



EURÓPSKA
KOMISIA

V Bruseli 27. 11. 2013
COM(2013) 842 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Európsky systém na sledovanie financovania terorizmu (TFTS EÚ)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Európsky systém na sledovanie financovania terorizmu (TFTS EÚ)

V nadväznosti na oznámenie z 13. júla 2011 [KOM(2011) 429] je cieľom tohto oznámenia informovať Európsky parlament a Radu o výsledkoch analýzy týkajúcej sa uskutočniteľnosti zavedenia systému EÚ na sledovanie financovania terorizmu (TFTS EÚ).

1. KONTEXT

1.1. Pôvod žiadosti a vymedzenie

Počas rokovaní, ktoré predchádzali uzatvoreniu dohody medzi Európskou úniou a Spojenými štátmi americkými o Programe na sledovanie financovania terorizmu (ďalej len „dohoda o TFTP medzi EÚ a USA“)¹, sa diskutovalo o tom, ako v kontexte tejto dohody zabezpečiť čo najlepšiu ochranu osobných údajov a rešpektovanie základných práv. Niektoré strany tvrdili, že extrahovaním údajov na území EÚ by sa limitoval objem údajov prenášaných do USA, čím by sa zabezpečila vyššia úroveň záruk ochrany údajov. Podľa niektorých členských štátov by vytvorenie nezávislého európskeho systému na sledovanie financovania terorizmu mohlo byť v dlhodobom horizonte pridanou hodnotou. Európsky parlament požiadal Radu a Komisiu, aby prijali všetky potrebné opatrenia na navrhnutie trvalého, právne bezchybného európskeho riešenia otázky extrahovania požadovaných údajov na území EÚ. Rada a Európsky parlament pri uzatváraní dohody o TFTP medzi EÚ a USA vyzvali Komisiu, aby do jedného roku odo dňa nadobudnutia platnosti dohody predložila právny a technický rámec na extrahovanie údajov na území EÚ a do troch rokov odo dňa nadobudnutia platnosti dohody predložila správu o pokroku pri rozvoji rovnocenného systému EÚ². V článku 11 dohody o TFTP medzi EÚ a USA sa okrem toho stanovuje, že počas platnosti tejto dohody Komisia uskutoční štúdiu možnosti zavedenia rovnocenného systému EÚ, ktorý umožní lepšie zacielené zasielanie údajov.

Na účely tohto oznámenia by rovnocenný systém EÚ mal byť odlišný od rámca na extrahovanie údajov na území EÚ. Pod *rámcom na extrahovanie údajov* na území EÚ sa rozumie systém umožňujúci vyhľadávanie údajov, ktoré v súčasnosti EÚ poskytuje Spojeným

¹ Ú. v. EÚ L 195, 27.7.2010, s. 5.

² Rozhodnutie Rady z 13. júla 2010, Ú. v. EÚ L 195, 27. 7. 2010, s. 3.

štátom, na území EÚ. Na rozdiel od toho *rovnocenný systém EÚ* by bol nezávislý európsky systém na sledovanie financovania terorizmu prostredníctvom prístupu k údajom určených poskytovateľov a vyhľadávania a analýzy týchto údajov. Zavedenie akéhokoľvek systému EÚ by si vyžadovalo zmenu dohody o TFTP medzi EÚ a USA.

1.2. Prijaté opatrenia

Komisia v decembri 2010 zadala vypracovanie *štúdie*, ktorá bola v júli 2011 rozšírená s cieľom preskúmať dodatočnú možnosť zavedenia režimu uchovávania a extrahovania. V rámci tejto štúdie Komisia usporiadala štyri stretnutia expertov, na ktorých sa zúčastnili zainteresované strany ako Europol, európsky dozorný úradník pre ochranu údajov, určený poskytovateľ TFTP³ a mnoho expertov z členských štátov, ktorí zastupovali zainteresované ministerstvá, orgány presadzovania práva a spravodajské služby, a orgány pre ochranu údajov.

Komisia 13. júla 2011 vo svojom *oznámení Európskemu parlamentu a Rade (ďalej len „oznámenie z roku 2011“)* predstavila päť možností, ktoré identifikovala v súvislosti so systémom EÚ na sledovanie financovania terorizmu (TFTS EÚ). Tri z nich sa považovali za uskutočniteľné. Cieľom oznámenia z roku 2011 bolo vyvolať diskusiu o ďalšom postupe, ktorá by mohla byť prínosná pre požadované posúdenie vplyvu.

