



EVROPSKÁ
KOMISE

V Bruselu dne 27.11.2013
COM(2013) 842 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Evropský systém sledování financování terorismu (EU TFTS)

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

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Evropský systém sledování financování terorismu (EU TFTS)

V návaznosti na sdělení ze dne 13. července 2011 (KOM(2011) 429) je cílem tohoto sdělení informovat Evropský parlament a Radu o výsledcích analýzy proveditelnosti, pokud jde o zřízení evropského systému sledování financování terorismu (EU TFTS).

1. SOUVISLOSTI

1.1. Původ žádosti a definice

Během jednání, která předcházela uzavření Dohody o Programu sledování financování terorismu (dohoda o TFTP mezi EU a USA)¹, probíhaly diskuse o tom, jak nejlépe chránit osobní údaje a dodržovat základní práva v rámci této dohody. Některé zúčastněné strany tvrdily, že extrahování údajů na území Evropy by omezilo množství údajů předávaných do USA, a tak by se zajistila vyšší úroveň záruk ochrany údajů. Některé členské státy se domnívaly, že v dlouhodobém horizontu je smysluplné vyvinout nezávislý evropský systém sledování financování terorismu. Evropský parlament požádal Radu a Komisi, aby přijaly veškerá opatření nezbytná pro návrh trvalého, zákonného evropského řešení otázky extrahování požadovaných údajů na území EU. Rada a Evropský parlament při schvalování TFTP mezi EU a USA vyzvaly Komisi, aby do jednoho roku ode dne vstupu dohody v platnost předložila právní a technický rámec pro získávání údajů na území EU a do tří let ode dne vstupu dohody v platnost zprávu o pokroku dosaženém při rozvoji rovnocenného systému EU². Kromě toho článek 11 dohody o TFTP mezi EU a USA uvádí, že během platnosti dohody Komise vypracuje studii o možném zavedení rovnocenného systému EU, jenž by umožňoval cílenější předávání údajů.

Pro účely tohoto sdělení by měl být odlišován rovnocenný systém EU od rámce pro extrahování údajů na území EU. *Rámcem pro extrahování údajů* na území EU se rozumí systém, jenž umožňuje provádět vyhledávání údajů, které EU v současné době poskytuje do USA, na území EU. Naopak, *rovnocenným systémem EU* by byl nezávislý evropský systém sledování financování terorismu, a to prostřednictvím přístupu k údajům, vyhledávání

¹ Úř. věst. L 195, 27.7.2010, s. 5.

² Rozhodnutí Rady ze dne 13. července 2010, Úř. věst. L 195, 27.7.2010, s. 3.

a analýzy údajů určených poskytovateli. Zavedení takového systému EU by si vyžádalo změnu dohody o TFTP mezi EU a USA.

1.2. Přijatá opatření

V prosinci 2010 Komise zadala *studii*, která byla v červenci 2011 rozšířena tak, aby prověřila dodatečnou variantu zavedení režimu uchovávání a extrahování. V rámci této studie Komise uspořádala čtyři setkání odborníků za účasti zúčastněných stran, jako jsou Europol, evropský inspektor ochrany údajů, určený poskytovatel TFTP³ a mnozí odborníci z členských států, kteří zastupovali zúčastněná ministerstva, donucovací orgány a zpravodajské služby a orgány odpovědné za ochranu údajů.

Dne 13. července 2011 Komise ve svém *sdělení Evropskému parlamentu a Radě („sdělení z roku 2011“)* představila pět možných variant pro vytvoření evropského systému sledování financování terorismu (dále jen „EU TFTS“). Z toho byly tři považovány za proveditelné. Cílem sdělení z roku 2011 bylo zahájit diskusi o dalším postupu, a přispět tak k požadovanému hodnocení dopadů.

Tato otázka byla v říjnu 2011 předložena v Radě pro spravedlnost a vnitřní věci a ve Výboru Evropského parlamentu pro občanské svobody.

