



EURÓPAI BIZOTTSÁG

Brüsszel, 2011.7.13.
COM(2011) 429 végleges

**A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A
TANÁCSNAK, A GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK
BIZOTTSÁGÁNAK**

**A terrorizmus finanszírozásának felderítésére szolgáló európai rendszer: rendelkezésre
álló lehetőségek**

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, A GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

A terrorizmus finanszírozásának felderítésére szolgáló európai rendszer: rendelkezésre álló lehetőségek

1. BEVEZETÉS

Amikor a Tanács jóváhagyta az Európai Unió és az Amerikai Egyesült Államok közötti, az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmusfinanszírozás felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás (a továbbiakban: EU-USA TFTP-megállapodás)¹ megkötését, egyúttal felkérte a Bizottságot, hogy a megállapodás hatálybalépésétől (2010. augusztus 1.) számított egy éven belül nyújtsa be az Európai Parlament és a Tanács részére „az adatlehívás uniós területen történő jogi és műszaki keretét”². Az Európai Parlament szintén folyamatosan sürgette, hogy hosszú távon a kért adatok Európa területén való megszerzésének problémájára vonatkozó, fenntartható és jogi szempontból megalapozott európai megoldást dolgozzanak ki.³ „Az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé” című közlemény már leszögezte, hogy a Bizottság 2011-ben uniós szakpolitikát fog kidolgozni az EU területén tárolt pénzügyi üzenetadatok kivonatolására és elemzésére.⁴ Figyelembe véve az amerikai TFTP bizonyított eredményességét, az európai rendszer várhatóan jelentősen hozzájárul azokhoz az erőfeszítésekhez, amelyek a terroristák finanszírozáshoz és egyes anyagokhoz való hozzáféréseinek megakadályozására, valamint ügyleteik nyomon követésére irányulnak. Emellett hivatkozhatunk az EU-USA TFTP-megállapodás 11. cikkére, amely kimondja, hogy a megállapodás érvényességi ideje alatt az Európai Bizottság tanulmányt készít egy, az adatok célzottabb továbbítását lehetővé tévő, egyenértékű uniós TFTP-rendszer lehetséges bevezetéséről. A mostani közlemény az e cikkre és a tanácsi felkérésre adott bizottsági válaszlépések első szakasza. A dokumentum ismerteti, hogy a Bizottság milyen intézkedéseket tett a „jogi és műszaki keret” kialakítására, továbbá bemutatja az e cél eléréséhez fontolóra vett különböző szakpolitikai lehetőségeket. A közlemény a mostani szakaszban nem jelöli meg az előnyben részesített lehetőséget, ugyanakkor bemutatja a figyelembe vett szakpolitikai lehetőségek mérlegelése során releváns szempontokat. Tekintettel a kérdés politikai jelentőségére, valamint jogi és műszaki bonyolultságára, a Bizottság tájékoztatni kívánja a Tanácsot és az Európai Parlamentet a helyzet jelenlegi állásáról, továbbá vitát szeretne kezdeményezni. A Bizottság megítélése szerint e további vita hasznos volna azt megelőzően, hogy a hatásvizsgálat alapján konkrét javaslatok előterjesztésére kerülne sor.

Ezzel összefüggésben hangsúlyozni kell, hogy e közlemény nem előlegezi meg azt a javaslatot, amelyet a Bizottság előterjeszt majd. Bármely jövőbeni javaslat figyelembe fogja venni a fent említett eszmecsereket, valamint a hatásvizsgálatot, amely a Bizottság által 2010 második félévében megrendelt tanulmányra épül majd. Mivel a jogalkotási javaslat érintené

¹ HL L 195., 2010.7.27., 5. o.

² A Tanács 2010. július 13-i határozata, HL C 195., 2010.7.27., 3. o.

³ Lásd például a P7_TA(2010)0143. sz. állásfoglalást, valamint az A7-0224/2010. sz. ajánlás Indokolását.

⁴ COM(2010) 673 végleges, 2010.11.22. Lásd a 2. célkitűzés 2. fellépését, 8. o.

az alapvető jogokat, kiváltképpen az adatvédelmet, a hatásvizsgálat kitüntetett figyelmet fog szentelni a Bizottság esetleges javaslatában szereplő intézkedések szükségességének és arányosságának. Ennek érdekében a Bizottság azt az iránymutatást fogja követni, amelyet az Alapjogi Charta végrehajtására irányuló stratégiáról szóló közleményében⁵ határozott meg.

Emellett a hatásvizsgálat szükséges műszaki háttéranyagot szolgáltat, valamint részletes elemzést ad valamennyi rendelkezésre álló szakpolitikai lehetőségről. Az említett kérdéseket már megvitatták az e területen tevékenykedő számos érdekelttel, köztük a tagállami hatóságokkal, az adatvédelmi hatóságokkal, az Europollal és a kijelölt szolgáltatóval. A fent említett tanulmány végleges eredményei csak az idei év végére válnak hozzáférhetővé. A hatásvizsgálat elkészítésének támogatása érdekében az Európai Bizottság három szakértői találkozót szervezett a fent említett érdekelttel, valamint a TFTP üzemeltetésében részt vevő amerikai hatóságok bevonásával. Az e közleményben tárgyalt szakpolitikai lehetőségek a tanulmány előzetes eredményein és az említett szakértői találkozók során elhangzott vitákon alapulnak.

2. A TERRORIZMUS FINANSZÍROZÁSÁNAK FELDERÍTÉSÉRE SZOLGÁLÓ UNIÓS RENDSZER CÉLKITŰZÉSEI

Az alábbi két fő okból kell uniós rendszert létrehozni a terrorizmus finanszírozásának felderítésére (TFTS):

- a rendszernek hatékony hozzá kell járulnia a terrorizmus és annak finanszírozása ellen az Európai Unión belül folytatott küzdelemhez;
- a rendszernek hozzá kell járulnia a harmadik országok számára átadott személyes adatok mennyiségének korlátozásához. A rendszernek elő kell írnia az Unió területén történő üzemeltetéséhez szükséges adatok feldolgozását, az uniós adatvédelmi elvek és jogszabályok tiszteletben tartása mellett.

