TERRORELHÁRÍTÁSI KÖZPONT
1101 Budapest, Zách u. 4.

dr. Somosközi Áron főhadnagy

Transzatlanti együttműködés a terrorfinanszírozás elleni küzdelemben

- Terrorist Finance Tracking Programme -

Abstract

The 9/11 terrorist attacks were milestones in many ways in the history of international terrorism, or global terrorism as it has been more widely used ever since. Naturally, globalization affects organizations involved in the fight against terrorism; it is very important to put them in international context even in country-specific analysis and in identifying effective counter-measures. After 9/11, financing of terrorism became an important issue as events pointed out that devastating terrorist attacks could be funded from mundane, ordinary financial resources and via simple channels. As a result, the defence and intelligence agencies, in addition to their usual duties, needed to engage in financial intelligence evaluation and analysis related to individuals, groups and organizations linked to terrorism.

Bevezetés

A 2001. szeptember 11-i, USA érdekeltségek elleni terrortámadás következményei többrétűek voltak. Többek között rávilágítottak arra, hogy a terrorellenes küzdelemben elkerülhetetlen a globális, de legalább a multinacionális és a transzatlanti együttműködés. A terrorizmus jelenségének egyik leginkább globalizálódó területévé annak finanszírozása vált a pénzügyi- és bankrendszer hasonlóan globális jellegéből adódóan. A terrorizmus finanszírozásának felderítésére, illetve a terrorista szervezetek, csoportok anyagi bázisának és jövőbeni bevételeinek ellehetetlenítésére, csökkentésére átfogó, sokszor határon, sőt kontinenseken átnyúló programokat kell az együttműködő országoknak indítani, mert csak ez vezethet eredményre.

A 2001-es eseményeket követően – értelemszerűen az USA kezdeményezése alapján – az illetékesek felismerték azt, hogy a terrorizmus elleni küzdelem sikerességében nagy szerepet

játszik a finanszírozása elleni tevékenység. Az akkori amerikai álláspont szerint, amely nem csak az Al-Qaida kapcsán állja meg a helyét, amennyiben a szervezet, csoport alól elvonják vagy legalábbis korlátozzák a pénzügyi bázist, az közvetlen hatással van a terrorszervezet cselekvési potenciáljára is és így az általa jelentett fenyegetettségre. A pénzügyi kapcsolatok vizsgálatának azonban van egy másik, legalább ennyire fontos vetülete. Nevezetesen az, hogy nagymértékben hozzájárul a terrorszervezet tagjainak, szimpatizánsainak, anyagi támogatóinak illetve végső soron az egész infrastruktúrája azonosításához is.

Leginkább a pénzügyi kapcsolatok elemzésére, és az ezzel kapcsolatos adatgyűjtésre igaz, hogy az akkor hatékony, ha rendszer-szerű szemlélettel párosul, amely az érintett személyeket, objektumokat, szervezeteket nem elkülönülten, hanem azok pénzügyi viszonyrendszerébe ágyazva vizsgálja. Mindennek azonban ki kell egészülnie egy olyan vizsgálati szempontrendszerrel, amely hatékonyan képes kiszűrni a hatalmas mennyiségű adatállományból azokat, amelyek terrorelhárítási szempontból figyelmet érdemelnek.

A 2001-es terrortámadások utólagos elemzése, az abban résztvevő személyek, valamint a végrehajtott cselekmények pénzügyi körülményeinek, jellemzőinek feltárása sok olyan tulajdonságot, körülményt felszínre hozott, amely később a generális szabályozásra is hatással volt.

Összefoglalóan állítható, hogy a terrorfinanszírozásra szánt pénzek sok esetben legális forrásból származó jövedelmek, olyan pénzeszközök, amelyeket azok későbbi felhasználási céljuk (terrorcselekmény elkövetése, toborzás, kiképzés, a szervezet működésének költségei) tesz terrorelhárítási szempontból figyelmet érdemlővé. Ez már önmagában hordozza azt a tényt, hogy a terrorfinanszírozás vizsgálatával foglalkozó szervezeteknek a „mindennapi” adatok közül kell kiválasztani az ugyan „mindennapinak” tűnő, de a tranzakció, a pénzügyi kapcsolat mögötti szándék miatt már a terrorfinanszírozás fogalomkörébe vonható információkat.

A 9/11-i eseményeket[1] vizsgáló bizottság jelentése szerint[2] a terrortámadások összköltsége[3] 400-500 000 USD közötti összegre tehető, amelyből kb. 300 000 USD a 19 elkövető amerikai bankszámláin volt. Az anyagi bázist tengerentúli átutalásokból, a készpénz fizikai behozatalából, ill. külföldi pénzintézeteknél elhelyezett számlákhoz való hozzáférés révén biztosították. Az összegek felhasználása teljesen hétköznapi volt (pl. repülési iskolában tanulás, élelmiszer, szállás költségek).

Fentiek alapján megállapítható, hogy a hatékony terrorfinanszírozási vizsgálatoknak, elemzéseknek kifejezetten célirányosnak kell lenniük, amihez elengedhetetlen, hogy hírszerzési, vagy egyszerűbben fogalmazva titkosszolgálati illetve bűnüldözési információk álljanak rendelkezésre, amelyek alapján el lehet kerülni az adat-bányászatot,[4] illetve azt, hogy egyes szervezetek parttalan adatkéréseket eszközöljenek, noha adatok beszerzésére, és tárolására, feldolgozására egyébként jogosultak lennének.

Az állami és a nemzetközi szabályozás a terrorfinanszírozás kapcsán megalkotott normákban a terrorfinanszírozást elsősorban a pénzmosás tevékenységével együtt kívánta szabályozás tárgyává tenni, azonban a két tevékenység éppen ellentétes irányú, noha a jelenségek tekintetében találhatóak közös tulajdonságok. Míg a pénzmosás általában illegális forrásból származó jövedelmek kifehérítését célozza, addig a terrorfinanszírozás éppen azzal ellentétes folyamatot jelent. Mindenesetre megállapítható az, hogy a pénzügyi tranzakciót éppen a mögötte húzódó szándék miatt kell figyelemmel kísérni, noha minden más tekintetben teljesen átlagos jegyeket hordoz. Az is megállapítható továbbá, hogy az iszlamista terrorszervezetek (pl.: Al-Qaida) főként államok és magánszemélyek anyagi támogatásából, non-profit szervezetek (NGO) működéséből tartja fent magát, addig a klasszikus szeparatista/marxista-leninista típusú szervezetek (a kurd PKK, illetve a tamil LTTE) legális

---

[1] A közhasználatú elnevezés a 2001. 09. 11-én, az Egyesült Államok több helyszínén (New York, Virginia, Pennsylvania) összehangoltan végrehajtott repülőgépes terrortámadásokra utal, a 9/11 kifejezés a jelzett dátum amerikai írásmódja.

[2] John *Roth*, Douglas *Greenburg*, Serena *Wille*: Monograph on Terrorist Financing, Staff report to the commision, States Chapter 1. p. 13. (2004. 07. 22.) http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf (2012.07.11.)