Táto záležitosť sa v októbri 2011 predložila Rade pre spravodlivosť a vnútorné veci a Výboru Európskeho parlamentu pre občianske slobody.

Vzhľadom na to, že členské štáty a Európsky parlament jednoznačne neuprednostnili žiadnu z možností, rozhodlo sa, že Komisia všetky tieto možnosti preskúma v posúdení vplyvu a ďalej ich rozpracuje, pričom predloží rôzne čiastkové možnosti. Toto oznámenie vychádza z posúdenia vplyvu⁴.

³ Spoločnosť pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT).

⁴ SWD 2013 (xx) z .

2. HLAVNÉ ZÁSADY A MOŽNOSTI, KTORÉ KOMISIA IDENTIFIKOVALA

2.1. Zásady stratégie riadenia informácií prijatej počas švédskeho predsedníctva

Komisia vo svojej analýze navrhovaného ďalšieho postupu zohľadňuje hlavné zásady, ktoré boli stanovené v stratégii riadenia informácií z roku 2009⁵ a neskôr začlenené do oznámenia Komisie „Prehľad o riadení informácií v oblasti slobody, bezpečnosti a spravodlivosti“ z roku 2010⁶ a do oznámenia o európskom modeli výmeny informácií z roku 2012⁷, v ktorých boli ďalej rozpracované.

V tomto ohľade majú rozhodujúci význam zásady ochrany základných práv, nevyhnutnosti, proporcionality a nákladovej účinnosti.

Ochrana *základných práv*, ako je zakotvená v Charte základných práv Európskej únie, a najmä práva na súkromie a ochranu osobných údajov, je prvoradým záujmom pri príprave nových návrhov Komisie, ktoré zahŕňajú spracovanie osobných údajov v oblasti vnútornej bezpečnosti. V článkoch 7 a 8 charty sa vyhlasuje, že každý má právo na „rešpektovanie svojho súkromného a rodinného života“ a na „ochranu osobných údajov, ktoré sa ho týkajú“. V článku 16 Zmluvy o fungovaní Európskej únie, ktorá je záväzná pre všetky členské štáty a inštitúcie, agentúry a orgány Únie, sa potvrdzuje, že každý má právo na „ochranu osobných údajov, ktoré sa ho týkajú“. Podľa článku 52 charty za predpokladu dodržiavania zásady proporcionality možno práva a slobody uznané chartou obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.

Zásah do práva na súkromie sa považuje za *nevyhnutný*, pokiaľ reaguje na naliehavú potrebu, je primeraný sledovanému cieľu a ak sú dôvody uvedené vnútroštátnymi orgánmi na jeho odôvodnenie relevantné a dostatočné.

Aj keď je z finančného hľadiska ťažké vyčíslieť všetky náklady spôsobené terorizmom, zásada *nákladovej účinnosti* zostáva relevantná. *Nákladovo účinný* prístup zohľadňuje už existujúce riešenia s cieľom minimalizovať duplicitu a maximalizovať možné synergie. Je potrebné posúdiť, či by bolo možné dosiahnuť ciele návrhu lepším využitím existujúcich nástrojov.

⁵ Závery Rady z 30. novembra 2009 o stratégii riadenia informácií v oblasti vnútornej bezpečnosti EÚ 16637/09.

⁶ KOM(2010) 385 z 20. júla 2010.

⁷ COM(2012) 735 zo 7. decembra 2012.

2.2. Prístup

Komisia v súvislosti s uvedenými zásadami skúmala, či by TFTS EÚ bol v porovnaní so súčasnou situáciou nevyhnutný a primeraný z hľadiska nákladov, prínosov a jeho vplyvu na základné práva.

Pokiaľ ide o *prínosy*, systém EÚ by mohol zvýšiť možnosti prístupu EÚ a jej členských štátov k príslušným údajom a posilniť ich analytické kapacity v súvislosti so sledovaním a identifikáciou teroristov na základe finančných transakcií. Keďže finančné transakcie môžu prinášať cenné spravodajské informácie, ktoré nemusia byť prístupné z iných zdrojov, tento nástroj by mal osobitný význam pri odhaľovaní teroristických aktivít a zapojených subjektov. TFTS EÚ by preto mohol predstavovať doplnkový nástroj spravodajských služieb a vyšetrovania v boji proti terorizmu a pri zvyšovaní bezpečnosti v EÚ, a to najmä ak by takýto systém zahŕňal viacerých poskytovateľov finančných údajov a rôzne typy transakcií. Odhadované náklady na zavedenie a prevádzku takehoto systému vrátane finančného zaťaženia, ktoré by z neho vyplývalo pre EÚ, členské štáty a určených poskytovateľov príslušných údajov, musia byť vyvážené prínosmi TFTS EÚ.