Az Egyesült Államokban a terrorizmus finanszírozásának felderítésére irányuló program (TFTP) igazolta, hogy komoly hozzáadott értéket jelent a terrorizmus és annak finanszírozása elleni küzdelemben. Ennek nem csupán az amerikai, hanem az európai uniós és harmadik országbeli hatóságok is hasznát vették. Az EU-USA TFTP-megállapodás⁶ közelmúltbeli felülvizsgálata megerősítette, hogy a TFTP amerikai létrehozása óta több mint 2 500 jelentést ismertettek harmadik országok hatóságaival, ezek túlnyomó többségét (1 700) az Európai Unióval. Az Egyesült Államokbeli program hatékonyságát, valamint a terrorizmus és annak finanszírozása elleni küzdelem terén mutatott értékét a Jean-Louis Bruguière bírő által előterjesztett két jelentés is megerősítette. A bírót az Európai Bizottság jelölte ki 2008-ban a program felülvizsgálata céljából. Az uniós hatóságokhoz eljuttatott TFTP-ből származó információk fontos nyomokat tartalmaztak több nagyszabású (megkísérelt) terrortámadással összefüggésben (Pl.: a madridi és a londoni terrortámadás, a tengerentúli járatok folyékony robbanószerek segítségével történő felrobbantására irányuló 2006. évi összeesküvés, valamint a Németországban található amerikai érdekeltségekkel szemben megkísérelt 2007-es támadás). Az uniós felülvizsgálati munkacsoport szintén arra a következtetésre jutott, hogy „a TFTP-nek a terrorizmus és annak finanszírozása elleni küzdelem szempontjából képviselt

⁵ COM(2010) 573 végleges, 2010.10.19.

⁶ SEC (2011) 438 végleges, 2011.3.30.

többlettértékére vonatkozóan is meggyőző információkat kapott”. E tapasztalatokra figyelemmel alapos indokokkal feltételezhető, hogy az uniós TFTS szintén jelentős többlettértéket fog képviselni az EU-nak és a tagállamoknak a terrorizmus és annak finanszírozása elleni küzdelme szempontjából.

Jóllehet nem fér kétség az amerikai TFTP-nek a terrorizmus és annak finanszírozása elleni küzdelem terén mutatott hatékonyságához, ugyanakkor komoly aggályok fogalmazódtak meg a polgárok alapvető jogaira gyakorolt hatásai tekintetében. Az említett aggályok főként azon kérdés köré csoportosultak, hogy az EU–USA TFTP megállapodás végrehajtása nagy mennyiségű személyes adatnak („tömeges adatok”) az Egyesült Államok hatóságai számára való átadását vonja maga után – ezen adatok többsége olyan polgárokat érint, akiknek semmi közük a terrorizmushoz és annak finanszírozásához. Az adatokat azért tömegesen adják át (a megfelelő adatkategóriák alapján) ahelyett, hogy egyéni alapon (egy vagy több személlyel kapcsolatos megkeresésre válaszoló) szolgáltatnának adatokat, mivel az érintett adatszolgáltató nem rendelkezik kellő műszaki kapacitással ahhoz, hogy egyéni alapon szolgáltatson adatokat. Emellett a szolgáltatónak célzott keresési és elemzési funkciót kellene kiépítenie ahhoz, hogy egyedi alapon bocsáthasson ki ilyen adatokat. A szolgáltató üzleti eljárásai nem teszik ezt szükségessé, és komoly forrásvonzatai is volnának. Továbbá az egyéni alapú adatkérés azt jelentené, hogy a szolgáltató tudomására hoznák, hogy mely személyekkel szemben folytatnak vizsgálatot a terrorizmussal és annak pénzügyi hátterével kapcsolatos nyomozati eljárások során. Mindez befolyásolhatná az ilyen nyomozások eredményességét.

A tömeges adatszolgáltatás ellentételezése céljából komoly biztosítékokat építettek ki az adatokkal való visszaélések megelőzésére. E biztosítékok arra is kiterjednek, hogy a megadott adatok kizárólag a terrorizmus és annak finanszírozása elleni küzdelem céljából kereshetők és használhatók fel. Az EU–USA TFTP megállapodás közelmúltbeli felülvizsgálata megerősítette, hogy az említett biztosítékokat valóban a megállapodás rendelkezéseinek megfelelően alkalmazták.

Mindazonáltal olyan állítások is megfogalmazódtak, hogy ilyen nagy mennyiségű személyes adat harmadik államnak való átadása az érintett polgárok alapvető jogainak nem kívánatos megsértését jelenti, mérlegelve e jogsértés szükségességét és arányosságát. Ezért a Tanács felkérte a Bizottságot, hogy terjesszen elő javaslatokat „az adatlehívás rendszerének uniós területen történő létrehozására”, azzal az átfogó céllal, hogy ezen adatok feldolgozására az uniós adatvédelmi jogszabályoknak és elveknek megfelelően, valamint az Európai Unió Alapjogi Chartájával összhangban kerüljön sor. Ezzel összefüggésben említést érdemel, hogy a pénzügyi adatok hatóságok általi gyűjtése és feldolgozása érinti a személyes adatok védelméhez való jogot, amelyet belefoglaltak az EUMSZ 16. cikkébe és a Charta 8. cikkébe.

A Charta 52. cikke (1) bekezdésének értelmében ezen alapvető jogok csak a törvény által, a kiszámíthatóság biztosításához szükséges pontossággal és minőségben, és e jogok lényeges tartalmának tiszteletben tartásával korlátozhatók. A korlátozásnak az Unió által elismert valamely általános érdekű célkitűzés eléréséhez szükséges és arányos mértékűre kell szorítkoznia. Az említett elveket tehát nem csupán annak eldöntésekkor kell szem előtt tartani, hogy létrehozunk-e uniós TFTS-t vagy sem, hanem a rendszer megvalósítására vonatkozóan rendelkezésre álló különféle szakpolitikai lehetőségek tekintetében is. Ezért ezek az elvek az olyan kérdésekkel kapcsolatos választásokat is befolyásolják, mint a rendszer alkalmazási köre, az alkalmazandó megőrzési időszakok, az egyének hozzáféréssel és törléssel kapcsolatos jogai, stb. A mostani közlemény nem tárgyalja részletesen ezeket a kérdéseket, amelyeket majd a hatásvizsgálatban kell kimerítően elemezni.