[3] A terrortámadások költségeinek részletes megoszlásának bemutatásához ld. *Dr. Gál István László PhD:* A terrorizmus finanszírozása. Pécs, PTE Állam- és Jogtudományi kar Gazdasági Büntetőjogi Kutatóintézete. 2010. 10-14.

[4] Adat-bányászat (data-mining) alatt jelen esetben a szerző a több forrásból származó információk, nyers adatok elemzését érti operatív felhasználásra alkalmas információk megszerzése érdekében.

forrásokat is használnak (pénzgyűjtés, kiadványok értékesítése) természetesen kiegészülve a szervezett bűnözésből származó bevételekkel.[5]

A terrorfinanszírozás jelensége kapcsán meg kell említeni, hogy a leküzdésére irányuló, és – adatelemzésekkel, adatgyűjtéssel és –feldolgozással megvalósuló – fellépés kapcsán kiemelt figyelmet kell fordítani az adatvédelmi előírások betartására. A korábban említett körülmény, miszerint a keresett adatok sokszor hétköznapi jellege magától generálja, hogy az adatelemzéseket végző szervezetek túlnyomórészt – a terrorfinanszírozás szempontjából legalábbis – irreleváns adatokat szereznek be a szolgáltatóktól, amelyek további felhasználására, tárolására, törlésére garanciális szabályokat kell alkalmazni.

Az elmúlt több mint tíz év nemzetközi terrorelhárítási tapasztalatai azt mutatják, hogy a 9/11 bekövetkezése után normalizálódtak azok az általános adatszerzési törekvések, amelyek sok esetben az adatvédelmi előírások negligálásával jártak. Ilyen volt többek között 2001-ben a National Security Agency engedély nélküli lehallgatási programja a tengerentúli telefonbeszélgetések tekintetében, amelyet először a New York Times amerikai napilap hozott nyilvánosságra.[6]

A terrorfinanszírozás elleni küzdelem és az adatvédelmi szabályok betartása feletti aggodalmak kiváló példája az USA Pénzügyminisztériuma által 9/11-et követően indított titkosszolgálati célokat szolgáló Terrorist Finance Tracking Programme (továbbiakban: TFTP).

A TFTP nyilvánosságra kerülése, a program célja

Az eredetileg minősített program 2006-ban került nyilvánosságra, amikor is több vezető amerikai napilapban jelentek meg cikkek,[7] amelyek beszámoltak arról, hogy a Bush-adminisztráció 9/11 után a terrorizmus elleni globális háború jegyében átfogó programot indított a terrorfinanszírozás feltárására, az ezzel kapcsolatos pénzügyi információszerzésre. A

---

[5] *Hans Ulrich Helfer*: Die Bekämpfung der Finanzierung des Terrorismus. Sicherheitspolitik. 2004. 6. sz. 11-15.

[6] James *Risen*, Eric Lichtbau: Bush lets U.S. spy on callers without courts. The New York Times, 2005.12.16., https://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all (2012.08.21.)

[7] James Risen, Eric Lichtbau: Bank data is sifted by U.S. in secret to block terror., The New York Times, 2006.06.22.,http://www.nytimes.com/2006/06/23/washington/23intel.html?hp&ex=1151121600&en=18f9ed2cf37511d5&ei=5094&partner=homepage (2012.06.23.)
Paul Blustein, Barton Gellman, Dafna Linzer: Bank records secretly tapped, Washington Post, 2006. 06. 23., http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062300167.html (2012.08.21.)

megjelent cikkek részletesen taglalták a program célját, és részleteit, és már a cikkek megjelenésének ténye is heves vitákat váltott ki a nemzetbiztonsági illetve az adatvédelmi érdekek védelmezői között. Előbbiek helyrehozhatatlan kárként írták le a TFTP működési mechanizmusának nyilvánosságra kerülését, mivel így a programmal célzott személyi kör megteheti a szükséges lépéseket, tevékenységük kikerülhet a látómezőből."

A megjelent sajtóhírek szerint a TFTP lényegét tekintve 9/11 után a terroristák pénzügyi bázisának, tevékenységének feltárására indult átfogó program, amelynek végrehajtásáért a amerikai Pénzügyminisztérium (Treasury Department) felelős. A jelzett program keretében a világ legnagyobb pénzügyi telekommunikációs vállalkozásának, a belga székhelyű SWIFT-nek[8] az USA területén elhelyezett tükör-szerverén tárolt adatait az amerikai hatóságok, a jogszabályi előírások betartásával szerezték be, amely óriási volumenű, tengerentúli pénzügyi tranzakcióval kapcsolatos adatokat eredményezett. Az adatok ugyan nem tették lehetővé a hagyományos pénzügyi tevékenységek (ATM-használat, bankszámlaegyenleg)[9] nyomon követését, a szolgáltatott információk retrospektív jellegűek. A közölt adatok multinacionális jellege, illetve a rendszerszerű kapcsolatról beszerezhető információk ténye azonban kiemelten hasznossá teszi a TFTP gyakorlati alkalmazását. SWIFT-üzenetekben gyakran szerepelnek az ügyfelek személyes adatai, bankszámlaszámai, ritka esetben kifejezetten szenzitív adatai.

Ezeket a beszerzett adatokat később terrorista tevékenységgel kapcsolatban folytatott vizsgálatok során elemezték, és hasznosították. Az amerikai kormányzati álláspont képviselői szerint a jelzett gyakorlat, így különösen a SWIFT azonban kivétel azon esetek alól, amikor a kormánynak a jogszabályok korlátozott hozzáférést biztosítanak a magánszemélyek pénzügyi adataihoz, mivel a SWIFT nem minősül pénzügyi szolgáltatónak.

---

[8] A Society for Worldwide Interbank Financial Telecommunication (SWIFT) egy belgiumi székhelyű nemzetközi pénzügyi telekommunikációs vállalkozás, amely 1973-ban jött létre azzal a céllal, hogy a nemzetközi pénzpiaci szereplők közötti tranzakciókhoz, egyéb pénzügyi kapcsolatokhoz nyújtson formalizált platformot, így csökkentve a költségeket. Jelenleg több mint 200 ország pénzügyi intézete használja

[9] Testimony of Stuart Levey, Under Secretary Terrorism and Financial Intelligence U.S. Department of the Treasury Before the House Financial Services Subcommittee on Oversight and Investigations: "It does not contain information on most ordinary domestic transactions made by individuals in the United States, such as deposits, withdrawals, ATM use, checks, or electronic bill payments. The SWIFT data consists of records of completed financial transactions; it does not provide access to individual bank account information. This program is consistent with privacy laws as well as Treasury's longstanding commitment to protect sensitive financial data. (2006.11.07.), http://www.treasury.gov/press-center/press-releases/Pages/hp05.aspx (2012.07.07.)

