése értelmében tett uniós megállapítással „összhangban” kell meghatároznia. Következésképpen a Commissioner nem léphet túl e megállapításon. Mivel a 2000/520 határozatában a Bizottság megállapította, hogy az Egyesült Államok megfelelő védelmi szintet biztosít a biztonságos kikötő elveit elfogadó cégek által kezelt adatok tekintetében, a Commissionernek az ezen védelem nem megfelelő voltával kapcsolatos panaszt szükségszerűen el kellett utasítania.

42. A High Court of Ireland, miközben megállapította, hogy a Commissioner szigorúan ragaszkodott az 95/46 irányelv és a 2000/520 határozat szövegéhez, rámutatott, hogy M. Schrems kifogása valójában magának a biztonságos kikötőről szóló szabályozásnak a tartalmára irányul, semmint arra a módra, ahogyan a Commissioner az adott esetben alkalmazta e szabályozást, kiemelve ugyanakkor, hogy a felperes közvetlenül nem vitatta sem a 95/46 irányelv, sem pedig a 2000/520 határozat érvényességét.

43. A High Court of Ireland szerint tehát a lényegi kérdés az, hogy a Commissioner – az uniós jogra, és különösen a Charta 7. és 8. cikkének azt követő hatálybalépésére tekintettel – továbbra is szigorúan kötve van-e a Bizottság 2000/520 határozatban megfogalmazott, az Egyesült Államok jogában és gyakorlatában szereplő adatvédelem megfelelősége tekintetében tett megállapításához.

19 — A High Court of Ireland különösen az emberi méltóság tiszteletben tartására és az egyén szabadságára (preambulum); a személyes autonómiára (40. cikk, (3) bekezdés, 1.és 2. pont); a magánlakás sérthetetlenségére (40. cikk, (5) bekezdés) és a családi élet védelmére (41. cikk) hivatkozott.

44. A High Court of Ireland emellett egyértelművé teszi, hogy az előtte folyamatban lévő ügyben soha nem merült fel kérdés a Facebook Ireland vagy a Facebook USA tevékenysége mint olyan tekintetében. Márpedig a 2000/520 határozat 3. cikke (1) bekezdésének b) pontja, amely lehetővé teszi a nemzeti hatóságok számára, hogy elrendeljék valamely vállalkozás harmadik országba irányuló adatáramlásának felfüggesztését, e bíróság szerint csak olyan körülmények esetében alkalmazható, amikor – a jelen ügytől eltérően – a panaszt e hivatkozott vállalkozás magatartásával szemben nyújtják be.

45. A High Court of Ireland rámutat, hogy ebből következően a valódi kifogás nem a Facebook USA magatartására mint olyanra irányul, hanem sokkal inkább arra a tényre, miszerint a Bizottság már megállapította, hogy az Egyesült Államok adatvédelmi joga és gyakorlata megfelelő védelmet biztosít, noha az E. Snowden által kiszivárogtatott információkból egyértelmű, hogy az Unió területén élő népesség Egyesült Államokba így továbbított személyes adatai tömeges és válogatás nélküli alapon hozzáférhetők az amerikai hatóságok számára. [20]

46. E kérdésben a High Court of Ireland úgy véli, nehezen érthető, hogy a 2000/520 határozat a gyakorlatban hogyan tehet eleget a Charta 7. és 8. cikkében foglalt követelményeknek, különösen a Bíróság által a Digital Rights Ireland és társai ügyben [21] hozott ítéletben kifejtett elvekre tekintettel. Különösen a Charta 7. cikkében szereplő és a tagállamok közös hagyományaiból eredő alapvető értékek által biztosított garancia sérülne, ha az elektronikus kommunikációhoz eseti és általános alapon hozzáférhetnének az állami hatóságok, anélkül hogy szükség lenne nemzetbiztonsági, vagy az érintett egyén vagy egyének konkrét tekintetében bűnmegelőzési megfontolásokra alapított, megfelelő és igazolható követelmények mellett történő objektív igazolásra. Mivel M. Schrems keresete felveti azt a lehetőséget, hogy a 2000/520 határozat önmagában véve összeegyeztethetetlen a Charta 7. és 8. cikkével, a Bíróság megfontolhatná azt, hogy lehetséges-e a 95/46 irányelvnek, és különösen a 25. cikk (6) bekezdésének, valamint a 2000/520 határozatnak olyan értelmezése, amely lehetővé tenné a nemzeti hatóságok számára saját vizsgálat lefolytatását az arról való megbizonyosodás érdekében, hogy a személyes adatok harmadik országba való továbbítása és azok általi tárolása eleget tesz-e a Charta 7. és 8. cikkéből eredő követelményeknek.

47. E körülmények között a High Court of Ireland felfüggesztette az eljárást, és előzetes döntéshozatal céljából a következő kérdéseket terjesztette a Bíróság elé:

„A [Commissioner] elé terjesztett, arra irányuló panasz elbírálása során, hogy olyan harmadik országba (a jelen ügyben az Amerikai Egyesült Államokba) továbbítottak személyes adatokat, amelynek joga és gyakorlata a panaszos állítása szerint nem nyújt megfelelő védelmet az érintett személy számára, a Charta 7., 8. és 47. cikkére tekintettel, valamint a 95/46 irányelv 25. cikkének (6) bekezdésétől függetlenül a [Commissioner-t] t teljes mértékben köti-e a 2000/520 határozatban szereplő, ezzel ellentétes [uniós] megállapítás?

Másodlagosan a [Commissionernek] lehet-e és/vagy kell-e saját vizsgálatot végeznie ebben a kérdésben a [2000/520] határozat első közzétételét követő időszakban bekövetkezett ténybeli fejleményekre tekintettel?”

20 — A High Court of Ireland megjegyzi, hogy e tekintetben a felperes által előtte kifejtett alapvető jogalap értelmében a Snowden által legutóbb közzétett információk, valamint a személyes adatok széles körének az Egyesült Államok titkosszolgálatai részére való hozzáférhetővé tétele ismeretében a Commissioner nem juthatott érvényesen arra a következtetésre, hogy e harmadik országban megfelelő szintű ezeknek az adatoknak a védelme.

21 — C-293/12 és C-594/12, EU:C:2014:238, 65–69. pont.

II – **Elemzés**

48. A High Court of Ireland az általa megfogalmazott két kérdéssel arra kéri a Bíróságot, hogy pontosítsa a nemzeti felügyeleti hatóságok hatáskörét azokban az esetekben, amikor személyes adatok harmadik országban székhellyel rendelkező vállalkozások részére történő továbbítására vonatkozó panaszt kell elbírálniuk, és az e panaszban szereplő állítás szerint e harmadik ország nem biztosítja a továbbított adatok megfelelő védelmét, noha a Bizottság a 95/46 irányelv 25. cikkének (6) bekezdése alapján határozatot fogadott el arról, hogy e harmadik ország megfelelő szintű védelmet nyújt.

49. Megjegyzem, hogy a M. Schrems által a Commissionerhez benyújtott panasz kétirányú. Kifogásolja a személyes adatoknak a Facebook Ireland részéről a Facebook USA részére történő továbbítását. M. Schrems azt kéri, hogy vessenek véget e továbbításnak, mivel véleménye szerint az Egyesült Államok nem biztosítja a biztonságos kikötő rendszerének keretében továbbított személyes adatok megfelelő szintű védelmét. Egészen pontosan azt rója fel e harmadik országnak, hogy a PRISM program létrehozásával az NSA tömeges szabad hozzáférést kapott az Egyesült Államok szerverein tárolt adatokhoz. Így a panasz konkrétan a személyes adatoknak a Facebook Irelandtől a Facebook USA részére történő továbbítására vonatkozik, emellett általánosságban ezeknek az adatoknak a biztonságos kikötő rendszerében biztosított védelmi szintjét vitatva.

50. A Commissioner úgy vélte, hogy a panasz kivizsgálása már azon bizottsági határozat léte miatt sem lehetséges, amely elismeri, hogy az Egyesült Államok a biztonságos kikötő rendszerén belül megfelelő védelmi szintet biztosít.

51. Együtt kell vizsgálni tehát a két kérdést, amelyek lényegében arra irányulnak, hogy a 95/46 irányelv 28. cikkét a Charta 7. és 8. cikkére tekintettel úgy kell-e értelmezni, mely szerint a Bizottság által ezen irányelv 25. cikkének (6) bekezdése alapján hozott határozat megakadályozhatja a nemzeti felügyeleti hatóságokat abban, hogy kivizsgálják azon panaszt, amely szerint valamely harmadik ország nem biztosít megfelelő védelmi szintet a továbbított személyes adatok számára, és adott esetben e hatóságok felfüggesszék ezen adatok továbbítását.

52. A Charta 7. cikke biztosítja a magánélet tiszteletben tartásához való jogot, míg a Charta 8. cikke kifejezetten kinyilvánítja a személyes adatok védelméhez való jogot. Ez utóbbi cikk (2) és (3) bekezdése úgy rendelkezik, hogy az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni, mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni, továbbá e szabályok tiszteletben tartását független hatóságnak kell ellenőriznie.

A – *A nemzeti felügyeleti hatóságok jogköreiről a Bizottság megfelelőségi határozata esetén*

53. Amint arra M. Schrems az alapügy tárgyát képező panaszának megerősítésére benyújtott észrevételeiben rámutat, a központi kérdés a személyes adatoknak a Facebook Irelandtól a Facebook USA részére történő továbbítása, figyelembe véve az NSA-nak és más amerikai nemzetbiztonsági ügynökségeknek a Facebook USA-nál tárolt adatokhoz való általános hozzáférését, amelyet az amerikai jogszabályokban rájuk ruházott jogkörök biztosítanak számukra.

54. M. Schrems, amikor panaszt nyújtott be, amelyben vitatta azt a megállapítást, mely szerint valamely harmadik ország megfelelő védelmi szintet biztosít a továbbított adatok számára, úgy vélte, hogy a nemzeti felügyeleti hatóságnak, amennyiben rendelkezik az e panaszban foglalt állítások megalapozottságának megítéléséhez szükséges adatokkal, jogában áll elrendelni az említett panaszban megjelölt vállalkozás általi adattovábbítás felfüggesztését.

55. Figyelembe véve a Commissioner azon kötelezettségét, hogy védelemben részesítse M. Schrems alapvető jogait, ez utóbbi azt állítja, hogy a Commissioner nem csak a vizsgálat lefolytatására köteles, hanem amennyiben a panasznak helyt ad, használnia kell a jogkörét arra, hogy felfüggessze a Facebook Ireland és a Facebook USA közötti adatforgalmat.

56. Márpedig a Commissioner a jogköreit felsoroló adatvédelmi törvény rendelkezései alapján elutasította a panaszt. A Commissioner ezt a következtetést azon véleményére alapozta, mely szerint köti a 2000/520 határozat.

57. Ebből következően a jelen ügyben a központi probléma az, hogy a Bizottságnak a 2000/520 határozatban a védelem megfelelőségére vonatkozó megállapítása abszolút módon köti-e a nemzeti adatvédelmi hatóságot, és megakadályozza-e az ezen megállapítást vitató állítások kivizsgálását. Az előzetes döntéshozatali kérdések tehát a nemzeti adatvédelmi hatóságok vizsgálati jogkörének terjedelmére vonatkoznak a Bizottság megfelelőségi határozatának léte esetén.

58. A Bizottság szerint figyelembe kell venni a bizottsági jogkörök és a nemzeti adatvédelmi hatóságokra ruházott jogkörök közötti viszonyt. Ez utóbbi hatóságok hatáskörei az e tárgyban hozott jogszabályok egyedi esetekre történő alkalmazása köré csoportosulnak, míg a Bizottság jogkörébe a 2000/520 határozat alkalmazásának általános felülvizsgálata tartozik, ideértve a felfüggesztésre vagy a hatályon kívül helyezésre irányuló bármely eljárást.

59. A Bizottság arra hivatkozik, hogy M. Schrems nem adott elő olyan egyedi érveket, amelyekből arra lehetne következtetni, hogy a Facebook Ireland és a Facebook USA közötti adattovábbítás révén súlyos károsodás veszélye fenyegeti őt. Épp ellenkezőleg, a M. Schrems által kifejezett, az amerikai nemzetbiztonsági ügynökségek megfigyelési programjaival kapcsolatos aggodalmak elvont és általános jellegük miatt megegyeznek azokkal, amelyek a Bizottságot a 2000/520 határozat felülvizsgálatának kezdeményezésére késztették.

60. A Bizottság szerint a nemzeti felügyeleti hatóságok, amikor kizárólag strukturális és elvont panaszok alapján hoznak intézkedéseket, elvonják az arra irányuló jogkörét, hogy újratárgyalja az Egyesült Államokkal e határozat feltételeit, illetve szükség szerint felfüggessze azt.

61. Nem osztom a Bizottság véleményét. Álláspontom szerint a Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alapján elfogadott határozat léte nem teheti semmissé és nem is csökkentheti a nemzeti felügyeleti hatóságok ezen irányelv 28. cikkében biztosított hatáskörét. A Bizottság érvelésével szemben, amennyiben a nemzeti felügyeleti hatóságokat egyedi panasszal keresik meg, véleményem szerint a nyomozati jogköreik és függetlenségük értelmében ez a határozat nem akadályozhatja meg őket egy harmadik országban biztosított védelmi szinttel kapcsolatosan saját véleményük érvényesítésében, és abban, hogy az egyedi ügyekben folytatott határozathozatal során ebből következtetéseket vonjanak le.

62. A Bíróság állandó ítélkezési gyakorlatából az következik, hogy valamely uniós jogi rendelkezés értelmezéséhez nemcsak annak szövegét, hanem annak szövegkörnyezetét, és annak a szabályozásnak a célkitűzéseit is figyelembe kell venni, amelynek az részét képezi. [22]

63. A 95/46 irányelv (62) preambulumbekezdéséből kitűnik, hogy „a tagállamokban a feladataikat teljes függetlenséggel gyakorló felügyelő hatóságok létrehozása alapvető eleme az egyének védelmének a személyes adatok feldolgozása [helyesen: kezelése] tekintetében”.

22 — Lásd többek között: Koushkaki-ítélet (C-84/12, EU:C:2013:862, 34. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

64. Ezen irányelv 28. cikke (1) bekezdésének első albekezdése értelmében „[m]inden tagállamnak rendelkeznie kell arról, hogy az ezen irányelv értelmében a tagállam által elfogadott nemzeti rendelkezéseknek a területén történő alkalmazását valamely hatóság vagy hatóságok felügyeljék”. Az említett irányelv 28. cikke (1) bekezdése második albekezdésének rendelkezése szerint „[e] hatóságok a rájuk ruházott feladatok gyakorlása során teljes függetlenségben járnak el.”