Az adatlehívás rendszerének uniós területen történő létrehozása természetesen a meglévő EU–USA TFTP megállapodásra is hatást gyakorolna, amint azt a megállapodás 11. cikkének (3) bekezdése is elismeri, megállapítva, hogy mivel egy uniós TFTP-rendszer felállítása jelentősen módosíthatja e megállapodás kereteit, ha az Európai Unió ilyen rendszer felállításáról határoz, a Feleknek konzultációt kell folytatniuk annak megállapítására, hogy szükséges-e a megállapodás megfelelő kiigazítása. Így az összes szakpolitikai lehetőség hatást gyakorolna a meglévő EU–USA TFTP megállapodás jövőbeni végrehajtására és ennek megfelelő kiigazítására is.

3. A TERRORIZMUS FINANSZÍROZÁSÁNAK FELDERÍTÉSÉRE SZOLGÁLÓ UNIÓS RENDSZER FŐ FUNKCIÓI

A fent említett érdekeltekkel folytatott megbeszélések során felmerült első kérdések egyikét illetően az érdekeltek túlnyomó többsége azon a véleményen van, hogy amennyiben uniós rendszert kell létrehozni a terrorizmus finanszírozásának felderítésére (uniós TFTS), ezt annak érdekében kell megtenni, hogy biztonságot nyújtson az uniós polgárok számára. A rendszer nem hozható létre pusztán azért, hogy az érintett információkat átadják az amerikai hatóságoknak, ugyanis a tagállamok hatóságainak szintén reális érdeke fűződik e rendszer eredményeihez. E megközelítésből az is következik, hogy – bár az amerikai TFTP bizonyosan ötletet adhat e rendszer létrehozásának módja tekintetében – a megfelelő európai rendszernek nem szükségképpen kell másolnia az amerikai TFTP összes elemét. Emellett az európai rendszer létrehozásakor figyelembe kell venni az uniós jogi és igazgatási keret sajátosságait, beleértve a fent említett, alkalmazandó alapjogok tiszteletét.

Mindazonáltal a fent körvonalazott fő céloknak megfelelően, a terrorizmus finanszírozásának felderítésére irányuló bármely rendszernek elő kell irányoznia a következő alapvető funkciók teljesítését:

- a felhatalmazott címzettnak vagy címzetteknek megadandó nyers adatokra vonatkozó kérések előkészítése és (jogilag érvényes) kiadása a pénzügyi üzenetküldési szolgáltatásokra kijelölt szolgáltató(k) számára. Mindez felöleli az igényelhető üzenetkategóriák meghatározását, az ilyen üzenetküldés gyakoriságának megállapítását, továbbá az e kérdéseket érintő kapcsolattartást a szolgáltatókkal;
- a kijelölt szolgáltató(k)hoz intézett, ilyen nyersadatokra vonatkozó kérések nyomon követése és engedélyezése. Ez kiterjed annak ellenőrzésére, hogy a nyersadat-kérés az alkalmazandó korlátozásoknak megfelelően történt-e;
- a kijelölt szolgáltató(k)tól érkező nyers adatok fogadása és tárolása (feldolgozása), beleértve a megfelelő fizikai és elektronikus adatbiztonsági rendszer bevezetését;
- a megadott adatokban való keresések tényleges futtatása a vonatkozó jogszabályokkal összhangban; a tagállami hatóságoknak, az Egyesült Államok vagy más harmadik államok hatóságainak e keresésekre vonatkozó, világosan meghatározott feltételeknek és biztosítékoknak megfelelő kérései alapján, vagy az adatok feldolgozásával megbízott hatóság (vagy hatóságok) saját kezdeményezésére;
- a megadott adatokban folytatott keresések futtatásának nyomon követése és engedélyezése;

- a keresések eredményeinek elemzése oly módon, hogy összevetik ezeket az eredményeket az egyébként rendelkezésre álló információkkal vagy hírszerzési értesülésekkel;
- a keresések eredményeinek (további elemzés nélküli) vagy a felhatalmazott címzettek számára készített elemzéseknek a terjesztése;
- megfelelő adatvédelmi rendszer kiépítése, ideértve a megfelelő adatmegőrzési időket, adatnapló-vezetési kötelezettségeket; a hozzáférés, helyesbítés és törlés stb. iránti kérések kezelését.

Az említett alapvető funkciókat a választott szakpolitikai lehetőség függvényében uniós, tagállami, vagy mindkét szinten megfelelő jogi aktusokban kellene megállapítani.

4. A RENDELKEZÉSRE ÁLLÓ SZAKPOLITIKAI LEHETŐSÉGEK MÉRLEGELÉSE SORÁN FIGYELEMBE VEENDŐ LEGFONTOSABB ELVEK

A rendelkezésre álló szakpolitikai lehetőségek közötti választás – a fentiekben vázolt alapvető funkciók tiszteletben tartására vonatkozó megfontolások mellett – nagymértékben attól is függ, hogy azok milyen teljesítményt nyújtanak több olyan kulcsfontosságú kérdés vonatkozásában, amelyet jelenleg a hatásvizsgálat keretében mérlegelünk, és az alábbiakban részletesebben is tárgyalunk.

4.1. Eredményesség

Kulcsfontosságú tényezőnek számít a különféle szakpolitikai lehetőségek várható eredményessége a terrorizmus és annak finanszírozása elleni küzdelem alapvető céljának teljesítése terén. E tekintetben előnyben kell részesíteni a nemzetközi adatmegosztás és elemzés lehetőségeit kiszélesítő szakpolitikai lehetőségeket, mivel az ilyen adatmegosztás és elemzés fokozza az eredményességet és több hozzáadott értéket nyújt. Kiváltképpen az adatok elemzésével, valamint az elemzések eredményeinek a megfelelő hatóságokhoz történő eljuttatásával megbízandó szervezet(ek) kiválasztása gyakorol komoly hatást a rendszer átfogó eredményességére, valamint az átadandó adatok mennyiségére. Ennek ellenére, a jelenlegi gyakorlatnak megfelelően a tagállamoknak továbbra is teljes körű ellenőrzést kell gyakorolniuk afelett, hogy az információik vagy hírszerzési értesüléseik megoszthatók-e más hatóságokkal.