A TFTP részleteinek napvilágra kerülése nemcsak az USA terrorellenes politikájának, és terrorizmus elleni „háborújának” kezdeti parttalanságára, és a 9/11 utáni időszak túlkapásaira irányította a figyelmet, hanem felszínre hozta és fenntartotta a nemzetbiztonsági érdek illetve személyi adatok védelméhez fűződő érdek közötti összeütközés kérdését is. Utóbbi kapcsán ugyanis felmerült, hogy a TFTP keretében európai uniós állampolgárok személyi adatai kerültek átadásra a SWIFT részéről, amellyel utóbbi megsértette az uniós jogot.

A TFTP jogi alapját az USA szemszögéből az 1977-es International Emergency Economic Powers Act (IEEPA) adta, amely feljogosította a kormányt, hogy amennyiben az elnök szükségállapotot hirdet, abban az esetben a kormány adatszolgáltatást kényszeríthessen ki.[10] George W. Bush a 2001. 09. 24-én hatályba lépett Executive Order 13224 keretein belül - tekintettel az USA-t fenyegető további terrorcselekmények bekövetkezésének lehetőségére - szükségállapotot hirdetett, és ennek keretében feljogosította[11] a Pénzügyminisztériumot a szükséges intézkedések megtételére a terrorfinanszírozás felderítése területén a rendelet szellemével összhangban. A szükséges adatok megszerzése érdekében a Pénzügyminisztérium adminisztratív kérésekkel (idézésekkel) fordult jelen esetben a SWIFT-hez, és igényelte az USA területén lévő operatív központjában[12] tárolt, pénzügyi tranzakciókat kísérő adatokat. A SWIFT akkori vezetője szerint az USA kormányzat havi rendszerességi adatkéréseit eleinte túlságosan tág szempontok alapján fogalmazták meg, azonban idővel a keresési szempontok szűkültek.

A TFTP leginkább neuralgikus pontja az volt, hogy az amerikai Pénzügyminisztérium önálló szervezeti egysége[13] olyan nagy mennyiségű személyes adathoz jutott, amelynek csak elenyésző része „hasznosult” a terrorfinanszírozás kapcsán folytatott vizsgálatok keretein belül. A TFTP minősített, ha úgy tetszik titkos jellegéből adódóan nem álltak rendelkezésre olyan részletes jogi szabályok, illetve bizonyítékok, amelyek alapján megalapozottan lehetett

---

[10] U.S. International Emergency Economic Powers Act (IEEPA) Chapter 50, § 1701, http://www.treasury.gov/resource-center/sanctions/Documents/ieepa.pdf (2012. 06.07.)

[11] Executive order 13224 – Blocking property and prohobiting transactions with persons who commit, threaten to commit or support terrorism, sec 5. – sec. 7. http://www.treasury.gov/resource-center/sanctions/Programs/Documents/terror.pdf (2012.05.12.)

[12] A belgiumi (La Hulpe) székhelyű SWIFT abban az időszakban az USA területén működtetett egy tükör-szervert, amelyen 124 napon keresztül biztonsági megfontolásokból tárolták az adatokat, majd ezt követően törlésre kerültek, Az USA pénzügyminisztériuma ennek alapján fordult megkereséssel a SWIFT irányába az adatok beszerzése érdekében.

[13] U.S. Treasury’s Office of Foreign Assets Control (OFAC).

volna állást foglalni egyrészt a személyi adatok védelmére vonatkozó jogi előírások teljesüléséről vagy megsértéséről, illetőleg a beszerzett adatok gyakorlati hasznosulásáról.

A 9/11 utáni generális, és ezáltal óriási mennyiségű adatot eredményező megkeresések elemzését már az USA Pénzügyminisztériuma végezte, saját kereső szoftverrel, amely már a terrorizmussal összefüggésbe hozható személyek, intézmények egyedi azonosító adatai alapján tudta a szükséges válogatást elvégezni.

A TFTP, illetve az USA pénzügyminisztériuma és a SWIFT közötti együttműködés napvilágra kerülését követően, tekintettel a SWIFT belgiumi székhelyére a Belga Adatvédelmi Bizottság (Comission de la protection de la vie privee) véleményt adott ki 2006. 09. 27-én, többek közt arról, hogy a SWIFT által folytatott adattovábbítás az USA Pénzügyminisztériuma részére sértette-e a belga jogot.[14] A jelzett bizottsági véleményben részletesen szerepel a SWIFT által tárolt adatok jellege, továbbításának módja. A bizottság kiemeli véleményében, hogy a megkeresések igencsak generálisak voltak (földrajzi, időbeli, állampolgársági szempontok), sőt a SWIFT akkori illetékese egy interjúban úgy fogalmazott, hogy a Pénzügyminisztérium eleinte az összes adatot beszerezte.

A vélemény kitér arra is, hogy az amerikai hatóságok már 9/11 előtt is éltek megkeresésekkel a SWIFT amerikai leányvállalata felé, azonban ezek teljesítésre nem kerültek, egyrészt a 124 napos időkorlát miatt, másrészt azért, mert a SWIFT érdemben tudott azzal érvelni, hogy a hatóság közvetlenül keresse meg a tranzakcióban érintett bankot. Továbbá a SWIFT nem is rendelkezett azokkal a technikai (szoftveres) feltételekkel, amelyek az egyedi keresések végrehajtását lehetővé tették volna.

A bizottsági vélemény megállapította, hogy a SWIFT székhelye és tevékenységének tényleges központja Belgiumban található, így alkalmazható rá a belga adatvédelmi törvény. A további distinkció arra irányult, hogy a SWIFT adatkezelőnek vagy adatfeldolgozónak minősül-e tevékenysége során. A SWIFT érvelésével ellentétesen a bizottság arra az álláspontra helyezkedett, hogy a SWIFT a pénzügyi üzenetek továbbítására működtetett számítástechnikai rendszer tekintetében adatkezelőnek minősül, mivel erős központi

[14] *Belgian Data Protection Comission*: Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas, Opinion no.37/2006. http://www.steptoe.com/assets/attachments/2644.pdf (2012.07.21.)

irányítással rendelkezik, amely a vizsgált esetben meghozta azokat a döntéseket, amelyek az USA Pénzügyminisztériuma részére az adatok átadását eredményezte.

A bizottság összegzett véleménye megállapította, hogy a SWIFT egyrészt a pénzügyi adatok továbbítására kialakított számítástechnikai rendszer (SWIFTNet FIN) működtetése során, másrészt a jelzett adatoknak az USA Pénzügyminisztériuma részére történő átadásával megsértette a belga jogot illetve az uniós adatvédelmi irányelveket különösen az arányosság és átláthatóság terén.

Az akkori belga miniszterelnök (Guy Verhofstadt) a bizottsági vélemény ismertetésén túl, hangsúlyozta ugyanakkor annak fontosságát, hogy a terrorizmus elleni küzdelem során, a transzatlanti együttműködés keretén belül pénzügyi adatokat használjanak fel a hatóságok, de ennek feltételeit tiszta, átlátható szabályokban kell rögzíteni és nem titkos megállapodásokban.