Jelikož členské státy a Evropský parlament jasně neupřednostnily žádnou z variant, bylo rozhodnuto, že je Komise všechny přezkoumá v posouzení dopadů a rozpracuje je předložením různých subvariant. Toto sdělení vychází z uvedeného posouzení dopadů⁴.

2. HLAVNÍ ZÁSADY A VARIANTY ZJIŠTĚNÉ KOMISÍ

2.1. Zásady strategie pro správu informací přijaté v rámci švédského předsednictví

Ve své analýze návrhů dalšího postupu Komise zohledňuje hlavní zásady uvedené ve strategii pro správu informací z roku 2009⁵, které byly později začleněny do sdělení Komise o přehledu o správě informací v prostoru svobody, bezpečnosti a práva z roku 2010⁶ a o evropském modelu pro výměnu informací z roku 2012⁷ a dále v nich rozvíjeny.

³ Společnost pro celosvětovou mezibankovní finanční telekomunikaci (SWIFT).

⁴ SWD 2013 (xx) ze dne

⁵ Závěry Rady ze dne 30. listopadu 2009 o strategii pro správu informací pro vnitřní bezpečnost EU 16637/09.

⁶ KOM(2010) 385 ze dne 20. července 2010.

⁷ COM(2012) 735 ze dne 7. prosince 2012.

V tomto ohledu jsou nesmírně důležité zásady ochrany základních práv, nezbytnosti, proporcionality a efektivnosti nákladů.

Při vypracovávání nových návrhů, které zahrnují zpracování osobních údajů v oblasti vnitřní bezpečnosti, má Komise v první řadě na zřeteli ochranu *základních práv* zakotvených v Listině základních práv Evropské unie, a zejména práva na soukromí a ochranu osobních údajů. V listině se prohlašuje, že každý má právo na „respektování svého soukromého a rodinného života“ (článek 7) a „ochranu osobních údajů, které se ho týkají“ (článek 8). Článek 16 Smlouvy o fungování Evropské unie, který je závazný pro všechny členské státy, orgány Unie, agentury a subjekty, potvrzuje, že každý má právo na „ochranu osobních údajů, které se jej týkají“. Podle článku 52 listiny mohou při dodržení zásady proporcionality být omezení výkonu práv a svobod uznaných touto listinou zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.

Zásah do práva na soukromí je považován za *nezbytný*, jestliže reaguje na naléhavou potřebu, jestliže je přiměřený sledovanému cíli a jestliže důvody přednesené veřejným orgánem dokládající oprávněnost zásahu jsou relevantní a dostatečné.

Ačkoliv je z finančního hlediska obtížné vyčíslit všechny náklady způsobené terorismem, zásada *efektivnosti nákladů* přetrvává. *Nákladově efektivní* přístup bere v úvahu již existující řešení, aby se co nejméně překrývala a co nejvíce se zvýšila možná součinnost. Je třeba posoudit, zda není možné dosáhnout cílů návrhu lepším využitím stávajících nástrojů.

2.2. Přístup

S ohledem na výše uvedené zásady Komise zkoumala, zda by systém EU TFTS byl ve srovnání se současnou situací nezbytný a přiměřený z hlediska nákladů, přínosů a jeho dopadu na základní práva.

Pokud jde o *přínosy*, systém EU by mohl zvýšit možnosti přístupu EU a jejích členských států k příslušným údajům a posílit jejich analytické kapacity pro sledování a identifikaci teroristů na základě finančních transakcí. Jelikož finanční transakce mohou poskytnout hodnotné zpravodajské informace, jež nemusí být dostupné z jiných zdrojů, měl by tento nástroj zvláštní význam pro odhalování teroristických činností či zapojených subjektů. Proto by systém EU TFTS mohl představovat další nástroj zpravodajských služeb a vyšetřování v boji

proti terorismu a při zvyšování bezpečnosti v EU, zejména pokud by takový systém zahrnoval několik poskytovatelů finančních údajů a různé typy transakcí. Je třeba, aby přínosy systému EU TFTS byly v rovnováze s odhadovanými náklady na jeho zavedení a provoz, včetně finanční zátěže pro EU, členské státy a pro určené poskytovatele příslušných údajů.