4.2. Adatvédelem

Az információk és hírszerzési értesülések nemzetközi megosztására és elemzésére csupán szilárd és fejlett adatvédelmi keret alapján kerülhet sor. E keret eredményessége nem csak az adatalanyokat jogaik gyakorlására feljogosító, alkalmazandó jogi rendelkezésektől függ, hanem attól is, hogy rendelkezésre áll-e tapasztalt személyzet (pl.: adatvédelmi tisztviselő, valamint független és tapasztalt adatvédelmi ellenőrző hatóság). Az uniós TFTS kialakításába bevonható szervezetek némelyike már rendelkezik ilyen struktúrával, másoknak viszont ki kellene alakítaniuk azokat. Ezért gondosan elemezni kell a különféle szakpolitikai lehetőségek adatvédelmi vonatkozásait, összhangban az e közlemény 2. szakaszában említett, az alapvető jogok tiszteletben tartására vonatkozó átfogó elvekkel.

4.3. Adatbiztonság

A határozott adatvédelmi rendelkezésekkel egyidejűleg korszerű adatvédelmi infrastruktúrát és technológiát kell alkalmazni. Az adatvédelmi megfontolások abba az irányba mutatnak, hogy korlátozzuk azon weboldalak számát, ahol a megadott adatok feldolgozhatók, továbbá korlátozzuk az adatokhoz való külső hozzáférés minden formáját. A legbiztonságosabb megoldás az volna, ha egy helyen tárolnák az adatokat külső hozzáférési lehetőség nélkül. A TFTS üzemeltetésébe bevonható szervezetek nagy többsége már jelenleg is biztonságos adatfeldolgozási technológiákkal rendelkezik, de jelenleg nem mindegyiküknek van kapacitása az EU Restricted-nél magasabb szinten titkosított adatok kezelésére.

4.4. Adattárolás

Az adattárolás akár tagállami, akár uniós szinten végezhető. Uniós szinten a kijelölt szolgáltatóktól megkapott adatok tárolhatók az Europolnál vagy egyéb EU-s szervnél, pl.: a szabadságon, biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökségnél (IT ügynökség)⁷, amelynek felállítása folyamatban van. Mivel az adattárolás elválaszthatatlanul összekapcsolódik az adatvédelmi és adatbiztonsági kérdésekkel, az adattároló szervezetre vonatkozó döntést szorosan ahhoz kell kötni, hogy az adott szervezetek milyen adatvédelmi és adatbiztonsági rendszert tudnak biztosítani.

4.5. A meglévő struktúrák és eszközök kihasználása

Amennyire lehetséges, minden opciónak ki kell használnia a meglévő eszközöket. Ez csökkenti a költségeket, és lehetőséget ad a megszerzett tapasztalatok, és a meglévő infrastruktúra hasznosítására. A meglévő eszközök felhasználásához arra van szükség, hogy a meglévő szervezetnek adott új feladat jól illeszkedjen az adott szervezet jelenlegi megbízatásához. Például fontóra vehető, hogy az Europol, az Eurojust vagy a nemzeti igazságügyi hatóságok töltsék be a kijelölt szolgáltató(k)hoz intézett adatszolgáltatás iránti kéréseket ellenőrző és engedélyező hatóság szerepét.

4.6. A felelős hatóságok közötti együttműködés

Az alább körvonalazott szakpolitikai lehetőségek eltérő mértékben biztosítják a tagállami hatóságok közötti, illetve a tagállami és az európai hatóságok közötti együttműködést, valamint az információk és a hírszerzési értesülések cseréjét. A különböző tagállamok eltérő módokat honosítottak meg hatóságaiknak a terrorizmus elleni küzdelem terén folytatott együttműködése tekintetében, továbbá bármely uniós szintű fellépésnek tiszteletben kell tartania az EUMSZ-nek a közrend fenntartása, valamint a belső biztonság megőrzése tekintetében élvezett tagállami előjogokról szóló 72. cikkében megállapított korlátozásokat. Ezért bármely uniós TFTS-nek lehetővé kell tennie, hogy a tagállamok jelentős mértékű ellenőrzést gyakoroljanak azon információk és hírszerzési értesülések felett, amelyeket hajlandók megosztani a rendszer keretei között. Az alábbiakban említett szervezetek e kérdésben különböző megközelítéseket dolgoztak ki, amelyek némelyike közvetlenül alkalmazható a létrehozandó rendszerre.

⁷ COM(2010) 93 végleges, 2010.3.19.

4.7. A különböző szakpolitikai lehetőségek lehetséges pénzügyi hatásának első általános áttekintése

Az uniós TFTS létrehozatalának összköltsége, és a költségek uniós és tagállami szint közötti megosztása nagymértékben a szakpolitikai opció megválasztásától függ. A költségek mindenesetre felölelik az alábbiakat:

- a kijelölt szolgáltató(k)tól kapott adatok biztonságos továbbításával és tárolásával összefüggő költségek;
- a keresések futtatásához és a keresési eredmények megadásához szükséges szoftver kifejlesztésével és karbantartásával összefüggő költségek;
- a keresési eredmények vagy elemzések felhatalmazott címzettek részére történő terjesztésének költségei;
- a kereséseket futtató, valamint az eredményeket elemző és terjesztő személyzet személyi költségei;
- a nyomkövetési és ellenőrzési funkciókért felelős személyzet személyi költségei;
- az adatvédelemért és a polgárok jogaiért felelős személyzet személyi költségei.

Jóllehet a részletes költségkalkulációk e szakaszban még nem állnak rendelkezésre, a kezdeti számítások azt jelzik, hogy a tisztán uniós megközelítés, valamint az alábbiakban tárgyalt összes vegyes opció költségei 33–47 millió eurós induló költséget, továbbá 7–11 millió eurós éves üzemeltetési költséget foglalnának magukba. A különböző szakpolitikai lehetőségeket e közlemény alábbi 6. részében ismertetjük. A 3. szakpolitikai lehetőség volna a legdrágább: az EU-t 43 millió EUR, a tagállamokat (összesen) pedig 3,7 millió EUR induló költség, továbbá az EU-t 4,2 millió EUR, a tagállamokat (összesen) pedig 6,8 millió EUR éves üzemeltetési költség terhelné. A 2. opció volna a legolcsóbb: az EU-t 33 millió EUR induló költség terhelné, és uniós szinten 3,5 millió EUR éves üzemeltetési költség jelentkezne, valamint 3,3 millió EUR éves üzemeltetési költséget viselnének a tagállamok (összesen). A 1. opció az alábbi költségekkel járna: az EU-t 40,5 millió EUR induló költség terhelné, és uniós szinten 4 millió EUR éves üzemeltetési költség jelentkezne, valamint 5 millió EUR éves üzemeltetési költséget viselnének a tagállamok (összesen). Természetesen alacsonyabbak volnának ezek a költségek, ha igénybe vehetnénk a meglévő szervezetek személyzetét, illetve a meglévő infrastruktúrát, továbbá szoftvereket és hardvereket. A tisztán tagállami rendszer felállításának és üzemeltetésének költségei sokkal magasabbak volnának (390 millió induló, és 37 millió éves üzemeltetési költség), mivel minden tagállam köteles volna létrehozni magas biztonsági fokú adatfeldolgozó rendszereket, és személyzetet kellene foglalkoztatniuk a rendszer üzemeltetésére.