A fenti véleményt visszhangozza a svájci Szövetségi Adatvédelmi és Információs biztos megállapítása is,[15] amely összegzésében megállapítja, hogy a terrorizmus elleni küzdelem kapcsán alkalmazott bármely megoldásnak egyrészt tiszteletben kell tartania a nemzeti adatvédelmi jogszabályokat, másrészt politikai megállapodások tárgyát kell, hogy képezze, és nem titkos megegyezésekét.

Az Európai Adatvédelmi Biztosnak az ügyben kiadott előzetes megállapításai alapján az Európai Központi Bank már 2002-ben értesült az amerikai hatóságoktól a SWIFT kapcsán eszközölt adatkérésekről, azonban az EKB nem tette meg a szükséges tájékoztatást az európai adatvédelmi hatóságok irányába.[16]

A belga adatvédelmi bizottság vizsgálatán túl szintén a TFTP gyakorlati megvalósulását vette górcső alá az Európai Unió adatvédelmi tanácsadó testülete (Working Party 29),[17] amely

---

[15] Access to SWIFT Transaction Data- Opinion of the Federal Data Protection and Information Commisioner, 4. o. http://ww.edoeb.admin.ch/themen/00794/01066/index.htmllang=en&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCDdIR8gmym162epYbg2c_JjKbNoKSn6A (2012.08.01.)

[16] *SWIFT*: EDPS preliminary findings on the role of the ECB. (2006.10.04.), http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/06/10&format=HTML&aged=1&language=EN&guiLanguage=en (2012.07.26.)

[17] A jelzett munkacsoport az EU tanácsadó testülete adatvédelmi kérdésekben, amelynek alapja az EP és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének

véleményét 2006. november 22-én hozta nyilvánosságra.[18] A jelzett vélemény sokkal szigorúbb hangvételű végkövetkeztetésekre jut, mint a belga vizsgálat, és kiemeli, hogy a SWIFT a jelzett gyakorlattal folyamatosan és súlyosan megsértette az irányadó EU-s, és a tevékenységet nemzeti szinten szabályozó belga jog rendelkezéseit. A sokrétű, közel 30 oldalas vélemény szintén vizsgálja a SWIFT adatkezelő vagy adatfeldolgozó jellegét, amellyel összefüggésben megállapítja, hogy az adatvédelmi szabályok megsértéséért nemcsak a SWIFT, hanem szervezeti felépítéséből adódóan (szövetkezeti jelleg, amelynek működésében, irányításában a vele kapcsolatban álló pénzintézetek is szerepet vállalnak) a pénzintézetek is egyfajta felelősséget viselnek.[19] A 29-es Munkacsoport, egyetértésben a belga hatósággal, úgy ítélte meg, hogy a SWIFT a szokásos adatfeldolgozói szerepen túlmutató lépéseket tett, amelynek jó példája az, hogy az adatigénylése kapcsán tagjaival való egyeztetés nélkül bocsátkozott tárgyalásokba a továbbítandó adatok köréről, valamint az adattovábbítás módjáról.[20]

A SWIFT kapcsán megemlíti a vélemény, hogy az amerikai joghatóság alá helyezett tükörszerver létrehozásával a vállalkozás egyfajta szándékossággal idézett elő olyan helyzetet, hogy később az USA Pénzügyminisztériuma megkereséseinek tárgyává váljon.

A munkacsoport részletesen taglalta a SWIFT magatartásának és az EU vonatkozó irányelvének összeegyeztethetőségét, amellyel kapcsolatban több kifogást is emelt, többek között az adatoknak az USA területén történő tárolása, az arányosság, a célhoz kötöttség, ill. a tájékoztatási kötelezettség kapcsán.

A megfogalmazott vélemények egyik közös megállapítása volt, hogy a SWIFT az USA-ban történő adattárolással, majd az adatoknak a terrorizmus elleni küzdelem során való felhasználásához való továbbításával egy olyan ország számára tette elérhetővé a személyes

---

védelméről és az ilyen adatok szabad áramlásáról. A jelzett irányelv 29. cikk 1. bekezdése hívta életre a munkacsoportot.

[18] 10/2006. vélemény a személyes adatok Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi feldolgozásáról, 2006.11.22., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_hu.pdf (2012.06.18.)

[19] *Jusin Santolli*: The Terrorist Finance Tracking Program: Illuminating the shortcomings of the European Union's antiquated data privacy directive. The George Washington International Law Review. 2008. 40. sz. 568. o.

[20] *Dr. Szabó* Endre Győző: A SWIFT adatkezeléséről, 2007.06.05., http://www.jogiforum.hu/files/adatvedelem/a_SWIFT_adatkezeleserol[jogi_forum].pdf (2012. 06. 22.)

adatokat, amely nem nyújt az EU adatvédelmi rendelkezéseivel egyenrangú adatvédelmi jogi környezetet.[21]

A sajtónyilvánosság és az európai adatvédelmi szervek jogi véleménye egyben ki is jelölte az amerikai és európai résztvevők jövőbeni tevékenységének irányát, miszerint kiemelt figyelmet kell fordítani a TFTP adatvédelmi garanciáinak vizsgálatára, és az EU-szabályokkal való összhangba hozatalra.

A SWIFT, az eset napvilágra kerülését követően, a piacon betöltött hegemón szerepének megőrzése, valamint az elszenvedett presztízsveszteség kiküszöbölése érdekében teljes elkötelezettséggel vállalta az európai normáknak való jövőbeni megfelelést. Ezzel párhuzamosan azonban – mintegy mentve múltbeli magatartását – kiemelte, hogy a SWIFT „két joghatóság" csapdájába esett, amikor az USA területén tárolt adatainak az USA Pénzügyminisztériuma részére való továbbításával megfelelt az amerikai jogszabályoknak,[22] és eközben ugyanakkor a cég tevékenységére irányadó európai előírásokat viszont megszegte.

A SWIFT az adatvédelmi előírásoknak való megfelelés és a korábbi adattovábbítás folytatása érdekében adatvédelmi munkacsoportot állított fel, illetve rövid időn belül adminisztratív aktussal is eleget tett annak az elvárásnak, hogy az USA területén kifejtett tevékenysége (adattárolás, adattovábbítás) megfeleljen az európai adatvédelmi kívánalmaknak. 2007 júniusában a SWIFT amerikai leányvállalata ugyanis csatlakozott a Safe Harbour egyezményhez,[23] amely az USA területén is tevékenységet folytató vállalkozások számára teremt lehetőséget arra, hogy az európai adatvédelmi elveknek és előírásoknak megfelelően továbbíthassanak adatokat.

A jelzett Safe Harbour (Biztonságos Kikötő) keretrendszer 2000-ben jött létre az USA és EU közötti egyeztetések eredményeképpen,[24] amelynek célja, hogy a két adatvédelmi

---

[21] Patrick M. *Connorton:* Tracking Terrorist Financing Through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide, 76 Fordham L. Rev. 283 (2007), http://ir.lawnet.fordham.edu/flr/vol76/iss1/7 (2012.07.13.)