2.3. Představení variant

Zvažovala se celá řada variant jak ohledně *rámce pro extrahování údajů na území EU*, tak ohledně *rovnocenného systému EU*.

2.3.1. Rámec pro extrahování údajů na území EU

Rámec pro extrahování údajů na území EU by mohl mít podobu systému uchovávání a extrahování údajů držených určenými poskytovateli, jenž by umožňoval přímý přístup k údajům, které jsou v současnosti poskytovány USA v rámci TFTP. Tento přímý přístup by byl poskytnut analytikům USA nebo odborníkům pro tento účel zmocněným.

Podle této varianty by jednou z možností bylo po určitou dobu uchovávat údaje na serveru určeného poskytovatele a vyhledávat přímo na tomto serveru. Nicméně stávající určený poskytovatel v rámci dohody o TFTP mezi EU a USA zavedl přísná opatření na ochranu údajů a bezpečnostní opatření, která nepřipouští identifikaci osob zmíněných v obsahu zpráv, takže jeho databáze neumožňuje vyhledávání na základě osobních údajů. Musela by se proto vytvořit samostatná databáze.

Případně by údaje mohly být extrahovány a uchovávány na jiném zabezpečeném místě v EU. Analytici nebo odborníci z USA oprávnění vyhledávat by mohli být buď fyzicky přítomni v prostorách určeného poskytovatele nebo by mohli mít dálkový přístup k údajům. V každém případě a bez ohledu na to, kde jsou tyto údaje umístěny, by měly být zavedeny komplexní a spolehlivé záruky přizpůsobené konkrétnímu uspořádání systému.

2.3.2. Rovnocenný systém EU

Ohledně zavedení rovnocenného systému EU byla posouzena řada variant (jak je uvedeno ve sdělení z roku 2011), včetně plně centralizovaného systému na úrovni EU, decentralizovaného systému na úrovni členských států a tří hybridních systémů, v nichž by určitou úlohu hrály EU i členské státy.

V rámci jednotlivých variant existují různé možnosti, pokud jde o rozsah systému EU. Je třeba rozhodnout, na jaké typy zpráv a které určené poskytovatele se bude vztahovat. Rovnocenný systém EU může zachovat typ finančních zpráv a určeného poskytovatele, na které se v současnosti vztahuje dohoda o TFTP mezi EU a USA, nebo mít širší záběr.

- Varianta plně centralizovaného systému na úrovni EU by znamenala, že by všechny klíčové funkce systému vykonával jediný subjekt EU: žádání o extrahování údajů, uchovávání údajů, vyhledávání, provádění zpravodajských analýz, ochranu a monitorování systému a poskytování zpravodajských informací členským státům. Tato varianta je však právně nevhodná, neboť by porušovala článek 72 Smlouvy o fungování Evropské unie, který potvrzuje, že primární odpovědnost za zachování práva a pořádku a ochranu vnitřní bezpečnosti nesou členské státy. Tento systém by nebyl pro členské státy proveditelný ani přijatelný, jelikož by vyžadoval vytvoření určité formy centralizované zpravodajské kapacity na úrovni EU.
- Plně decentralizovaný systém na úrovni členských států by znamenal, že by systém provozovaly příslušné orgány členských států, přičemž by žádné funkce nebyly prováděny na úrovni EU. To by znamenalo, že by údaje mohly být předávány a vyhledávány všemi 28 členskými státy současně. Tyto varianta by znásobila toky údajů, čímž by se značně zvýšily náklady. Vedla by také k tomu, že by se zvýšilo riziko nejednotného nakládání s údaji a zavedení odlišných mechanismů ochrany. Z tohoto důvodu se ani tato varianta nepovažuje za proveditelnou.

Obě tyto varianty tudíž byly vyloučeny z podrobnějšího posouzení.

