EIROPAS
KOMISIJA

Briselē, 27.11.2013.
COM(2013) 842 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Eiropas Teroristu finansēšanas izsekošanas sistēma (ES TFTS)

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

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Eiropas Teroristu finansēšanas izsekošanas sistēma (ES *TFTS*)

Balstoties uz 2011. gada 13. jūlija paziņojumu (COM (2011) 429), šī paziņojuma mērķis ir informēt Eiropas Parlamentu un Padomi par Eiropas Teroristu finansēšanas izsekošanas sistēmas (ES *TFTS*) izveides lietderīguma analīzes rezultātiem.

1. KONTEKSTS

1.1. Lūguma vēsture un definīcija

Sarunu ietvaros pirms ES un ASV *TFTP* Nolīguma[1] noslēgšanas notika diskusijas par to, kā Nolīguma kontekstā vislabāk aizsargāt personas datus un ievērot pamattiesības. Dažas puses pauda viedokli, ka, iegūstot datus Eiropā, tiktu ierobežots uz ASV pārsūtāmo datu apjoms un tādējādi panākts datu aizsardzības garantiju augstāks līmenis. Dažas dalībvalstis uzskatīja, ka ilgākā termiņā pievienotā vērtība būtu neatkarīgas Eiropas sistēmas teroristu finansēšanas izsekošanai izstrādei. Eiropas Parlaments aicināja Padomi un Komisiju veikt visus nepieciešamos pasākumus, lai rastu ilgtspējīgu, juridiski pareizu Eiropas risinājumu attiecībā uz prasīto datu iegūšanu Eiropā. Padome un Eiropas Parlaments, dodot piekrišanu ES un ASV *TFTP*, aicināja Komisiju viena gada laikā pēc Nolīguma stāšanās spēkā iesniegt juridisku un tehnisku satvaru datu ieguvei ES teritorijā un trīs gadu laikā pēc Nolīguma stāšanās spēkā iesniegt progresa ziņojumu par līdzvērtīgas ES sistēmas izstrādi[2]. Turklāt ES un ASV *TFTP* Nolīguma 11. pantā paredzēts, ka Nolīguma darbības laikā Komisija veiks pētījumu par iespēju ieviest līdzvērtīgu ES sistēmu, kas ļautu datus pārsūtīt tiešāk.

Šā paziņojuma nolūkā līdzvērtīga ES sistēma būtu jānošķir no satvara datu ieguvei ES terittorijā. Ar *satvaru datu ieguvei* ES teritorijā saprot sistēmu, kas meklēšanu datos, ko ES pašlaik sniedz ASV, ļautu veikt ES teritorijā. Savukārt *līdzvērtīga ES sistēma* būtu neatkarīga Eiropas sistēma teroristu finanšu izsekošanai, piekļūstot izraudzītā/-o pakalpojumu sniedzēja/-u datiem, veicot to meklēšanu un analizējot tos. Jebkādas ES sistēmas izveides dēļ būtu nepieciešams grozīt ES un ASV *TFTP* Nolīgumu.

[1] OV L 195, 27.7.2010., 5. lpp.
[2] Padomes 2010. gada 13. jūlija lēmums, OV L 195, 27.7.2010., 3. lpp.

1.2. Paveiktais

Komisija 2010. gada decembrī noslēdza līgumu par *pētījumu*, kas tika paplašināts 2011. gada jūlijā, aptverot papildu iespēju izveidot glabāšanas un ieguves režīmu. Šā pētījuma laikā Komisija rīkoja četras ekspertu sanāksmes, iesaistot tādas ieinteresētās personas kā Eiropols, Eiropas Datu aizsardzības uzraudzītājs, *TFTP* izraudzītais pakalpojumu sniedzējs[3] un daudzi dalībvalstu eksperti, kas pārstāvēja ieinteresētās ministrijas, tiesībaizsardzības un izlūkdatu vākšanas aģentūras un datu aizsardzības iestādes.

2011. gada 13. jūlijā Komisija savā *Paziņojumā Eiropas Parlamentam un Padomei (2011. gada paziņojums)* izklāstīja piecus iespējamos risinājumus, ko tā bija noteikusi attiecībā uz Eiropas Teroristu finansēšanas izsekošanas sistēmu (ES *TFTS*). No tiem trīs tika atzīti par iespējamiem. 2011. gada paziņojuma mērķis bija raisīt debates par turpmāko rīcību un sniegt informāciju veicamajam ietekmes novērtējumam.

Šis jautājums 2011. gada oktobrī tika izklāstīts TI padomes sanāksmē un Eiropas Parlamenta Pilsoņu brīvību komitejā.