2.3. Prezentácia jednotlivých možností

Zvážilo sa viacero možností tak pre *rámec na extrakciu* údajov na území EÚ, ako aj pre *rovnocenný systém EÚ*.

2.3.1. Rámec na extrakciu údajov na území EÚ

Rámec na extrakciu údajov na území EÚ by sa mohol vykonávať prostredníctvom systému uchovávaní a extrahovania údajov v držbe určeného poskytovateľa umožňujúceho priamy prístup k údajom, ktoré sa v súčasnosti poskytujú USA v rámci TFTP. Tento priamy prístup by sa poskytol analytikom USA alebo expertom splnomocneným na tento účel.

V rámci tejto možnosti by jednou z eventualít bolo uchovávať počas určitého obdobia údaje na serveri určeného poskytovateľa a vykonávať vyhľadávanie priamo na tomto serveri. Súčasný určený poskytovateľ však v rámci dohody o TFTP medzi EÚ a USA zaviedol prísne opatrenia na ochranu údajov a bezpečnostné opatrenia, ktoré neumožňujú identifikáciu osôb uvedených v obsahu správ, v dôsledku čoho súčasná databáza neumožňuje vyhľadávania na základe osobných údajov. Bolo by preto potrebné vytvoriť samostatnú databázu.

Prípadne by sa údaje mohli extrahovať a uchovávať na inom bezpečnom mieste v EÚ. Analytici USA alebo experti oprávnení vykonávať vyhľadávanie by buď mohli byť fyzicky prítomní v priestoroch určeného poskytovateľa, alebo by mohli mať k údajom diaľkový prístup. V každom prípade a bez ohľadu na to, kde sa údaje nachádzajú, by sa mali zaviesť komplexné a spoľahlivé záruky prispôbené konkrétnemu nastaveniu systému.

2.3.2. *Rovnocenný systém EÚ*

Pokiaľ ide o rovnocenný systém EÚ, posúdil sa rad možností (ako sa uvádza v oznámení z roku 2011) vrátane plne centralizovaného systému na úrovni EÚ, decentralizovaného systému na úrovni členských štátov a troch hybridných systémov, v ktorých by mali svoju úlohu EÚ aj členské štáty.

V rámci každej možnosti existujú tri rôzne možnosti súvisiace s rozsahom systému EÚ. Je potrebné rozhodnúť, aké typy správ a ktorých určených poskytovateľov bude tento systém zahŕňať. V rovnocennom systéme EÚ by sa mohol zachovať typ finančných správ a určeného poskytovateľa, na ktorých sa v súčasnosti vzťahuje dohoda o TFTP medzi EÚ a USA, alebo by sa mohol tento rámec prekročiť.

- Možnosť plne centralizovaného systému na úrovni EÚ by znamenala, že jediný subjekt EÚ by vykonával všetky kľúčové funkcie systému: žiadosti o extrahovanie údajov, uchovávanie údajov, vyhľadávanie, vykonávanie spravodajských analýz, ochranu a monitorovanie systému a poskytovanie spravodajských informácií členským štátom. Táto možnosť je však z právneho hľadiska nevyhovujúca, pretože by sa ňou porušoval článok 72 ZFEÚ, v ktorom sa potvrdzuje, že zodpovednosť za udržiavanie verejného poriadku a zabezpečovanie vnútornej bezpečnosti nesú v prvom rade členské štáty. Takýto systém by nebol ani uskutočniteľný, ani prijateľný pre členské štáty, keďže by si vyžadoval vytvorenie určitej formy centralizovanej spravodajskej kapacity na úrovni EÚ.
- Plne decentralizovaný systém na úrovni členských štátov by znamenal, že by systém prevádzkovali príslušné orgány členských štátov, pričom na úrovni EÚ by sa nevykonávali žiadne funkcie. To by znamenalo, že prenos údajov a vyhľadávanie v údajoch by mohlo vykonávať všetkých 28 členských štátov súčasne. Táto možnosť by znásobila toky údajov, čím by sa výrazne zvýšili náklady. Viedla by takisto

k zvýšenému riziku nejednotného spracúvania údajov a vytvorenia odlišných mechanizmov ochrany. Z tohto dôvodu sa ani táto možnosť nepovažuje za uskutočniteľnú.

Tieto dve možnosti sa preto z podrobnejšieho posúdenia vylúčili.