[22] Jennifer K. *Elsea*, M. Maureen *Murphy*: Treasury's Terrist Finance Program's acces to information held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 2006.07.07., 3-4. http://www.fas.org/sgp/crs/natsec/RS22469.pdf (2012.03.16.).

[23] Sofia Marques *da Silva*: The TFTP Agreement: A legal and contextual analysis. 5. http://www.fas.org/sgp/crs/natsec/RS22469.pdf. (2012.07.01.)

[24] 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. (HL 215., 2000.8.28.). http://www.bankszovetseg.hu/anyag/feltoltott/EU_bizottsag_hatarozata.pdf (2012.06.18.)

szabályozási rendszer közötti eltéréseket az USA Kereskedelmi Minisztériuma felügyelete alá tartozó vállalkozások esetében kiküszöbölje, és kellő biztosítékot jelentsen az EU szempontjából elfogadható szintű adatvédelmi joggyakorlathoz. A Safe Harborhoz csatlakozott amerikai vállalkozások kötelezettséget vállalnak arra, hogy adatkezelésük során az Európai Unió adatvédelmi szintjének megfelelő módon járnak el.

A Safe Harbour rendszer az elmúlt években több kritika tárgya is volt, mivel az ahhoz való csatlakozás önkéntes és sokszor a deklaráción túl az érintett vállalkozások érdemben nem tartják be az adatvédelmi előírásokat.

A TFTP másik résztvevőjeként az USA Pénzügyminisztériuma folyamatos egyeztetéseket folytatott az EU képviselőivel annak érdekében, hogy az uniós jognak megfelelő jogi alapot teremtsenek a kérdésben.[25] Ezek a tárgyalások végül az USA Pénzügyminisztériumának egyoldalú tényvázlatával zárultak 2007 júniusában,[26] amely részletesen ismerteti azokat a garanciális feltételeket, és ellenőrzési mechanizmusokat, amelyek az EU-ból származó adatok lehető legnagyobb védelmét szolgálják. A tényvázlat az USA egyoldalú kötelezettségvállalásait tartalmazta, amelyek korántsem voltak nemzetközi szerződésben vállalt, jogilag kötelező erejű megállapodásoknak tekinthetők.

A jelzett tényvázlat legfontosabb elemei:

- a kapott adatokat kizárólag a terrorizmus elleni küzdelem céljára használják,
- az adatokhoz kizárólag a terrorizmus elleni küzdelemben részt vevő elemzők férhetnek hozzá olyan már meglévő információk alapján folytatott speciális keresések céljából, amelyek okkal engednek arra következtetni, hogy az azonosított személy terrorista tevékenységet folytat vagy részt vesz annak finanszírozásában,
- meghatározott időtartamon – általában öt éven belül – törlik az adatokat,

[25] Kristin *Archick:* U.S-EU Cooperation against terrorism. Congressional Research Service Report for Congress. 7. http://www.fas.org/sgp/crs/row/RS22030.pdf (2012.06.13.)

[26] Federal Register Vol. 72. No. 204. (2007.10.23.) p. 60054-60066, http://www.fda.gov/OHRMS/DOCKETS/98fr/E7-20855.pdf (2012. 08.11.) illetve OJ C166//18 (2007.07.20.), http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_166/c_16620070720en00180025.pdf (2012.05.01.)

- javasolt megállapodás értelmében egy európai igazságügyi hatóság fogja meghozni az adatoknak az USA Pénzügyminisztériuma részére történő átadását engedélyező határozatot, mely hatóságnak ellenőriznie kell a megkeresés jogszerűségét is.[27]

A jelzett tényvázlatban az amerikai fél felajánlja annak lehetőségét, hogy az Európai Bizottság által kijelölt személy, kétévente visszatérően ellenőrzés keretében vizsgálja meg a TFTP gyakorlati működése során az EU-ból származó személyes adatok védelmének szintjét és formáját.

Az Európai Bizottság 2008 áprilisában Jean-Louis Bruguiére francia bírót jelölte ki[28] az említett vizsgálat lefolytatására, aki megállapításait 2008 decemberére készítette el. A jelzett jelentés EU titkos minősítésű, azokat 2009 júliusában továbbították a tagállamok állandó képviselőinek.

A Bruguiére-jelentés kapcsán közölt megállapítások szerint a kijelölt bíró az ellenőrzés során három alkalommal járt Washingtonban. 2008. júniusban megismerkedett a TFTP hátterével, a SWIFT által rendelkezésre bocsátott adatok feldolgozásának módjával, s az abból történő releváns adatok kinyerésének módszerével. Megbeszéléseket folytatott továbbá azon szervek magas rangú képviselőivel, amelyek részére a Pénzügyminisztérium az USA törvényei alapján továbbította a TFTP révén szerzett adatokat, valamint háttérmegbeszéléseket bonyolított az elnök nemzetbiztonsági tanácsadójával.

2008. szeptemberben Bruguiére kizárólag a SWIFT által biztosított adatoknak a szakértők által történő elemzését, „kinyerését” vizsgálta, valamint a SWIFT részéről alkalmazott ellenőrzési mechanizmusokat, amelyek annak biztosítására voltak hivatottak, hogy a TFTP keretében végrehajtott adatkérések, és ennek eredményeképpen az adatbázisban folytatott keresések kizárólag terrorizmussal összefüggő vizsgálatok kapcsán történhessenek meg.

---

[27] Megállapodás az Európai Unió és az Amerikai Egyesült Államok között a pénzügyi üzenetadatoknak az USA terrorizmusfinanszírozás felderítésére irányuló programja céljából történő feldolgozásáról és átadásáról. Kérdések és válaszok. 2009. november http://www.consilium.europa.eu/uedocs/NewsWord/HU/jha/111756.doc

[28] Judge Jean-Louis *Bruguiere*: Summary of the first annual report on the processing of EU originating personal data held by the US Treasury Department for Counter Terrorism purposes: Terrorist Finance Tracking Programme, 2008. december, p. 4-5., http://www.statewatch.org/news/2011/apr/eu-usa-tftp-swift-1st-report-2008-judge-bruguiere.pdf (2012.07.19.).

2008. novemberben, a vizsgálat záró fázisában, Bruguiére a kinyert adatok felhasználását, ezen belül különösen az adatok harmadik félnek (többek között nyomozó szerveknek, szolgálatoknak, illetve harmadik országoknak, köztük EU-tagállamoknak) történő átadását vizsgálta.

A fentiekben említetteken kívül a jelentés érdemi megállapításai közé tartozik, hogy a TFTP gyakorlati haszna kimutatható módon jelentkezett a terrorelhárítási területen, közel 1500 esetben továbbított az USA az EU-tagországok számára a TFTP keretében kinyert adatokat, amelyek néhány esetben konkrét terrorcselekmény bekövetkezését hiúsították meg, más esetekben pedig nagymértékben segítették a folyamatban lévő vizsgálatok sikerét. Többek között a TFTP révén kinyert adatok segítségével 2007 nyarán azonosították az Iszlám Dzsihád Unió németországi tagjainak pénzügyi tevékenységét, továbbá nagymértékben hozzájárultak a jelzett csoport németországi létesítmények ellen tervezett támadásainak kapcsán folytatott nyomozáshoz.