Tā kā dalībvalstis un Eiropas Parlaments nepauda skaidru atbalstu kādam no risinājumiem, tika nolemts Komisijas ietekmes novērtējumā aplūkot tos visus un izvērst tos, izstrādājot dažādus apakšrisinājumus. Šis paziņojums balstās uz ietekmes novērtējumu[4].

2. KOMISIJAS PAMATPRINCIPI UN NOTEIKTIE RISINĀJUMI

2.1. Zviedrijas prezidentūras laikā pieņemtās Informācijas pārvaldības stratēģijas principi

Izvērtējot ierosināto turpmāko rīcību, Komisija ņem vērā pamatprincipus, kas izklāstīti 2009. gada Informācijas pārvaldības stratēģijā[5] un vēlāk iekļauti un sīkāk izstrādāti Komisijas 2010. gada paziņojumā "Pārskats par informācijas pārvaldību brīvības, drošības un tiesiskuma jomā"[6] un 2012. gada paziņojumā par Eiropas Informācijas apmaiņas modeli[7].

[3] Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība *(SWIFT)*.
[4] SWD 2013 (xx), ...
[5] Padomes 2009. gada 30. novembra secinājumi par ES iekšējās drošības informācijas pārvaldības stratēģiju, 16637/09.
[6] COM (2010) 385, 2010. gada 20. jūlijs.
[7] COM(2012) 735, 2012. gada 7. decembris.

Šajā sakarā īpaši nozīmīgi ir pamattiesību, nepieciešamības, proporcionalitātes un izmaksu lietderības garantēšanas principi.

Izstrādājot jaunus priekšlikumus, kas saistīti ar personas datu apstrādi iekšējās drošības jomā, Komisijas galvenās rūpes būs garantēt personu *pamattiesības* atbilstīgi Eiropas Savienības Pamattiesību hartā noteiktajam, jo īpaši tiesības uz privātumu un personas datu aizsardzību. Hartas 7. un 8. pantā paredzētas visu personu tiesības uz "savas privātās un ģimenes dzīves neaizskaramību" un "savu personas datu aizsardzību". Dalībvalstīm, Savienības iestādēm, aģentūrām un struktūrām saistošā Līguma par Eiropas Savienības darbību 16. pantā ir vēlreiz apstiprinātas ikvienas personas tiesības uz "savu personas datu aizsardzību". Saskaņā ar Hartas 52. pantu, ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības.

Iejaukšanās tiesībās uz privātumu tiek uzskatīta par *nepieciešamu*, ja tā ir risinājums neatliekamai sociālai vajadzībai, ja tā ir proporcionāla sasniedzamajam mērķim un ja publiskās iestādes izvirzītie iemesli šādas iejaukšanās pamatojumam ir būtiski un pietiekami.

Kaut arī ir grūti novērtēt visas terorisma radītās izmaksas finanšu izteiksmē, paliek spēkā *izmaksu lietderīguma* princips. *Izmaksu ziņā lietderīgā* pieejā tiek ņemti vērā jau pastāvošie risinājumi, lai mazinātu pārklāšanos un palielinātu iespējamo sinerģiju. Ir nepieciešams novērtēt, vai ir iespējams panākt priekšlikuma mērķus, labāk izmantojot spēkā esošos instrumentus.

2.2. Pieeja

Ņemot vērā iepriekš minētos principus, Komisija ir izskatījusi, vai ES *TFTS* būtu nepieciešama un proporcionāla, salīdzinājumā ar pašreizējo situāciju ņemot vērā tās izmaksas, ieguvumus un ietekmi uz pamattiesībām.

Attiecībā uz *ieguvumiem* ES sistēma palielinātu ES un tās dalībvalstu spējas piekļūt būtiskiem datiem un varētu stiprināt to analītiskās spējas, balstoties uz finanšu darījumiem, izsekot un identificēt teroristus. Tā kā finanšu darījumi var sniegt vērtīgus izlūkdatus, kas var nebūt pieejami no citiem avotiem, šis rīks būtu īpaši vērtīgs teroristu darbību un iesaistīto personu atklāšanā. Tādēļ ES *TFTS* varētu būt papildu izlūkdatu vākšanas un izmeklēšanas rīks cīņā pret terorismu un drošības nostiprināšanā ES, īpaši, ja šāda sistēma aptvertu vairākus finanšu

datu sniedzējus un darījumu veidus. ES *TFTS* ieguvumus nepieciešams samērot ar šādas sistēmas ieviešanas un uzturēšanas lēstajām izmaksām, tostarp finansiālo slogu ES un dalībvalstīm, kā arī attiecīgajiem izraudzītajiem pakalpojumu sniedzējiem, kuri nodrošina datus.

2.3. Risinājumu izklāsts

Ir apsvērti vairāki risinājumi gan *satvaram datu ieguvei* ES teritorijā, gan *līdzvērtīgai ES sistēmai*.