65. A 95/46 irányelv 28. cikkének (3) bekezdése felsorolja a valamennyi felügyeleti hatóságot megillető jogosultságokat, azaz a vizsgálati jogkört, a tényleges beavatkozási jogosultságokat, amelyek lehetővé teszik számukra többek között az adatkezelés átmeneti vagy végleges tilalmának megállapítását, valamint a bírósági eljárásban való részvétel jogát az irányelv értelmében elfogadott nemzeti rendelkezések megsértése esetén, továbbá e jogsértések igazságszolgáltatási hatóságok elé terjesztésének jogát.

66. Másrészről a 95/46 irányelv 28. cikke (4) bekezdésének első albekezdése értelmében „[a] felügyelő hatóságok foglalkoznak a személyes adatok feldolgozása [helyesen: kezelése] vonatkozásában az egyének jogainak vagy szabadságainak védelmével kapcsolatos, bármely személy […] által benyújtott kérelmekkel”. Ezen irányelv 28. cikk (4) bekezdésének második albekezdése pontosítja, hogy „[a] felügyelő hatóságoknak foglalkozniuk kell különösen az adatfeldolgozás törvényességének ellenőrzésére irányuló, bármely személy által benyújtott kérelemmel, amennyiben az [említett] irányelv 13. cikkének értelmében elfogadott nemzeti rendelkezések alkalmazhatóak”. Megjegyzem, hogy ez utóbbi rendelkezés teszi lehetővé a tagállamok számára, hogy jogszabályokat fogadjanak el a 95/46 irányelvben foglalt jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás többek között a nemzetbiztonság, a honvédelem, a közbiztonság, valamint bűncselekmények megelőzése, vizsgálata, felderítése és az ezekkel kapcsolatos eljárások lefolytatása biztosításához szükséges.

67. Amint arra a Bíróság korábban már rámutatott, a természetes személyek személyes adataik kezelése tekintetében történő védelmére vonatkozó uniós szabályok tiszteletben tartásának független hatóság általi felügyeletére vonatkozó követelmény az elsődleges uniós jogból, nevezetesen a Charta 8. cikkének (3) bekezdéséből és az EUMSZ 16. cikkének (2) bekezdéséből is következik.[23] Emlékeztetett arra is, hogy „[a] független felügyelő hatóságok tagállamokban való létrehozatala lényeges eleme az egyének személyes adatok kezelése tekintetében való védelmének”[24].

68. A Bíróság azt is megállapította, hogy „a 95/46 irányelv 28. cikke (1) bekezdésének második albekezdését úgy kell értelmezni, hogy a személyes adatok kezelését felügyelő hatóságoknak olyan függetlenséggel kell rendelkezniük, amely lehetővé teszi számukra, hogy feladataik ellátása során külső befolyástól mentesen járjanak el. E függetlenség kizár többek között bármilyen összefonódást vagy bármely más formában jelentkező, akár közvetlen, akár közvetett külső befolyást, amely hatással lehetne határozataikra, és így akadályozhatná az említett hatóságoknak a magánélet védelméhez való alapvető jog és a személyes adatok szabad áramlása közötti helyes egyensúly létrehozásában álló feladatuk teljesítését”.[25]

23 — Lásd: Bizottság kontra Ausztria ítélet (C-614/10, EU:C:2012:631, 36. pont); Bizottság kontra Magyarország ítélet (C-288/12, EU:C:2014:237, 47. pont).

24 — Lásd többek között: Bizottság kontra Magyarország ítélet (C-288/12, EU:C:2014:237, 48. pont, valamint az ott hivatkozott ítélkezési gyakorlat). Lásd továbbá: Digital Rights Ireland és társai ítélet (C-293/12 és C-594/12, EU:C:2014:238, 68. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

25 — Lásd többek között: Bizottság kontra Magyarország ítélet (C-288/12, EU:C:2014:237, 51. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

69. A Bíróság azt is kimondta, hogy „[a] nemzeti ellenőrző hatóságok függetlensége garantálásának célja a személyes adatok kezelése vonatkozásában az egyének védelmére vonatkozó rendelkezések tiszteletben tartásának ellenőrzése hatékonyságának és megbízhatóságának biztosítása”[26]. E függetlenség biztosításának előírására az „[ezen nemzeti ellenőrző] hatóságok[…] határozatai[…] által érintett személyek és szervezetek védelmének megerősítése érdekében”[27] kerül sor.

70. Amint az különösen a 95/46 irányelv (10) preambulumbekezdéséből és 1. cikkéből kitűnik, annak célja az Unión belül „az alapvető jogok és szabadságok védelmének biztosítása a személyes adatok kezelése tekintetében”[28]. A Bíróság szerint „[a] 95/46 irányelv 28. cikkében szereplő ellenőrző hatóságok tehát az említett alapvető jogok és szabadságok őrzői”[29].

71. Figyelembe véve azon szerep jelentőségét, amelyet a nemzeti felügyelő hatóságok a természetes személyek számára a személyes adataik kezelésével kapcsolatosan biztosított védelem terén betöltenek, beavatkozási jogkörüknek sértetlennek kell maradnia még akkor is, ha a Bizottság a 95/46 irányelv 25. cikkének (6) bekezdése alapján határozatot fogadott el.

72. Ezzel összefüggésben megjegyzem, semmi sem utal arra, hogy a személyes adatok harmadik országba történő továbbítására vonatkozó rendszerek ne tartoznának a Charta 8. cikke (3) bekezdésének hatálya alá, mivel ez utóbbi az uniós jogszabályok hierarchiájának legmagasabb szintjén hirdeti a nemzeti hatóságok által a személyes adatok védelmére vonatkozó szabályok betartása felett gyakorolt felügyelet fontosságát.

73. Amennyiben a nemzeti felügyeleti hatóságokat abszolút módon kötnék a Bizottság határozatai, ez elkerülhetetlenül korlátozná teljes függetlenségüket. Az alapvető jogok és szabadságok őrzőiként betöltött szerepüknek megfelelően a személyek személyes adataik kezelésével kapcsolatos védelmének magasabb rendű érdekében a nemzeti felügyeleti hatóságoknak jogosultnak kell lenniük arra, hogy a hozzájuk benyújtott panaszokat teljes függetlenséggel vizsgálják.

74. Emellett, amint azt a belga kormány és az Európai Parlament a tárgyaláson helytállóan megjegyezte, nincs hierarchikus kapcsolat a 95/46 irányelvnek a személyes adatok harmadik országokba irányuló továbbításáról rendelkező IV. fejezete és – többek között – a nemzeti felügyeleti hatóságok szerepéről szóló VI. fejezete között. A VI. fejezetben semmi sem utal arra, hogy a nemzeti felügyeleti hatóságokra vonatkozó rendelkezések bármilyen módon a 95/46 irányelv IV. fejezetében található, a továbbításra vonatkozó különböző rendelkezéseknek lennének alávetve.

75. Épp ellenkezőleg, ezen irányelv IV. fejezete 25. cikkének (1) bekezdéséből kifejezetten kiderül, hogy csak akkor megengedett a személyes adatok megfelelő védelmi szintet biztosító harmadik országba történő továbbítása, ha az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseket betartják.

76. E tekintetben emlékeztetek arra, hogy e rendelkezés értelmében a tagállamoknak a nemzeti jogszabályaikban rendelkezniük kell arról, hogy a feldolgozásra kerülő vagy továbbítás után feldolgozásra szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha – a 95/46 irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül – az adott harmadik ország megfelelő védelmi szintet biztosít.

26 — Bizottság kontra Németország ítélet (C-518/07, EU:C:2010:125, 25. pont).

27 — Ua.

28 — Uo., 22. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

29 — Uo., 23. pont. Lásd e tekintetben: Bizottság kontra Ausztria ítélet (C-614/10, EU:C:2012:631, 52. pont); Bizottság kontra Magyarország ítélet (C-288/12, EU:C:2014:237, 53. pont).

77. Ezen irányelv 28. cikke (1) bekezdésének megfelelően a nemzeti felügyeleti hatóságok feladata, hogy felügyeljék az ezen irányelv értelmében a tagállam által elfogadott nemzeti rendelkezéseknek a területükön történő alkalmazását.

78. E két rendelkezés kapcsolata arra enged következtetni, hogy a 95/46 irányelv 25. cikkének (1) bekezdésében szereplő szabály, mely szerint a személyes adatok csak akkor továbbíthatók, ha a címzett harmadik ország megfelelő védelmi szintet tud biztosítani számukra, azon szabályok közé tartozik, amelyek végrehajtását a nemzeti felügyeleti hatóságoknak kell felügyelniük.

79. A Charta 8. cikkének (3) bekezdése alapján tágan kell értelmezni azon vizsgálati jogkört, amelyet a nemzeti felügyeleti hatóságok a 95/46 irányelv 28. cikke alapján hozzájuk benyújtott panaszok tárgyában teljes függetlenséggel gyakorolnak. E jogosultságokat tehát nem korlátozhatja az Unió által – ezen irányelv 25. cikkének (6) bekezdése értelmében a harmadik ország által biztosított védelem megfelelőségének megállapítása céljából – a Bizottságra ruházott jogalkotói jogkör.

80. A nemzeti felügyeleti hatóságoknak, figyelembe véve a személyes adatok védelmében betöltött alapvető szerepüket, jogosultnak kell lenniük vizsgálat lefolytatására, amikor olyan tényekre hivatkozó panaszt nyújtanak be hozzájuk, amelyek kétségbe vonhatják a valamely harmadik ország által biztosított védelem megfelelő szintjét, ideértve azt az esetet is, amikor a Bizottság a 95/46 irányelv 25. cikkének (6) bekezdése alapján megállapította, hogy a harmadik ország megfelelő védelmi szintet biztosít.

81. Amennyiben a nemzeti felügyeleti hatóság az általa lefolytatott vizsgálat eredményeképpen megállapítja, hogy a vitatott adattovábbítás sérti az uniós polgárokat személyes adataik kezelése tekintetében megillető védelmet, e hatóság a Bizottság határozatában szereplő általános értékeléstől függetlenül felfüggesztheti a szóban forgó adatok továbbítását.

82. A 95/46 irányelv 25. cikkének (2) bekezdése alapján ugyanis megállapítható, hogy a harmadik ország által nyújtott védelem szintjének megfelelőségét általános jogi és ténybeli körülmények figyelembevételével kell értékelni. Amennyiben e körülmények valamelyike megváltozik, és alkalmas a harmadik ország által biztosított védelem megfelelő szintjének kétségbe vonására, a hozzá benyújtott panasz ügyében eljáró nemzeti felügyeleti hatóságnak jogosultnak kell lennie arra, hogy a vitatott továbbításra vonatkozóan ebből jogkövetkezményeket állapítson meg.

83. Amint arra Írország rámutatott, a Commissionert a többi állami hatósághoz hasonlóan valóban köti a 2000/520 határozat. Az EUMSZ 288. cikkének negyedik bekezdése szerint ugyanis a valamely uniós intézmény által hozott határozat teljes egészében kötelező. Következésképpen a 2000/520 határozat kötelezi a címzett tagállamokat.

84. E tekintetben megjegyzem, hogy a 2000/520 határozat maga rendelkezik 5. cikkében arról, hogy „[a] tagállamok meghozzák azokat az intézkedéseket, amelyek szükségesek ahhoz, hogy [ennek] legkésőbb a tagállamok felé történő értesítésétől számított 90 napos időszak végéig megfeleljenek”. Emellett, e határozat (6) cikke megerősíti, hogy „[e]nnek a határozatnak a tagállamok a címzettjei”.

85. Ugyanakkor úgy vélem, hogy a 95/46 irányelv és a Charta fent hivatkozott rendelkezései alapján a 2000/520 határozat kötelező hatálya nem zárja ki teljes mértékben a Commissioner vizsgálatát azon panaszokkal kapcsolatosan, amelyek szerint a személyes adatoknak az Egyesült Államokba ezen határozat keretében történő továbbítása során nem biztosítottak az uniós jog által előírt védelemhez szükséges garanciák. Más szóval egy ilyen kötelező erő nem írja elő minden ilyen jellegű panasz sommás, azaz azonnali és a megalapozottság vizsgálata nélkül történő elutasítását.

86. Hozzáteszem, a 95/46 irányelv 25. cikkében szereplő rendelkezések rendszeréből továbbá kiderül, hogy mind a tagállamok, mind pedig a Bizottság megállapíthatja, hogy valamely harmadik ország megfelelő védelmi szintet biztosít-e, vagy sem. Megosztott jogkörről van tehát szó.

87. Ezen irányelv 25. cikkének (6) bekezdéséből következően, amennyiben a Bizottság megállapítja, hogy a harmadik ország megfelelő védelmi szintet biztosít az említett irányelv 25. cikkének (2) bekezdése értelmében, a tagállamok megtesznek minden szükséges intézkedést a Bizottság határozatának teljesítésére.

88. Mivel egy ilyen határozat következtében a személyes adatokat olyan harmadik országba lehet továbbítani, amelynek védelmi szintjét a Bizottság megfelelőnek ítélte meg, a tagállamoknak tehát főszabály szerint lehetővé kell tenniük, hogy a területükön székhellyel rendelkező vállalkozások az adatokat ilyen módon továbbítsák.

89. A 95/46 irányelv 25. cikke ugyanakkor nem ruházza fel a Bizottságot kizárólagos jogkörrel a továbbított személyes adatok védelmi szintjének megfelelő, illetve nem megfelelő voltára vonatkozó megállapítására. E cikk rendszere igazolja, hogy a tagállamoknak szintén szerep jut e tárgyban. A Bizottság határozata valóban fontos szerepet játszik a továbbítás tagállamokban hatályos feltételeinek egységesítésében. Ugyanakkor ez az egységesítés csak addig érvényes, amíg ez a megállapítás kétségessé nem válik.

90. A személyes adatok harmadik országba történő továbbítására vonatkozó feltételek egységesítésének szükségessége mellett szóló érv véleményem szerint korlátozott a jelen ügyhöz hasonló esetben, amikor éppen a Bizottság az, aki azon túl, hogy tudomást szerzett arról, hogy a megállapítása kritika tárgya lett, maga is ilyen kritikákat fogalmaz meg és tárgyalásokat folytat ezek orvoslására.