A SWIFT 2009-ben strukturális változások végrehajtását jelentette be,[29] amely alapvető hatással volt a TFTP helyzetére. A SWIFT ugyanis 2010. 01. 01-től az európai adatokat már nem kívánta az USA területén található tükörszerverén tárolni, hanem egy új, svájci szervert kívánt üzembe helyezni. Az USA Pénzügyminisztériuma számára ezzel megszűnt volna az adminisztratív megkeresések révén valamennyi releváns adat beszerzésének lehetősége, így a továbbiakban az USA rákényszerült arra, hogy kifejezetten az Európai Unióból származó pénzügyi adatok beszerzése érdekében új nemzetközi megállapodást dolgozzon ki az EU-val együttműködve.

2009. júliusban a tagállamok egyhangúlag megbízták az akkori uniós elnökséget, hogy folytasson egyeztetéseket az USA képviselőivel egy olyan új megállapodásról, amely a TFTP keretében addig kialakított adatszolgáltatást a továbbiakban is biztosítja. Tekintettel arra, hogy a Lisszaboni Szerződés[30] hatályba lépésének pontos időpontja ekkor még nem volt ismert, ezért a megállapodás időtartamát 9 hónapban határozták meg, hogy annak lejártát követően az Európai Parlament (EP) gyakorolhassa új hatásköri jogosítványait.

---

[29] Countering terrorist threats – In the air and on the ground. 2010. 41. sz. http://www.eurunion.org/eu/images/euinsight-counterterr-apr2010.pdf (2012.08.26.)

[30] Hivatalos nevén Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról. http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:en:HTML (2012.08.20.)

Miután az Európai Parlament megvonta támogatását az átmeneti TFTP megállapodás kapcsán, már az új, 2009. december 1-jén hatályba lépett Lisszaboni Szerződés rendelkezései alapján kellett a megállapodást elfogadni. A Lisszaboni Szerződés elsődleges célja egy gyorsabb és hatékonyabb európai döntéshozatal megalkotása volt, amely nagyobb szerepet kívánt adni az Európai Parlamentnek. A Lisszaboni Szerződés V. címe (A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség) esetében ez a korábbi döntéshozatali eljárástól eltérő, új rendszert alakított ki, amely egyrészt bevezette a szabályozási körben a minősített szavazati többséget az Európai Unió Tanácsa vonatkozó döntései kapcsán, másrészt szükségessé tette az Európai Parlamenttel való együttes döntéshozatali eljárást. Utóbbi az EP számára tényleges befolyásolási lehetőséget adott a Bel- és Igazságügyi területen, mivel a korábbi konzultációs szerepe helyett már megerősítő funkciója lett, ami nélkül új kezdeményezés nem valósulhat meg a jelzett területen.

A TFTP vonatkozásában az USA részéről a Lisszaboni Szerződés által életre hívott szabályokat átmeneti bizalmatlansággal fogadták, mert az Európai Parlamentet olyan szereplőnek tekintették, amely USA-ellenes retorikájával sokszor torpedózta meg a kezdeményezéseket a verbalitás szintjén, azonban tényleges ráhatása nem volt a döntések tartalmára. Ez a szerepe most átváltozott tényleges döntéshozó jogosítvánnyá, amely az USA terrorellenes erőfeszítései kapcsán átmenetileg felértékelte a bilaterális kapcsolatokat, mivel az USA azon az álláspontón volt, hogy az EU sosem lesz képes arra, hogy olyan szupranacionális rendőri vagy titkosszolgálati szervet hozzon létre, amely egyenrangú partnere lehetne az amerikai félnek ebben a vonatkozásban.[31]

A jelenleg hatályos EU-USA megállapodás[32]

Az Európai Parlament – a Lisszaboni Szerződés rendelkezései alapján – 2010. június 28-án jóváhagyta, és egyetértését adta, így a megállapodás 2010. augusztus 1-jén hatályba lépett.

A megállapodás több tartalmi eleme a fentiekben már ismertetésre került, így a továbbiakban csak azon új elemeket kívánom kiemelni, amelyek eddig nem váltak ismertté és gyakorlati szempontból jelentőséggel bírnak.

---

[31] *Paul Rosenzweig*: How the EU's Lisbon Treaty affects U.S. National Security. Backgrounder. 2010. No. 2390. 6. o.

[32] Megállapodás az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról. O.J. L 195./5, (2010. 07. 27.)

A szerződés egyik legfontosabb újítása volt, hogy az USA Pénzügyminisztériuma és a SWIFT közötti adatigénylésbe illetve adattovábbításba beillesztett egy európai szervezetet, nevezetesen az Europolt. Három feladatot telepített a szerződés az Europolra. Egyrészt az USA Pénzügyminisztériumának megkereséseit (adat-előállítási utasításait) ellenőrzi a SWIFT általi teljesíthetőség szempontjából (4. cikk), illetve egyirányú információtovábbítást végez a TFTP adatok eseti továbbítása kapcsán (9. cikk) és TFTP-lekeresések iránti uniós megkereséseket továbbít (10. cikk).

Ezen rendelkezéseknek az elsődleges célja az volt, hogy olyan uniós szervezet is részese legyen az adatkérési illetve adattovábbítási folyamatnak, amelynek révén a korábbi adatvédelmi aggályok kiküszöbölhetőek, köszönhetően az Europol feletti átfogó ellenőrzésnek, monitorozásnak.

Az Europol ezen új, ellenőrző-jóváhagyó és adattovábbító szerepkörének ellátásához szükséges technikai és adminisztratív változásokat (4. cikk (9) bekezdés) a felek kölcsönös egyeztetéseit követően hajtotta végre, meglehetősen rövid idő alatt.

Ennek keretében az Europol létrehozott egy külön egységet (Unit O9) az Operatív Részlegen belül (Operational Department), amely kifejezetten a TFTP-megállapodás 4. cikkében foglalt ellenőrző szerepkör végrehajtására hivatott, 3 fős személyzettel. A 9. és 10. cikk rendelkezései alapján, az Europol által fogadott TFTP-adatok tárolására, feldolgozására megnyitottak egy Elemző Munka Fájl-t (Analysis Work File).

Az Europol részletes eljárást alakított ki a 4. cikk alapján érkezett megkeresések ellenőrzésére,[33] megerősítésére, amelyet a szerződés hatályba lépése után 6 hónappal felülvizsgáltak (13. cikk előírása) és a szükséges változtatásokat (köztük az Europol adatvédelmi részlege szerepének erősítése) végrehajtották. Az Europol eleinte „korlátozott terjesztésű” (EU Restricted) minősítéssel látta el a 4. cikk alapján érkezett megkereséseket, de az USA egy esetleges titoksértés következményei miatti aggodalmára tekintettel, és egy saját kockázatelemzés elvégzését követően 2010. novembertől kezdve – visszamenőlegesen is – titkossá (EU Secret) minősítette a megkereséseket és az azok kapcson keletkezett iratokat.