2.3.1. Satvars datu ieguvei ES teritorijā

Satvaru datu ieguvei ES teritorijā varētu īstenot ar izraudzīto pakalpojumu sniedzēju turēto datu glabāšanas un ieguves sistēmu, kas ļautu tieši piekļūt datiem, kurus pašlaik sniedz ASV *TFTP* ietvaros. Šādu tiešu piekļuvi piešķirtu ASV analītiķiem vai ekspertiem, kas ir pilnvaroti minētajam mērķim.

Šajā risinājumā viena iespēja būtu noteiktu laiku glabāt datus uz izraudzītā pakalpojumu sniedzēja servera un veikt meklēšanu tieši šajā serverī. Taču pašreizējais ES un ASV *TFTP* Nolīguma izraudzītais pakalpojumu sniedzējs ir ieviesis stingrus datu aizsardzības un drošības pasākumus, kas neļauj identificēt ziņojuma datu saturā minētās personas, tādēļ pašreizējā datubāze neļauj veikt meklēšanu, balstoties uz personas datiem. Tādēļ būtu nepieciešams veidot atsevišķu datubāzi.

Alternatīvi datus varētu iegūt un glabāt citā drošā vietā ES. ASV analītiķi vai eksperti, kuri ir pilnvaroti veikt meklēšanu, varētu vai nu fiziski atrasties izraudzītā pakalpojumu sniedzēja telpās vai viņiem varētu būt attālināta piekļuve datiem. Visos gadījumos un neatkarīgi no datu atrašanās vietas, būtu jāievieš visaptveroši un stingri aizsardzības pasākumi un tie jāpielāgo konkrētajai sistēmas struktūrai.

2.3.2. Līdzvērtīga ES sistēma

Ir novērtēti vairāki risinājumi līdzvērtīgai ES sistēmai (kā izklāstīts 2011. gada paziņojumā), tostarp pilnīgi centralizēta sistēma ES līmenī, decentralizēta sistēma dalībvalstu līmenī un trīs hibrīdas sistēmas, kurās sava loma būtu gan ES, gan dalībvalstīm.

Katrā risinājumā ir dažādas iespējas attiecībā uz ES sistēmas darbības jomu. Jāizvēlas, kādus ziņojumu veidus un izraudzītos pakalpojumu sniedzējus iekļaut. Līdzvērtīga ES sistēma

varētu saglabāt tos pašus ziņojumu veidus un izraudzītos pakalpojumu sniedzējus, kurus pašlaik aptver ES un ASV *TFTP* Nolīgums, vai arī tos paplašināt.

- Pilnībā centralizētas ES līmeņa sistēmas risinājums nozīmētu, ka viena ES struktūra veiktu sistēmas visas galvenās funkcijas – pieprasītu datu ieguvi, glabātu datus, veiktu meklēšanu, veiktu izlūkdatu analīzi, nodrošinātu un uzraudzītu sistēmu un izplatītu uzvedinošo izlūkinformāciju dalībvalstīm. Šis risinājums nav pareizs no juridiskā viedokļa, jo tajā netiek ievērots LESD 72. pants, kas apstiprina, ka likumības un kārtības uzturēšana un iekšējās drošības nodrošināšana pirmām kārtām ir dalībvalstu pienākums. Šāda sistēma dalībvalstīm nebūtu ne īstenojama, ne pieņemama, jo tai būtu nepieciešams izveidot tāda vai citāda veida centralizētu izlūkdatu vākšanas spēju ES līmenī.
- Pilnībā decentralizēta sistēma dalībvalstu līmenī nozīmētu, ka sistēmas darbību nodrošinātu dalībvalstu kompetentās iestādes un ES līmenī nekādas funkcijas netiktu veiktas. Tas nozīmē, ka datus paralēli varētu pārsūtīt un meklēt visas 28 dalībvalstis. Šis risinājums pavairotu datu plūsmas, un tam būtu būtiska ietekme uz izmaksām. Tas arī palielinātu risku, ka dati netiek apstrādāti saskaņoti, un tas arī novestu pie nevienādiem datu aizsardzības mehānismiem. Tādēļ arī šis risinājums nav īstenojams.

Tādējādi minētie divi risinājumi nav ietverti sīkākā novērtējumā.

Trīs atlikušie līdzvērtīgas ES sistēmas risinājumi paredz dažādu funkciju sadali dažādām organizācijām ES un valstu līmenī ("hibrīdās sistēmas").

Visās šajās hibrīdajās sistēmās datus uz pastāvīga un atkārtota pamata pieprasītu no izraudzītā/-ajiem pakalpojumu sniedzēja/-iem, iegūtu un glabātu datubāzē drošā vietā ES. Faktisko meklēšanu veiktu šajā centrālajā datubāzē. Visos risinājumos līdzīgā veidā tiktu izveidoti pienācīgi datu aizsardzības pasākumi.

