



EURÓPAI
BIZOTTSÁG

Brüsszel, 2013.11.27.
COM(2013) 842 final

**A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A
TANÁCSNAK**

A terrorizmus finanszírozásának felderítésére szolgáló európai rendszer (TFTS)

{SWD(2013) 488 final}

{SWD(2013) 489 final}

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

A terrorizmus finanszírozásának felderítésére szolgáló európai rendszer (TFTS)

Tekintettel a Bizottság 2011. július 13-i (COM (2011) 429) közleményére, jelen közlemény célja a terrorizmus felderítésére szolgáló rendszer (EU TFTS) megvalósíthatóságával kapcsolatban készített elemzés eredményéről szóló tájékoztatás az Európai Parlament és Tanács számára.

1. HÁTTÉR

1.1. A felkérés eredete és a fogalmak meghatározása

Az EU és az USA közötti, a terrorizmus finanszírozásának felderítésére szolgáló programról (TFTP) szóló megállapodás¹ megkötését megelőző tárgyalások során egyeztetések folytak arról, hogyan biztosítható a legjobban a személyes adatok védelme és az alapvető jogok tiszteletben tartása a megállapodás keretei között. Néhány fél azzal érvelt, hogy amennyiben az adatlehívás európai területen történne, az korlátozná az USA-ba történő adattovábbítás mennyiségét, és ezáltal magasabb szintű adatvédelmi garanciákat eredményezne. Néhány tagállam szerint hosszú távon többletértéket jelent egy, a terrorizmus finanszírozásának felderítésére szolgáló független európai rendszer kifejlesztése. Az Európai Parlament felkérte a Tanácsot és a Bizottságot, hogy tegyenek meg minden szükséges intézkedést a kért adatok Európa területén való lehívásának problémáját rendező fenntartható, jogi szempontból megalapozott európai megoldás érdekében. Az EU–USA TFTP-megállapodás megkötésekor a Tanács és az Európai Parlament felkérte a Bizottságot, hogy a megállapodás hatálybalépésétől számított egy éven belül nyújtsa be az adatok Európa területén való lehívásának jogi és technikai kereteit ismertető dokumentumot, a hatályba lépéstől számított három éven belül pedig nyújtson be jelentést az egyenértékű uniós rendszer kialakítása terén elért előrehaladásról². Továbbá a EU–USA TFTP-megállapodás 11. cikke értelmében a megállapodás érvényességi ideje alatt az Európai Bizottság tanulmányt készít egy, az adatok célzottabb továbbítását lehetővé tévő, egyenértékű uniós rendszer lehetséges bevezetéséről.

¹ HL L 195., 2010.7.27., 5. o.

² 2010. július 13-i tanácsi döntés, HL L 195., 2010.7.27., 3. o.

E közlemény alkalmazásában az egyenértékű uniós rendszert külön kell választani az uniós területen történő adatleltár kereteitől. Az uniós területen történő *adatleltár keretei* alatt egy olyan rendszer értendő, amely az uniós területén belül keresési lehetőséget biztosít a jelenleg az EU-tól az USA-nak szolgáltatott adatok között. Ezzel ellentétben az *egyenértékű uniós rendszer* egy teljesen független, a terrorizmus finanszírozásának felderítésére szolgáló európai rendszer lenne, amely biztosítaná kijelölt szolgáltató(k) adataihoz történő hozzáférést, ezen adatok elemzését és az adatok körében végzett keresést. Bármely uniós rendszer létrehozása az EU–USA TFTP-megállapodás módosítását kívánná meg.

1.2. Megtett intézkedések

2010 decemberében a Bizottság megrendelt egy *tanulmányt*, amelyet 2011 júliusában kiterjesztettek egy adatmegőrzési és -leltári rendszer további lehetőségére. A tanulmány készítése során a Bizottság négy szakértői találkozót rendezett. Ezeken egyebek mellett az Europol, az európai adatvédelmi biztos, a TFTP kijelölt szolgáltatója³, valamint az érdekelt minisztériumokat, bűnüldöző és hírszerző ügynökségeket, továbbá az adatvédelmi hatóságot képviselő tagállami szakértők vettek részt.

A Bizottság a 2011. július 13-i *Európai Parlamenthez és a Tanácshoz címzett közleményében* („2011-es közlemény”) az európai terrorizmus finanszírozásának felderítésére szolgáló öt lehetséges rendszer megoldását vázolta fel (EU TFS). Ezek közül három tűnt megvalósíthatónak. A 2011-es közlemény célja a továbblépésről való vita előmozdítása és a hatásvizsgálat előkészítése volt.