91. A harmadik ország által biztosított védelmi szint megfelelőségének megítélése a tagállamok és a Bizottság közötti együttműködést is eredményezhet. A 95/46 irányelv 25. cikkének (3) bekezdése e tekintetben úgy rendelkezik, hogy „[a] tagállamok és a Bizottság értesítik egymást azokról az esetekről, amelyekben úgy vélik, hogy valamely harmadik ország nem biztosít megfelelő védelmi szintet a (2) bekezdés értelmében”. Így, amint a Parlament megjegyzi, ez jól mutatja, hogy a tagállamoknak és a Bizottságnak egyformán fontos szerep jut azon esetek meghatározásában, amikor egy harmadik ország nem biztosít megfelelő védelmi szintet.

92. A megfelelőségi határozat tárgya a személyes adatok adott harmadik országba történő továbbításának engedélyezése. Ez nem jelenti azt, hogy az uniós polgárok nem nyújthatnak be többé a hatóságokhoz a személyes adataik védelmére irányuló kérelmet. E tekintetben megjegyzem, hogy a 95/46 irányelv 28. cikke (4) bekezdésének első albekezdése, mely szerint „[a] felügyelő hatóságok foglalkoznak a személyes adatok feldolgozása vonatkozásában az egyének jogainak vagy szabadságainak védelmével kapcsolatos, bármely személy […] által benyújtott kérelmekkel”, nem tartalmaz ezen elv alól olyan kivételt, amely a Bizottság által ezen irányelv 25. cikkének (6) bekezdése alapján hozott határozat esetére vonatkozna.

93. Ennek megfelelően, habár a Bizottság által az ez utóbbi rendelkezéssel ráruházott végrehajtási jogkör alapján hozott határozat következtében a személyes adatok továbbíthatók valamely harmadik országba, e határozat ugyanakkor nem foszthatja meg teljes mértékben a tagállamokat és különösen a nemzeti felügyeleti hatóságokat a jogköreiktől, és még csak nem is korlátozhatja azokat, amikor az alapvető jogok megsértésére vonatkozó állításokkal találkoznak.

94. A nemzeti felügyeleti hatóságnak olyan helyzetben kell lennie, hogy a 95/46 irányelv 28. cikkének (3) bekezdésében meghatározott jogkörét gyakorolhassa, ideértve a személyes adatok kezelésének ideiglenes vagy végleges megtiltását. Bár a jogkörök e rendelkezésben szereplő felsorolása nem tartalmazta kifejezetten a valamely tagállamból harmadik országba történő továbbításra vonatkozó jogkört, az ilyen továbbítást véleményem szerint akkor is adatkezelésnek kell tekinteni.[30] Amint az

30 — Lásd: Léger főtanácsnok Parlament kontra Tanács és Bizottság ügyre vonatkozó indítványa (C-317/04, EU:C:2005:710, 92–95. pont). Lásd továbbá: Parlament kontra Tanács és Bizottság ítélet (C-317/04 és C-318/04, EU:C:2006:346, 56. pont).

említett rendelkezés szövegéből kiderül, a felsorolás ráadásul nem kimerítő jellegű. Mindenesetre, figyelembe véve a nemzeti felügyeleti hatóságok által a 95/46 irányelv által létrehozott rendszerben játszott alapvető szerepet, ez utóbbi hatóságoknak jogosultnak kell lenniük az adattovábbítás felfüggesztésére az alapvető jogok bizonyított sérelme vagy a sérelem bekövetkeztének veszélye esetén.

95. Hozzáteszem, hogy nemcsak a függetlenség elvével, hanem a 95/46 irányelvnek az 1. cikke (1) bekezdésében található célkitűzésével is ellentétes lenne, ha a nemzeti felügyeleti hatóságokat megfosztanák azon jogkörüktől, hogy a jelen ügyhöz hasonló esetben vizsgálatot folytassanak le.

96. Amint arra a Bíróság rámutatott, „[a] 95/46 irányelv (3), (8) és (10) preambulumbekezdéséből az következik, hogy az uniós jogalkotó meg kívánta könnyíteni a személyes adatok szabad áramlását a jogszabályok közelítése által a személyek alapvető jogainak, különösen a magánélet tiszteletben tartásához való jog védelme mellett, magas védelmi szint biztosításával az Unión belül. Ezen irányelv 1. cikke ennek megfelelően előírja, hogy a tagállamoknak a személyes adatok kezelése tekintetében biztosítaniuk kell az egyének szabadságainak és alapvető jogainak a védelmét, különösen magánéletük tiszteletben tartását.” [31]

97. A 95/46 irányelv rendelkezéseit tehát azon célkitűzésének megfelelően kell értelmezni, amely a személyeket a személyes jogok Unión belüli feldolgozása során megillető alapvető jogok és szabadságok, különösen a magánélet tiszteletben tartásához való jog magas védelmi szintjének biztosítására irányul.

98. E célkitűzés jelentősége és a tagállamok által ennek elérésében betöltendő szerep azt is jelenti, hogy ha az egyedi körülmények alapvető kétségekre adnak okot egy harmadik országba történő adattovábbítás során a Charta által biztosított alapvető jogok tiszteletben tartására vonatkozóan, a tagállamokat, és így a nemzeti felügyeleti hatóságaikat sem kötheti abszolút módon a Bizottság megfelelőségi határozata.

99. A Bíróság már kimondta, hogy a 95/46 irányelvnek az alapvető szabadságok és különösen a magánélet tiszteletben tartásához való jog megsértésére alkalmas személyesadat-kezelést szabályozó rendelkezéseit szükségszerűen az alapvető jogok fényében kell értelmezni, amelyek az állandó ítélkezési gyakorlat szerint azon általános jogelvek szerves részét képezik, amelyek tiszteletben tartását a Bíróság biztosítja, és amelyek immár a Charta részét képezik” [32].

100. Többek között arra az ítélkezési gyakorlatra hivatkozom, mely szerint „a tagállamoknak, amellett hogy saját nemzeti jogukat az uniós joggal összhangban kell értelmezniük, arra is ügyelniük kell, hogy a másodlagos jog valamely szabályának ne olyan értelmezését vegyék alapul, amely ellentétes az uniós jogrend révén védelemben részesített alapvető jogokkal vagy az uniós jog más általános elveivel” [33].

101. A Bíróság úgy ítélkezett az N. S. és társai ítéletben, [34] hogy „a 343/2003[/EK] rendelet[[35]] azon megdönthetetlen vélelem alapján történő alkalmazása, amely szerint a kérelemért elsődlegesen felelős tagállamban tiszteletben fogják tartani a menedékkérő alapvető jogait, nem egyeztethető össze a tagállamok arra irányuló kötelezettségével, hogy a 343/2003 rendeletet az alapvető jogokkal összhangban kell értelmezniük és alkalmazniuk” [36].

31 — Lásd többek között: IPI-ítélet (C-473/12, EU:C:2013:715, 28. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

32 — Lásd többek között: Google Spain és Google ítélet (C-131/12, EU:C:2014:317, 68. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

33 — Lásd többek között: N. S. és társai ítélet. (C-411/10 és C-493/10, EU:C:2011:865, 77. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

34 — C-411/10 és C-493/10 ítélet, EU:C:2011:865.

35 — Az egy harmadik ország állampolgára által a tagállamok egyikében benyújtott menedékjog iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló, 2003. február 18-i 343/2003 tanácsi rendelet (HL L 50., 1. o.; magyar nyelvű különkiadás 19. fejezet, 6. kötet, 109. o.).

36 — Ezen ítélet 99. pontja.

102. E tekintetben a Bíróság a tagállamok – mint a menedékjogi ügyekkel összefüggő valamennyi jogi és gyakorlati kérdésben egymás vonatkozásában biztonságosnak tekintett származási országok – jogállásával összefüggésben megállapította, hogy azt kell vélelmezni, hogy a menedékkérőkkel kapcsolatos bánásmód minden tagállamban megfelel a Charta, a menekültek helyzetére vonatkozó, 1951. július 28-án Genfben aláírt egyezmény [37] és az emberi jogok és alapvető szabadságok védelméről szóló, Rómában 1950. november 4-én aláírt európai egyezmény követelményeinek. [38] Ugyanakkor a Bíróság úgy ítélte meg, hogy „[n]em zárható […] ki, hogy a gyakorlatban ez a rendszer egy adott tagállamban súlyos működési nehézségekkel szembesül, és így komoly veszélye áll fenn annak, hogy a menedékkérők az e tagállamnak történő átadásuk esetén alapvető jogaikkal összeegyeztethetetlen bánásmódnak lesznek kitéve” [39].

103. Következésképpen a Bíróság úgy határozott, „hogy a tagállamok – ideértve a nemzeti bíróságokat – kötelessége, hogy ne adják át a menedékkérőt a 343/2003 rendelet értelmében »felelős tagállamnak«, ha tudomással kell bírniuk arról, hogy a felelős tagállamban a menekültügyi eljárást és a menedékkérők befogadásának feltételeit illetően tapasztalható rendszeres zavarok miatt alapos okkal, bizonyítottan feltételezhető, hogy a kérelmező a Charta 4. cikke értelmében embertelen vagy megalázó bánásmód tényleges veszélyének lesz kitéve” [40].

104. Az N. S. és társai ítélet [41] kiterjeszthetőnek tűnik az olyan ügyre is, mint amely az alapeljárásban szerepel. Ennek megfelelően az Unió másodlagos jogának azon a megdönthetetlen vélelmen alapuló értelmezése, mely szerint a tagállamok, a Bizottság, vagy a harmadik országok tiszteletben fogják tartani az alapvető jogokat, nem egyeztethető össze a tagállamok arra irányuló kötelezettségével, hogy az Unió másodlagos jogát az alapvető jogokkal összhangban kell értelmezniük és alkalmazniuk. A 95/46 irányelv 25. cikkének (6) bekezdése tehát nem ír elő az alapvető jogok tiszteletben tartására vonatkozó ilyen megdönthetetlen vélelmet arra az esetre, amikor a Bizottság egy harmadik ország által biztosított védelmi szint megfelelőségét értékeli. Épp ellenkezőleg, megdönthetőnek kell tekinteni az e rendelkezés alapjául szolgáló vélelmet, amely szerint a valamely harmadik országba történő adattovábbítás tiszteletben tartja az alapvető jogokat. [42] Következésképpen az említett rendelkezést nem lehet úgy értelmezni, hogy megkérdőjelezhetőek legyenek a személyes adatok védelméhez való jog védelmére és tiszteletben tartására irányuló, többek között a 95/46 irányelv 28. cikkének (3) bekezdésében és a Charta 8. cikkének (3) bekezdésében szereplő biztosítékok.

105. Az említett ítéletből így az a következtetés vonható le, hogy amikor abban a harmadik országban, ahová a személyes adatokat továbbítják, rendszeres zavarok jelentkeznek, a tagállamoknak jogosultaknak kell lenniük a Charta 7. és 8. cikkében biztosított alapvető jogok védelméhez szükséges intézkedések meghozatalára.

106. Másfelől, amint arra az olasz kormány észrevételeiben rámutatott, a Bizottság által elfogadott megfelelőségi határozat nem csökkentheti az uniós polgárok védelmét adataik harmadik országba történő továbbítása során történő kezelésével kapcsolatban, ahhoz képest, mint ami ezeket a polgárokat megilletné adataiknak az Unió területén belüli kezelése esetén. Következésképp a nemzeti felügyeleti hatóságoknak olyan harmadik országba történő adattovábbítással szemben is közbe kell lépniük, és gyakorolniuk kell jogköreiket, amelyre vonatkozóan a Bizottság megfelelőségi határozatot fogadott el. Ellenkező esetben az uniós polgárok alacsonyabb fokú védelmet élveznének, mintha adataikat az Unión belül kezelnék.

37 — *Recueil des traités des Nations unies* (1954), 189. kötet, 150. o., 2545. sz. (kihirdette: az 1989. évi 15. tvr.).

38 — Lásd: N. S. és társai ítélet (C-411/10 és C-493/10, EU:C:2011:865, 80. pont).

39 — Uo., 81. pont.

40 — Uo., 94. pont.

41 — C-411/10 és C-493/10, EU:C:2011:865.

42 — Ezen ítélet 104. pontja.

107. Ennek megfelelően a Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alkalmazásában elfogadott határozatnak kizárólag az a következménye, hogy megszünteti a személyes adatok olyan harmadik országokba történő továbbítására vonatkozó általános tilalmat, amelyek nem biztosítanak az ezen irányelv által nyújtott védelemhez hasonló védelmi szintet. Más szóval nem a kivételek olyan egyedi rendszerének létrehozásáról van szó, amely az említett irányelv által az Unión belüli adatkezelés vonatkozásában létrehozott általános rendszerhez képest alacsonyabb védelmet nyújt az uniós polgárok számára.

108. Kétségtelen, hogy a Bíróság a Lindqvist-ítélet [43] 63. pontjában rámutatott arra, hogy „[a] 95/46 irányelv[nek a] 25. cikkét magában foglaló IV. fejezete sajátos szabályokat tartalmazó különleges rendszert” hozott létre. Ugyanakkor véleményem szerint ez nem jelenti azt, hogy egy ilyen rendszer alacsonyabb fokú védelmet nyújthatna. Épp ellenkezőleg, a 95/46 irányelv 1. cikkének (1) bekezdésében foglalt, a személyes adatok védelmére irányuló cél elérése érdekében ugyanezen irányelv 25. cikke számos kötelezettséget ró a tagállamokra és a Bizottságra, [44] és e cikk felállítja azt az elvet, mely szerint amennyiben valamely harmadik ország nem biztosít megfelelő szintű védelmet, a személyes adatoknak e harmadik országba irányuló továbbítása tilos. [45]

109. Egészen konkrétan, a Bizottság csak a 2000/520 határozat 3. cikke (1) bekezdésének b) pontja keretében tartja lehetségesnek a nemzeti felügyeleti hatóságok részéről a biztonságos kikötő rendszerébe történő beavatkozást és az adatforgalom felfüggesztését.

110. E határozat (8) preambulumbekezdése szerint „[a]z átláthatóság érdekében és a tagállamok illetékes hatóságainak azon képessége megőrzése céljából, hogy a személyes adatok kezelése vonatkozásában biztosítsa az egyének védelmét, ebben a határozatban pontosan meg kell határozni azokat a rendkívüli körülményeket, amelyek esetén indokolt a meghatározott adatáramlás felfüggesztése, függetlenül attól, hogy a védelmet megfelelőnek találják”.