- A) Pirmajā hibrīdajā sistēmā tiktu izveidota ES centrāla vienība – ES *TFTS* koordinācijas un analītiskais dienests. Tā uzdevums būtu pieprasīt datus no izraudzītā/-ajiem pakalpojumu sniedzēja/-iem, veikt meklēšanu, analizēt izlūkdatus un izplatīt rezultātus. Atšķirība no pilnībā centralizētas sistēmas būtu tāda, ka

dalībvalstīm būtu tieša piekļuve sistēmai un tās varētu lūgt centrālajai vienībai veikt meklēšanu to vārdā vai to lūgt saviem analītiķiem.

- B) Arī otrajā hibrīdajā sistēmā – ES *TFTS* ieguves dienestā tiktu izveidota ES centrāla vienība. Taču šajā risinājumā meklēšanu pēc dalībvalstu lūguma veiktu ES struktūra, un tā izplatītu rezultātus dalībvalstīm, neanalizējot izlūkdatus. Tomēr ES struktūra varētu veikt pati savu meklēšanu un analizēt šīs meklēšanas rezultātus.

- C) Pēdējā hibrīdajā sistēmā – Finanšu ziņu vākšanas vienību *(FIU)*[8] koordinācijas dienestā – tiktu izveidota *ad hoc* ES platforma. Tā nebūtu pastāvīga struktūra, bet gan drīzāk finanšu ziņu vākšanas ekspertu grupa, kas piedalās sanāksmēs. Šajā nolūkā, iespējams, *FIU* platformu varētu uzlabot. Katra dalībvalsts ieceltu vienu pārstāvi, kas darbotos tās vārdā. Šī *ad hoc* iestāde apkopotu katras dalībvalsts *FIU* lūgumus un, pamatojoties uz dalībvalstu lūgumiem, iesniegtu datu pieprasījumu izraudzītajam/-iem pakalpojumu sniedzējam/-iem. Katras dalībvalsts pārstāvis būtu atbildīgs par meklēšanu, analīzes veikšanu un rezultātu pārvaldību savas dalībvalsts vārdā. Izmeklēšanas uzvedinošās informācijas izmantošana un tās izplatīšana valsts līmenī būtu dalībvalstu kompetento iestāžu ziņā.

2.3.3. Status quo – ES un ASV TFTP nolīgums

Pašlaik ES un dalībvalstis var lūgt ASV veikt meklēšanu saskaņā ar ES un ASV *TFTP* Nolīgumu, kas regulē finanšu ziņojumapmaiņas datu apstrādi un pārsūtīšanu no Eiropas Savienības uz ASV Teroristu finansējuma izsekošanas programmas *(TFTP)* nolūkos.

TFTP ir pretterorisma rīks, ko ASV izstrādāja pēc 11. septembra teroristu uzbrukumiem. Tā balstās uz izraudzītā pakalpojumu sniedzēja sniegto datu, tostarp no ES pārsūtīto datu, meklēšanu.

ES un ASV *TFTP* Nolīgums sīki regulē procesu, kā ASV iestādes pieprasa datus. Eiropols pārbauda, vai no ASV saņemtie datu pieprasījumi ir saskanīgi ar Nolīgumu un jo īpaši vai tie ir cik iespējams precīzi noteikti, lai līdz minimumam samazinātu pārsūtāmo datu apjomu. Vairāki noteikumi attiecas uz drošu rīcību ar datiem, to glabāšanu un dzēšanu. Sniegtie dati tiek turēti drošā fiziskā vidē un tiek glabāti atsevišķi no jebkādiem citiem datiem. Nolīgumā

[8] Padomes Lēmums (2000. gada 17. oktobris) par sadarbības pasākumiem starp dalībvalstu finanšu ziņu vākšanas vienībām attiecībā uz informācijas apmaiņu.

noteikts piecu gadu glabāšanas termiņš un pienākums regulāri izvērtēt datu glabāšanas nepieciešamību. Starp neatkarīgajiem pārraugiem, kas atrodas ASV, ir divi ES izraudzīti pārraugi. Viņi nepārtraukti kontrolē, kādā veidā tiek īstenota sistēmas darbība, un viņiem ir iespēja pārbaudīt katru ASV Valsts kases departamenta veikto meklēšanu, lai pārliecinātos, ka meklēšanas subjektam ir saikne ar terorismu vai tā finansēšanu.