[33] A 4. cikk rendelkezései alapján az USA Pénzügyminisztériuma a megkeresést a SWIFT részére juttatja el, azonban annak másolati példányát és a megállapodás által előírt, az adatkérés indokoltságát alátámasztó dokumentációt az Europol részére továbbítja. Az Europol ellenőrzi annak jogszerűségét és indokoltságát, majd az adatkérés kapcsán kialakított állásfoglalásáról értesti a SWIFT-et, amely annak függvényében teljesíti az adatszolgáltatást az USA Pénzügyminisztériuma felé.

A 4. cikk kapcsán folytatott USA adatkérések jóváhagyásának gyakorlati megvalósulásáról – a megállapodás hatályba lépése óta eltelt időszak alapján – elmondható, hogy az USA Pénzügyminisztériumának megkeresései általában 1 havi időtartamra vonatkoznak, átlagosan 56 oldalas dokumentációban öltenek testet, bár az utóbbi időszakban – a kért adatok terrorizmussal való összefüggésének igényére tekintettel – egyre részletesebb dokumentációkkal támasztják alá a megkereséseket. 2012. májusig 23 alkalommal élt megkereséssel az USA Pénzügyminisztériuma a megállapodás 4. cikke alapján, amelyet az Europol valamennyi esetben jóváhagyott, így a SWIFT a kért adatokat továbbította az USA részére.

A kért adatok kapcsán a megállapodás további korlátozó rendelkezése, hogy a megkeresések nem irányulhatnak az Egységes Eurofizetési Térség (SEPA) adatainak megszerzésére.

A megállapodás 9. cikke alapján az USA Pénzügyminisztériuma a TFTP keretében szerzett adatok elemzése révén megismert azon információkat, amelyek az Európai Unió területén folytatott terrorizmus elleni küzdelemhez szükségesek, haladéktalanul továbbítja a tagállamok illetékes szerveinek, továbbá az Europol ill. Eurojust[34] részére (eseti információszolgáltatás).

A megállapodás 10. cikke alapján az EU tagállamának illetékes hatósága, az Europol, vagy az Eurojust, amennyiben alaposan feltételezhető, hogy az adatkérés alanya összefüggésbe hozható a terrorizmussal vagy annak finanszírozásával, kérheti a TFTP révén szerzett vonatkozó információk lekeresését.

A megállapodás további fontos rendelkezése az annak felülvizsgálatára vonatkozó előírás (13. cikk), amelynek értelmében az amerikai és európai fél közösen vizsgálja felül és értékeli a hatályba lépést követő 6 hónap elteltével a megállapodásban foglaltak gyakorlati megvalósulását. Az Európai Bizottság 2011. március 17-én tette közzé megállapításait.[35]

---

[34] Az Eurojustot a Tanács 2002/187/IB határozata hozta létre, amelyet a Tanács 2008. december 16-i 2009/426/IB határozata módosított (Eurojust Határozat). Az Eurojust feladata a nemzeti nyomozó hatóságok és ügyészségek hatékonyságának növelése a határokon átívelő, súlyos és szervezett bűncselekmények ügyeiben, és végső soron annak előmozdítása, hogy a bűncselekményt elkövetők felelősségre vonása gyorsan és eredményesen megtörténjék. Az Eurojust jövőképe az, hogy igazságügyi szinten kulcsszereplő és szakértői központ legyen a határokon átívelő, szervezett bűnözés elleni hatékony fellépés terén az Európai Unióban. *http://eurojust.europa.eu/Pages/languages/hu.aspx*

[35] Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.,

A Bizottságon túlmenően az Europol egész tevékenysége felett ellenőrzést gyakorol adatvédelmi szempontból a Joint Supervisory Body (JSB),[36] amelynek ezen feladatköre elsősorban arra terjed ki, hogy az Europol a tevékenysége (adatok tárolása, feldolgozása, továbbítása) során az egyén információs alapjogai nem sérülnek-e. A JSB már a megállapodás 2010. 08. 01-jei hatályba lépése előtt jelezte, hogy felülvizsgálati szerepkörét a TFTP vonatkozásában is el kívánja látni, és szorosan figyelemmel követi, hogy a TFTP megállapodás gyakorlati megvalósulása – az Europol vonatkozásában – mennyiben felel meg a prudens EU-s adatvédelmi szabályoknak.

A JSB 2010. 10. 11-én megtartott tanácskozásán kijelölt egy vizsgáló-csoportot, amelynek mandátuma arra irányult, hogy az Europol a TFTP megállapodásban foglalt, rá irányadó rendelkezéseknek mennyiben felel meg a gyakorlatban. A TFTP-ről és az Europol ezzel kapcsolatos szerepéről első alkalommal 2010. novemberben folytatott vizsgálatot, amelynek végleges formáját 2011 márciusában küldte meg az Europol részére.[37]

A vizsgálat legfontosabb megállapítása – tekintettel a megállapodás hatályba lépése óta eltelt rövid időre – az volt, amely az USA Pénzügyminisztériumát arra igyekszik rávenni, hogy megkereséseit sokkal részletesebb írásos dokumentációval támassza alá.[38] A JSB második vizsgálatával kapcsolatos sajtóanyagát – tekintettel arra, hogy maga a vizsgálati jelentés minősített – 2012. március 21-én tette közzé.[39] Ennek megállapításai között szerepel, hogy a TFTP keretében az USA Pénzügyminisztériuma havi lebontásban megszerzi a SWIFT egy meghatározott szempontrendszer alapján individualizált adatbázisát, azonban az Europolnak azon túl, hogy az USA megkereséseit vagy jóváhagyja, vagy nem, arról nincsen semmilyen információja, hogy valójában mekkora mennyiségű adat kerül átadásra az USA

2011.02.17-18. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/commission_report_joint_review_tftp.pdf (2012.05.03.)

[36] A Tanács határozata (2009. április 6.) az Európai Rendőrségi Hivatal (Europol) létrehozásáról (2009/371/IB): „*Egy független közös ellenőrző szerv kerül létrehozásra, hogy e határozattal összhangban ellenőrizze az Europol tevékenységeit annak biztosítása érdekében, hogy az Europol birtokában levő adatok tárolása, feldolgozása és felhasználása ne sértse a magánszemélyek jogait.*" http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0037:HU:PDF (2012.08.06.)

[37] Report on the inspection of Europol's implementation of the TFTP agreement, conducted in november 2010 by the Europol Joint Supervisory Body, Report no. JSB/Ins. 11-07. Brussels, 2011. 03. 01. http://www.dsk.gv.at/DocView.axd?CobId=47068 (2012.07.08.)

[38] Report ont he inspection of Europol's implementation of the TFTP agreement, conducted in november 2010 by the Europol Joint Supervisory Body, Report no. JSB/Ins. 11-07. Brussels, 2011. 03. 01., 6.