Zostávajúce tri možnosti týkajúce sa rovnocenného systému EÚ zahŕňajú rozdelenie rôznych funkcií medzi viaceré organizácie na úrovni EÚ a na vnútroštátnej úrovni (ďalej len „hybridné systémy“).

Vo všetkých týchto hybridných systémoch by bolo potrebné určeného poskytovateľa alebo určených poskytovateľov priebežne a opakovane žiadať o tieto údaje, extrahovať ich a ukladať do databázy na bezpečnom mieste v EÚ. Samotné vyhľadávanie by sa potom uskutočňovalo v tejto centrálnej databáze. Podobne pri všetkých hybridných možnostiach by sa museli zaviesť vhodné opatrenia na ochranu údajov.

- A) V prvom hybridnom systéme, Koordinačnej a analytickej službe TFTS EÚ, by sa musela vytvoriť centrálna jednotka. Jej úlohou by bolo žiadať údaje od určeného poskytovateľa alebo určených poskytovateľov, vykonávať vyhľadávania, analyzovať spravodajské informácie a šíriť výsledky. Rozdiel medzi plne centralizovaným systémom by spočíval v tom, že členské štáty by mali priamy prístup k systému a mohli by požiadať o vyhľadávanie, ktoré by vykonala v ich mene centrálna jednotka alebo by ho vykonali ich vlastní analytici.
- B) Druhý hybridný systém, Extrakčná služba TFTS EÚ, by takisto zahŕňal vytvorenie centrálnej jednotky EÚ. Pri tejto možnosti by však vyhľadávanie vykonával na požiadanie členských štátov orgán EÚ, ktorý by zasielal výsledky členským štátom bez toho, aby analyzoval spravodajské informácie. Tento orgán EÚ by však mohol vykonávať svoje vlastné vyhľadávania a analyzovať výsledky týchto vyhľadávaní.
- C) V poslednom hybridnom systéme, Koordinačnej službe pre finančné spravodajské jednotky⁸ (FIU), by sa vytvorila *ad hoc* platforma EÚ. Nešlo by o trvalý orgán, ale skôr o skupinu expertov v oblasti finančného spravodajstva, ktorí by sa zúčastňovali na zasadnutiach. Na tento účel by sa mohol zriadiť vyšší stupeň platformy FIU. Každý

⁸ Rozhodnutie Rady zo 17. októbra 2000 upravujúce spoluprácu pri výmene informácií medzi finančnými informačnými jednotkami členských štátov.

členský štát by vymenoval jedného zástupcu, ktorý by konal v jeho mene. Tento *ad hoc* orgán by zhromažďoval žiadosti od finančných spravodajských jednotiek každého členského štátu a na základe týchto žiadostí členských štátov by vydával žiadosti o údaje adresované určenému poskytovateľovi alebo určeným poskytovateľom. Každý zástupca členského štátu by bol zodpovedný za vykonávanie vyhľadávaní a analýz a za riadenie výsledkov v mene svojho členského štátu. Potom by bolo na príslušných orgánoch členských štátov, ako by spravodajské informácie využívali a ďalej šírili na vnútroštátnej úrovni.

2.3.3. *Súčasný stav: Dohoda o TFTP medzi EÚ a USA*

V súčasnosti môžu EÚ a členské štáty žiadať USA o vyhľadávanie na základe dohody o TFTP medzi EU a USA, ktorá upravuje spracovanie a zasielanie údajov obsiahnutých vo finančných správach z Európskej únie do Spojených štátov amerických na účely Programu na sledovanie financovania terorizmu (TFTP).

TFTP je nástroj boja proti terorizmu, ktorý vyvinuli Spojené štáty po teroristických útokoch z 11. septembra. Je založený na vyhľadávaní údajov poskytovaných určeným poskytovateľom vrátane údajov prenášaných z EÚ.

Dohoda o TFTP medzi EÚ a USA podrobne upravuje postup, ktorým orgány USA žiadajú o údaje. Europol overuje, či žiadosti o údaje prijímané od orgánov USA sú v súlade s dohodou, a najmä či sú čo najužšie formulované, aby sa objem prenášaných údajov obmedzil na minimum. Mnohé ustanovenia sa týkajú bezpečného zaobchádzania s údajmi, ich uchovávanie a výmazu. Poskytované údaje sa uchovávajú v zabezpečenom fyzickom prostredí a oddelene od akýchkoľvek iných údajov. V dohode sa predpisuje päťročná lehota archivovania údajov a povinnosť pravidelne posúdiť potrebu archivovania údajov. Nezávislí kontrolóri nachádzajúci sa v USA zahŕňajú dvoch nezávislých kontrolórov vybraných EÚ. Títo kontrolóri vykonávajú nepretržitý dohľad nad spôsobom fungovania systému a môžu overiť každé vyhľadávanie vykonané Ministerstvom financií USA, aby sa ubezpečili, že predmet vyhľadávania má súvislosť s terorizmom alebo jeho financovaním.