Nolīgumā ir ietverti arī noteikumi par tiesībām uz piekļuvi personas datiem un uz to labošanu, kā arī par tiesību aizsardzības procedūrām. Nolīgumā noteikts, ka jebkurai personai, kura uzskata, ka tās personas dati ir apstrādāti pretrunā Nolīgumam, ir tiesības izmantot iedarbīgus tiesību aizsardzības līdzekļus administratīvā kārtā vai tiesā saskaņā ar attiecīgi Eiropas Savienības, tās dalībvalstu un ASV tiesību aktiem. Nolīgumā noteikts, ka visām personām neatkarīgi no valstspiederības vai dzīvesvietas valsts saskaņā ar ASV tiesību aktiem ir pieejamas procedūras tiesību aizsardzībai tiesā pret prettiesisku administratīvu rīcību.

Attiecīgie tiesību akti, saskaņā ar kuriem meklēt tiesību aizsardzību Valsts kases departamenta prettiesiskas administratīvas rīcības gadījumā attiecībā uz personas datiem, kas saņemti saskaņā ar Nolīgumu, ir Administratīvo procedūru akts un Informācijas brīvības akts. Administratīvo procedūru akts ļauj personām, kam ASV valdības rīcības rezultātā ir nodarīts kaitējums, prasīt minēto rīcību izskatīt tiesā. Informācijas brīvības akts ļauj personām izmantot administratīvos un tiesas aizsardzības līdzekļus, lai iegūtu piekļuvi valdības datiem. Esošās vienveidīgās procedūras attiecībā uz to, kā piekļūt personas datiem un/vai tos labot, dzēst vai liegt tiem piekļuvi, par kurām vienojušās Komisija, ASV un 29. panta darba grupa, ir paredzētas, lai atvieglotu ES pilsoņiem šo tiesību īstenošanu. Nolīguma un tā aizsardzības pasākumu un kontroles pasākumu īstenošana tiek regulāri pārskatīta saskaņā ar Nolīguma 13. pantu. Divas šādas pārskatīšanas tika veiktas 2011.[9] un 2012. gadā[10], un tajās tika secināts, ka Nolīgums ir ticis īstenots pareizi. Trešā pārskatīšana ir paredzēta 2014. gada pavasarī. Kopīgais ziņojums par *TFTP* pārsūtīto datu vērtību, kuru sagatavo saskaņā ar Nolīguma 6. pantu, pierāda, ka *TFTP* ir devusi ieguldījumu terorisma un tā finansēšanas novēršanā un apkarošanā un vairākas dalībvalstis ir izmantojušas *TFTP*. *TFTP* informācija un tās precizitāte ļauj identificēt un izsekot teroristu un to atbalsta tīklus visā pasaulē. Tā sniedz ieskatu par

[9] SEC(2011)438, 2011. gada 30. marts.
[10] SWD(2012) 454, 2012. gada 14. decembris.

esošām teroristu organizāciju finanšu struktūrām un ļauj identificēt jaunas finansiālā atbalsta plūsmas un iesaistītos procesa dalībniekus.

3. NOVĒRTĒJUMS

Vērtējot, vai ierosināt ES *TFTS* izveidi, Komisija ir saskaņojusi dažādus viedokļus un to, kas tiek sagaidīts, saistībā ar ES sistēmas tvērumu. ES *TFTS* mērķus dažādas ieinteresētās personas un lēmumu pieņēmēji redz dažādi. Komisija izskatīja abu scenāriju iespējas un sekas, balstoties uz iepriekš izklāstītajiem jaunas politikas iniciatīvas izstrādes un īstenošanas principiem. Katrs risinājums tika īpaši apsvērts no nepieciešamības, proporcionalitātes un izmaksu lietderīguma viedokļa.

3.1. Satvars datu ieguvei ES teritorijā

Kā aprakstīts 2.3.1. nodaļā, glabāšanas un ieguves režīma risinājums būtu veids, kā ES teritorijā vākt, glabāt un meklēt datus, kurus pašlaik saskaņā ar ES un ASV *TFTP* Nolīgumu pārsūta uz ASV. Tas neradītu ES vai dalībvalstīm papildu ieguvumus izmeklēšanas jomā salīdzinājumā ar pašreizējo situāciju. Tieši otrādi, glabājot *TFTP* datus ASV un ES, tiktu sadrumslatota meklēšana, ko patlaban veic, izmantojot vienu *TFTP* datu kopumu, bet tam var būt negatīva ietekme uz izmeklēšanas uzvedinošās informācijas vienību kvalitāti un skaitu un tas var pasliktināt *TFTP* vispārējo efektivitāti. Turklāt tas var būtiski palēnināt analīzes procesu, jo turpmākai rīcībai saistībā ar izmeklēšanas uzvedinošo informāciju varētu būt nepieciešams veikt dažādas secīgas meklēšanas *TFTP* datos, kas tiek glabāti divās vietās. Izmeklēšanās pret teroristiem bieži svarīgs ir ātrums.