111. A jelen ügyben különösen az említett határozat 3. cikke (1) bekezdése b) pontjának alkalmazása vitatott. Így ezen rendelkezés értelmében az adatáramlás felfüggesztését határozhatják el a nemzeti felügyeleti hatóságok, amennyiben „az elvek megszegésének nagy a valószínűsége; okkal feltételezik, hogy az érintett végrehajtási mechanizmus sem most, sem később nem tesz megfelelő és időszerű lépéseket az adott eset rendezésére; a folytatódó adattovábbítás az érintettek súlyos károsodásának veszélyével fenyeget; és a tagállam illetékes hatóságai a körülményekhez képest elfogadható erőfeszítéseket tettek, hogy a szervezetet értesítsék, és lehetőséget adjanak neki a válaszadásra”.

112. Az említett rendelkezés több feltételt tartalmaz, amelyeket a jelen eljárásban a felek többféleképpen értelmeztek. [46] Anélkül, hogy belemennék ezen értelmezések részleteibe, kiderül belőlük, hogy e feltételek szigorú korlátok között határozzák meg a nemzeti felügyeleti hatóságok adatforgalom felfüggesztésére irányuló jogkörét.

113. Márpedig ellentétben azzal, amire a Bizottság hivatkozik, a 2000/520 határozat 3. cikke (1) bekezdésének b) pontját a 95/46 irányelvnek a személyes adatok védelmére irányuló célkitűzésével összhangban és a Charta 8. cikkének figyelembevételével kell értelmezni. Az alapvető jogoknak megfelelő értelmezés követelménye e rendelkezés tág értelmezése mellett szól.

43 — C-101/01, EU:C:2003:596.

44 — 65. pont.

45 — 64. pont.

46 — M. Schrems szerint nem teljesül az első feltétel, mely szerint „az elvek megszegésének nagy a valószínűsége”. Márpedig nem vitatott, hogy a Facebook USA, amely részére az adatokat továbbították, öntanúsítást szerzett szervezetként maga is megszegte a biztonságos kikötő rendszerének alapelveit, amikor a birtokában lévő adatokhoz tömeges hozzáférést biztosított az amerikai hatóságok számára. A biztonságos kikötő elvének alapelveit ugyanis kifejezetten korlátozza az amerikai jog, amelyet 2000/520 határozat I. mellékletének negyedik albekezdése törvényként, kormányrendeletként vagy precedensjogként határoz meg.

114. Ebből következik, hogy a 2000/520 határozat 3. cikke (1) bekezdésének b) pontjában foglalt feltételek véleményem szerint nem akadályozhatják meg, hogy valamely nemzeti felügyeleti hatóság teljes függetlenségben gyakorolhassa a 95/46 irányelv 28. cikkének (2) bekezdésében rá ruházott jogköröket.

115. Amint lényegében arra a belga és az osztrák kormány a tárgyaláson rámutatott, a 2000/520 határozat 3. cikke (1) bekezdésének b) pontja által nyújtott kivételes megoldás olyan szűk körű, hogy nehézkes a gyakorlati alkalmazása. Együttes feltételeket követel meg, és túl magasra helyezi a lécet. Márpedig a Charta 8. cikkének (3) bekezdése fényében a nemzeti felügyeleti hatóságoknak a 95/46 irányelv 28. cikkének (3) bekezdéséből eredő előjogaira vonatkozó mozgásterét nem lehet olyan módon korlátozni, hogy ezáltal e jogköreiket ne gyakorolhassák többé.

116. E tekintetben a Parlament helytállóan mutatott rá arra, hogy az uniós jogalkotó döntött arról, mely jogkörök tartoznak a nemzeti felügyeleti hatóságokhoz. Márpedig, az uniós jogalkotó által a 95/46 irányelv 25. cikkének (6) bekezdésében a Bizottságra ruházott végrehajtási jogkör nem érinti az ugyanezen jogalkotó által ezen irányelv 28. cikkének (3) bekezdésében a nemzeti felügyeleti hatóságokra ruházott jogköröket. Más szóval a Bizottság nem rendelkezik hatáskörrel a nemzeti felügyeleti hatóságok jogkörének korlátozására.

117. Következésképpen, a személyek személyes adataik kezelésével kapcsolatos alapvető jogainak biztosítása érdekében a nemzeti felügyeleti hatóságoknak felhatalmazással kell rendelkezniük arra, hogy az e jogok megsértésére vonatkozó állítások esetén vizsgálatot folytassanak le. Amennyiben az ilyen vizsgálatok eredményeként e hatóságok úgy ítélik meg, hogy valamely, megfelelőségi határozattal érintett harmadik országban komoly jelek utalnak arra, hogy sérül az uniós polgárok személyes adatainak védelmére irányuló jog, e hatóságoknak jogosultsággal kell rendelkezniük az e harmadik országban székhellyel rendelkező célállomás felé irányuló adattovábbítás felfüggesztésére.

118. Másként megfogalmazva, a nemzeti felügyeleti hatóságok számára a 2000/520 határozat 3. cikke (1) bekezdésének b) pontjában meghatározott korlátozó feltételektől függetlenül biztosítani kell azt, hogy lefolytathassák vizsgálataikat, és adott esetben felfüggesszék az adatok továbbítását.

119. Másrészről, a nemzeti felügyeleti hatóságoknak – azon, a 95/46 irányelv 28. cikkének (3) bekezdésében foglalt joga alapján, hogy az ezen irányelv értelmében elfogadott nemzeti rendelkezések megsértése esetén a bírósági eljárásokban vegyenek részt, továbbá e jogsértéseket igazságszolgáltatási hatóságok elé terjesszék – azzal a joggal is rendelkezniük kell, hogy amennyiben olyan tények jutnak a tudomásukra, amelyek alátámasztják, hogy valamely harmadik ország nem biztosít megfelelő védelmi szintet, a nemzeti bírósághoz forduljanak, amely adott esetben a Bizottság megfelelőségi határozata érvényességének elbírálása céljából előzetes döntéshozatalra utalhatja kérdést a Bíróság elé.

120. E körülmények összességéből következik, hogy a 95/46 irányelv 28. cikkét, a Charta 7. és 8. cikkére tekintettel úgy kell értelmezni, mely szerint a Bizottság által ezen irányelv 25. cikkének (6) bekezdése alapján hozott határozat léte nem akadályozhatja meg a nemzeti felügyeleti hatóságokat abban, hogy kivizsgálják azon panaszt, amely azt állítja, hogy valamely harmadik ország nem biztosít a megfelelő védelmi szintet a továbbított személyes adatok számára, és adott esetben e hatóság felfüggessze ezen adatok továbbítását.

121. Habár a High Court of Ireland az előzetes döntéshozatalra utaló határozatában kiemeli, hogy M. Schrems az alapeljárásban benyújtott keresetében alakilag nem vitatta sem a 95/46 irányelv, sem a 2000/520 határozat érvényességét, ugyanakkor kiderül e határozatból, hogy a M. Schrems által megfogalmazott legfőbb kifogás annak az állításnak a kétségbe vonására irányul, mely szerint az Egyesült Államok a biztonságos kikötő rendszerén belül a személyes adatok továbbításának megfelelő védelmi szintjét biztosítja.

122. A Commissioner észrevételeiből az is kiderül, hogy M. Schrems panasza közvetlenül a 2000/520 határozatot vitatja. E panasz benyújtásával M. Schrems magának a biztonságos kikötő rendszerének tartalmát és működését kívánta megtámadni azzal az indokkal, hogy az Egyesült Államokba továbbított személyes adatok tömeges megfigyelése igazolta, hogy e harmadik ország jogrendszerében és gyakorlatában nem áll fenn ezen adatok tényleges védelme.

123. Ráadásul a kérdést előterjesztő bíróság maga is észlelte, hogy a Charta 7. és 8. cikkében biztosított garanciák és a tagállamok alkotmányos hagyományaiban közös alapvető értékek sérülnének, ha az állami hatóságok számára lehetővé válna az elektronikus kommunikációhoz eseti és általános alapon történő hozzáférés anélkül, hogy szükség lenne nemzetbiztonsági, illetve az érintett egyének konkrét tekintetében bűnmegelőzési megfontolásokra alapított, megfelelő és igazolható követelmények melletti objektív igazolásra. [47] Ily módon a kérdést előterjesztő bíróság közvetve kétségeit fejezi ki a 2000/520 határozat érvényességére vonatkozóan.

124. Annak értékelése tehát, hogy az Egyesült Államok a biztonságos kikötő rendszerén belül megfelelő védelmi szintet biztosít-e a személyes adatok továbbítása vonatkozásában, mindenképpen e határozat érvényességének felülvizsgálatát eredményezi.

125. Ezzel összefüggésben meg kell említeni, hogy a nemzeti bíróságok és a Bíróság között az EUMSZ 267. cikke által bevezetett együttműködési eszköz tekintetében a Bíróság különleges körülmények fennállása esetén, még ha kizárólag az uniós jog értelmezésére vonatkozó kérdést terjesztettek is elő előzetes döntéshozatalra, vizsgálhatja a másodlagos jog rendelkezéseinek érvényességét.

126. Ennélfogva a Bíróság több alkalommal hivatalból érvénytelennek nyilvánított olyan aktust, amelynek csak az értelmezését kérték. [48] A Bíróság azt is megállapította, hogy „amennyiben úgy látszik, hogy a nemzeti bíróság által előterjesztett kérdések inkább az [uniós] aktusok érvényességének vizsgálatára, mint azok értelmezésére vonatkoznak, a Bíróság feladata, hogy az [EUMSZ 267.] cikk által létrehozott mechanizmusok természetével összeegyeztethetetlen, az eljárás elhúzódásához vezető alaki követelmények kizárásával, haladéktalanul felvilágosítást adjon az említett bíróságnak” [49]. Másfelől a Bíróság már megállapította, hogy egy kérdést előterjesztő bíróság által, valamely másodlagos jogi aktusnak az alapvető jogok védelméről szóló szabályokkal való összeegyeztethetőségével kapcsolatban kifejezett kétségek alkalmasak e jogi aktus uniós jog szerinti érvényességének kétségbevonására. [50]

127. Emlékeztetek arra is, hogy a Bíróság ítélkezési gyakorlata szerint az uniós intézmények, szervek és szervezetek jogi aktusait megilleti a jogszerűség vélelme, amely azt jelenti, hogy ezek az aktusok mindaddig joghatásokat váltanak ki, amíg azokat vissza nem vonják, megsemmisítés iránti kereset alapján meg nem semmisítik, illetve előzetes döntéshozatal iránti kérelem vagy jogellenességi kifogás következtében nem nyilvánítják érvénytelennek. Egyedül a Bíróság rendelkezik hatáskörrel az uniós jogi aktusok érvénytelenné nyilvánítására, amely hatáskör célja a jogbiztonság garantálása az uniós jog egységes alkalmazásának biztosítása révén. A Bizottság általi érvénytelenné nyilvánítás, módosítás vagy hatályon kívül helyezés hiányában a határozat kötelező marad minden elemében, és továbbra is közvetlenül alkalmazandó minden tagállamban. [51]

128. Véleményem szerint ahhoz tehát, hogy a kérdést előterjesztő bíróság számára teljeskörű választ lehessen adni, és a jelen eljárásban a 2000/520 határozat érvényességével kapcsolatban felmerült kétségek eloszlathatók legyenek, a Bíróságnak meg kell vizsgálnia e határozat érvényességét.

47 — Az előzetes döntéshozatal iránti kérelem 24. pontja.

48 — Lásd többek között: Strehl-ítélet (62/76, EU:C:1977:18, 10–17. pont); Roquette Frères-ítélet (145/79, EU:C:1980:234, 6. pont); Schutzverband der Spirituosen-Industrie ítélet (C-457/05, EU:C:2007:576, 32–39. pont).

49 — Schwarze-ítélet (16/65, EU:C:1965:117, 1094. o.).

50 — Lásd: Hauer-ítélet (44/79, EU:C:1979:290, 16. pont).

51 — Lásd többek között: CIVAD-ítélet (C-533/10, EU:C:2012:347, 39–41. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

129. Ennélfogva azt is pontosítani kell, hogy a 2000/520 határozat érvényességének megállapítására irányuló vizsgálatot a jelen eljárás keretében folytatott vita tárgyát képező kifogások alapján kell körülhatárolni. Ezen eljárás keretében nem vitatták meg ugyanis a biztonságos kikötő rendszerének működésére vonatkozó valamennyi kérdést, ezért úgy vélem, hogy nem lehetséges e rendszer hiányosságainak kimerítő vizsgálata.

130. Ezzel szemben a jelen eljárásban a Bíróság előtt folytatott vita tárgya az, hogy az amerikai hírszerző szolgálatoknak a továbbított személyes adatokhoz való általános és célmeghatározás nélküli hozzáférése alkalmas-e arra, hogy érintse a 2000/520 határozat jogszerűségét. E határozat érvényességét tehát ebből a szemszögből kell megítélni.

B – *A 2000/520 határozat érvényességéről*

1. Azon elemekről, amelyeket a 2000/520 határozat érvényességének vizsgálata során figyelembe kell venni

131. Emlékeztetni kell az ítélkezési gyakorlatra, mely szerint „megsemmisítés iránti keresettel összefüggésben valamely jogi aktus jogszerűségét az aktus meghozatalának időpontjában fennálló ténybeli és jogi elemek függvényében kell elbírálni, a Bizottság értékelését csak akkor lehet helyteleníteni, ha az a szóban forgó szabályozás elfogadásának időpontjában rendelkezésére álló tényekre tekintettel nyilvánvalóan hibás” [52].

132. A Gaz de France – Berliner Investissement ítéletében [53] a Bíróság emlékeztetett arra az elvre, mely szerint „valamely aktus érvényességének mérlegelését, amelyet az előzetes döntéshozatalra utalás keretében a Bíróságnak kell elvégeznie, főszabály szerint az aktus elfogadásának időpontjában fennálló helyzet alapján kell elvégezni” [54]. Ugyanakkor, úgy tűnik, elfogadta, hogy „valamely aktus érvényessége bizonyos esetekben az elfogadása után bekövetkezett új tények alapján is mérlegelhető” [55].