A fentiek előzetes összegek, amelyeket a hatásvizsgálat eredményeinek fényében tovább kell elemezni és részletezni.

5. FIGYELEMBE VEENDŐ KÉRDÉSEK

Attól függetlenül, hogy a különböző szakpolitikai opciók közül melyiket választjuk ki az uniós TFTP létrehozására és üzemeltetésére, több fontos kérdést is mérlegelni kell az esetleges uniós TFTP alkalmazási köre tekintetében. E kérdéseket az alábbiakban tárgyaljuk.

5.1. A terrorizmus és annak finanszírozása vagy tágabb alkalmazási kör?

A pénzügyi üzenetadatokhoz való hozzáférés nem kizárólag a terrorizmus és annak finanszírozása elleni küzdelemben hasznos. Aligha kétséges, hogy e hozzáférés a súlyos bűnözés egyéb formái – különösen a szervezett bűnözés és a pénzmosás – terén is értékes eszköznek bizonyulna. Mindazonáltal az EU–USA TFTP megállapodás keretében arányossági megfontolásokból gondosan betartották azt a korlátozást, hogy az adatok csak a terrorizmus és annak finanszírozása elleni küzdelem céljából használhatók fel. A mostanáig lefolytatott előzetes eszmecserek azt jelzik, hogy széles körű egyetértés alakult ki a tekintetben, hogy az említett arányossági megfontolások hasonlóan korlátozott alkalmazási körű európai rendszer létrehozása irányába mutatnak, összhangban az e közlemény 2. részében tárgyalt, az alapvető jogok tiszteletben tartására vonatkozó általános megfontolásokkal.

5.2. Több szolgáltató?

Az EU–USA TFTP megállapodás az adatkéréseket jelenleg csak egyetlen, nemzetközi pénzügyi üzenetküldő szolgáltatásokat végző szolgáltatóra korlátozza. Jóllehet ez a szolgáltató egyértelműen a világ legjelentősebb szereplője az említett üzenetküldő szolgáltatások terén, azonban egyéb szolgáltatók is tevékenykednek a piacon. Az összes piaci szereplő számára azonos versenyfeltételek megteremtésének szükségessége, valamint hatékonysági megfontolások egyaránt olyan rendszer létrehozását kívánják meg, amely a nemzetközi pénzügyi üzenetküldő szolgáltatások terén tevékenykedő valamennyi szolgáltatóra alkalmazandó. A rendelkezésre álló opciók közötti választásnál minden esetben szem előtt kell tartani a pénzügyi üzenetküldő szolgáltatásokat nyújtó vállalatok adminisztratív terheit.

5.3. Kizárólag nemzetközi üzenetküldő szolgáltatások vagy pedig nemzeti is?

Az EU–USA TFTP megállapodás jelenleg kizárólag olyan szolgáltatóktól történő adatkérésekre korlátozódik, akik nemzetközi – vagyis transznacionális (pl.: tagállamok közötti) ügyletek végrehajtásához használt – pénzügyi üzenetküldő szolgáltatásokat nyújtanak, de kizárja az egységes eurófizetési térségre (SEPA) vonatkozó pénzügyi üzenetadatokat. Az uniós TFTP esetében azt a lehetőséget is meg kell vizsgálni, hogy kiterjesszük-e a rendszert a tagállamok közötti nem pénzügyi üzenetküldő szolgáltatásokra is, vagy korlátozzuk azt a pénzügyi üzenetadatok nemzetközi cseréjére. A tisztán nemzeti pénzügyi üzenetküldő szolgáltatások (amelyeket kizárólag nemzeti pénzügyi ügyletek során alkalmaznak) jelenleg nem tartoznak az EU-USA TFTP megállapodás hatálya alá. Az ilyen nemzeti pénzügyi üzenetküldő szolgáltatásokhoz való hozzáférés hasznos volna a terrorizmus és a bűnözés egyéb formái elleni küzdelem szempontjából. Ugyanakkor még ha eltekintünk is attól a kérdéstől, hogy az ilyen tisztán nemzeti ügyletekhez való hozzáférés szabályozható-e európai szinten, az előzetes megbeszéléseken az résztvevők többsége aránytalannak tekintette az ilyen hozzáférést, ezért azt ki kell zárni az uniós rendszer hatálya alól.

5.4. Milyen típusú pénzügyi üzenetadatokra kellene alkalmazni a rendszert?

A nemzetközi bankrendszerben sok különféle típusú pénzügyi üzenetadatot használnak. Az EU–USA TFTP megállapodás jelenleg a pénzügyi üzenetadatok egy konkrét típusára korlátozódik. A más típusú pénzügyi üzenetadatokhoz való hozzáférés hasznos volna a terrorizmus és annak finanszírozása – illetve lehetőség szerint a bűnözés egyéb formái – elleni küzdelem szempontjából. Azonban az arányossággal és a polgárok alapvető jogainak tiszteletével kapcsolatos megfontolások e választás tekintetében is azt támasztják alá, hogy korlátozni kell a rendszer alkalmazási körébe tartozó üzenettípusokat. E műszaki kérdés további részletei megtalálhatók a hatásvizsgálatban.

6. AZ UNIÓS TFTS OPCIÓI

Az alábbiakban ismertetendő opciókat a Bizottság jelenleg vizsgálja a most folyó hatásvizsgálat keretében. Az alábbi felsorolás nem feltétlenül taxatív, és semmi esetre sem előlegezi meg a végleges hatásvizsgálatot, és a Bizottság arra alapuló esetleges döntését.