A kérdést 2011 októberében tárgyalták az IB Tanács és az Európai Parlament Állampolgári Jogi Bizottsága előtt.

Mivel sem a tagállamok, sem az Európai Parlament nem jelezte, hogy egyértelműen támogatná valamelyik megoldást, az a döntés született, hogy a hatásvizsgálat során a Bizottság valamennyit megvizsgálja majd, és különböző alternatívákat dolgoz ki velük kapcsolatban. Jelen közlemény a hatásvizsgálat alapul⁴.

³ Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT).

⁴ SWD 2013 (xx)

2. A BIZOTTSÁG FŐ ELVEI ÉS AZ AZONOSÍTOTT SZAKPOLITIKAI VÁLASZTÁSI LEHETŐSÉGEK

2.1. A svéd elnökség alatt elfogadott információkezelési stratégia alapelvei

A javasolt lehetőségek elemzése során a Bizottság figyelembe veszi a 2009-es információkezelési stratégiában⁵ megfogalmazott alapelveket, amelyeket később a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott információkezelés áttekintéséről szóló 2010. évi bizottsági közlemény⁶, és az európai információcsere-modellről szóló 2012. évi közlemény⁷ integrált és továbbfejlesztett.

Az olyan alapelvek, mint az alapvető jogok védelme, a szükségesség, az arányosság és a költséghatékonyság kiemelkedő fontossággal bírnak ebben a tekintetben.

Az Európai Unió Alapjogi Chartájában rögzített *alapvető jogok* – különösen a magánélethez és a személyes adatok védelméhez való jog – védelme elsődleges szempont a Bizottság számára a belső biztonság területén megvalósuló, személyes adatok feldolgozását is érintő új javaslatok kidolgozása során. A Charta 7. és 8. cikke kimondja, hogy mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát és kapcsolattartását tiszteletben tartsák, továbbá mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. Az Európai Unió működéséről szóló szerződés 16. cikke – amely kötelező a tagállamokra, az Unió intézményeire, szerveire és hivatalaira – megerősíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. A Charta 52. cikke értelmében, az arányosság elvére is figyelemmel, a Charta által elismert jogok és szabadságok gyakorlását csak akkor lehet korlátozni, ha az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

A magánéletbe való beavatkozás *szükségesnek* tekinthető, ha sürgős szükséghelyzetben kerül rá sor, ha arányban áll a kitűzött céllal, és ha az igazolására a hatóság által felhozott érvek relevánsak és kielégítőek.

Bár a terrorizmus elleni harc költségeit nehéz megbecsülni pénzügyi értelemben, a *költséghatékonyságnak* továbbra is érvényesülnie kell. Egy *költséghatékonny* megközelítés az

⁵ Az uniós belső biztonság terén alkalmazandó információkezelési stratégiáról szóló 2009. november 30-i tanácsi következtetések (16637/09).

⁶ COM (2010) 385., 2010. július 20.

⁷ COM (2012) 735., 2012. december 7.

átfedések minimalizálása és a szinergiák lehetséges maximalizálása érdekében számol a már létező megoldásokkal. Elemezni kell, hogy a meglévő eszközök jobb használatával el lehet-e érni a javaslat céljait.

2.2. Megközelítés

A fent hivatkozott alapelvek tükrében a Bizottság megvizsgálta, hogy egy uniós TFTS szükséges és arányos lenne-e költségei, előnyei és az alapvető jogokra gyakorolt hatásai tükrében a jelenlegi helyzethez viszonyítva.

Előnyeit illetően egy uniós rendszer elősegíthetné az EU és tagállamainak releváns információkhoz való hozzáférését, és erősíthetné azokat az elemzői képességeiket, amelyek célja a terroristák az általuk végrehajtott pénzügyi tranzakciókon keresztül történő felderítése és azonosítása. Mivel a pénzügyi tranzakciók olyan értékes információt jelenthetnek, amely más forrásokból elérhetetlen lehet, ezen eszköz különösen értékes lehet a terrorista tevékenység és az abban részt vevők felderítése szempontjából. Ezért egy uniós TFTS további hírszerzési és felderítési eszközt jelentene a terrorizmus elleni harcban és a biztonság megteremtésében az EU-ban, különösen akkor, ha a rendszer lefedné a különböző pénzügyi adatszolgáltatókat és a különböző tranzakciótípusokat. Az uniós TFTS előnyeinek egyensúlyban kell lennie a bevezetésének és fenntartásának költségeivel, beleértve az EU, a tagállamok és a kijelölt szolgáltatók számára jelentett pénzügyi terhet.