133. A Bíróság által alkalmazott ilyen nyitást rendkívüli mértékben irányadónak tekintem a jelen ügyben.

134. A Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alapján elfogadott határozatok ugyanis eltérő jellegűek. Annak értékelésére szolgálnak, hogy megfelelő-e a személyes adatok harmadik országban biztosított védelmi szintje. Olyan értékelésről van szó, amelynek célja a harmadik országban fennálló ténybeli és jogi környezet értékelése.

135. Tekintettel arra, hogy a megfelelőségi határozat egyedi határozati típust képvisel, az a szabály, mely szerint érvényességének megállapítása kizárólag az elfogadása időpontjában fennálló tények alapján lehetséges, a jelen esetben finomítást igényel. Egy ilyen szabály különben oda vezetne, hogy évekkel egy megfelelőségi határozat meghozatala után a Bíróság az e határozat érvényességének vizsgálata során nem vehetné figyelembe az utólag bekövetkezett eseményeket, noha az érvényesség vizsgálatára irányulő előzetes döntéshozatali eljárás időben nem korlátozott, és megindítására éppen a szóban forgó aktus hiányosságaira utaló későbbi tények következtében kerül sor.

52 — Lásd többek között: BVGD kontra Bizottság ítélet (T-104/07 és T-339/08, EU:T:2013:366, 291. pont), amely az IECC kontra Bizottság ítéletre (C-449/98 P, EU:C:2001:275, 87. pont) hivatkozik.

53 — C-247/08, EU:C:2009:600.

54 — 49. pont, valamint az ott hivatkozott ítélkezési gyakorlat.

55 — 50. pont, valamint az ott hivatkozott ítélkezési gyakorlat. Lásd e tekintetben: Lenaerts,K., Maselis, I., és Gutman, K., *EU Procedural Law*, Oxford University Press, 2014., mely kimondja, hogy „in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court” (10.16 pont, 471. o).

136. A jelen esetben az, hogy a 2000/520 határozat körülbelül tizenöt éve hatályban van, arról tanúskodik, hogy a Bizottság hallgatólagosan megerősíti a 2000-ben tett értékelését. Ennélfogva, amikor a Bíróságnak az előzetes döntéshozatal iránti kérelemmel kapcsolatban ennek, a Bizottság által hosszú időn át hatályban tartott értékelésnek az érvényességét kell megítélnie, nemcsak lehetséges, hanem szükséges is ezen értékelés szembesítése azon új körülményekkel, amelyek a megfelelőségi határozat elfogadását követően következtek be.

137. Figyelembe véve a megfelelőségi határozat sajátos jellegét, a Bizottságnak rendszeresen felül kell vizsgálnia azt. Amennyiben az időközben bekövetkező újabb események fényében a Bizottság nem módosítja a határozatát, ezt úgy kell tekinteni, hogy hallgatólagosan és szükségszerűen megerősíti az eredeti értékelését. Ezáltal azon megállapítását ismétli meg, mely szerint az érintett harmadik ország a továbbított személyes adatok megfelelő védelmi szintjét biztosítja. A Bíróságnak kell megvizsgálnia, hogy ez a megállapítás a később bekövetkezett körülmények ellenére továbbra is érvényes-e.

138. Az ilyen típusú határozat hatékony bírósági felülvizsgálatának biztosítása érdekében e határozat érvényességét tehát véleményem szerint az aktuális ténybeli és jogi háttér figyelembevételével kell megállapítani.

2. A megfelelő védelmi szint fogalmáról

139. A 95/46 irányelv 25. cikke teljes egészében azon az elven alapul, mely szerint a személyes adatok harmadik országba történő továbbítása csak akkor lehetséges, ha ez a harmadik ország megfelelő védelmi szintet biztosít az ilyen adatok számára. Ennélfogva e cikk célkitűzése a személyes adatok harmadik országba történő továbbítása esetén az ezen irányelvben biztosított védelem folyamatosságának fenntartása. E tekintetben emlékeztetnem kell arra, hogy az említett irányelv a személyes adataik kezelése vonatkozásában magas védelmi szintet nyújt az uniós polgárok számára.

140. Figyelembe véve azt a jelentős szerepet, amelyet a személyes adatok védelme a magánélet tiszteletben tartásához való alapjogra tekintettel betölt, ilyen magas szintű védelmet kell biztosítani, amely kiterjed a személyes adatok harmadik országba történő továbbításának esetére is.

141. Ezért úgy vélem, hogy a Bizottság nem vitathatja a 95/46 irányelv 25. cikkének (6) bekezdése alapján, hogy valamely harmadik ország akkor biztosít megfelelő védelmi szintet, ha a kérdéses harmadik országban létező jog és gyakorlat átfogó értékelése alapján megállapítható, hogy az ebben a harmadik országban biztosított védelmi szint lényegében megfelel az ezen irányelv által nyújtott védelem szintjének, még ha e védelem egyes módozatai eltérnek is az Unióban általánosan alkalmazott gyakorlattól.

142. Noha az angol „adequate” kifejezés nyelvészeti szempontból éppen kielégítő vagy elegendő védelmi szintként értelmezhető, és így szemantikailag eltér a francia „adéquat” fogalomtól, meg kell jegyeznem, hogy e kifejezés értelmezésénél az egyetlen szempont az alapvető jogok magas szintű védelmének célkitűzése, amint azt a 95/46 irányelv előírja.

143. A harmadik ország által nyújtott védelmi szint vizsgálatának két alapvető tényezőre kell irányulnia, nevezetesen az alkalmazandó szabályok tartalmára és az e szabályok tiszteletben tartását biztosító eszközökre. [56]

56 — Lásd: a Bizottság WP 12. sz., „Személyes adatok továbbítása harmadik országokba: az EU-adatvédelmi irányelv 25. és 26. cikkének alkalmazása” című munkadokumentuma, elfogadta 1998. július 24-én a személyes adatfeldolgozás vonatkozásában az egyének védelmével foglalkozó munkacsoport, 5. oldal.

144. Véleményem szerint az Unióban hatályos védelmi szinttel lényegében azonos védelem eléréséhez a biztonságos kikötő rendszerének, amely nagy mértékben az e rendszerhez önkéntesen csatlakozó vállalkozások öntanúsításán és önértékelésén alapul, megfelelő garanciákat és elegendő ellenőrzési mechanizmust kellene tartalmaznia. Ezáltal a személyes adatok harmadik országba történő továbbítását illető védelem szintje nem lehetne alacsonyabb az Unión belüli adatkezelés védelmi szintjénél.

145. Ezzel összefüggésben először is meg kell állapítani, hogy az Unióban az a felfogás érvényesül, mely szerint a független hatóság formájában gyakorolt külső felügyelet minden olyan rendszer szükséges eleme, amely a személyes adatok védelmére vonatkozó szabályok tiszteletben tartásának biztosítását szolgálja.

146. Másrészről, a 95/46 irányelv 25. cikke (1)–(3) bekezdése hatékony érvényesülésének biztosítása érdekében figyelembe kell venni azt, hogy a harmadik ország által biztosított védelmi szint megfelelősége olyan változékony helyzet, amely az idő során számos tényező alapján változhat. Ennélfogva a tagállamoknak és a Bizottságnak állandó figyelemmel kell kísérnie minden olyan, a körülményekben beálló változást, amely szükségessé teheti a harmadik országban biztosított védelmi szint megfelelőségének újraértékelését. E szint megfelelő jellegének értékelése nem rögzülhet egy adott pillanatban, és ezáltal nem tartható fenn a végtelenségig, függetlenül a körülmények bármely, a biztosított védelmi szint nem megfelelő jellegére utaló változásától.

147. A harmadik országok azon kötelezettsége, hogy megfelelő védelmi szintet biztosítsanak, ezért folyamatosan fennálló kötelezettség. Amennyiben az értékelés egy adott időpontban történt, a megfelelőségi határozat fenntartása azt eltételezi, hogy az azóta bekövetkezett körülmények közül egy sem alkalmas arra, hogy kétségbe vonja a Bizottság eredeti értékelését.

148. Nem veszíthetjük ugyanis szem elől a 95/46 irányelv 25. cikkének célkitűzését, mely szerint el kell kerülni azt, hogy az személyes adatokat olyan harmadik országba továbbítsák, amely nem biztosít megfelelő védelmi szintet, megsértve ezáltal a Charta 8. cikkében biztosított, a személyes adatok védelméhez való alapvető jogot.

149. Rá kell mutatnom, hogy az uniós jogalkotó által a 95/46 irányelv 2. cikkének (6) bekezdésében a Bizottságra ruházott jogkört, amelynek keretében ez utóbbi megállapíthatja, hogy egy harmadik ország megfelelő védelmi szintet biztosít-e, kifejezetten az a követelmény határozza meg, hogy e harmadik ország ilyen, az e cikk (2) bekezdése szerinti megfelelő védelmi szintet biztosítson. Amennyiben az új körülmények ezt a Bizottság eredeti értékelését kétségbe vonhatják, ez utóbbi következésképpen köteles határozatát módosítani.

3. Értékelésem

150. Emlékeztetek arra, hogy a 95/46 irányelv 25. cikkének (6) bekezdésének értelmében „[a] Bizottság a 31. cikk (2) bekezdésében említett eljárásnak megfelelően megállapíthatja, hogy a harmadik ország megfelelő védelmi szintet biztosít e cikk (2) bekezdése értelmében, az egyének magánéletének, jogainak és szabadságainak védelmére vonatkozó belföldi jog, vagy a vállalt nemzetközi kötelezettségek, különösen az (5) bekezdésben említett tárgyalások végeredménye alapján.” Ezen irányelv 25. cikkének (6) bekezdése és 25. cikkének (2) bekezdése együttesen értelmezve kimondja, hogy annak megítéléséhez, hogy valamely harmadik ország megfelelő védelmi szintet biztosít-e, a Bizottságnak együttesen kell értékelnie az ezen harmadik országban hatályos jogszabályok összességét, valamint azok alkalmazását.

151. Láthattuk, hogy azt, hogy a Bizottság az időközben bekövetkezett új ténybeli és jogi elemek ellenére fenntartotta 2000/520 határozatát, az eredeti értékelésének megerősítésére irányuló szándékaként kell érteni.

152. Nem a Bíróság feladata, hogy az előzetes döntéshozatal iránti kérelem keretén belül azokat a tényeket vizsgálja, amelyek azon jogvita alapját képezik, amelyek az előzetes döntéshozatali eljárás kezdeményezésére indították a nemzeti bíróságot. [57]

153. Ezért azokra a tényekre támaszkodom, amelyeket a kérdést előterjesztő bíróság az előzetes döntéshozatal iránti kérelmében megjelölt, és amelyeket ezen felül a Bizottság nagymértékben bizonyítottnak fogadott el. [58]

154. Ily módon az alábbiak szerint határozhatók meg azok a Bíróság előtt előadott tények, amelyek a biztonságos kikötő által az Unióból az Egyesült Államokba továbbított személyes adatok vonatkozásában biztosított védelmi szint megfelelőségét megállapító bizottsági értékelés megkérdőjelezésére szolgálnak.

155. Előzetes döntéshozatal iránti kérelmében a kérdést előterjesztő bíróság az alábbi két ténybeli megállapításból indul ki. Egyrészről a Facebook Irelandhoz hasonló vállalkozások által az Egyesült Államokban letelepedett anyavállalatukhoz továbbított személyes adatokba e továbbítást követően az NSA és más szövetségi ügynökségek betekinthetnek a tömeges és célmeghatározás nélküli megfigyelési és lehallgatási tevékenységük során. Az E. Snowden által közzétett információk következtében ugyanis a rendelkezésre álló bizonyítékok jelenleg nem vezethetnek más elfogadható következtetéshez. [59] Másrészről az uniós polgárok nem rendelkeznek tényleges meghallgatáshoz való joggal az adataik NSA vagy más amerikai nemzetbiztonsági ügynökség általi megfigyelésére és lehallgatására vonatkozó kérdésekkel kapcsolatban. [60]

156. A High Court of Ireland által tett ténybeli megállapításokat így a Bizottság megállapításai is alátámasztják.

157. Ily módon a Bizottság a védett adatkikötő működéséről az uniós polgárok és az EU-ban letelepedett vállalatok szempontjából szóló fent hivatkozott közleményében arra az álláspontra helyezkedett, hogy 2013 folyamán az amerikai hírszerzési programok nagyságrendjére és terjedelmére vonatkozó értesülések aggodalmat keltettek a védett adatkikötőre vonatkozó program keretében az Egyesült Államokba törvényesen továbbított személyes adatok védelmének folyamatossága tekintetében. Például a jelek szerint a PRISM programban résztvevő és az amerikai hatóságok számára az Egyesült Államokban tárolt és feldolgozott valamennyi adathoz hozzáférést biztosító valamennyi vállalat rendelkezik védett adatkikötőre vonatkozó tanúsítvánnyal. A Bizottság véleménye szerint ennek alapján a védett adatkikötőre vonatkozó program az egyik olyan csatorna, amelyen keresztül az amerikai hírszerzési hatóságok hozzájuthatnak az eredetileg az Unióban feldolgozott személyes adatokhoz. [61]

158. Ezekből következően az Egyesült Államok joga és gyakorlata széles körben lehetővé teszi az uniós polgároknak a biztonságos kikötő rendszerén belül továbbított személyes adatainak vonatkozó gyűjtését anélkül, hogy e polgárok hatékony jogi védelmet élveznének.

159. Ezek a ténybeli megállapítások véleményem szerint azt mutatják, hogy a 2000/520 határozat nem tartalmaz elég biztosítékot. A biztosítékok ilyen hiányossága miatt e határozat végrehajtási módja nem felel meg a Chartában és a 95/46 irányelvben foglalt követelményeknek.

57 — Lásd többek között: Fallimento Traghetti del Mediterraneo ítélet (C-140/09, EU:C:2010:335, 22. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

58 — Lásd: a Bizottságnak a 2. oldal alján található lábjegyzetben említett határozata, valamint „A védett adatkikötő működése az uniós polgárok és az EU-ban letelepedett vállalatok szempontjából” című, az Európai Parlamenthez és a Tanácshoz intézett bizottsági közlemény (COM(2013) 847 final).

59 — Lásd: az előzetes döntéshozatal iránti kérelem 7. pontjának c) bekezdése.

60 — Lásd: az előzetes döntéshozatal iránti kérelem 7. pontjának b) bekezdése.

61 — A közleményének 19. oldala.