Datu ieguve Eiropas teritorijā, nevis ASV, negarantētu personas datu labāku aizsardzību *per se*. Pareizas rīcības ar datiem nodrošināšanā būtiski ir aizsargāt piekļuvi datiem neatkarīgi no vietas. Šajā nolūkā būtu nepieciešams ieviest stingru aizsardzības pasākumu kopumu, kas garantētu datu apstrādes un rīcības ar datiem atbilstību nepieciešamajām prasībām. Sistēma būtu jāaprīko ar kontroles funkciju, kuras pienākums būtu verificēt lūgumus veikt meklēšanu un to pamatojumu. Neatkarīgajiem uzraugiem būtu svarīga loma, nodrošinot, ka datus izmanto tikai tiem mērķiem, kas noteikti izveides nolīgumā. Būtu jāveic pasākumi, lai nepieļautu nesankcionētu piekļuvi datiem vai to izpaušanu, piemēram, dati būtu jāglabā drošā fiziskā vidē. Būtu jāiestrādā procedūras piekļuvei personas datiem un to labošanai un

atbilstīgas tiesību aizsardzības procedūras. Būtu jāpasūta neatkarīga revīzija, lai nodrošinātu sistēmas pareizu darbību.

Saskaņā ar ES un ASV *TFTP* Nolīgumu ASV nav piekļuves visiem izraudzītā pakalpojumu sniedzēja datiem, bet tikai tiem datu kopumiem, kurus ASV ir pieprasījušas un Eiropols apstiprinājis, pamatojoties uz agrāko un pašreizējo terorisma riska analīzi. Ja netiktu izveidots līdzīgs mehānisms datu pieprasījumu sākotnējai sašaurināšanai, lai varētu veikt tiešu meklēšanu visos izraudzītā pakalpojumu sniedzēja datos, vēl vairāk tiktu palielināta datu pakļaušana darbībām un ietekme uz datu aizsardzības tiesībām. Tādēļ būtu ievērojami jāpārveido izraudzītā pakalpojumu sniedzēja darba metodes un tas, kā dati tiek glabāti. Pašlaik finanšu ziņojumus, uz kuriem attiecas Nolīgums, glabā tādā formā, kas neļauj identificēt personas, kuras ir minētas ziņojuma datu saturā. Katrs finanšu ziņojums ir šifrēts, un tajā var meklēt tikai metadatus, t.i., datumu, kad ziņojums nosūtīts, ziņojuma veidu un iesaistīto sūtītāju un saņēmēju banku. Izraudzītais pakalpojumu sniedzējs ir ieviesis stingrus datu aizsardzības un drošības pasākumus, lai aizsargātu savu klientu datus visā pasaulē. Tādēļ, lai varētu veikt tiešu meklēšanu izraudzītā pakalpojumu sniedzēja serverī, visi šie ziņojumi vispirms būtu jāatšifrē. Tas būtu pārmērīgi un neproporcionāli, jo izraudzītā pakalpojumu sniedzēja serverī ir vairāk ziņojumu, nekā vienīgi tie, kas nepieciešami terorisma finansēšanas apkarošanas nolūkā. Turklāt tieša piekļuve meklēšanas nolūkā būtu nepieļaujama iejaukšanās izraudzītā pakalpojumu sniedzēja ikdienas darbībā un radītu būtiskus darbības, drošības un sistēmiskos riskus. Tādēļ būtu nepieciešams izveidot atsevišķu datubāzi ES teritorijā, lai glabātu nepieciešamos izraudzītā pakalpojumu sniedzēja datus.

Lai ieviestu šādu sistēmu un garantētu tās pilnīgu atbilstību drošības aizsardzības pasākumiem, būtu nepieciešami būtiski ieguldījumi. Izraudzītā pakalpojumu sniedzēja telpas vai cita droša vieta būtu jāpielāgo īpašajām prasībām, būtu jāizstrādā un jāuztur IT un tehniskie risinājumi, un būtu jāpieņem darbā un jāapmāca augsti kvalificēti darbinieki, kas pārvaldītu un pārraudzītu sistēmu.

Šajā risinājumā ES un dalībvalstis uzņemtos visas neērtības un izmaksas, kas saistītas ar mehānismu, kurš izveidots vienīgi, lai kalpotu *TFTP*, kas ir trešās valsts instruments. Pašlaik šis risinājums nešķiet ne nepieciešams, ne proporcionāls, nedz arī izmaksu ziņā lietderīgs, jo tas nedotu papildu ieguvumus izlūkdatu jomā, tā izveide būtu dārga un sarežģīta, un tas varētu radīt riskus personas datu aizsardzības jomā.