2.3. A szakpolitikai választási lehetőségek bemutatása

Mind az uniós területen történő *adatlehívás kereteire*, mind az *egyenértékű uniós rendszerre* vonatkozóan több megoldási lehetőséget mérlegelt a Bizottság.

2.3.1. Az uniós területen történő adatlehívás keretei

Az uniós területen történő adatlehívás keretei a kijelölt szolgáltató birtokában lévő adatok megőrzésének és lehívásának rendszerén keresztül valósulhatnak meg, közvetlen hozzáférést biztosítva azokhoz az információkhoz, amelyeket jelenleg a TFTP alapján az USA kap meg. Ezt a közvetlen hozzáférést az e célra kijelölt amerikai elemzőknek vagy szakértőknek biztosítanák.

E változat szerint az egyik lehetőség az lenne, hogy a kijelölt szolgáltató szerverein őriznék bizonyos ideig az adatokat, és a kereséseket közvetlenül ezen a szerveren hajtánák végre.

Mindazonáltal az EU–USA TFTP megállapodás szerinti jelenlegi kijelölt szolgáltató szigorú adatvédelmi és biztonsági intézkedéseket vezetett be, amelyek nem teszik lehetővé az üzenetadatokban említett személyek azonosítását, ezért a jelenlegi adatbázisban nem lehet személyes adatok alapján keresni. Szükséges lenne tehát egy különálló adatbázis létrehozása.

Alternatív megoldásként az adatokat egy elkülönített és biztonságos helyen lehetne lehívni és tárolni. A keresésre felhatalmazott amerikai elemzők vagy szakértők a kijelölt szolgáltató telephelyén fizikailag lehetnének jelen, vagy távoli hozzáférésük lenne az adatokhoz. Az adatok elhelyezkedésétől függetlenül, minden esetben átfogó, szilárd és a rendszer struktúrájához igazodó biztosítékokat kell életbe léptetni.

2.3.2. *Az egyenértékű uniós rendszer*

A vizsgálat kiterjedt az egyenértékű uniós rendszer számos lehetséges változatára (ezek ismertetését lásd a 2011-es közleményben): egy teljesen központosított uniós szintű rendszerre, egy tagállami szintű decentralizált rendszerre és három vegyes rendszerre, amelyben mind az EU, mind a tagállamok részt vennének.

Minden változatban több lehetőség is felmerül az uniós rendszer alkalmazási körétől függően. Az üzenettípusoktól és a kijelölt szolgáltatóktól függően, akiket szintén bele kellene venni, többféle választási lehetőség van. Egy egyenrangú uniós rendszer vagy szorosan igazodna az EU–USA TFTP-megállapodáshoz, vagy túllépne a jelenleg az EU-USA TFTP-megállapodás hatálya alá tartozó pénzügyi üzenettípusokon és kijelölt szolgáltatón.

- Egy teljesen központosított uniós szintű változatban egyetlen uniós szerv látná el a rendszer minden kulcsfontosságú funkcióját: adatlehívás kérése, adattárolás, keresés, információelemzés, a rendszer védelme és ellenőrzése, hírszerzési információk továbbítása a tagállamokhoz. Ez a változat jogilag nem állja meg a helyét, mivel nem tartja tiszteletben az EUMSZ 72. cikkét, melynek értelmében a közrend fenntartásának és a belső biztonság megőrzésének biztosításához szükséges intézkedések meghozatala tagállami hatáskör. Egy ilyen rendszer sem megvalósítható, sem elfogadható nem lenne a tagállamok részéről, mivel uniós szintű központi hírszerzés megszervezését jelentené valamilyen formában.

- Egy tagállami szintű decentralizált rendszer azt jelentené, hogy a rendszert a tagállami illetékes hatóságok működtetnék, és nem lennének uniós szinten végrehajtott feladatok. Eszerint mind a 28 tagállamhoz lehetne továbbítani az adatokat, és mind a 28 tagállam végezhetne azokban keresést. Ez a változat többszörözné az adatáramlást, és súlyos költségvonzatokkal járna, továbbá növelné az adatok nem egységes kezelésének kockázatát, és eltérő adatvédelmi mechanizmusokhoz vezetne. Éppen ezért ez a változat sem tűnik életképesnek.

Ezt a két változatot így kizártuk egy részletesebb vizsgálat lefolytatásából.

Az egyenrangú uniós rendszerre vonatkozó három további változatban a különböző feladatok megoszlának a különböző – uniós, illetve nemzeti szintű – szervezetek között (vegyes rendszerek).