Az új kezdeményezések és az azokat kísérő hatásvizsgálatok elkészítése során mérlegelt egyik lehetőség mindig a meglévő helyzet (*status quo*) fenntartása, ami ebben az esetben azt jelentené, hogy érvényben hagyjuk az EU–USA TFTP megállapodást, és nem terjesztünk elő uniós TFTS-re vonatkozó javaslatot. Ez az opció nem adna választ a Tanácsnak és a Parlamentnek a Bizottsághoz intézett – e közlemény 1. részében említett – azon felkérésére, hogy terjesszen elő javaslatot „az adatlehívás uniós területen történő jogi és műszaki keretének” benyújtására. Emellett ez a lehetőség nem járulna hozzá a harmadik országoknak átadott személyes adatok mennyiségének korlátozásához, továbbá nem írná elő az adatok uniós területen történő – az uniós adatvédelmi elveknek és jogszabályoknak megfelelő – feldolgozását. Az alábbiakban részletesebben kifejtett többi opció mindegyike az uniós TFTS létrehozatalának lehetséges módjait mutatja be.

Elméletileg az uniós TFTS-nek az e közlemény 3. részében meghatározott összes alapfunkciója kialakítható volna uniós vagy tagállami szinten is. Egy vagy több különböző szervezet is megbízható e funkciókkal, az adott szervezetek jelenlegi felelősségi körének megfelelően, illetve új szervezetek is létrehozhatók azok ellátására. E szervezetek akár európaiak, akár tagállamiak is lehetnek. Ebből következően – ugyancsak elvben – elképzelhető kizárólag európai megközelítés, amely szerint uniós szintű szervezeteket bízánk meg az összes alapfunkció ellátásával, illetve kizárólag tagállami megközelítés is, amely szerint az összes funkciót tagállami szinten látnák el. Általában véve azt is szem előtt kell tartani, hogy e konkrét esetben a központosított, decentralizált vagy vegyes rendszer közötti választás nem feltétlenül esik egybe a terrorizmus és a szervezett bűnözés elleni küzdelemre irányuló adatfeldolgozással járó egyéb kezdeményezések tekintetében hozott hasonló döntésekkel, ugyanis az e területen születő egyes kezdeményezéseket azok sajátos tartalma alapján kell megítélni.

A tisztán központosított és a kizárólag nemzeti megközelítés egyaránt komoly hátrányokkal jár. Például a kizárólagosan európai megközelítés esetén bizonyosan hátrányt jelentene a tagállami bűnüldöző és hírszerző szervekkel és gyakorlatokkal való kapcsolat hiánya, és így az nem volna igazán hatékony. Az e kérdések intézéséért felelős tagállami hatóságok hozzájárulásának hiányában csaknem lehetetlen volna meghatározni, hogy mely adatkategóriákat kell lekérni a kijelölt szolgáltató(k)tól. A rendszer hasznossága akkor is csorbát szenvedne, ha csupán az uniós szinten rendelkezésre álló hírszerzési értesülések

alapján keresnének, ugyanis az európai integráció jelenlegi fokán az ilyen hírszerzési információk nagyrészt csak nemzeti szinten állnak rendelkezésre. Emellett nem valószínű, hogy a tagállamok elfogadnának egy tisztán uniós szintű megközelítést, mivel az nem nyújtana hozzáadott értéket a terrorizmus és annak finanszírozása elleni küzdelemben tett saját erőfeszítéseikhez. A konzultációk során a tagállamok azt is jelezték, hogy ez az opció jogi és operatív okok miatt politikailag nehezen volna keresztülvihető számukra.

A másik véglet, a tisztán tagállami megközelítés azzal a kockázattal járna, hogy a különböző tagállamok eltérő módon valósítják meg, továbbá fokozott veszélyt jelentene az adatbiztonságra, mivel a szolgáltatott adatokról 27 különböző másolatot kellene készíteni. A tisztán tagállami megközelítés nehézségeket okozna az összehangolt adatvédelmi keret, valamint az egyéb szükséges korlátozások (ellenőrzésére) – pl. a terrorizmus és annak finanszírozása elleni célhoz kötöttségre – vonatkozó összehangolt megközelítés kialakítása tekintetében is. Továbbá, tisztán nemzeti megközelítés esetén nem egyértelmű, hogy mely tagállamok felelnének a harmadik országokból érkező megkeresések kezeléséért, valamint elveszne az a pótlólagos előny, amit a keresési eredmények európai szintű elemzése biztosítana. Emellett – amint a fentiekben jeleztük – az ezen opcióhoz társuló költségek jóval magasabbak volnának, mivel az összes tagállam köteles volna létrehozni magas biztonsági fokú adatfeldolgozó rendszereket, és személyzetet kellene foglalkoztatniuk a rendszer üzemeltetésére.

Ennélfogva az érdekeltekkel együtt végzett előkészítő tevékenység során hamar megállapítottuk, hogy a lehetséges opciók skálájának két szélén elhelyezkedő megoldások nem támogathatók – olyan konszenzus alakult ki, miszerint az a leginkább valószínűsíthető, hogy a különböző szervezetek közötti uniós és tagállami szintű feladatmegosztást eredményező vegyes megoldás biztosítaná a legjobb eredményt a két fő cél tekintetében. Jóllehet e konszenzus elősegíti a legmegfelelőbb opció meghatározását, a vegyes megközelítés még mindig számos választási lehetőséget takar. Az alábbi szakaszokban azt a három vegyes opciót mutatjuk be némileg részletesebben, amelyek a mostani előkészítő munka során a leginkább megvalósíthatónak bizonyultak. Az opciókat táblázatos formában is bemutatjuk a mellékletben.