Zbývající tři varianty pro zavedení rovnocenného systému EU zahrnují rozdělení různých funkcí mezi různé organizace na úrovni EU a na vnitrostátní úrovni (dále jen „hybridní systémy“).

Ve všech těchto hybridních systémech by bylo třeba určené poskytovatele žádat o údaje průběžně a opakovaně a tyto údaje by se musely extrahovat a ukládat do databáze na zabezpečeném místě v EU. Ke skutečnému vyhledávání by pak docházelo v této ústřední databázi. Podobně pro všechny varianty platí, že by musela být zavedena vhodná opatření na ochranu údajů.

- A) V rámci prvního hybridního systému by musela být vytvořena ústřední jednotka EU, koordináční a analytická služba systému EU TFTS. Jejím úkolem by bylo žádat údaje od určených poskytovatelů, vyhledávat, analyzovat zpravodajské informace a šířit výsledky. Na rozdíl od plně centralizovaného systému by členské státy měly přímý přístup k systému a měly by možnost žádat o vyhledávání, které by ústřední jednotka nebo jejich vlastní analytici prováděli jejich jménem.
- B) Druhý hybridní systém – služba systému EU TFTS pro extrahování údajů – by také znamenal vytvoření ústřední jednotky EU. V tomto případě by však subjekt EU vyhledával údaje na žádost členských států a sdílel by výsledky s členskými státy, aniž by prováděl zpravodajskou analýzu. Tento subjekt EU by však byl schopen provádět vlastní vyhledávání a analyzovat jejich výsledky.
- C) V posledním hybridním systému by byla vytvořena *ad hoc* platforma na úrovni EU – koordináční služba finanční zpravodajské jednotky⁸ (dále jen „FIU“). Nejednalo by se o trvalý orgán, ale spíše o skupinu odborníků na finanční zpravodajství, kteří by se scházeli podle potřeby. Platforma FIU by případně mohla být pro tento účel modernizována. Každý členský stát by jmenoval jednoho zástupce, který by jednal jeho jménem. Tento *ad hoc* orgán by shromažďoval žádosti od finančních zpravodajských jednotek každého členského státu a na základě těchto žádostí členských států by žádal o údaje určené poskytovatele. Každý zástupce členského státu by byl odpovědný za vyhledávání, provádění analýz a řízení výsledků jménem svého členského státu. Pak by záleželo na příslušných orgánech členských států, jak by zpravodajské informace využívaly a dále šířily na vnitrostátní úrovni.

2.3.3. *Současný stav: Dohoda o TFTP mezi EU a USA*

EU a členské státy mohou v současné době žádat Spojené státy o vyhledávání na základě dohody mezi EU a USA o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu sledování financování terorismu (dále jen „TFTP“).

⁸ Rozhodnutí Rady ze dne 17. října 2000 o způsobech spolupráce mezi finančními zpravodajskými jednotkami členských států při výměně informací.

TFTP vyvinuly Spojené státy jako protiteroristický nástroj po teroristických útocích dne 11. září. Je založen na vyhledávání údajů poskytnutých určeným poskytovatelem, včetně údajů předávaných z EU.

Dohoda o TFTP mezi EU a USA podrobně upravuje postup, jak musí orgány USA žádat o údaje. Europol ověří, že žádosti o údaje doručené od orgánů USA jsou v souladu s dohodou, a zejména, že jsou pokud možno úzce zaměřené, aby se objem dat, která se předávají, omezil na minimum. Bezpečné nakládání s údaji, jejich uchovávání a výmaz je upraveno řadou ustanovení. Poskytované údaje se uchovávají v bezpečném fyzickém prostředí, odděleně od veškerých dalších údajů. Dohoda předepisuje pětiletou lhůtu pro uchovávání údajů a rovněž povinnost pravidelně posoudit potřebu uchovávat údaje. Nezávislé orgány dohledu se sídlem v USA zahrnují dva orgány dohledu vybrané EU. Soustavně dohlíží na to, jakým způsobem systém funguje, a mají možnost ověřit každé vyhledávání provedené ministerstvem financí USA, aby se ujistily, že předmět vyhledávání je spojen s terorismem nebo jeho financováním.