Dohoda obsahuje aj ustanovenia o práve prístupu k osobným údajom a práve na ich opravu a o opravných prostriedkoch. V dohode sa stanovuje, že každá osoba, ktorá sa domnieva, že jej osobné údaje sa spracovali v rozpore s touto dohodou, má nárok žiadať o účinnú správnu

a súdnu nápravu podľa práva EÚ, jej členských štátov a Spojených štátov. Podľa dohody majú všetky osoby bez ohľadu na národnosť alebo krajinu ich bydliska podľa práva USA k dispozícii postup, ktorým môžu žiadať o súdnu nápravu v prípade neoprávneného správneho opatrenia.

Príslušné predpisy upravujúce žiadosť o súdnu nápravu v prípade neoprávneného správneho opatrenia ministerstva financií v súvislosti s osobnými údajmi prijatými podľa dohody zahŕňajú zákon o správnom konaní a zákon o slobodnom prístupe k informáciám. Zákon o správnom konaní umožňuje osobám, ktoré utrpeli škodu v dôsledku konania vlády USA, domáhať sa súdneho preskúmania takehoto konania. Zákon o slobodnom prístupe k informáciám umožňuje osobám využívať správne a súdne opravné prostriedky na vyžiadanie vládnych záznamov. Cieľom existujúcich jednotných postupov na prístup k osobným údajom a/alebo na ich opravu, výmaz alebo zablokovanie, na ktorých sa dohodli Komisia, USA a pracovná skupina zriadená podľa článku 29, je uľahčiť občanom EÚ výkon týchto práv. Vykonávanie dohody a jej záruk a kontrol podlieha pravidelnému preskúmaniu podľa článku 13 dohody. Zatiaľ sa uskutočnili dve takéto preskúmania, a to v roku 2011⁹ a 2012¹⁰, pričom v oboch prípadoch sa dospelo k záveru, že dohoda sa vykonáva náležitým spôsobom. Tretie preskúmanie by sa malo uskutočniť na jar 2014. Spoločná správa o hodnote poskytnutých údajov vypracovaná podľa článku 6 dohody potvrdzuje prínosy TFTP pre predchádzanie terorizmu a boj proti nemu a jeho financovaniu a svedčí o tom, že TFTP využili viaceré členské štáty. Informácie TFTP a ich presnosť umožňujú identifikáciu a sledovanie teroristických a ich podporných sietí na celom svete. Ozrejmuje existujúce finančné štruktúry teroristických organizácií a umožňuje identifikáciu nových tokov finančnej podpory a zapojených aktérov.

3. POSÚDENIE

Pri posudzovaní, či by sa malo alebo nemalo navrhnuť zavedenie TFTS EÚ, musí Komisia zosúladiť rôzne stanoviská a očakávania týkajúce sa úrovne ambícií tohto systému EÚ. Jednotlivé zainteresované strany a subjekty s rozhodovacou právomocou nazierajú na ciele TFTS EÚ rôznym spôsobom. Komisia na základe uvedených zásad tvorby a implementácie

⁹ SEK(2011) 438 z 30. marca 2011.

¹⁰ SWD(2012) 454 zo 14. decembra 2012.

nových politických iniciatív preskúmala možnosti a dôsledky oboch scenárov. Každá možnosť sa posúdila najmä z hľadiska nevyhnutnosti, proporcionality a nákladovej účinnosti.

3.1. Rámec na extrakciu údajov na území EÚ

Ako sa uvádza v oddiele 2.3.1, možnosť zavedenia režimu uchovávaní a extrahovania by umožnila zhromažďovať, uchovávať a vyhľadávať údaje, ktoré sa v súčasnej dobe prenášajú do USA v rámci dohody o TFTP medzi EÚ a USA, na území EÚ. V porovnaní so súčasnou situáciou by to nemalo dodatočné prínosy pre EÚ alebo členské štáty z hľadiska spravodajských informácií. Naopak by tento režim mohol mať negatívny vplyv na kvalitu a počet spravodajských informácií a zhoršiť celkovú efektívnosť TFTP vzhľadom na to, že údaje by boli uchovávané v USA aj v EÚ, čo by viedlo k fragmentácii vyhľadávaní, ktoré sa v súčasnosti vykonávajú v rámci jedného súboru údajov. Mohol by takisto výrazne spomaliť proces analýzy, keďže na ďalšie sledovanie spravodajských informácií by mohlo byť potrebné vykonať rôzne po sebe nasledujúce vyhľadávania v údajoch TFTP uchovávaných na dvoch rôznych miestach. Pri vyšetrowaní terorizmu je však často rozhodujúca práve rýchlosť.