160. Márpedig a Bizottság által a 95/46 irányelv (25) cikkének (6) bekezdése alapján elfogadott határozat annak megállapítására irányul, hogy valamely harmadik ország megfelelő védelmi szintet „biztosít-e”. A jelen időben ragozott „biztosít” kifejezés azt jelenti, hogy egy ilyen határozat akkor tartható fenn, ha olyan harmadik országra vonatkozik, amely az említett határozat elfogadását követően továbbra is biztosítja a megfelelő védelmi szintet.

161. Valójában a kiszivárogtatások, amelyek az NSA számára a biztonságos kikötő rendszere keretében továbbított adatokat felhasználó tevékenységeire vonatkoztak, rávilágítottak a 2000/520 határozat által alkotott jogalap gyengeségeire.

162. A jelen eljárásban napfényre került hiányosságok különösen e határozat I. mellékletének negyedik albekezdésében találhatók.

163. Emlékeztetek arra, hogy e rendelkezés értelmében „[a biztonságos kikötő] elve[ine]k elfogadása korlátozódhat: a) a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez szükséges mértékben; b) törvény, kormányrendelet vagy precedensjog által, amelyek az elvekkel ellentétes kötelezettségeket vagy kifejezett felhatalmazásokat hoznak létre, feltéve hogy bármilyen ilyen felhatalmazás gyakorlása során a szervezet bizonyítani tudja, hogy az elvek nem teljesítése az ilyen felhatalmazás által támogatott törvényes érdekek teljesítéséhez szükséges mértékre korlátozódik”.

164. A probléma lényegében abból ered, hogy az amerikai hatóságok az említett határozatban engedélyezett eltéréseket alkalmazzák. Ezeket az eltéréseket túlságosan általános megfogalmazásuk miatt e hatóságok a szükségesség szigorú korlátján túl is alkalmazhatják.

165. Ehhez a túlzottan általános megfogalmazáshoz hozzáadódik az a körülmény, hogy az uniós polgárok nem rendelkeznek megfelelő jogorvoslati lehetőséggel személyes adataiknak azon céloktól eltérő kezelésével szemben, amely célból eredetileg összegyűjtötték, és az Egyesült Államokba továbbították azokat.

166. A 2000/520 határozatban többek között a nemzetbiztonsági követelményekkel kapcsolatosan megfogalmazott, a biztonságos kikötő elveinek alkalmazásától való eltérésekhez egy olyan független felügyeleti mechanizmust kellett volna rendelni, amely alkalmas a magánélethez való jog megállapított sérelmének elkerülésére.

167. Ennélfogva az amerikai hírszerző szolgálatok által a biztonságos kikötő keretén belül továbbított adatokkal kapcsolatosan folytatott általános megfigyelési tevékenységre vonatkozó gykorlatot érintő kiszivárogtatások rávilágítottak a 2000/520 határozat hiányosságaira.

168. A jelen ügyben említett állítások nem a biztonságos kikötő elveinek Facebook általi megsértésére vonatkoznak. Ha egy, a Facebook USA-hoz hasonló tanúsított vállalkozás hozzáférést ad az amerikai hatóságok számára a tagállamok valamelyikéből kapott adatokhoz, ezt úgy kell tekinteni, hogy ezáltal az amerikai jogszabályoknak tesz eleget. Tekintettel arra, hogy ezt a helyzetet a 2000/520 határozat az eltérések széleskörű megfogalmazása révén kifejezetten jóváhagyja, a jelen ügyben ténylegesen felmerül az a kérdés, hogy ezek az eltérések összeegyeztethetők-e az Unió elsődleges jogával.

169. E tekintetben ki kell emelni, hogy a Bíróság ítélkezési gyakorlatából az is következik, hogy az emberi jogok tiszteletben tartása az uniós jogi aktusok jogszerűségének feltétele, és nem engedhetők meg olyan intézkedések az Unión belül, amelyek összeegyeztethetetlenek ezek tiszteletben tartásával. [62]

62 — Lásd többek között: Kadi és Al Barakaat International Foundation kontra Tanács és Bizottság ítélet (C-402/05 P és C-415/05 P, EU:C:2008:461, 284. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

170. A Bíróság ítélkezési gyakorlatából többek között az is következik, hogy személyes adatok közjogi, vagy magánjogi harmadik személyekkel való közlése „az így közölt információk későbbi felhasználásától függetlenül” a magánélet tiszteletben tartásához való jogba történő beavatkozásnak minősül.[63] Emellett a Digital Rights Ireland és társai ítéletben[64] a Bíróság megerősítette, hogy az illetékes nemzeti hatóságok felhatalmazása az ilyen adatokhoz való hozzáférésre az ezen alapjogba való további és elkülönült beavatkozásnak minősül.[65] Ráadásul a személyes adatok kezelésének valamennyi formája a Charta 8. cikkének hatálya alá tartozik, és így az ilyen adatok védelméhez való alapvető jogba történő beavatkozást valósít meg.[66] Az amerikai hírszerző szolgálatokat megillető, a továbbított adatokhoz való hozzáférési jog tehát szintén a személyes adatoknak a Charta 8. cikkében biztosított védelméhez való alapvető jogba történő beavatkozást jelent, mivel az ilyen hozzáférés a személyes adatok kezelését valósítja meg.

171. Hasonlóan ahhoz, amit a Bíróság ebben az ítéletben megállapított, az így azonosított beavatkozás széles körű, és azt különösen súlyosnak kell tekinteni, figyelembe véve az érintett felhasználók és a továbbított adatok nagy számát. A beavatkozást rendkívül súlyossá teszik ezek a tényezők, amelyekhez társul az Egyesült Államokban székhellyel rendelkező vállalkozások számára továbbított személyes adatok vonatkozásában az amerikai hírszerző szolgálatokat megillető hozzáférés titkos jellege.

172. Ehhez adódik az a körülmény, hogy az uniós polgárokat, mint Facebook-felhasználókat, nem tájékoztatják arról a tényről, hogy személyes adataik általánosan elérhetők lesznek az amerikai nemzetbiztonsági ügynökségek számára.

173. Hangsúlyt kell helyezni a kérdést előterjesztő bíróság azon megállapítására is, mely szerint az Egyesült Államokban az uniós polgárok nem rendelkeznek tényleges meghallgatáshoz való joggal az adataik megfigyelésére és lehallgatására. Az Egyesült Államokban a felügyeletet a FISC gyakorolja, az előtte folyó eljárás azonban *ex parte* és titkos.[67] Úgy vélem, hogy ezen a ponton beavatkoznak az uniós polgárokat a Charta 47. cikkében védelemben részesített, hatékony jogorvoslathoz való jogba.

174. Megállapítható tehát hogy a biztonságos kikötő elveitől való eltérések, amelyek 2000/520 határozat I. mellékletének negyedik albekezdésében szerepelnek, a Charta 7., 8. és 47. cikkében biztosított alapjogokba való beavatkozást tesznek lehetővé.

175. Most meg kell vizsgálni, hogy ez a beavatkozás indokolt-e.

176. A Charta 52. cikk (1) bekezdésének megfelelően a Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, e jogok lényeges tartalmának tiszteletben tartásával korlátozható. Az arányosság elvére figyelemmel az említett jogok és szabadságok korlátozására csak akkor és annyiban kerülhet sor, ha az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

177. A Charta által védett jogok és szabadságok korlátozásának ily módon felállított feltételeit figyelembe véve erősen kétlem, hogy a jelen ügyben vitatott korlátozásokat úgy lehetne tekinteni, mint amelyek tiszteletben tartják a Charta 7. és 8. cikkének lényeges tartalmát. Az amerikai hírszerző szolgálatoknak a továbbított adatokhoz való hozzáférése ugyanis, úgy tűnik, kiterjed az elektronikus közlések tartalmára, ami pedig a Charta 7. cikkében védett magánélet tiszteletben tartásához való

63 — Österreichischer Rundfunk és társai ítélet (C-465/00, C-138/01 és EU:C:2003:294, 74. pont).

64 — C-293/12 és C-594/12 ítélet, EU:C:2014:238.

65 — 35. pont.

66 — 36. pont.

67 — Az előzetes döntéshozatalra utaló határozat 7. pontjának b) bekezdése.

alapvető jog és más jogok lényegét sértheti. Emellett, mivel a 2000/520 határozat I. mellékletének negyedik albekezdésében foglalt korlátozások túlzottan széles körű megfogalmazása lehetővé teszi a biztonságos kikötő valamennyi elvének alkalmazásától való eltérést, úgy tekinthetjük, hogy ezek a korlátozások sértik a személyes adatok védelméhez való alapvető jog lényeges tartalmát.[68]

178. Azon kérdést illetően, mely szerint a megállapított beavatkozás megfelel-e valamilyen közérdekű célnak, emlékeztetek arra, hogy a 2000/520 határozat I. melléklete negyedik albekezdésének b) pontja értelmében a biztonságos kikötő elveinek elfogadását korlátozhatja „törvény, kormányrendelet vagy precedensjog […], amelyek az elvekkel ellentétes kötelezettségeket vagy kifejezett felhatalmazásokat hoznak létre, feltéve hogy bármilyen ilyen felhatalmazás gyakorlása során a szervezet bizonyítani tudja, hogy az elvek nemteljesítése az ilyen felhatalmazás által támogatott törvényes érdekek teljesítéséhez szükséges mértékre korlátozódik”.

179. Meg kell állapítanom, hogy nem történt meg az e rendelkezésben említett „törvényes érdekek” pontosítása. Mindez bizonytalanságot eredményez az elveket elfogadó vállalkozások számára fennálló, a biztonságos kikötő elveitől való eltérés potenciálisan meglehetősen tág alkalmazási területére vonatkozóan.

180. A 2000/520 határozat „Kifejezett, jogszabályon alapuló meghatalmazások” címet viselő IV. mellékletének B) címében található magyarázatok szövege megerősíti ezt a benyomást, különösen az az állítás, mely szerint „[n]yilvánvaló, hogy ahol az Egyesült Államok jogszabályai ellentmondó kötelezettségeket szabnak, az Egyesült Államok szervezeteinek – akár a »biztonságos kikötő«-ben, akár nem – be kell tartania a jogszabályokat”. Másrészről, a kifejezett meghatalmazásokat illetően megjegyzi, hogy „bár a »biztonságos kikötő« elvek célja a különbségek áthidalása az Egyesült Államok és Európa kormányzati rendszere között az adatvédelem tekintetében – tiszteletben kell tartanunk választott törvényhozóink jogalkotói előjogait”.

181. Véleményem szerint ebből az következik, hogy ez az eltérés ellentétes a Charta 7., 8. és 52. cikkének (1) bekezdésével, mivel nem szolgál kellő pontossággal meghatározott általános érdekű célt.

182. Mindenesetre az az engedékeny és általános mód, amellyel maga a 2000/520 határozat az I. melléklete negyedik bekezdésének b) pontjában és a IV. mellékletének B. pontjában rendelkezik arról, hogy a biztonságos kikötő elveitől el lehet tekinteni az amerikai jog alkalmazása során, nem összeegyeztethető azzal a feltétellel, amely szerint a személyes adatok védelmére vonatkozó szabályoktól kizárólag a szigorúan szükséges mértékben lehet eltérni. E rendelkezések valóban megemlítik a szükségesség feltételét, azonban azon túl, hogy e feltételt az érintett vállalkozásnak kell bizonyítania, nem látom át, hogyan vonhatja ki magát egy ilyen vállalkozás azon kötelezettsége alól, amely szerint a rá kötelező jogszabályok alapján mellőznie kell a biztonságos kikötő elveit.

183. Ennélfogva véleményem szerint a 2000/520 határozatot érvénytelennek kell nyilvánítani, mivel ez az eltérés, amely általános és pontatlan módon lehetővé teszi a biztonságos kikötő rendszerének mellőzését, maga teszi lehetetlenné annak elfogadását, hogy ez a rendszer megfelelő védelmi szintet biztosít az Unióból az Egyesült Államokba továbbított személyes adatok számára.

184. Mivel a jelen ügyben a 2000/520 határozat I. melléklete negyedik albekezdésének a) pontjában meghatározott korlátozások első kategóriájáról van szó, amely a nemzetbiztonsági előírásokkal, a közérdekkel és a bűnüldözés követelményeivel kapcsolatos, ezek közül egyedül az első cél elég pontos ahhoz, hogy a Charta 52. cikkének (1) bekezdése értelmében az Unió által elfogadott általános érdekű célnak lehessen tekinteni.

68 — Lásd e tekintetben: Digital Rights Ireland és társai ítélet (C-293/12 és C-594/12, EU:C:2014:238, 39. és 40. pont).

185. Ezen a ponton a megállapított beavatkozás arányosságát kell megvizsgálni.

186. E tekintetben emlékeztetnem kell arra, hogy „az arányosság elve – a Bíróság állandó ítélkezési gyakorlata értelmében – megköveteli, hogy az uniós intézmények aktusai alkalmasak legyenek a szóban forgó szabályozás által kitűzött jogszerű célok elérésére, és ne haladják meg az e célok eléréséhez szükséges mértéket.” [69]

187. E feltételek tiszteletben tartásának bírósági felülvizsgálata tekintetében elmondható, hogy „amennyiben alapvető jogokba való beavatkozásról van szó, az uniós jogalkotó mérlegelési jogkörének terjedelme korlátozott lehet bizonyos körülményektől függően, amelyek között szerepel többek között az érintett terület, a szóban forgó, Charta által biztosított jog jellege, a beavatkozás jellege és súlyossága, valamint annak célja.” [70]

188. Véleményem szerint a Bíróság teljeskörűen ellenőrzi a Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alapján elfogadott határozatokban alkalmazott értékelés arányosságát, amelyben ez utóbbi intézmény megállapítja, hogy egy harmadik ország megfelelő védelmi szintet biztosít-e a „belföldi jog, vagy a vállalt nemzetközi kötelezettségek alapján”.

189. E tekintetben meg kell jegyezni, hogy a Digital Rights Ireland és társai és társai ítéletben [71] a Bíróság már úgy határozott, hogy „figyelembe véve egyrészről azt a fontos szerepet, amelyet a személyes adatok védelme tölt be a magánélet tiszteletben tartásához való alapvető jog tekintetében, másrészről pedig az e jogot érintő, [megtámadott] irányelv által megvalósított beavatkozás mértékét és súlyosságát, az uniós jogalkotó mérlegelési jogköre korlátozott, és ezért azt szigorú felülvizsgálatnak kell alávetni.” [72]

190. Egy ilyen beavatkozásnak alkalmasnak kell lennie a szóban forgó uniós jogi aktus által kitűzött célok elérésére, és szükségesnek kell lennie e cél eléréséhez.