3.2. Līdzvērtīga ES sistēma

Sīkākā novērtējumā netika iekļauta pilnībā centralizēta ES *TFTS*, jo tai trūkst juridiskā pamata, un ir maz ticams, ka dalībvalstis piekristu ES centralizētai lomai jomā, kas ir dalībvalstu kompetencē. Pilnībā decentralizēta sistēma netika iekļauta, pamatojoties uz to, ka tai būtu liela ietekme uz izmaksām un dažāda ietekme uz datu aizsardzības tiesībām. Trīs novērtētās hibrīdās sistēmas dažādā pakāpē ļautu dalībvalstīm kontrolēt meklēšanu, ko veic tās vai centralizēta ES struktūra.

Paplašinot līdzvērtīgas ES sistēmas darbības jomu, lai aptvertu automatizētos klīringa centrus, elektronisko naudu un citus ar *FIN* nesaistītus datus, tiktu panākts ieguvums izlūkdatu vākšanā, jo pieaugtu ES spējas izsekot maksājumus ES iekšienē, un tādējādi varētu radīt "drošākas nākotnes" sistēmu nekā tā, kas apstrādā vienīgi *FIN* ziņojumapmaiņu. Tomēr, katrreiz pievienojot papildu izraudzīto pakalpojumu sniedzēju, pieaugtu datu aizsardzības tiesību pārkāpumu risks, un tādējādi būtu nepieciešams stingri noteikts nosacījumu, aizsardzības pasākumu un kontroles pasākumu kopums. Tas palielinātu administratīvo slogu izraudzītajiem pakalpojumu sniedzējiem. Turklāt daudzu datu sniedzēju un ziņojumu pievienošana, lai radītu šādu kompleksu, organizatoriski un tehniski sarežģītu sistēmu, būtiski palielinātu izmaksas.

Šīs analīzes rezultātā tika secināts, ka praktiski īstenojama ES *TFTS* izmantotu tikai *FIN* ziņojumu datus, jo Komisija uzskata, ka papildu ieguvums, ko sniedz daudzu datu veidu un sniedzēju izmantošana, nav samērojams ar šādas sistēmas radītajām būtiskajām izmaksām privātiem uzņēmumiem un kaitējumu privātumam un datu aizsardzības tiesībām. Tādējādi, tā kā ES sistēma aptvertu vienīgi tos pašus izraudzītos pakalpojumu sniedzējus un ziņojumu veidus kā *TFTP*, saņemtās izmeklēšanas uzvedinošās informācijas kvalitāte un apjoms, kā arī datu pakļautība darbībām būtu salīdzināma ar ES un ASV *TFTP*.

Kā izklāstīts iepriekš, līdzvērtīgai ES sistēmai ir trīs iespējamie risinājumi: A) ES *TFTS* koordinācijas un analītiskais dienests, B) ES *TFTS* ieguves dienests un C) *FIU* koordinācijas dienests.

A) risinājumam, domājams, būtu pozitīva ietekme uz terorisma novēršanu un drošības stiprināšanu ES. Tas, ka meklēšanu un rezultātu analizēšanu veiktu gan ES, gan dalībvalstu grupas, zināmā mēra nodrošinātu, ka tiek pilnībā ņemtas vērā ES un dalībvalstu īpašās

izlūkdatu vākšanas prasības un ka sistēma ir vērsta īpaši uz "ES apdraudējumu". Tomēr šāds uzlabojums būtu atkarīgs no tā, vai vidējā un ilgākā termiņā palielināsies dalībvalstu vēlme un spējas dalīties ar informāciju un analīzes rezultātiem. Nav skaidrs, kādā apmērā var paļauties uz šādu palielinātu informācijas plūsmu. Turklāt dalībvalstis saglabātu iespēju lūgt ASV veikt meklēšanu saskaņā ar *TFTP*, šai sistēmai būtu nepieciešama būtiska dalībvalstu ieinteresētība un sadarbība, lai tā varētu sniegt saskanīgāku ES ainu.

B) risinājumam varētu būt zināma pozitīva ietekme uz terorisma novēršanu un drošības stiprināšanu ES. Sistēma labāk reaģētu uz ES apdraudējuma analīzi, jo meklēšana tiktu veikta atbilstīgi dalībvalstu konkrētām izlūkdatu vākšanas prasībām. Tomēr centralizētas ES struktūras loma būtu ierobežota, to attiecinot uz meklēšanas veikšanu un tajā iegūto datu pārsūtīšanu pieprasītājai dalībvalstij; tai būtu vairāk vārtu sarga loma. Tā rezultātā netiktu veikta analizēšana ES līmenī un, lai iegūtu saskanīgu ES izlūkdatu ainu, sistēma pilnībā balstītos uz dalībvalstu veiktās analīzes rezultātu savstarpējo apmaiņu ārpus sistēmas. Sistēmas nespēja garantēt vienveidīgu pieeju meklēšanas definīcijām palielinātu nepareizu pozitīvu iznākumu risku, līdz ar to pārkāpjot tiesības uz datu aizsardzību un privātumu.