Extrahovanie údajov na území EÚ namiesto v USA by samo o sebe nezaručilo lepšiu ochranu osobných údajov. Na zabezpečenie náležitého zaobchádzania s údajmi je bez ohľadu na ich umiestnenie rozhodujúca ochrana prístupu k nim. Na tento účel by bolo potrebné zaviesť prísne ochranné opatrenia, ktoré by zaručili, že údaje sa budú spracúvať a bude sa s nimi zaobchádzať v súlade s potrebnými požiadavkami. Systém by musel byť vybavený kontrolnou funkciou na overovanie žiadostí o vyhľadávanie údajov a ich odôvodnení. Úloha nezávislých kontrolórov by bola zásadná pre zabezpečenie, aby sa údaje používali len na obmedzené účely, ktoré by sa vymedzili v dohode o zriadení systému. Museli by sa prijať opatrenia na zabránenie neoprávnenému prístupu k údajom alebo zverejňovaniu údajov, napr. uchovávanie údajov vo fyzicky zabezpečenom prostredí. Museli by sa začleniť postupy prístupu k údajom a opráv údajov, ako aj príslušné opravné prostriedky. Na zabezpečenie správneho fungovania systému by bolo potrebné zadať externý audit.

Podľa dohody o TFTP medzi EÚ a USA nemajú USA prístup k všetkým údajom určeného poskytovateľa, ale len k tým súborom údajov, ktoré si na základe analýzy minulých a súčasných rizík terorizmu vyžiadali a ktorých sprístupnenie schválil Europol. Ak sa nezavedie podobný mechanizmus počiatočného zúženia žiadostí o údaje, umožnenie priamych vyhľadávaní vo všetkých údajoch určeného poskytovateľa ďalej zvýši expozíciu

údajov a dosah na práva na ich ochranu. To by si vyžadovalo uskutočniť významné zmeny v spôsobe, akým určený poskytovateľ pracuje a ako sa údaje uchovávajú. Finančné správy, ktoré sú predmetom dohody, sa v súčasnosti uchovávajú vo forme, ktorá neumožňuje identifikáciu osôb uvedených v obsahu správ. Všetky finančné správy sú zašifrované a je možné ich vyhľadávať iba na základe metadát, t. j. dátumu odoslania finančnej správy, typu správy a názvu odosielajúcej a prijímajúcej banky. Určený poskytovateľ zaviedol prísne pravidlá ochrany údajov a bezpečnostné opatrenia s cieľom chrániť údaje svojich zákazníkov v celosvetovom rozsahu. Na umožnenie vykonávania vyhľadávaní priamo na serveri súčasného určeného poskytovateľa by preto všetky tieto správy bolo potrebné najprv dešifrovať. To by však predstavovalo nadmernú a neprimeranú záťaž, keďže server určeného poskytovateľa obsahuje aj iné správy než tie, ktoré sú potrebné na účel boja proti financovaniu terorizmu. Priamy prístup na účely vyhľadávania by bol okrem toho nadmerne rušivý pre každodenné činnosti určeného poskytovateľa a vytváral by značné operačné, prevádzkové, bezpečnostné a systémové riziká. Preto by bolo potrebné vytvoriť samostatnú databázu na uchovávanie príslušných údajov určeného poskytovateľa na území EÚ.

Zavedenie systému a zaručenie jeho úplného súladu s bezpečnostnými zárukami by si vyžiadalo značné investície. Priestory určeného poskytovateľa alebo iné bezpečné miesto by museli byť prispôsobené osobitným požiadavkám, museli by sa znovu vyvinúť a udržiavať riešenia v oblasti informačných technológií a technické riešenia a museli by sa prijať a vyškoliť zamestnanci s náležitou kvalifikáciou, ktorí by systém spravovali a dohliadali naň.