E vegyes rendszerek mindegyikében az adatokat folyamatos és ismétlődő alapon a kijelölt szolgáltatótól lehetne igényelni, és azokat az Unió területén, egy biztonságos, helyen lévő adatbázisban hívnák le és tárolnák. A tényleges kereséseket így ebben a központi adatbázisban lehetne végrehajtani. A többi változathoz hasonlóan megfelelő adatvédelmi biztosítékokról kellene gondoskodni.

- A) Az első vegyes rendszerben – az EU TFTS koordinációs és elemző szolgálatban – egy központi uniós egységet kellene felállítani. Feladata a kijelölt szolgáltatótól való adatbeszerzés, keresések lefuttatása, információelemzés és az eredmények továbbítása lenne. A teljesen központosított rendszertől abban különbözne, hogy a tagállamoknak közvetlen hozzáférésük lenne a rendszerhez, továbbá kereséseket kezdeményezhetnének a rendszerben, amelyeket a központi egység vagy nemzeti elemzőik hajtának végre.
- B) A második vegyes rendszerben – az EU TFTS adatle hívási szolgálatban – szintén létre kellene hozni egy uniós központi egységet. Ebben a változatban a tagállamok kérésére az uniós szerv végezné el a kereséseket, és az eredményeket az adatok elemzése nélkül továbbítaná a tagállamok felé. Az uniós szerv ugyanakkor saját maga is tudna kereséseket végezni, és azok eredményét is elemezhetné.

- C) Az utolsó vegyes rendszerben – a pénzügyi hírszerző egység⁸ (FIU) koordinációs szolgáltatban egy eseti jellegű uniós platformot állítanának fel. Ez nem egy állandó szerv lenne, hanem inkább pénzügyi hírszerző szakértők csoportja, amely találkozókat rendezne. A már létező FIU-platformot valószínűleg tovább lehetne fejleszteni e cél érdekében. Minden egyes tagállam kijelölhetne egy nevében eljáró képviselőt. Ez az eseti hatóság összegyűjtené a tagállami FIU-tól érkező kéréseket, és adatkérés formájában továbbítaná azokat a kijelölt szolgáltató felé. A kereséseket, elemzéseket és az eredmények kezelését az egyes tagállamok nevében a tagállamok képviselői végeznék. Ezt követően a tagállamok illetékes hatóságainak feladata lenne a hírszerzési információk felhasználása és további, nemzeti szintű terjesztése.

2.3.3. *Status quo: EU–USA TFTP-megállapodás*

Jelenleg az EU és a tagállamok keresést kérhetnek az USA-tól az EU–USA TFTP-megállapodás értelmében, amely szabályozza a pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítésére szolgáló program céljából történő feldolgozását és átadását.

A TFTP a szeptember 11-i terrorista támadásokat követően az USA-által kifejlesztett terrorizmusellenes eszköz. A kijelölt szolgáltatótól kapott adatokban való keresésen alapul, amibe beletartoznak az EU-ból kapott adatok is.

Az EU–USA TFTP-megállapodás részletesen szabályozza az amerikai hatóságok adatigénylésére vonatkozó eljárást. Az Europol ellenőrzi, hogy az adatátadásra irányuló, USA-tól kapott akérések összhangban vannak-e a megállapodással, különös tekintettel arra, hogy megfogalmazásuk a lehető legpontosabb-e annak érdekében, hogy a kért adatok mennyisége a lehető legkisebb legyen. Számos rendelkezés vonatkozik az adatok biztonságos kezelésére, tárolására és törlésére. A továbbított adatokat biztonságos fizikai helyen tárolják, elkülönítve minden más adattól. A megállapodás ötéves tárolási időszakot ír elő, és rendelkezik az adattárolás szükségességének rendszeres felülvizsgálatára vonatkozó köteleességről. Az USA-ban működő független ellenőrök közül kettőt az EU választ ki. Az ellenőrök folyamatos ellenőrzést gyakorolnak a rendszer felett, és minden az Egyesült Államok Pénzügyminisztériuma által végrehajtott keresést ellenőrizhetnek a tekintetben, hogy

⁸ A Tanács 2000. október 17-i határozata a tagállamok pénzügyi hírszerző egységeinek az információcsere terén folytatott együttműködésére vonatkozó rendelkezésekről.

a keresés valóban a terrorizmussal vagy annak finanszírozásával kapcsolatban álló alanyra vonatkozik-e.