Dohoda rovněž obsahuje ustanovení o právu na přístup k osobním údajům a jejich opravu a o opravných prostředcích. Dohoda dále stanoví, že domnívá-li se některá osoba, že její osobní údaje byly zpracovány v rozporu s touto dohodou, může se domáhat účinné správní nebo soudní nápravy v souladu s právními předpisy Evropské unie, jejích členských států a USA. Podle dohody mají všechny osoby bez ohledu na státní příslušnost nebo zemi bydliště k dispozici možnost domáhat se podle práva USA soudní nápravy v případě správního úkonu, který je v jejich neprospěch.

V případě nepříznivého správního úkonu ministerstva financí v souvislosti s osobními údaji obdrženy podle dohody se lze domáhat nápravy podle zákona o správním řízení a zákona o svobodném přístupu k informacím. Zákon o správním řízení umožňuje osobám, které utrpěly škodu v důsledku jednání státních orgánů USA, domáhat se soudního přezkumu uvedeného jednání. Zákon o svobodném přístupu k informacím umožňuje osobám využívat správní a soudní opravné prostředky pro vyžádání státních záznamů. Stávající jednotné postupy pro přístup k osobním údajům a/nebo opravu, výmaz nebo blokování osobních údajů dohodnuté mezi Komisí, USA a pracovní skupinou zřízenou podle článku 29 mají za cíl usnadnit občanům EU výkon těchto práv. Provádění dohody a jejích záruk a kontrol je předmětem pravidelných přezkumů podle článku 13 dohody. U obou dosavadních přezkumů, které se

uskutečnily v letech 2011⁹ a 2012¹⁰, se dospělo k závěru, že dohoda byla řádně prováděna. Třetí přezkum se plánuje na jaro 2014. Společná zpráva týkající se hodnoty poskytovaných údajů předložená podle článku 6 dohody ukazuje, jak je TFTP při předcházení terorismu a boji proti terorismu a jeho financování přínosný a že TFTP využilo několik členských států. Přesné informace TFTP umožňují identifikaci a sledování teroristických skupin a jejich podpůrných sítí po celém světě. Tyto informace osvětlují stávající finanční struktury teroristických organizací a umožňují odhalovat nové toky finanční podpory a zúčastněné subjekty.

3. POSOUZENÍ

Při posuzování, zda by mělo či nemělo být navrženo zavedení EU TFTS, musí Komise sladit různá stanoviska a očekávání ohledně cílů systému EU. Různé zainteresované subjekty a osoby s rozhodovací pravomocí mají na cíle EU TFTS různý názor. Komise již dříve posoudila možnosti a důsledky obou scénářů na základě zásad rozvoje a zavádění nových politických iniciativ popsanych dříve. Každá varianta byla zejména posouzena z hlediska nezbytnosti, proporcionality a nákladové efektivity.

3.1. Rámec pro extrahování údajů na území EU

Jak je popsáno v oddíle 2.3.1., varianta zavedení režimu uchovávání a extrahování by umožnila shromažďovat, uchovávat a vyhledávat údaje, které se v současné době předávají do USA v rámci dohody o TFTP mezi EU a USA, na území EU. Pokud jde o zpravodajské údaje, neznamenalo by to v porovnání se současnou situací pro EU nebo členské státy žádný další přínos. Naopak, tím, že by byly údaje TFTP uchovávány v USA i v EU, mohla by fragmentace vyhledávání, která v současné době probíhají v rámci jediného souboru údajů TFTP, mít negativní dopad na kvalitu a počet důležitých zpravodajských informací a zhoršit celkovou účinnost TFTP. Mohl by se rovněž výrazně zpomalit proces analýzy, jelikož by za účelem dalšího sledování důležitých zpravodajských informací mohlo být třeba provést různá po sobě jdoucí vyhledávání údajů TFTP uchovávaných na dvou různých místech. Při vyšetřování terorismu je však rychlost často rozhodující.