Pri tejto možnosti by EÚ a členské štáty znášali všetky komplikácie a náklady spojené s mechanizmom zriadeným iba na účely TFTP, ktorý je nástrojom vlastneným treťou krajinou. V súčasnej situácii táto možnosť zrejme nie je nevyhnutná, primeraná, ani nákladovo účinná vzhľadom na to, že by nebola spojená so žiadnym ďalším prínosom v oblasti spravodajských informácií, jej realizácia by bola náročná z finančného aj časového hľadiska a mohla by vytvárať riziká týkajúce sa ochrany osobných údajov.

3.2. Rovnocenný systém EÚ

Plne centralizovaný TFTP EÚ bol vylúčený z podrobnejšieho posúdenia vzhľadom na nedostatočný právny základ a malú pravdepodobnosť, že by členské štáty prijali centralizovanú úlohu EÚ v oblasti patriacej do právomoci členských štátov. Plne decentralizovaný systém bol vylúčený z dôvodu vysokých nákladov, s ktorými by bol

spojený, a zvýšeného dosahu na práva na ochranu údajov. Tri posudzované hybridné systémy by členským štátom umožňovali rôznu mieru kontroly vyhľadávani vykonávaných samotnými štátmi alebo centralizovaným orgánom EÚ.

Rozšírenie rozsahu pôsobnosti rovnocenného systému EÚ na automatizované klíringové centrá, elektronické peniaze a iné nefinančné údaje by bolo prínosom z hľadiska spravodajských informácií, pretože by sa zvýšila schopnosť EÚ sledovať platby vnútri EÚ, a mohol by sa tak vytvoriť systém, ktorý by bol lepšie pripravený na budúci vývoj než systém, ktorý by sa zaoberal iba správami FIN. Každé pridanie určeného poskytovateľa by však zvýšilo riziko porušovania práv na ochranu údajov, a vyžadovalo by si preto zavedenie prísnych podmienok, záruk a kontrolných opatrení. Tým by sa takisto zvýšila administratívna záťaž určených poskytovateľov. Pridanie viacerých poskytovateľov údajov a typov správ by si vyžadovalo vytvorenie komplexného, organizačne a technicky náročného systému, čím by sa výrazne zvýšili náklady.

Z tejto analýzy vyplýva, že uskutočniteľný je iba taký systém TFTS EÚ, ktorý by sa obmedzoval len na údaje zo správ FIN, keďže podľa Komisie by dodatočné prínosy plynúce z rôznych typov údajov a rôznych poskytovateľov nevyvážili značné náklady pre súkromné spoločnosti a zásahy do práva na súkromie a ochranu osobných údajov, ktoré by boli s takýmto systémom spojené. Vzhľadom na to, že systém EÚ by sa vzťahoval iba na rovnakého určeného poskytovateľa a rovnaký typ správy ako TFTP, kvalita aj kvantita získaných spravodajských informácií, ako aj expozícia údajov by bola porovnateľná s TFTP medzi EÚ a USA.

Ako už bolo uvedené, existujú tri možnosti rovnocenného systému EÚ: A) Koordinačná a analytická služba TFTS EÚ, B) Extrakčná služba TFTS EÚ a C) Koordinačná služba pre finančné spravodajské jednotky (FIU).

Možnosť A by pravdepodobne mala pozitívny vplyv na predchádzanie terorizmu a posilnenie bezpečnosti v EÚ. Vyhľadávaniami a analýzou výsledkov, ktoré by vykonávali EÚ aj členské štáty, by sa do určitej miery zabezpečilo, že sa v plnej miere zohľadnia špecifické spravodajské požiadavky EÚ a členských štátov a že sa systém bude zameriavať na špecifické hrozby pre EÚ. Toto zlepšenie je však podmienené vyššou ochotou a schopnosťou členských štátov zdieľať informácie a analýzy v strednodobom až dlhodobom horizonte. Nie je jasné, do

akej miery je možné spoliehať sa na tento zvýšený tok informácií. Okrem toho, keďže by zostala zachovaná možnosť, aby členské štáty žiadali USA o vyhľadávanie v rámci TFTP, boli by potrebné veľké investície a vysoká miera spolupráce členských štátov, ak by mal tento systém poskytovať ucelenejší prehľad o EÚ.

Možnosť B by mohla mať určitý pozitívny vplyv na predchádzanie terorizmu a posilnenie bezpečnosti v EÚ. Tento systém by lepšie reagoval na analýzy hrozieb EÚ, keďže vyhľadávania by sa vykonávali podľa špecifických spravodajských požiadaviek členských štátov. Úloha centralizovaného orgánu EÚ by sa však obmedzovala na vykonávanie vyhľadávania a prenos príslušných údajov žiadajúcemu členskému štátu. Hlavnou úlohou tohto orgánu by teda bola najmä kontrola prístupu. V dôsledku toho by sa na úrovni EÚ nevykonávali žiadne analýzy a pri vytváraní súboru ucelených spravodajských informácií v rámci celej EÚ by bol systém v plnej miere závislý od toho, ako by si členské štáty navzájom vymieňali svoje analýzy mimo tento systém. Neschopnosť systému zaručiť jednotný prístup k vymedzeniu vyhľadávania by zvýšila riziko falošne pozitívnych výsledkov, čím by bolo dotknuté právo na súkromie a právo na ochranu údajov.