6.1. Az uniós TFTS koordinációs és elemzési szolgáltatás (1. opció)

Ez az opció azt jelentené, hogy központi uniós TFTS egységet hoznánk létre az uniós szinten végzendő feladatok és funkciók legnagyobb részének kezelésére. Egyaránt uniós szinten zajlana a kijelölt szolgáltató(k)hoz intézett „nyers” adatok iránti kérelmek kiadása, e kérések ellenőrzése, az adatok keresése és futtatása iránti kérések kezelése, a keresési eredmények igazgatása, és jelentések továbbítása a kereséseket kérő felekhez. Mindazonáltal a kijelölt szolgáltató(k)hoz intézendő kérések előkészítésére a tagállamok felelős hatóságaival történő konzultáció alapján kerülhetne sor, továbbá a tagállamok azt is választhatnák, hogy saját elemzőiket kirendelik a központi egységhez, hogy azok részt vegyenek a keresések futtatásában. A teljes mértékben központosított opcióval ellentétben a tagállamok kérhetnék, hogy – az amerikai TFTP-ben zajló jelenlegi eljáráshoz hasonlóan – futtassák le számukra a kereséseket, vagy pedig azt, hogy saját elemzőik futtassák le a keresést.

A tagállamoknak meg kellene osztaniuk az információkat az uniós TFTS központi egységgel annak érdekében, hogy – mielőtt elindíthatnák a keresést – alátámasszák kérésüket és annak a terrorizmushoz fűződő kapcsolatát, illetve hogy nemzeti hatóságaik „előzetesen engedélyezzék” a kéréseiket. Például a nemzeti terrorelhárítással foglalkozó ügyészek vagy nyomozási bírók tölthetnék be e nemzeti hatóságok szerepét – ha engedélyeznék a

szolgáltatott adatokban való konkrét keresést, az uniós TFTS központi egység további ellenőrzés nélkül elfogadhatná a keresések futtatását. E foratókönyv szerint nem kellene további hírszerzési értesüléseket megadni az uniós TFTS központi egység számára. Az uniós TFTS központi egység továbbítaná a keresések eredményeit és az elemzését, továbbá saját kezdeményezésére is nyújthatna információkat. Az Egyesült Államoknak és más harmadik országoknak – hasonló eljárást követően – szintén kérniük kellene a keresések futtatását.

A biztosítékoknak és ellenőrzési előírásoknak való megfelelés figyelemmel kísérését szintén központosítanák, esetleg külső érdekeltek – pl.: a kijelölt szolgáltató(k) képviselői vagy független felügyelőnek kinevezett személyek – felügyelete mellett. Az adatvédelmet, -integritást és -biztonságot is központi szinten biztosítanánk.

Az Europol és az Eurojust volnának a rendszert alkotó legfontosabb szervek. Ebben az esetben az Europol és az Eurojust által ellátandó feladatoknak összhangban kellene lenniük a szervezeteknek az Európai Unió működéséről szóló szerződésben (EUMSZ) megállapított feladatkörével. Továbbá meg kellene határozni, hogy milyen mértékben kell módosítani a működésüket jelenleg szabályozó jogi aktusokat. Ha az Europolat választanának ki az uniós TFTS központi hatóság szerepére, a szervezetnek kezelnie kellene az adatalanyok hozzáférés, kiigazítás és letiltás iránti kéréseit is, összhangban az Europol meglévő jogi keretével és adatvédelmi rendelkezéseivel. Az uniós TFTS központi egység a meglévő jogi keretnek megfelelően látná el a feladatát, továbbá a jogorvoslati és fellebbezési eseteket szintén a meglévő jogi rendelkezések szerint intézné. Nemzeti szinten a tagállami bűnüldöző hatóságok vennének részt a keresések iránti kérések ellenőrzésében és engedélyezésében. Új tagállami szervek létrehozásának lehetőségét is fontolóra lehetne venni, de a szubszidiaritás elve alapján az volna a leghelyesebb, ha e döntés jogát meghagynánk a tagállamoknak.⁸

6.2. Az uniós TFTS adatle hívási szolgáltatás (2. opció)

Az első szakpolitikai lehetőséghez hasonlóan ez az opció is uniós TFTS központi egység felállításával járna, amelynek feladatköre felölelné a kijelölt szolgáltató(k)hoz intézett „nyers” adatok iránti kérelmek kiadását, a kérések ellenőrzését, a keresések futtatását, valamint a keresések iránti kérések kezelését. Mindazonáltal e lehetőség alapján az uniós TFTS központi egység nem elemezhetné a keresési eredményeket, és nem hasonlíthatná össze azokat egyéb rendelkezésre álló információkkal vagy hírszerzési értesülésekkel, amennyiben e kereséseket tagállami hatóságok kérésére végzik. Ilyen esetekben a központi egység feladata arra szorítkozna, hogy megfelelő módon elkészítse és szétossza a keresési eredményeket.

Az 1. opciónak megfelelően a kijelölt szolgáltató(k)hoz intézett „nyers” adatok iránti kérelmek elkészítése során részletesen egyeztetnének a tagállamokkal. Utóbbiak ismertethetnék sajátos igényeiket a központi TFTS egységgel, amely elemezné azokat, majd ezen elemzés alapján fogalmazná meg a kérés(ek)e)t.

A tagállami hatóságok igényelhetnék, hogy futassanak le kereséseket a számukra. Nemzeti szinten ellenőriznék és validálnák, hogy e kérések mennyire indokoltak és milyen mértékben kapcsolódnak a terrorizmushoz. Az uniós TFTS központi egység lefuttatná a keresést, és az összes eredményt megfelelő módon megszerkesztve visszaküldené a tagállamoknak.

⁸ Ebben a szakaszban a rendszer végrehajtásában esetleg szerepet kapó uniós ügynökségek költségvetésére gyakorolt hatások még nem ismertek.

Kizárólag a tagállami hatóságok végezhetnék el a keresések elemzését, továbbá úgy is dönthetnének, hogy a saját kezdeményezésükre szolgáltatnak információkat.

Az uniós TFTS központi egység feladata volna a keresések végzése, valamint az eredmények elemzése az uniós intézmények, az Egyesült Államok és más harmadik országok számára. A központi egység ennek alapján saját kezdeményezésére is szolgáltatna információt.

Az előző opciónak megfelelően a biztosítékoknak és ellenőrzési előírásoknak való megfelelés figyelemmel kísérését központosítanák, esetleg külső érdekeltek – pl.: a kijelölt szolgáltató(k) képviselői vagy független felügyelőnek kinevezett személyek – felügyelete mellett. Az adatvédelmet, adatintegritást és adatbiztonságot is központi szinten biztosítanánk.