⁹ SEK(2011) 438 ze dne 30. března 2011.

¹⁰ SWD(2012) 454 ze dne 14. prosince 2012.

Extrahování údajů na území EU namísto v USA by samo o sobě nezaručilo lepší ochranu osobních údajů. Pro zajištění řádného zpracování údajů je bez ohledu na jejich umístění rozhodující, jak je přístup k údajům chráněn. Za tímto účelem bylo by nutné zavést přísná ochranná opatření, která by zaručila, že budou údaje zpracovávány a že s nimi bude nakládáno v souladu s nezbytnými požadavky. Systém by musel být vybaven kontrolní funkcí k ověřování žádostí o vyhledání údajů a jejich odůvodnění. Při zajišťování toho, aby byly údaje používány jen pro omezené účely definované v případné zřizovací dohodě, by měla zásadní význam úloha nezávislých orgánů dohledu. Musela by se přijmout opatření, která by zabránila neoprávněnému přístupu k údajům nebo zveřejňování údajů, např. uchovávání údajů ve fyzicky zabezpečeném prostředí. Musely by se stanovit postupy pro přístup k osobním údajům a jejich opravu a příslušné opravné prostředky. Aby se zajistilo správné fungování systému, musel by se zadat externí audit.

Podle dohody o TFTP mezi EU a USA nemají Spojené státy přístup ke všem údajům určeného poskytovatele, avšak pouze k souborům údajů, které si na základě analýzy minulých a současných rizik terorismu USA vyžádaly a jejichž předání schválil Europol. Nebude-li zaveden podobný mechanismus počátečního omezení žádostí o údaje, přímé vyhledávání ve veškerých údajích určeného poskytovatele by vedlo k vyšší expozici údajů a dalšímu dopadu na práva na ochranu údajů. To by si vyžádalo významné změny ve způsobu, jakým určený poskytovatel pracuje a jak jsou údaje uchovávány. V současné době se finanční zprávy, které jsou předmětem dohody, uchovávají ve formě, která nepřipouští identifikaci osob uvedených v obsahu zpráv. Všechny finanční zprávy jsou zašifrovány a je možné v nich vyhledávat pouze na základě metadat (datum odeslání zprávy, druh zprávy a název odesílající a přijímající banky). Určený poskytovatel zavedl přísná ochranná a bezpečnostní opatření v zájmu ochrany údajů svých zákazníků na celém světě. Aby tedy bylo možné vyhledávat přímo na serveru současného určeného poskytovatele, musely by být všechny tyto zprávy nejprve dešifrovány. To by ovšem znamenalo nadměrnou a nepřiměřenou zátěž, neboť server určeného poskytovatele obsahuje více zpráv, než je pro účely boje proti financování terorismu třeba. Kromě toho by přímý přístup pro účely vyhledávání nepřipustně zatěžoval každodenní činnosti určeného poskytovatele a způsoboval by značná provozní, bezpečnostní a systémová rizika. Proto by musela být vytvořena samostatná databáze nezbytných údajů určeného poskytovatele na území EU.

Zavedení systému a zaručení jeho úplného souladu s bezpečnostními zárukami by si vyžádalo značné investice. Prostory určeného poskytovatele nebo jiné zabezpečené místo by musely být přizpůsobeny zvláštním požadavkům, musela by být navržena a používána řešení v oblasti informačních technologií a technická řešení a museli by být zaměstnání a vyškoleni dobře kvalifikovaní pracovníci, kteří by systém spravovali a dohlíželi na něj.

Při této variantě by veškeré těžkosti a náklady spojené s mechanismem zřízeným pouze pro účely TFTP, jenž je nástrojem ve vlastnictví třetí země, nesly EU a členské státy. Nezdá se, že by v současné době byla tato varianta nutná, přiměřená nebo nákladově efektivní, protože by neměla žádný další přínos v oblasti zpravodajství, provedení by bylo finančně i časově náročné a mohla by ohrozit ochranu osobních údajů.