[39] Europol JSB inspection for the second year the implementation of the TFTP agreement Public Statement, Brussels, 2012.03.14. http://europoljsb.consilium.europa.eu/media/205081/tftp%20public%20statement%20-%20final%20-%20march%202012.pdf. (2012.07.19.)

Pénzügyminisztériuma részére. Az Europol ugyanis nem rendelkezik semmilyen hozzáféréssel az igényelt illetve továbbított adatokhoz. Ennek kapcsán a JSB kiemeli annak fontosságát és szükségességét, hogy az USA részletes, naprakész információkkal támassza alá minden egyes megkeresését, amely így nemcsak az Europol tevékenységét, hanem utóbbi tevékenysége felülvizsgálatára hivatott szervek munkáját is megkönnyíti. A JSB elfogadhatatlannak tartja, hogy az USA Pénzügyminisztériuma számos esetben az írásos megkeresések kiegészítéseként szóbeli tájékoztatást is adott az adatigényléshez, amelynek később nagy szerepe volt az Europol adatkiadásra vonatkozó pozitív döntésében. A JSB kizárólag a részletes és írásos dokumentációt tartja elfogadhatónak, és a megállapodás rendelkezéseivel összeegyeztethetőnek az Europol 4. cikkben meghatározott tevékenysége kapcsán.

A JSB a TFTP valamint a megállapodás összefoglaló értékeléseként leszögezi, hogy azok működésének megismerésére –céljuk veszélyeztetése nélkül – szélesebb körben kellene lehetőséget teremteni, amely így hozzájárulhatna ahhoz, hogy a korábban felmerült aggodalmakat végleg eloszlassa. Szintén a nagyobb nyilvánosság igényével lépett fel az Európai Parlament LIBE Bizottságának elnöke a levelében, amely 2012. május 29-én érkezett meg az Europol igazgatójához (Rob Wainwright).[40] A levél megérkezését követően az Europol a nyilvánosságra hozatal igényével kapcsolatban megkereséssel élt a JSB ill. az USA Pénzügyminisztériuma irányába, vonatkozó állásfoglalásaik megismerése érdekében.

Az európai rendszer kialakításának igénye (TFTS)[41]

A megállapodás hatályba lépésével egyidejűleg az Európai Bizottság (EB) felé folyamatos igényként merült fel a Tanács és az EP részéről, hogy egy éven belül nyújtsa be az Európai Parlament és a Tanács részére „az adatlehívás uniós területen történő jogi és műszaki keretét.[42] Maga a megállapodás is rendelkezik a 11. cikkben arról, hogy a Bizottság egy tanulmány keretében vizsgálja meg egy egyenértékű uniós TFTP-rendszer bevezetésének lehetőségét.

[40] http://www.statewatch.org/news/2012/jun/eu-usa-tftp-europol-ep-letter.pdf (2012.07.01.)

[41] A szerző következő tanulmánya részletesen foglalkozik majd a TFTS lehetséges, kialakításra kerülő rendszerével, az ezzel kapcsolatban keletkezett dokumentumok bemutatásával, az alternatívák nemzetközi (transzatlanti), uniós és magyarországi hatásaival.

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

A Bizottság a fenti kötelezettségnek eleget téve 2011. júliusban ismertette elképzeléseit[43]. A részletes munkaanyag legfontosabb megállapításai visszhangozzák a korábbi, elsősorban az uniós adatvédelmi aggályokat megfogalmazó grémiumok megállapításait, de egyben világossá teszik, hogy a TFTP eredményeit egy esetlegesen létrehozásra kerülő európai rendszernek is biztosítania kell, vagyis legalább olyan hatékonynak kell lennie, mint a mostani együttműködés.

Összegzés, a szerző véleménye

A TFTP gyakorlati működése és annak terrorelhárítási területen kifejtett pozitív hatása, mint ahogyan azt a Bruguiére-féle, illetve egyéb (EU-USA közös felülvizsgálat, JSB jelentés) vizsgálati jelentések is általában leszögezik, nehezen megítélhető a nyilvánosság számára, mivel nem hozzáférhetőek a jelentések nagyrészt minősített megállapításai. Álláspontom szerint a jelenlegi „nyilvánossági küszöb", a TFTP megállapodás vonatkozó garanciái, az Europol feletti szerteágazó ellenőrzési „szervezeti háló" (EP, Bizottság, JSB) eleget tesznek a kontroll kapcsán kialakult társadalmi és szakmai igénynek.

Véleményem szerint a TFTP működési mechanizmusának részletes nyilvánosságra kerülése nagymértékben veszélyeztetné annak eddig elért sikereit.

A TFTP 2006-os nyilvánosságra kerülése óta eltelt időszakban az USA és a SWIFT effektív lépéseket tett annak érdekében, hogy az EU által megfogalmazott adatvédelmi kifogások figyelembe vételével működtesse a rendszert. A 2010-ben hatályba lépett és jelenleg érvényben lévő megállapodás legfontosabb adatvédelmi garanciája magának az Europolnak a folyamatba történő beemelése volt, azt most nem vizsgálva, hogy az Europol szakmailag a legalkalmasabb szervezet volt-e a megállapodás vonatkozó rendelkezéseinek végrehajtására.

A jelenleg hatályos megállapodás, véleményem szerint kellő adatvédelmi garanciákat és jogvédelmi lehetőséget biztosít az egyén számára, amennyiben információs jogainak sérelmét valószínűsíti. Mindezzel együtt azonban naivitás lenne azt feltételezni, hogy az egyén számára teljes mértékben nyomon követhető lenne az adatok USA joghatósági területén történő felhasználásának teljes folyamata, személyes adatainak sorsa. Utóbbi a titkosszolgálati, és

[43] 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. Brüsszel, 2011.7.13. COM(2011) 429 végleges.

bűnüldöző szervek terrorelhárítási területen kifejtett tevékenységének működési elveiből következik, amely a nyilvánosság számára korlátozott hozzáférést engedélyez, és a múltban már nem egyszer a szakmai, operatív haszonszerzés az alapjogok kárára érvényesült.

A jelen megállapodás – véleményem szerint – további adatvédelmi erősítést nem tud végrehajtani, arra az önálló, európai TFTS rendszer lesz hivatott, amely lehetőség szerint az Europol 4. cikk kapcsán előírt tevékenységének korlátozottságát (az Europol nem fér hozzá a SWIFT adatokhoz, annak mennyiségéről nincs információja) is megszünteti majd.

A TFTS létrehozásával - annak konkrét megvalósulási formájától függetlenül – egy olyan európai pénzügyi terrorelhárítási rendszer jöhet létre, amely reményeink szerint a TFTP kapcsán megismert szakmai előnyök mellett adatvédelmi garanciák nyújtásával lesz képes elősegíteni a terrorfinanszírozási területen folytatott titkosszolgálati megelőző és bűnüldözői nyomozási tevékenységet.

✉ 1903 Budapest, Pf. 314. ☎ (06 1)265 6200 BM:69 000 Fax: (06 1)265 6209 BM:69 009 E-mail: tek@tek.gov.hu