A megállapodás rendelkezéseket tartalmaz a személyes adatokhoz való hozzáférés és helyesbítés jogát illetően, illetve a jogorvoslati eljárásra vonatkozóan is. A megállapodás értelmében bárki, aki úgy érzi, hogy személyes adatait a megállapodás megsértésével kezelték hatékony bírósági és közigazgatási jogorvoslatot kérhet az EU, a tagállamok és az Egyesült Államok joga szerint. A megállapodás állampolgárságra és tartózkodási helyre tekintet nélkül biztosítja magánszemélyek számára az amerikai jog szerint elérhető jogorvoslati eljárásra való lehetőséget a hátránnyal járó igazgatási intézkedésekkel szemben.

A megállapodás értelmében kapott személyes adatokkal kapcsolatban hozott, hátránnyal járó pénzügyminisztériumi igazgatási intézkedésből adódó jogorvoslat iránti igényre vonatkozó releváns egyesült államokbeli jogszabályok magukba foglalják a közigazgatási eljárási törvényt és az információhoz való szabad hozzáférésről szóló törvényt is. A közigazgatási eljárási törvény biztosítja a bírósági jogorvoslati lehetőségét azon személyek számára, akiket valamely amerikai kormányzati intézkedés eredményeképpen ért kár. Az információhoz való szabad hozzáférésről szóló törvény biztosítja a személyek számára, hogy a kormányzati nyilvántartások adataihoz történő hozzáférés érdekében közigazgatási és bírósági jogorvoslatot vehessenek igénybe. A már létező hozzáférési és helyesbítési, törlési, vagy személyes adatok korlátozására irányuló egységes eljárások célja a e jogok gyakorlásának megkönnyítése az állampolgárok számára, ahogyan arról a Bizottság, az USA és a 29. cikk szerinti munkacsoport megállapodott. A megállapodás végrehajtását, annak biztosítékait és kontrollmechanizmusait rendszeresen felülvizsgálják a megállapodás 13. cikke értelmében. Eddig két ilyen felülvizsgálatot végeztek (2011-ben ⁹és 2012-ben¹⁰), melyek során megállapították, hogy a megállapodást megfelelően hajtották végre. Előreláthatólag 2014-ben kerül sor a harmadik vizsgálatra. A megállapodás 6. cikke értelmében készített, a rendelkezésre bocsátott adatok jelentőségéről szóló közös jelentés bemutatja a TFTP előnyeit a terrorizmus és annak finanszírozása elleni küzdelem és a megelőzés terén, és ismerteti a TFTP tagállami használatát. A TFTP keretében átadott információk és azok pontossága lehetővé teszi a terroristák és támogató hálózatuk felderítését és azonosítását, bárhol

⁹ SEC (2011) 438 (2011. március 30.).

¹⁰ SWD (2012) 454 (2012. december 14.).

helyezkedjenek el a világban. Új megvilágításba helyezi a terrorista szervezetek meglévő pénzügyi struktúráit, lehetővé teszi a pénzügyi támogatás új irányainak és az abban részt vevőknek az azonosítását.

3. ÉRTÉKELÉS

Amikor a Bizottság mérlegeli, hogy javasolja-e vagy sem uniós TFTS létrehozását, összhangba kell hoznia egy esetleges uniós rendszer horderejére vonatkozó különböző nézeteket és elvárásokat. Az uniós TFTS céljait különbözően látják a különböző résztvevők és döntéshozók. A Bizottság mindkét forgatókönyv lehetőségét és következményeit megvizsgálta a korábban részletezett új szakpolitikai kezdeményezések fejlődésének és végrehajtásának elvei tükrében. Mindegyik változatot súlyozta szükségesség, arányosság és költséghatékonyság tekintetében.

3.1. Az uniós területen történő adatlehívás keretei

Ahogy a 2.3.1. szakaszban ismertettük, egy adatmegőrzési és -lehívási rendszerre vonatkozó változat a jelenleg az EU–USA megállapodás értelmében az USA számára továbbított adatok európai területen történő gyűjtésére, tárolására és keresésére szolgálna. Ez nem járna további hírszerzési előnyökkel sem az EU, sem a tagállamok számára a jelenlegi helyzettel összehasonlítva. Ezzel ellentétben, amennyiben a TFTP-adatokat az USA-ban és az EU-ban tárolnák, a jelenleg egyetlen TFTP-adathalmazon végrehajtott keresések szétaprózódása negatív hatással lenne a hírszerzési információk mennyiségére és minőségére, és összességében csökkentené a TFTP hatékonyságát. Ez jelentősen lelassíthatja az elemzés folyamatát, mivel a két helyszínen tárolt TFTP-adatbázisban különböző egymást követő keresések lehetnek szükségesek a hírszerzési információk lekövetése érdekében. A gyorsaság gyakran létfontosságú a terrorizmus felderítése szempontjából.