3.2. Rovnocenný systém EU

Plně centralizovaný systém EU TFTP byl z podrobnějšího posouzení vyloučen vzhledem k chybějícímu právnímu základu a malé šanci, že by členské státy mohly přijmout ústřední úlohu EU v oblasti spadající do pravomoci členských států. Varianta plně decentralizovaného systému byla rovněž vyloučena, neboť by byla spojena s vysokými náklady a měla četné dopady na práva na ochranu údajů. Tři posuzované hybridní systémy by členským státům umožňovaly v různé míře kontrolovat vyhledávání, která provádějí samy nebo centralizovaný subjekt EU.

Rozšíření oblasti působnosti rovnocenného systému EU na automatizovaná zúčtovací střediska, elektronické peníze a další nefinanční údaje by bylo v oblasti zpravodajství přínosné, neboť by se zvýšila schopnost EU sledovat platby uvnitř EU, a mohlo by vést k vytvoření systému, jenž by v budoucnosti obstál lépe než systém, který by se zabýval pouze finančními zprávami. Nicméně s každým dalším určeným poskytovatelem by se zvýšilo riziko porušování práv na ochranu údajů, což by vyžadovalo zavedení přísných podmínek, záruk a kontrolních opatření. Tím by se určeným poskytovatelům rovněž zvýšila administrativní zátěž. Rozšířením na více poskytovatelů údajů by vytvoření tak komplexního, organizačně a technicky náročného systému rovněž podstatně zvýšilo náklady.

Protože se Komise domnívá, že další výhody rozšíření počtu datových typů a poskytovatelů nevyváží značné náklady pro soukromé společnosti a poškození práva na ochranu soukromí a údajů, které by tento systém znamenal, byl by v důsledku této analýzy proveditelný pouze

systém EU TFTS vztahující se výlučně na finanční údaje. Jelikož by se systém EU vztahoval pouze na stejného určeného poskytovatele a stejný typ zprávy jako TFTP, byla by kvalita a kvantita získaných zpravodajských informací, jakož i expozice údajů srovnatelná s TFTP mezi EU a USA.

Jak je uvedeno výše, připadají v úvahu tři varianty rovnocenného systému EU: A) koordinační a analytická služba systému EU TFTS; B) služba systému TFTS EU pro extrahování údajů a C) koordinační služba finanční zpravodajské jednotky.

Varianta A by pravděpodobně měla na předcházení terorismu a zlepšení bezpečnosti v EU pozitivní dopad. Kdyby vyhledávání a analýzu výsledků prováděly týmy EU i členských států, bylo by do jisté míry zajištěno, že budou plně zohledněny zvláštní zpravodajské požadavky EU a členských států a že se systém bude zaměřovat na specifické „hrozby pro EU“. Toto zlepšení by však stále záviselo na vyšší ochotě a schopnosti členských států ve střednědobém až dlouhodobém horizontu sdílet informace a analýzy. Není jasné, do jaké míry lze na tento zvýšený tok informací spoléhat. Jelikož by si členské státy ponechaly možnost žádat o vyhledávání ze strany USA v rámci TFTP, vyžadoval by tento systém, pokud by měl podávat ucelenější přehled o EU, navíc od členských států velké investice a vysokou míru spolupráce.

Varianta B by mohla mít na předcházení terorismu a zlepšení bezpečnosti v EU určitý pozitivní dopad. Tento systém by lépe reagoval na analýzy hrozeb provedené EU, neboť vyhledávání by se prováděla podle zvláštních zpravodajských požadavků členských států. Ovšem úloha centralizovaného subjektu na úrovni EU by byla omezena na vyhledávání a předávání odpovídajících údajů žádajícímu členskému státu; působil by tedy spíše jako kontrolor přístupu než cokoli jiného. V důsledku toho by nebyly prováděny analýzy na úrovni EU a systém, pokud jde o vytvoření uceleného zpravodajského přehledu EU, by byl zcela závislý na tom, že by členské státy vzájemně sdílely své analýzy mimo daný systém. Neschopnost systému zaručit jednotný přístup k definicím vyhledávání by zvýšil riziko falešně pozitivních výsledků, čímž by byla omezena práva na ochranu údajů a soukromí.