Ismét az előző opcióhoz hasonlóan, az Europol és az Eurojust volnának a rendszert alkotó legfontosabb szervek. Nemzeti szinten a tagállami bűnüldöző vagy hírszerző hatóságok volnának a legfontosabb részt vevő szervek. Az előbbiekhöz hasonlóan, a szubszidiaritás elve alapján a tagállamokra bízánk annak eldöntését, hogy létrehoznak-e új nemzeti szerveket. Az Europol és/vagy a nemzeti egységek kezelnék az uniós polgárok hozzáférési, kiigazítási és törlési kéréseit a nemzeti adatvédelmi hatóságok és az Europol közös ellenőrző szerve bevonásával. A jogorvoslati és fellebbezési eseteket az alkalmazandó tagállami és uniós jogi rendelkezéseknek megfelelően intéznék.⁹

6.3. A Pénzügyi Hírszerző Egység (FIU) koordinációs szolgáltatás (3. opció)

Ez az opció azt jelentené, hogy a tagállami FIU-kból álló, korszerűsített FIU-platformot hoznak létre. Az eseti uniós szintű hatóság a FIU-k által meghatározott igények alapján egységes kérést állítana össze, amelyet szintén központilag ellenőriznének és engedélyeznének, majd ennek alapján „nyers” adatok iránti kéréseket intézne a kijelölt szolgáltató(k)hoz.

Minden FIU felelős volna a tagállama nevében futtatott keresésekért és a keresési eredmények kezeléséért, valamint az elemzések elvégzéséért, és az általa illetékesnek tekintett szervek számára történő továbbításáért. Nemzeti szinten ellenőriznék és validálnák, hogy a kérések mennyire indokoltak és milyen mértékben kapcsolódnak a terrorizmushoz. A FIU-k felelnének a saját kezdeményezésükre történő információszolgáltatásért is.

A korszerűsített FIU-platform képes volna kereséseket végezni és elemezni az eredményeket az uniós intézmények, valamint az EU-val megállapodást kötött más harmadik országok számára. A platform saját kezdeményezésére is szolgáltatna információkat.

A biztosítékoknak és ellenőrzési előírásoknak való megfelelés figyelemmel kísérését központosítanák, esetleg külső érdekeltek – pl.: a kijelölt szolgáltató(k) képviselői vagy független felügyelőnek kinevezett személyek – felügyelete mellett. Az adatvédelmet, -integritást és -biztonságot is központi szinten biztosítanánk.

A korszerűsített FIU-platform számára meghatározott szerepeket és felelősségeket tartalmazó hivatalos jogállást biztosítanánk. Nemzeti szinten a FIU-k, valamint a tagállami bűnüldöző és hírszerző hatóságok volnának a legfontosabb részt vevő szervek.

⁹ Lásd a 8. lábjegyzetet.

Unió szintű hatóság kezelné az uniós polgárok hozzáférési, kiigazítási és törlési kéréseit, a jogorvoslati és fellebbezési eseteket pedig az alkalmazandó tagállami és uniós jogi rendelkezéseknek megfelelően intéznék.

7. KÖVETKEZTETÉS

E közlemény – a Bizottság által eddig elvégzett előkészítő munka alapján, valamint a hatásvizsgálat eredményeire figyelemmel – ismerteti a terrorizmus finanszírozásának felderítésére szolgáló rendszer keretében „az adatlehívás uniós területen történő jogi és műszaki keretének” kiépítésére vonatkozó különféle lehetséges opciókat. Az e közleménybe meghatározott különböző szakpolitikai választási lehetőségek azt mutatják, hogy még komoly választások és döntések állnak előttünk, ideértve az alapvető jogok tiszteletben tartásának szempontjait, valamint hogy számos jogi, műszaki, szervezési és pénzügyi kérdés vár részletesebb kidolgozásra a további előkészítő munka során. Az említett komoly kihívásokra figyelemmel a Bizottság úgy ítéli meg, hogy elegendő időt kell hagyni a további előkészítő munkára, valamint a Tanáccsal és a Parlamenttel folytatandó eszmecsere lebonyolítására.

* * *

Melléklet: A vegyes szakpolitikai lehetőségek táblázatos áttekintése

	Az uniós Tfts koordinációs és elemzési szolgáltatás (1. opció)	Az uniós Tfts adatlehívási szolgáltatás (2. opció)	A Pénzügyi Hírszerző Egység (FIU) koordinációs szolgáltatás (3. opció)
„Nyers adatok” iránti kérelmek előkészítése és kiadása	Uniós Tfts központi egység a tagállamokkal együttműködésben	Uniós Tfts központi egység a tagállamokkal együttműködésben	Korszerűsített FIU-platform
„Nyers adatok” iránti kérelmek nyomon követése és engedélyezése	Eurojust vagy más meglévő szerve	Eurojust vagy más meglévő szerve	Eurojust vagy más meglévő szerve
A „nyers adatok” fogadása és tárolása, adatbiztonság	Europol vagy egyéb uniós szerv, pl.: az IT ügynökség	Europol vagy egyéb uniós szerv, pl.: az IT ügynökség	Europol vagy egyéb uniós szerv, pl.: az IT ügynökség
A „nyers adatokban” végzett keresések futtatása	Uniós Tfts központi egység, kirendelt tagállami elemzők vagy a kettő kombinációja	Uniós Tfts központi egység	FIU-k, korszerűsített FIU-platform
A keresések futtatásának nyomon követése és engedélyezése	Független felügyelők, esetleg nemzeti hatóságok	Független felügyelők, nemzeti hatóságok	Független felügyelők
A keresési eredmények elemzése	Uniós Tfts központi egység, kirendelt tagállami elemzők vagy a kettő kombinációja	Nemzeti hatóságok a nemzeti kutatások esetében, az Uniós Tfts központi egység elemzői az uniós keresések és harmadik országok keresései esetében	Korszerűsített FIU-platform, nemzeti FIU-k
A keresési eredmények elosztása	Europol-elemzők vagy kirendelt tagállami elemzők	Nemzeti hatóságok a nemzeti kutatások esetében, az Uniós Tfts központi egység elemzői az uniós keresések és harmadik országok keresései esetében	Korszerűsített FIU-platform, nemzeti FIU-k
Megfelelő adatvédelmi rendszer kialakítása	Europol vagy egyéb uniós szerv, pl.: az IT ügynökség	Europol vagy egyéb uniós szerv, pl.: az IT ügynökség	Europol vagy egyéb uniós szerv, pl.: az IT ügynökség