191. E tekintetben „[a] magánélet tiszteletben tartásához való jog kapcsán elmondható, hogy a Bíróság állandó ítélkezési gyakorlata szerint ezen alapvető jog védelme […] megköveteli, hogy a személyes adatok védelme alóli kivételek és e védelem korlátozásai a feltétlenül szükséges határokon belül maradjanak.” [73]

192. A felügyelet során a Bíróság figyelembe veszi azt a körülményt is, hogy „a személyes adatoknak a Charta 8. cikkének (1) bekezdésében szereplő kifejezett kötelezettségből eredő védelme különös jelentőséggel bír a Charta 7. cikkében szereplő, magánélet tiszteletben tartásához való jog szempontjából.” [74]

193. A Bíróság szerint, amely e tekintetben az Emberi Jogok Európai Bíróságának joggyakorlatára hivatkozik, „[a] szóban forgó uniós szabályozásnak tehát egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása vonatkozásában, és minimális követelményeket kell előírnia annak érdekében, hogy azon személyek, akiknek az adatait megőrizték, elegendő olyan biztosítékkal rendelkezzenek, amely lehetővé teszi személyes adataiknak a visszaélések veszélyeivel, valamint az ezen adatokat érintő minden jogellenes hozzáféréssel és felhasználással

69 — Digital Rights Ireland és társai ítélet (C-293/12 és C-594/12, EU:C:2014:238, 46. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

70 — Uo., 47. pont, valamint az ott hivatkozott ítélkezési gyakorlat.

71 — C-293/12 és C-594/12, EU:C:2014:238.

72 — 48. pont.

73 — Digital Rights Ireland és társai ítélet (C-293/12 és C-594/12, EU:C:2014:238, 52. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

74 — Uo., 53. pont.

szembeni hatékony védelmét”[75]. A Bíróság rámutat arra, hogy „[a]z ilyen biztosítékokkal való rendelkezés szükségessége még fontosabb abban az esetben, ha […] a személyes adatokat automatikusan kezelik és jelentős veszélye áll fenn az említett adatokhoz való jogellenes hozzáférésnek.”[76]

194. Véleményem szerint hasonlóság áll fenn a 2000/520 határozat I. melléklete negyedik albekezdésének a) pontja és a 95/46 irányelv 13. cikkének (1) bekezdése között. Az első rendelkezés megállapítja, hogy a „biztonságos kikötő” elveinek elfogadása korlátozódhat „a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítéséhez szükséges mértékben”. A második szerint a tagállamok jogszabályokat fogadhatnak el ezen irányelv 6. cikkének (1) bekezdésében, 10. cikkében. 11. cikkének (1) bekezdésében, valamint a 12. és a 21. cikkében foglalt jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás a nemzetbiztonság, a honvédelem, a közbiztonság, a bűncselekmények megelőzésének, vizsgálatának, felderítésének és az ezekkel kapcsolatos eljárások lefolytatásának biztosításához szükséges.

195. Amint arra a Bíróság az IPI-ítéletben[77] már rámutatott, a 95/46 irányelv 13. cikke (1) bekezdésének megfogalmazásából következik, hogy a tagállamok kizárólag akkor írhatják elő az e rendelkezésben meghatározott intézkedéseket, amennyiben ezek szükségesek. A tagállamok számára az említett rendelkezésben biztosított lehetőség ily módon az intézkedések „szükséges” jellegétől függ.[78] Az ezen irányelv 13. cikkében a személyes adatok Unión belüli kezelésére vonatkozóan szabályozott korlátozásokat úgy kell értelmezni, hogy azoknak szigorúan a cél eléréséhez szükséges mértékre kell korlátozódniuk. Véleményem szerint hasonló a helyzet a biztonságos kikötő elveinek a 2000/520 határozat I. mellékletének negyedik albekezdésében foglalt korlátozásaival is.

196. Márpedig meg kell jegyeznem, hogy nem említi minden nyelvi változat a szükségesség kritériumát a 2000/520 határozat I. mellékelet negyedik albekezdése a) pontjának szövegében. Így többek között a francia változat szerint „[l]’adhésion aux principes peut être limitée par … les exigences relatives à la sécurité nationale, l’intérêt public et le respect des lois aux États-Unis”, míg például a spanyol, a német és az angol változat rámutat, hogy az alkalmazott korlátozásoknak a fent említett célok eléréséhez szükséges mértékűeknek kell lenniük.

197. Akárhogyan is, ezek, a kérdést előterjesztő bíróság által és a Bizottság fent hivatkozott közleményében egyaránt előadott tények világosan bizonyítják, hogy a gyakorlatban e korlátozások alkalmazása nem korlátozódik az érintett célok eléréséhez szigorúan szükséges mértékre.

198. Ezzel összefüggésben megfigyelhető, hogy az amerikai hírszerző szolgálatoknak a továbbított személyes adatokhoz való hozzáférése általános jelleggel vonatkozik valamennyi személyre és valamennyi elektronikus hírközlési eszközre, valamint az e kommunikációval terjedő továbbított adatok összességére, anélkül hogy az általános érdekű cél alapján bármilyen megkülönböztetést, korlátozást vagy kivételt alkalmazna.[79]

199. Az amerikai hírszerző szolgálatok hozzáférése a továbbított adatokhoz ugyanis átfogóan vonatkozik valamennyi olyan személyre, aki elektronikus hírközlési szolgáltatásokat vesz igénybe, azonban annak a megkövetelése nélkül, hogy az érintett személyek fenyegetést jelentsenek a nemzetbiztonságra.[80]

75 — Uo., 54. pont, valamint az ott hivatkozott ítélkezési gyakorlat.

76 — Uo., 55. pont, valamint az ott hivatkozott ítélkezési gyakorlat.

77 — C-473/12, EU:C:2013:715.

78 — 32. pont.

79 — Lásd analógia útján: Digital Rights Ireland és társai ítélet (C-293/12 és C-594/12, EU:C:2014:238, 57. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

80 — Uo., 58. és 59. pont.

200. Egy ilyen tömeges és válogatás nélküli megfigyelés jellegénél fogva aránytalan, és indokolatlanul beavatkozik a Charta 7. és 8. cikkében biztosított jogokba.

201. Amint azt a Parlament észrevételeiben helytállóan megjegyezte, mivel az uniós jogalkotónak vagy a tagállamoknak nem áll módjában olyan jogszabály elfogadása, amely a Charta megsértésével tömeges és célmeghatározás nélküli megfigyelést ír elő, ebből szükségszerűen következik, hogy egyetlen harmadik országról sem lehet eleve megállapítani, hogy az európai polgárok személyes adatainak megfelelő szintű védelmét biztosítják, amennyiben jogszabályaik ténylegesen felhatalmazást tartalmaznak az ilyen jellegű adatok tömeges és célmeghatározás nélküli megfigyelésére és lehallgatására.

202. Ki kell továbbá emelni, hogy a biztonságos kikötő rendszere, a 2000/520 határozat által létrehozott formájában, nem tartalmaz a továbbított adatok tömeges és általános megfigyelésének elkerülésére alkalmas biztosítékokat.

203. E tekintetben megjegyzem, hogy a Bíróság a Digital Rights Ireland és társai ítéletben [81] kiemelte a „Charta 7. és 8. cikkében foglalt alapvető jogokba való beavatkozás terjedelmét szabályozó egyértelmű és pontos szabályok” előírásának fontosságát. [82] Egy ilyen beavatkozást a Bíróság szerint „pontosan körül [kell] határoln[iuk] olyan rendelkezések[nek], amelyek lehetővé teszik, hogy az ténylegesen a feltétlenül szükséges mértékre korlátozódjon. [83] A Bíróság ugyanezen ítéletben kihangsúlyozta „a Charta 8. cikkében előírtaknak megfelelő olyan garanci[a előírásának szükségességét], amely lehetővé tenné a megőrzött adatoknak a visszaélések veszélyével, valamint bármilyen jogellenes hozzáféréssel vagy felhasználással szemben történő hatékony védelmének biztosítását” [84].

204. Márpedig rá kell mutatni arra, hogy a választottbírósági mechanizmusok, valamint az FTC, amelynek szerepe a kereskedelmi jogvitákra korlátozódik, nem rendelkezik eszközzel arra, hogy vitassa az amerikai hírszerző szolgálatok hozzáférését az Unióból továbbított személyes adatokhoz.

205. Az FTC hatáskörébe a tisztességtelen vagy megtévesztő kereskedelmi eljárások vagy gyakorlatok tartoznak, így az nem terjed ki az adatok nem kereskedelmi célú gyűjtésére és felhasználására. [85] Az FTC korlátozott hatásköre az egyének jogait a személyes adataik védelmére szűkíti le. Az FTC-t nem azért hozták létre, hogy az Unión belül működő nemzeti felügyeleti hatóságokhoz hasonlóan a magánélethez való egyéni jogot védje, hanem abból a célból, hogy tisztességes és megbízható kereskedelmet biztosítson a felhasználók számára, ami *de facto* korlátozza a beavatkozási jogkörét a személyes adatok védelmére vonatkozó biztonságos kikötővel kapcsolatosan. Az FTC tehát nem tölt be olyan szerepet, mint amilyen a 95/46 irányelv 28. cikkének megfelelően a nemzeti felügyeleti hatóságokat megilleti.

206. Azok az uniós polgárok, akiknek személyes adatait továbbították, olyan, az Egyesült Államokban székhellyel rendelkező, erre szakosodott mediátorokhoz fordulhatnak, mint a TRUSTe és a BBBOnline, és pontosítást kérhetnek abban a kérdésben, hogy a személyes adataikat tároló vállalkozás megsérti-e az öntanúsítás rendszerének feltételeit. A TRUSTe-hez hasonló szervezetek által biztosított választottbíráskodás csak akkor foglalkozhat a személyes adatok védelméhez fűződő jog megsértésével, ha azt öntanúsított vállalkozás követte el, egyéb szervezetek vagy hatóságok esetén nem járhat el. Ezek a mediátorok nem rendelkeznek hatáskörrel arra, hogy ítéletet hozhassanak az amerikai nemzetbiztonsági ügynökségek tevékenységeinek törvényességére vonatkozóan.

81 — C-293/12 és C-594/12, EU:C:2014:238.

82 — 65. pont.

83 — Uo.

84 — Uo., 66. pont.

85 — Lásd ezzel összefüggésben: 2000/520 határozat II. melléklet 11. GYFK „Az FTC fellépése” című pontja és e határozat III., V. és VII. mellékelte.

207. Sem az FTC, sem más mediátor nem jogosult tehát az amerikai nemzetbiztonsági ügynökségekhez hasonló közjogi szereplők által a személyes adatok védelmének elvével szemben elkövetett lehetséges jogsértések ellenőrzésére. Ugyanakkor az ilyen jogkör alapvető fontosságú lenne az ezen adatok hatékony védelméhez való jog teljes körű biztosítása szempontjából. Így a Bizottság a 2000/520 határozatában és ez utóbbi hatályban tartásával nem jelenthette ki, hogy az Egyesült Államokba továbbított személyes adatok összességnek védelme eléri a Charta 8. cikkének (3) bekezdésében biztosított megfelelő szintet, azaz azt, hogy független hatóság hatékonyan felügyeli az ezen adatok védelmére és biztonságára vonatkozó előírások betartását.

208. Következésképpen meg kell állapítani, hogy a 2000/520 határozatban létrehozott biztonságos kikötő rendszerében nincs olyan független hatóság, amely felügyelhetné azt, hogy a biztonságos kikötő elveitől való eltérés alkalmazása a feltétlenül szükséges mértékre korlátozódik-e. Márpedig láthattuk, hogy az Unió szempontjából az ilyen felügyelet lényeges eleme az egyének személyes adatok kezelése tekintetében való védelmének. [86]

209. E tekintetben hangsúlyoznom kell azt a szerepet, amelyet a személyes jogok védelmének az uniós jogban hatályos rendszerében a nemzeti felügyeleti hatóságok betöltenek a 95/46 irányelv 13. cikkében foglalt korlátozásokkal kapcsolatban. Ezen irányelv 28. cikk (4) bekezdésének második albekezdése szerint „[a] felügyelő hatóságoknak foglalkozniuk kell különösen az adatfeldolgozás törvényességének ellenőrzésére irányuló, bármely személy által benyújtott kérelemmel, amennyiben az ezen irányelv 13. cikkének értelmében elfogadott nemzeti rendelkezések alkalmazhatóak”. Analógiát alkalmazva úgy vélem, hogy a biztonságos kikötő elveinek alkalmazása alóli kivételeknek a 2000/520 határozat I. mellékletének negyedik albekezdésében történő megemlítése mellett létre kellett volna hozni egy, a személyes adatok védelmére szakosodott független hatóság által biztosított felügyeleti rendszert is.

210. A független felügyeleti hatóságok beavatkozása ugyanis a személyes adatok védelmét biztosító európai rendszer lényege. Így természetes, hogy egy ilyen hatóság létezését eleve a harmadik ország által biztosított védelmi szint megfelelőségének megállapításához szükséges feltételek egyikének tekintik. Olyan feltételről van szó, amely azt szolgálja, hogy ne kerüljön sor a tagállamokból e harmadik országba irányuló adatáramlás megtiltására a 95/46 irányelv 25. cikke alapján. [87] Amint azt az irányelv 29. cikke által felállított munkacsoport vitaanyagában megjegyzi, Európában széles körű egyetértés van abban a kérdésben, hogy „a független hatóság formájában gyakorolt külső felügyelet minden olyan rendszer szükséges eleme, amely a személyes adatok védelmére vonatkozó szabályok tiszteletben tartásának biztosítását szolgálja” [88].