Ar C) risinājumu tiktu risinātas konkrētas dalībvalstu izlūkdatu vākšanas vajadzības, un tādējādi tam būtu pozitīva ietekme uz terorisma novēršanu un drošības stiprināšanu. Tomēr, tā kā par dalībvalsts veikto meklēšanu un analizēšanu būtu atbildīgas valstu *FIU*, šim risinājumam piemīt tie paši trūkumi kā B) risinājumam – skaidru ainu varētu gūt vienīgi, dalībvalstīm pastiprināti sadarbojoties ārpus sistēmas. Turklāt *FIU* uzmanības lokā ir tikai finanšu izlūkdati, un šīs informācijas nošķiršana no plašākas izlūkdatu ainas varētu apgrūtināt saikņu konstatēšanu un teroristu finansēšanas pamanīšanu. Arī šajā risinājumā ES iesaiste ir ļoti neliela, un spējas galvenokārt tiktu stiprinātas valstu līmenī.

Visi šie risinājumi radītu ievērojamas izmaksas ES, dalībvalstīm un izraudzītajam pakalpojumu sniedzējam, cita starpā tās būtu IT izstrādes, infrastruktūras, drošu telpu izmaksas, kā arī izmaksas saistībā ar desmitiem, ja ne simtiem darbinieku, kas būtu atbildīgi par sistēmas pārvaldību un aizsardzības pasākumu un kontroles pasākumu īstenošanu. Tomēr katrai no šīm sistēmām piemīt potenciāls veicināt Eiropas drošības situācijas uzlabošanos, jo tajās tiktu izmantots apdraudējuma novērtējums atbilstoši Eiropas vajadzībām.

Ja Eiropas teritorijā būtu neatkarīgs izlūkdatu vākšanas un izmeklēšanas rīks, vairs nebūtu nepieciešams pārsūtīt datus uz ASV. Taču jebkādai ES *TFTS* tik un tā būtu nepieciešami plaši datu aizsardzības pasākumi un kontroles pasākumi, kas būtu līdzīgi tiem, kas jau ir spēkā saskaņā ar ES un ASV *TFTP* Nolīgumu, un jebkurā gadījumā tai būtu jāatbilst ES un dalībvalstu datu aizsardzības noteikumu kopumiem. Visi lūgumi veikt datu meklēšanu ES sistēmās būtu jāpārbauda, vai tie atbilst stingri noteiktajam mērķa ierobežojumam – cīņai pret terorismu un tā finansēšanu –, tostarp pārbaudot, vai datu pārsūtīšana ir pamatota. Īpaši būtu nepieciešami kvalificēti neatkarīgi pārraugi, kas verificētu, vai katra ES un katra dalībvalsts meklēšana bija pienācīgi atļauta un bija nepieciešama cīņas pret terorismu un tā finansēšanu nolūkā. Būtu jānodrošina datu droša apstrāde un glabāšana un jānovērš nesankcionēta piekļuve datiem. Būtu nepieciešama sistēmas un visu tās aizsardzības pasākumu pareizas darbības neatkarīga revīzija. Sistēmā būtu jāiekļauj visas procedūras, kas nepieciešamas piekļuvei personas datiem un to labošanai, kā arī attiecīgās tiesību aizsardzības procedūras.

Apkopojot iepriekš izklāstīto, saskaņā ar Eiropas Parlamenta un Padomes lūgumiem Komisija ir novērtējusi ES *TFTS* iespējamos risinājumus, tostarp ieguves un glabāšanas režīmu.

Šajā novērtējumā ir ņemti vērā principi, kas paredzēti Informācijas pārvaldības stratēģijā, kuru pieņēma Zviedrijas prezidentūras laikā. Izveidotajai sistēmai jābūt nepieciešamai, proporcionālai un izmaksu ziņā lietderīgai, un tai ir jāievēro pamattiesības. Komisijas veiktā analīze, kas sīkāk izklāstīta iepriekš un ietekmes novērtējumā, liecina, ka katram no iespējamajiem risinājumiem ir savas priekšrocības un trūkumi. Kā paskaidrots iepriekš, Komisija nav ņēmusi vērā tos risinājumus, kas nav reāli īstenojami.

Ņemot vērā savākto informāciju, pašlaik nav pietiekama pamata iesniegt priekšlikumu par ES *TFTS*.

Komisija aicina Eiropas Parlamentu un Padomi paust viedokļus par šo paziņojumu.