Önmagában az európai és nem amerikai területen történő adatlehívás nem garantálja jobban a személyes adatok védelmét. Az adatok megfelelő kezelése tekintetében az adatokhoz való hozzáférés védelme kulcsfontosságú, tekintet nélkül azok elhelyezkedésére. Ennek érdekében jelentős biztosítékokról kellene gondoskodni, amelyek garantálnák az adatfeldolgozás és kezelés szükséges követelményeinek való megfelelést. A rendszert ellenőrző funkcióval kellene ellátni, amely a keresési kéréseket és azok megalapozottságát ellenőrizné. A különböző ellenőrök szerepe létfontosságú lenne annak biztosításában, hogy az adatokat csak

az alapító megállapodásban meghatározott, korlátozott célokra használják. Olyan intézkedéseket kellene hozni, amelyek megakadályozzák az adatokhoz való jogosulatlan hozzáférést vagy azok közzétételét. Ilyen lehet például az adatok biztonságos fizikai környezetben történő tárolása. Integrálni kellene a rendszerbe a személyes adatokhoz való hozzáférésre és azok helyesbítésére vonatkozó eljárásokat és a kapcsolódó jogorvoslati eljárásokat is. A rendszer megfelelő működésének biztosítása érdekében külső ellenőrzést kellene lefolytatni.

Az EU–USA TFTP-megállapodás értelmében az USA nem fér hozzá a kijelölt szolgáltató minden adatához, csak az adatok általa kért és az Europol által múltbeli és jelenlegi terrorfenyegetettségi elemzések alapján jóváhagyott részéhez. Hacsak egy hasonló, az adatkérések kezdeti leszűkítésére vonatkozó mechanizmus nem kerül alkalmazásra, a kijelölt szolgáltató összes adatában végzett közvetlen keresés engedélyezése tovább növelné az adatkitettségi mértékét és az adatvédelmi jogokra gyakorolt hatásokat. Ez a kijelölt szolgáltató munkamódszerének és adattárolási rendszerének jelentős mértékű megújítását kívánná meg. Jelenleg a megállapodás hatálya alá tartozó pénzügyi üzeneteket olyan formában tárolják, amely nem teszi lehetővé a közleményben említett személyek azonosítását. Minden egyes pénzügyi üzenetet titkosítanak, továbbá az üzenetek csak törzsadatokkal kereshetőek (ilyen adat például az üzenet küldésének dátuma, az üzenet típusa, a küldő és fogadó bank). A kijelölt szolgáltató jelentős adatvédelmi és biztonsági intézkedéseket vezetett be a világ minden részén elhelyezkedő ügyfelei adatainak védelme érdekében. Ezért a jelenlegi kijelölt szolgáltató szerverén való közvetlen kereséshez először minden üzenetet dekódolni kellene. Ez túlzott és aránytalan lenne, mivel a kijelölt szolgáltató szervere több üzenetet tartalmaz, mint amennyit a terrorizmus finanszírozása elleni küzdelem célja megkövetel. Sőt, keresési célokból való közvetlen hozzáférés mérhetetlenül nagy megterhelést jelentene a kijelölt szolgáltató napi működésére, és jelentős működési, biztonsági és rendszerbeli kockázatokkal járna. Ezért a szükséges adatok tárolása a kijelölt szolgáltatónál egy különálló, uniós területen levő adatbázis létrehozását kívánná meg.

Jelentős beruházásra lenne szükség a rendszer felállításához és a biztonsági biztosítékoknak való teljes megfelelés garantálásához. A kijelölt szolgáltató telephelyének vagy más biztonságos helyszínnek alkalmazkodnia kellene a speciális követelményekhez: informatikai

és technikai megoldásokat kellene kifejleszteni és fenntartani, továbbá magasan képzett személyzetet kellene alkalmazni és képezni, akik képesek a rendszert irányítani és felügyelni.

E változat szerint az EU és a tagállamok viselnék egy harmadik ország tulajdonában álló eszköz, a TFTP kiszolgálására felállított mechanizmus minden költségét és a vele járó kényelmetlenségeket. Jelen pillanatban ez a változat nem tűnik szükségesnek, arányosnak vagy költséghatékonyak, tekintettel arra, hogy nem járna további hírszerzési előnyökkel, sokba kerülne és munkaigényes lenne a felállítása, továbbá kockázatot jelentene a személyes adatok védelmének szempontjából.