211. Hangsúlyozom emellett, hogy a FISC nem biztosít tényleges jogorvoslatot azon uniós polgárok számára, akiknek a személyes adatait az Egyesült Államokba továbbították. A kormányzati szervek által a külföldi hírszerző szolgálatok felügyeletéről szóló 1978. évi törvény 702. szakasza keretében folytatott megfigyelésekkel szemben ugyanis védelmet csak az amerikai polgárok, valamint az Egyesült Államokban jogszerűen letelepedett és tartósan ott tartózkodó külföldi állampolgárok élvezhetnek. Amint arra maga a Bizottság is rámutatott, az amerikai hírszerzés programok felügyelete javítható lenne a FISC szerepének megerősítésével és az egyének számára biztosított jogorvoslati lehetőségek bevezetésével. Ezek az eszközök csökkenthetnék az olyan adatkezelések számát, melyek nemzetbiztonsági szempontból nem érintett uniós polgárok személyes adataira vonatkoznak. [89]

86 — Lásd: Digital Rights Ireland és társai ítélet (C-293/12 és C-594/12, EU:C:2014:238, 68. pont, valamint az ott hivatkozott ítélkezési gyakorlat).

87 — Lásd: Poullet, Y., „L’autorité de contrôle: ‘vues’ de Bruxelles”, *Revue française d’administration publique*, 89. sz., 1999. január–március, 69. o., és különösen 71. o.

88 — Lásd: a Bizottság WP 12. sz., a fenti 58. oldalon található lábjegyzetben említett munkadokumentuma.

89 — Lásd: COM(2013) 846 final, 10. és 11. o.

212. Másfelől a Bizottság maga mutatott rá, hogy az uniós polgároknak nincs lehetőségük betekinteni az adatokba, azok helyesbítését, illetve törlését kérni, vagy közigazgatási, illetve bírósági jogorvoslattal élni személyes adataiknak az amerikai hírszerzési programok keretében zajló gyűjtése és további feldolgozása tekintetében. [90]

213. Végezetül meg kell említeni, hogy a magánélet védelméről szóló amerikai jogszabályokat az amerikai és a külföldi polgárokra vonatkozóan eltérően alkalmazzák. [91]

214. A fentiekből következik, hogy a 2000/520 határozat nem tartalmaz a Charta 7. és 8. cikkében foglalt alapvető jogokba való beavatkozás terjedelmét szabályozó egyértelmű és pontos szabályokat. Meg kell tehát állapítani, hogy ezen határozat és alkalmazása az uniós jogrendben, széles körben és különösen súlyosan beavatkozik ezen alapvető jogokba, anélkül hogy e beavatkozást pontosan körülhatárolnák olyan rendelkezések, amelyek lehetővé teszik, hogy az ténylegesen a feltétlenül szükséges mértékre korlátozódjon.

215. A Bizottság tehát azzal, hogy elfogadta a 2000/520 határozatot, és ezt követően hatályban tartotta, átlépte a Charta 7. és 8. cikkében, valamint 52. cikkének (1) bekezdésében felállított, az arányosság elvének tiszteletben tartásához szükséges korlátokat. Ehhez adódik az Uniós polgárok számára a Charta 47. cikkében biztosított, a hatékony jogorvoslathoz való jogba történő indokolatlan beavatkozás megállapítása.

216. Következésképpen ezt a határozatot érvénytelennek kell nyilvánítani, mivel az alapvető jogoknak a fentiekben leírt megsértése miatt nem fogadható el, hogy az e határozat által létrehozott biztonságos kikötő rendszere megfelelő védelmi szintet biztosít az Unióból az Egyesült Államokba továbbított személyes adatok számára.

217. Úgy gondolom, hogy az uniós polgárok alapvető jogainak ilyen sérelme esetén a Bizottságnak fel kellett volna függesztenie a 2000/520 határozat alkalmazását.

218. Ez a határozat határozatlan időre szól. Márpedig a jelen ügy bizonyítja, hogy a valamely harmadik ország által nyújtott védelem megfelelő jellege az említett határozat alapját képező ténybeli és jogi körülmények alakulása szerint az idő múlásával változhat.

219. Rámutatok, hogy a 2000/520 határozat maga is tartalmaz olyan rendelkezéseket, amelyek lehetőséget biztosítanak a Bizottság számára, hogy e határozatát a körülményekhez igazítsa.

220. Amint az e határozat (9) preambulumbekezdéséből kiderül, „[a]z elvek és GYFK által létrehozott »biztonságos kikötő« felülvizsgálatra szorulhat, figyelembe véve a tapasztalatokat, az adatvédelem fejlődését, olyan körülmények között, amelyekben a technológia egyre könnyebbé teszi a személyes adatok továbbítását és kezelését, valamint figyelembe véve az érintett végrehajtó hatóságok jelentéseit a megvalósításról”.

221. Hasonlóképpen, az említett határozat 3. cikkének (4) bekezdése értelmében „[h]a az (1), (2) és (3) bekezdés alapján összegyűjtött információk azt bizonyítják, hogy az Egyesült Államokban a gyakran felvetődő kérdésekkel összhangban bevezetett elveknek való megfelelés biztosításáért felelős bármely szerv nem hatékonyan tölti be szerepét, a Bizottság tájékoztatja az Egyesült Államok Kereskedelmi Minisztériumát, és szükség esetén […] intézkedéstervezeteket nyújt be e határozat visszavonása, felfüggesztése vagy hatályának korlátozása céljából”.

90 — Lásd: COM(2013) 847 final, 7.2. p., 20. o.

91 — Lásd ebben a kérdésben: Kuner, C., «Foreign Nationals and Data Protection Law: A Transatlantic Analysis», *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, 213. o., különösen a 216. és azt követő pontjai.

222. Emellett a 2000/520 határozat a 4. cikkének (1) bekezdése szerint „bármikor kiigazítható a végrehajtásával kapcsolatos tapasztalat fényében, illetve ha az Egyesült Államok jogszabályainak követelményei szigorúbbá válnak az elvek és a GYFK által biztosított védelmi szintnél. A Bizottság a tagállamok felé történő értesítése után három évvel minden esetben értékeli e határozat végrehajtását a rendelkezésre álló információk alapján, és beszámol a 95/46[…] irányelv 31. cikke alapján létrehozott bizottságnak bármilyen vonatkozó megállapításról, beleértve az olyan bizonyítékokat, amelyek hatással lehetnek annak értékelésére, hogy az e határozat 1. cikkében meghatározott rendelkezések a 95/46[…] irányelv 25. cikke értelmében megfelelő védelmet biztosítanak, illetve annak bizonyítékát, hogy ezt a határozatot megkülönböztető módon hajtják végre”. A 2000/520 határozat 4. cikkének (2) bekezdése értelmében „[a] Bizottság szükség esetén intézkedéstervezeteket terjeszt elő a 95/46/EK irányelv 31. cikkében említett eljárásnak megfelelően”.

223. A Bizottság észrevételeiben megállapította, hogy „a biztonságos kikötő elveinek elfogadása nagy valószínűség szerint korlátozott, anélkül hogy ez megfelelne a nemzetbiztonságra vonatkozó kivétel szigorúan körülhatárolt feltételeinek” [92]. E tekintetben megjegyzi, hogy „[a] kérdéses kiszivárogtatások olyan tömeges szintű, különbségtétel nélküli megfigyelésre világítottak rá, amely nem összeegyeztethető az ezen kivételben megszabott szükségesség feltételével, sem általában a Charta 8. cikkében található személyes adatok védelmével” [93]. A Bizottság másfelől maga is megállapította, hogy „[e] megfigyelési programok szerteágazása – az [uniós] polgárok nem egyenrangú kezelésével együtt – kérdésessé teszi a védett adatkikötőről szóló megállapodás által nyújtott védelem szintjét” [94].

224. Ráadásul a Bizottság a tárgyaláson kifejezetten elismerte, hogy a 2000/520 határozat jelenlegi alkalmazása során nincs garancia az uniós polgárokat megillető adatvédelmi jog biztosítására. Ez a megállapítás ugyanakkor a Bizottság szerint nem teszi érvénytelenné e határozatot. Ugyan a Bizottság egyetért azzal az állítással, mely szerint az új körülményekre válaszul cselekednie kell, azonban úgy tekinti, hogy a biztonságos kikötő rendszeréről szóló, az Egyesült Államokkal folytatandó tárgyalások megindításával meghozta a megfelelő és arányos intézkedéseket.

225. Nem osztom e véleményt. Ebben az átmeneti időszakban ugyanis lehetővé kellene tenni a nemzeti felügyeleti hatóságok kezdeményezésére, vagy e hatóságok előtt benyújtott panaszok alapján a személyes adatok Egyesült Államokba irányuló továbbításának felfüggesztését.

226. Egyébként úgy vélem, hogy az ilyen megállapítások alapján a Bizottságnak fel kellett volna függesztenie a 2000/520 határozat alkalmazását. A 95/46 irányelv, valamint a Charta 8. cikke által követett, a személyes adatok védelmére irányuló célkitűzés nemcsak a tagállamokra, hanem az Unió intézményeire is kötelezettségeket szab, amint az a Charta 51. cikkének (1) bekezdéséből következik.

227. A Bizottságnak a valamely harmadik országban nyújtott védelmi szintre vonatkozó értékelése során nem csak ennek az országnak a belső jogát és nemzetközi kötelezettségvállalásait kell vizsgálnia, hanem azt a módot is, ahogy a személyes adatok védelmét biztosítja. Amennyiben a gyakorlat vizsgálata működési zavarra világít rá, a Bizottságnak lépnie kell, és adott esetben haladéktalanul fel kell függesztenie, illetve módosítania kell a határozatát.

228. Amint a fenti okfejtésből láthatjuk, a tagállamok kötelezettsége elsősorban az, hogy nemzeti felügyeleti hatóságuk intézkedésével biztosítsa a 95/46 irányelvben szereplő szabályok tiszteletben tartását.

229. A Bizottság köteles az érintett országok részéről tapasztalt hiányosságok esetén felfüggeszteni az ezen irányelv 25. cikkének (6) bekezdése alapján hozott határozatok alkalmazását, akár az ezen országgal a hiányosságok megszüntetése céljából folytatott tárgyalások idején is.

92 — 44. pont.

93 — Uo.

94 — Lásd: a 2. lábjegyzetben említett bizottsági közlemény, 5. o.

230. Emlékeztetek arra, hogy a Bizottság által e rendelkezés alapján elfogadott határozat annak megállapítására irányul, hogy valamely harmadik ország megfelelő védelmi szintet „biztosít-e” az ezen országba továbbított személyes adatok számára. A jelen időben ragozott „biztosít” kifejezés azt jelenti, hogy egy ilyen határozat akkor tartható fenn, ha olyan harmadik országra vonatkozik, amely az említett határozat elfogadását követően folyamatosan biztosítja a megfelelő védelmi szintet.

231. A 95/46 irányelv (57) preambulumbekezdése szerint „a személyes adatoknak a megfelelő védelmi szintet biztosítani nem tudó harmadik országokba irányuló továbbítását meg kell tiltani”.

232. Ezen irányelv 25. cikkének (4) bekezdése értelmében „[a]mennyiben a Bizottság megállapítja a 31. cikk (2) bekezdésében foglalt eljárás során, hogy valamely harmadik ország nem biztosít megfelelő védelmi szintet ennek a cikknek a (2) bekezdése értelmében, a tagállamok megteszik a megfelelő intézkedéseket az azonos típusú adatoknak a szóban forgó harmadik országba irányuló továbbításának megakadályozására”. Másfelől az említett irányelv 25. cikkének (5) bekezdése szerint „[a] Bizottság megfelelő időben tárgyalásokat kezdeményez a (4) bekezdés szerinti megállapításból eredő helyzet megoldására”.

233. Ez utóbbi rendelkezésből következik, hogy a 95/46 irányelv 25. cikkében létrehozott rendszerben a harmadik országokkal folytatott tárgyalások célja, hogy orvosolja a megfelelő védelmi szintnek az ezen irányelv 31. cikkének (2) bekezdésében előírt eljárásban megállapított hiányát. A minket foglalkoztató esetben a Bizottság, ezen eljárásnak megfelelően formálisan nem állapította meg, hogy a biztonságos kikötő rendszere nem biztosít megfelelő védelmi szintet: így, noha a Bizottság úgy határozott, hogy tárgyalásokat folytat az Egyesült Államokkal, ennek az az oka, hogy korábban megállapította, hogy e harmadik ország által biztosított védelmi szint nem megfelelő.

234. Bár a Bizottság ismerte a 2000/520 határozat alkalmazása során fellépő működési zavarokat, e határozatot nem függesztette fel, és nem is módosította, így hozzájárult azon személyek alapvető jogainak folytatólagos megsértéséhez, akiknek személyes adatai folyamatosan továbbításra kerültek a biztonságos kikötő rendszerén belül.

235. Márpedig más összefüggésben a Bíróság már határozott úgy, hogy a Bizottság feladata, hogy ügyeljen a szabályozásnak az új adatokhoz való igazítására. [95]

236. A Bizottság ilyen mulasztása, amely közvetlenül sérti a Charta 7., 8., és a 47. cikkében biztosított alapvető jogokat, véleményem szerint további indokul szolgál a 2000/520 határozat érvénytelenségének kimondásához a jelen előzetes döntéshozatali eljárásban. [96]

III – **Végkövetkeztetések**

237. A fenti megállapításokra tekintettel azt javaslom, hogy a Bíróság a következő választ adja a High Court of Ireland által előterjesztett kérdésekre:

A személyes adatok feldolgozása [helyesen: kezelése] vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv 28. cikkét, az Európai Unió Alapjogi Chartájának 7. és 8. cikkére tekintettel úgy kell értelmezni, mely szerint az Európai Bizottság által a 95/46 irányelv 25. cikkének (6) bekezdése alapján hozott határozat

95 — Lásd e tekintetben: Agrarproduktion Staebelow ítélet (C-504/04, EU:C:2006:30, 40. pont).

96 — Bár a Bíróság a T. Port ítéletben (C-68/95, EU:C:1996:452) úgy rendelkezett, hogy „a szerződés nem teszi lehetővé, hogy a nemzeti bíróság előzetes döntéshozatal iránti kérelmében azt kérje a Bíróságtól, hogy előzetes döntéshozatal során állapítsa meg egy intézmény mulasztását” (53. pont), úgy tűnik, a Ten Kate Holding Musselkanaal és társai ítéletben (C-511/03, EU:C:2005:625, 29. pont) jóval kedvezőbb álláspontot foglalt el.

léte nem akadályozhat meg a nemzeti felügyeleti hatóságokat abban, hogy kivizsgálják azon panaszt, mely szerint valamely harmadik ország nem biztosít megfelelő védelmi szintet a továbbított személyes adatok számára, és adott esetben e hatóság felfüggessze ezen adatok továbbítását.

A 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott „biztonságos kikötő” adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló, 2000. július 26-i 2000/520/EK bizottsági határozat érvénytelen.