Varianta C by zohledňovala zvláštní zpravodajské potřeby členských států, a tak by měla na předcházení terorismu a zvyšování bezpečnosti určitý pozitivní dopad. Jelikož by však vnitrostátní finanční zpravodajské jednotky byly odpovědné za vyhledávání a analýzy svých

členských států, má tato varianta stejné nevýhody jako varianta B – jasný přehled o situaci lze získat pouze za posílené spolupráce členských států mimo systém. Navíc se finanční zpravodajské jednotky zaměřují pouze na finanční zpravodajství a rozlišování mezi těmito informacemi a ostatními zpravodajskými údaji by mohlo ztížit poznávání souvislostí a odhalování financování terorismu. V rámci této varianty by zapojení EU bylo možné jen ve velmi malé míře a kapacity by byly posíleny především na vnitrostátní úrovni.

Všechny tyto varianty by s sebou nesly značné náklady pro EU, členské státy a určeného poskytovatele, mimo jiné náklady na rozvoj infrastruktury informačních technologií, zabezpečené zařízení, jakož i náklady na desítky, ne-li stovky zaměstnanců odpovědných za správu systému, a dodržování záruk a provádění kontrol. Avšak každý z těchto možných systémů má potenciál přispívat ke zlepšení evropské bezpečnostní situace, jelikož by vycházel z analýz hrozeb odpovídajících evropským potřebám.

S nezávislým zpravodajským a vyšetřovacím nástrojem na evropském území by odpadla potřeba předávat údaje do USA. Avšak jakýkoli systém EU TFTS by stále vyžadoval zesílená opatření na ochranu údajů a kontroly podobné těm, které již platí na základě dohody o TFTP mezi EU a USA, jež by v každém případě vyhovovaly platnému *acquis* EU a právu členských států v oblasti ochrany údajů. U každé žádosti o vyhledávání údajů v systémech EU by se muselo ověřit, zda je dodrženo přísné účelové omezení na boj proti terorismu a jeho financování, včetně toho, zda je předání údajů oprávněné. Zejména by se využívaly kvalifikované nezávislé orgány dohledu, které by musely u každého vyhledávání na úrovni EU nebo v členských státech ověřovat, zda bylo řádně povoleno a zda bylo nezbytné pro účely boje proti terorismu a jeho financování. Dále by muselo být zajištěno bezpečné nakládání s údaji a jejich uchovávání a zabráněno neoprávněnému přístupu k údajům. Nutný by byl také externí audit řádného fungování systému a všech jeho záruk. Do systému by měly být začleněny všechny nezbytné postupy pro přístup k osobním údajům a jejich opravu a příslušné opravné prostředky.

Na závěr lze říci, že Komise v souladu s požadavky Evropského parlamentu a Rady posoudila možné varianty zřízení systému EU TFTS, včetně režimu extrahování a uchovávání.

Toto posouzení bere v úvahu zásady obsažené ve strategii pro správu informací, která byla přijata v rámci švédského předsednictví. Jakýkoli použitý systém musí být nezbytný, přiměřený a nákladově efektivní a musí ctít základní práva. Z analýzy provedené Komisí, jak je podrobně uvedeno výše a v posouzení dopadů, vyplývá, že každá proveditelná varianta má své výhody a nevýhody. Komise však nebrala v úvahu varianty, které nejsou z výše uvedených důvodů proveditelné.

Na základě získaných informací není jasné prokázáno, že by v této fázi bylo nutné předložit návrh na zřízení EU TFTS.

Komise uvítá názory Evropského parlamentu a Rady k tomuto sdělení.