3.2. Az egyenértékű uniós rendszer

Egy teljesen központosított uniós TFTS megvalósítását kizártuk a részletesebb vizsgálatból, mivel hiányzik a jogalap hozzá, továbbá kicsi az esélye annak, hogy a tagállamok elfogadják az EU központosított szerepét egy olyan területen, amely tagállami hatáskör. Egy teljesen decentralizált rendszert azért zártuk ki a vizsgálatból, mert komoly költségvonzatai lennének, és többszörözött hatással járna az adatvédelmi jogokra. Az értékelt három vegyes rendszer a tagállami ellenőrzés különféle szintjeit biztosítaná a tagállamok és a központosított uniós szerv által végrehajtott keresések felett.

Egy egyenértékű uniós rendszer alkalmazási körének kiterjesztése az automatizált elszámolóházakra, az elektronikus pénzre és más nem FIN típusú adatokra hírszerzési előnyöket eredményezne azáltal, hogy növelné az EU képességét az Unión belüli kifizetések felderítésére, és a csak FIN-üzenetekkel foglalkozó rendszernél időtállóbb rendszert teremtené. Mindazonáltal minden egyes további kijelölt szolgáltató hozzáadása a rendszerhez az adatvédelmi jogok megsértésének növekvő kockázatával járna, ezért szigorú feltételek, biztosítékok és ellenőrzési intézkedések elfogadását kívánná meg. Ez a kijelölt szolgáltatóra nehezedő adminisztratív terhet is növelné. Több adatszolgáltató és üzenettípus bevonása egy ilyen komplex, szervezeti és technikailag kihívást jelentő rendszerbe szintén számottevően növelné a költségeket.

Az elemzés arra a következtetésre jutott, hogy bármely megvalósítható uniós TFTS csak FIN-üzenetadatokat használna, mivel a Bizottság szerint a többféle adattípus nyújtotta előnyök nem ellensúlyozzák a magánvállalkozásokra nehezedő jelentős költségeket és a magánélethez és adatvédelemhez való jogban esett károkat, amelyek egy ilyen rendszerből adódnának. Ezért

mivel az uniós rendszer ugyanazzal a kijelölt szolgáltatóval és üzenettípussal működne, mint a TFTP, a szerzett hírszerzési információk minősége és mennyisége, továbbá az adatkitettség mértéke összehasonlítható lenne az EU–USA TFTP-vel.

A fent leírtaknak megfelelően így három változat létezik az egyenértékű uniós rendszer megvalósítására: A) az uniós TFTS koordinációs és elemző szolgálat, B) az uniós TFTS adatle hívási szolgálat, és C) a pénzügyi hírszerző egység koordinációs szolgálat.

Az A) változat valószínűleg pozitív hatással járna a terrorizmus elleni küzdelem és az EU biztonságának megerősítésére. Mivel mind az EU, mind a tagállami csoportok keresést és elemzést is végeznének, jórészt biztosítani lehetne az EU és a tagállamok speciális hírszerzési igényeinek maradéktalan számításba vételét, és azt, hogy a rendszer az uniót fenyegető sajátos veszélyekre koncentráljon. Ez a fejlesztés azonban közép- és hosszútávon a tagállamok növekvő információ- és elemzésmegosztási hajlandóságától függ. Nem tisztázott, hogy milyen mértékben lehet számítani ilyen megnövekedett információáramlásra. Emellett, mivel a tagállamok számára továbbra is lehetőség lenne TFTP szerinti kereséseket kérni az USA-tól, egy egységesebb uniós helyzetkép kialakítása csak a tagállamok jelentős elkötelezettsége és együttműködése esetén lenne biztosítható.

A B) változat pozitív hatással járna a terrorizmus elleni küzdelem és az EU biztonságának megerősítésére. A rendszer eredményesebbválaszokat kínálna az uniós fenyegetettség-elemzésekre, mivel a keresések a tagállamok speciális hírszerzési igényei szerint lennének lefuttatva. Ugyanakkor egy központosított uniós szerv szerepe a keresések lefuttatására és a kapott adatoknak a keresést kérő tagállam felé történő továbbítására korlátozódna, és így e szerv leginkább „kapuőrként” működne. Ennek eredményeképpen nem lennének uniós szintű elemzések, és egy egységesebb uniós hírszerzési helyzet-elemzés biztosításának lehetősége teljes mértékben a tagállami elemzéseknek a rendszeren kívül történő megosztásától függne. Mivel ez a rendszer képtelen lenne garantálni a keresés fogalmának egységes megközelítését, a hamis pozitív eredmények kockázata megnövekedne, aminek hatása az adatvédelmi és a magánélethez való jogokban csapódna le.