Pri možnosti C by sa zohľadňovali špecifické spravodajské potreby členských štátov, čo by malo určitý pozitívny vplyv na predchádzanie terorizmu a posilnenie bezpečnosti. Keďže by však za vykonávanie vyhľadávania a analýz boli zodpovedné národné finančné spravodajské jednotky, má táto možnosť rovnaké nevýhody ako možnosť B – jasný prehľad o situácii by bolo možné získať len prostredníctvom posilnenej spolupráce členských štátov mimo systém. Finančné spravodajské jednotky sa okrem toho zameriavajú iba na finančné spravodajstvo a rozlišovanie medzi týmito informáciami a ostatnými spravodajskými informáciami by mohlo sťažiť zisťovanie súvislostí a odhaľovanie financovania terorizmu. Pri tejto možnosti je zapojenie EÚ takisto veľmi malé a k posilneniu kapacít by došlo predovšetkým na vnútroštátnej úrovni.

Všetky tieto možnosti by znamenali značné náklady pre EÚ, členské štáty a určeného poskytovateľa, okrem iného náklady na rozvoj infraštruktúry informačných technológií, na bezpečnostné zariadenia a náklady na desiatky, ak nie stovky zamestnancov zodpovedných za riadenie systému a vykonávanie ochranných opatrení a kontrol. Každý z týchto možných systémov však má potenciál prispieť k posilneniu európskej bezpečnostnej situácie, keďže by sa zakladal na posudzovaní špecifických hrozieb podľa potrieb EÚ.

Nezávislý nástroj spravodajských služieb a vyšetrovania na území EÚ by odstránil potrebu prenosu údajov do USA. Akýkoľvek systém TFTP EÚ by si však takisto vyžadoval rozsiahle opatrenia na ochranu údajov a kontroly podobné tým, ktoré sa už uplatňujú v rámci dohody o TFTP medzi EÚ a USA, pričom by v každom prípade museli byť v súlade s *acquis* EÚ a členských štátov v oblasti ochrany údajov. Pri každej žiadosti o vyhľadávanie údajov v systémoch EÚ by bolo potrebné overiť, či je v súlade s požiadavkou prísneho obmedzenia účelu na boj proti terorizmu a jeho financovaniu, vrátane oprávnenosti prenosu údajov. Najmä kvalifikovaní nezávislí kontrolóri by museli pri každom vyhľadávaní na úrovni EÚ alebo v členských štátoch overovať, či bolo riadne povolené a či bolo nevyhnutné na účely boja proti terorizmu a jeho financovaniu. Muselo by sa zaistiť bezpečné zaobchádzanie s údajmi a ich uchovávanie a zabrániť neoprávnenému prístupu k údajom. Bol by potrebný externý audit riadneho fungovania systému a všetkých jeho záruk. Do systému by sa museli začleniť všetky potrebné postupy na prístup k osobným údajom a ich opravu a príslušné opravné prostriedky.

Na záver možno konštatovať, že Komisia v súlade s požiadavkami Európskeho parlamentu a Rady posúdila možnosti zavedenia systému TFTP EÚ vrátane režimu extrahovania a uchovávanía.

V tomto posúdení sa zohľadňujú zásady zakotvené v stratégii riadenia informácií, ktorá bola prijatá počas švédskeho predsedníctva. Akýkoľvek zriadený systém musí byť nevyhnutný, primeraný a nákladovo účinný a musí rešpektovať základné práva. Ako sa podrobne uvádza v predošlom texte a v posúdení vplyvu, na základe analýzy vykonanej Komisiou možno konštatovať, že každá uskutočniteľná možnosť má svoje výhody aj nevýhody. Komisia však nebrala do úvahy tie možnosti, ktoré nie sú z už uvedených dôvodov uskutočniteľné.

Na základe zhromaždených informácií nie je možné jasne preukázať potrebu predložiť v tejto fáze návrh na zavedenie systému TFTP EÚ.

Komisia uvíta názory Európskeho parlamentu a Rady na toto oznámenie.