A C) változat képes reagálni a tagállamok sajátos hírszerzési igényeire, és pozitív hatást gyakorolna a terrorizmus elleni küzdelem és a biztonság megerősítésére. Mivel a nemzeti FIU-k felelnének a tagállami keresésekért és elemzésekért, ez a változat ugyanazoktól a

hátrányoktól szenved, mint a B) változat – tiszta kép csak a rendszeren kívül, megerősített tagállami együttműködés keretében alakulhatna ki. Továbbá a FIU-k csak a pénzügyi hírszerzésre koncentrálnak, így ezen információk elválasztása egy szélesebb hírszerzési perspektívától megnehezítené a kapcsolódási pontok felfedezését és a terrorizmus finanszírozásának felderítését. Az Unió részvételének mértéke ezen változat szerint nagyon alacsony, és a kapacitások elsősorban nemzeti szinten erősödnének.

A változatok mindegyike jelentős költséget jelentene az Unió, a tagállamok és a kijelölt szolgáltató számára; idetartozik többek között az informatikai infrastruktúra fejlesztése, a biztonság megerősítése, a rendszert irányító, a biztosítékokat és az kontrollmechanizmusokat működtető több tíz vagy akár több száz fős személyzet alkalmazása. Ugyanakkor e lehetséges rendszerek mindegyike alkalmas arra, hogy elősegítse egy jobb európai biztonsági helyzet létrejöttét, mivel az európai igényekből kiinduló fenyegetettségértékeléseken alapulna.

Egy európai területen működő független hírszerzési és nyomozó eszköz megszüntetné az USA-ba történő adattovábbítás szükségességét. Ugyanakkor bármely uniós TFTP a jelenleg hatályban lévő EU–USA TFTP-megállapodáshoz hasonló, széleskörű adatvédelmi biztosítékok és kontrollmechanizmusok kialakítását igényelné, amelyeknek meg kellene felelniük az uniós és tagállami adatvédelmi vívmányoknak. Bármely uniós rendszerben történő keresésre irányuló kérelmet ellenőrizni kellene abból a szempontból, hogy megfelel-e a terrorizmus és annak finanszírozása elleni küzdelem szigorúan értelmezett céljának, beleértve azt is, hogy az adattovábbítás indokolt-e. Szakképzett, független ellenőrök feladata lenne mindenekelőtt az egyes uniós és tagállami megkeresések ellenőrzése a megfelelő felhatalmazás, továbbá a terrorizmus és annak finanszírozása elleni küzdelem céljának indokoltsága szempontjából. Biztosítani kellene az adatok biztonságos kezelését és tárolását, és meg kellene előzni a jogosulatlan hozzáférést. A rendszer megfelelő működését és biztosítékait külső ellenőrzés keretében kellene megvizsgálni. Integrálni kellene a rendszerbe a személyes adatokhoz való hozzáférésre és azok helyesbítésére vonatkozó eljárásokat és a kapcsolódó jogorvoslati eljárásokat.

Következtetésként megállapítható, hogy a Bizottság – a Parlament és a Tanács kérésének megfelelően – kiértékelte a terrorizmus finanszírozásának felderítésére szolgáló európai

rendszerre (TFTS) vonatkozó lehetséges változatokat, köztük egy adatmegőrző és -lehívó rendszer létrehozásának lehetőségét.

Ezen értékelés figyelembe veszi a svéd elnökség alatt elfogadott információkezelési stratégiában foglaltakat is. Bármely rendszernek szükségesnek, arányosnak és költséghatékonnak kellene lennie, továbbá tiszteletben kell tartania az alapvető jogokat. A Bizottság által a fentebb és a hatástanulmányban részletezettek szerint elvégzett elemzés azt mutatja, hogy minden egyes megvalósítható változatnak vannak előnyei és hátrányai. Ugyanakkor a Bizottság az elmondottak szerint nem vette figyelembe azokat a változatokat, amelyek nem megvalósíthatóak.

Az összegyűjtött információk fényében, egy uniós TFTS-re vonatkozó javaslat benyújtásának szükségessége a jelen szakaszban nem igazolható egyértelműen.

A Bizottság üdvözli az Európai Parlament és a Tanács e közleményről alkotott esetleges véleményét.