



EVROPSKA
KOMISIJA

Bruselj, 27.11.2013
COM(2013) 842 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Evropski sistem za sledenje financiranja terorističnih dejavnosti (EU TFTS)

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

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Evropski sistem za sledenje financiranja terorističnih dejavnosti (EU TFTS)

To sporočilo izhaja iz sporočila z dne 13. julija 2011 (COM(2011) 429) in njegov cilj je obvestiti Evropski parlament in Svet o rezultatu analize, ki se je nanašala na izvedljivost vzpostavitve Evropskega sistema za sledenje financiranja terorističnih dejavnosti (v nadaljnjem besedilu: evropski sistem TFTS).

1. OZADJE

1.1. Izvor Zaposila in opredelitev pojmov

Med pogajanjmi pred sklenitvijo sporazuma o sistemu za sledenje financiranja terorističnih dejavnosti med EU in ZDA¹ (v nadaljnjem besedilu: sporazum o evropskem sistemu TFTP med EU in ZDA) so potekale razprave, kako najbolje zaščititi osebne podatke in zagotoviti spoštovanje temeljnih pravic v okviru tega sporazuma. Nekatere strani so trdile, da bi s pridobivanjem podatkov na evropskih tleh omejili količino podatkov, posredovanih ZDA in bi tako zagotovili višjo raven jamstva o varstvu podatkov. Nekatere države članice so menile, da bo razvoj neodvisnega evropskega sistema za sledenje financiranja terorističnih dejavnosti dolgoročno prinesel dodano vrednost. Evropski parlament je pozval Svet in Komisijo, naj sprejmeta vse potrebne ukrepe za oblikovanje trajne in pravno ustrezne evropske rešitve vprašanja pridobivanja zahtevanih podatkov na evropskih tleh. Svet in Evropski parlament sta ob podelitvi soglasja k sporazumu o evropskem sistemu TFTP med EU in ZDA pozvala Komisijo, naj v enem letu od datuma začetka veljavnosti sporazuma predloži pravni in tehnični okvir za pridobivanje podatkov na ozemlju EU, v treh letih od datuma začetka veljavnosti sporazuma pa naj predstavi poročilo o napredku o razvoju enakovrednega sistema EU². Poleg tega člen 11 sporazuma o evropskem sistemu TFTP med EU in ZDA določa, da bo v času veljavnosti sporazuma Komisija izvedla študijo glede možne uvedbe enakovrednega sistema EU, ki bo omogočal bolj usmerjen prenos podatkov.

V tem sporočilu je treba enakovredni sistem EU razlikovati od okvira za pridobivanje podatkov na ozemlju EU. *Okvir za pridobivanje podatkov* na ozemlju EU pomeni sistem, ki

¹ UL L 195, 27.7.2010, str. 5.

² Sklep Sveta z dne 13. julija 2010, UL L 195, 27.7.2010, str. 3.

bo omogočal, da se bo iskanje podatkov, ki jih ZDA trenutno zagotavlja EU, izvajalo na tleh EU. Nasprotno pa bi bil *enakovredni sistem EU* neodvisen evropski sistem za sledenje financiranja terorističnih dejavnosti prek dostopa do podatkov imenovanega ponudnika(-ov), iskanja po njih in njihove analize. Za vzpostavitev kakršnega koli sistema EU bi bilo treba spremeniti sporazum o evropskem sistemu TFTP med EU in ZDA.

1.2. Sprejeti ukrepi

Komisija je decembra 2010 naročila *študijo*, ki je bila julija 2011 razširjena na dodatno možnost ureditve shranjevanja in pridobivanja podatkov. Med izvajanjem te študije je Komisija organizirala štiri strokovna srečanja, na katerih so bile prisotne zainteresirane strani, kot so Europol, Evropski nadzornik za varstvo podatkov, imenovani ponudnik v okviru programa TFTP³ in veliko strokovnjakov držav članic, ki so predstavljali zainteresirana ministrstva, organe kazenskega pregona in obveščevalne organe ter organe za varstvo podatkov.

Komisija je 13. julija 2011 v svojem *sporočilu Evropskemu parlamentu in Svetu (v nadaljnjem besedilu: sporočilo iz leta 2011)* predstavila pet možnosti, ki jih je opredelila za evropski sistem za sledenje financiranja terorističnih dejavnosti. Od teh možnosti naj bi bile izvedljive tri. Cilj sporočila iz leta 2011 je bil sprožiti razmišljanje o poti naprej in prispevati k oceni učinka, ki jo je treba sprejeti.

Vprašanje je bilo predstavljeno oktobra 2011 v Svetu PNZ in Odboru Evropskega parlamenta za državljanske svoboščine.

Ker države članice in Evropski parlament niso izrazili jasne podpore nobeni od teh možnosti, je bil sprejet sklep, da se proučijo v oceni učinka Komisije ter se podrobno raziščejo z razvijanjem različnih podmožnosti. To sporočilo temelji na oceni učinka⁴.

³ Združenje za svetovne finančne telekomunikacije med bankami (Society for Worldwide Interbank Financial Telecommunication – SWIFT).

⁴ SWD 2013 (xx) z dne

2. TEMELJNA NAČELA KOMISIJE IN RAZISKANE MOŽNOSTI

2.1. Načela strategije upravljanja podatkov, sprejete v okviru švedskega predsedovanja

Komisija v svoji analizi predlagane poti naprej upošteva temeljna načela iz strategije upravljanja informacij iz leta 2009⁵, ki je bila pozneje vključena in nadalje razvita v sporočilih Komisije o pregledu upravljanja informacij na območju svobode, varnosti in pravice iz leta 2010⁶ in o evropskem modelu za izmenjavo informacij iz leta 2012⁷.

S tem v zvezi so najpomembnejša načela spoštovanja temeljnih pravic, nujnosti, sorazmernosti in stroškovne učinkovitosti.

Varstvo *temeljnih pravic* posameznika, kakor je opredeljeno v Listini Evropske unije o temeljnih pravicah, zlasti spoštovanje pravice do zasebnosti in varstvo osebnih podatkov, je najpomembnejša naloga za Komisijo pri pripravljanju novih predlogov, ki vključujejo obdelavo osebnih podatkov na področju notranje varnosti. V členih 7 in 8 Listine je navedena pravica vsakogar do spoštovanja njegovega „zasebnega in družinskega življenja“ ter do „varstva osebnih podatkov, ki se nanj nanašajo“. Tudi člen 16 Pogodbe o delovanju Evropske unije, ki je zavezujoč za države članice, institucije, agencije in organe Unije, potrjuje pravico vsakogar do „varstva osebnih podatkov, ki se nanašajo nanj“. V skladu s členom 52 Listine so ob upoštevanju načela sorazmernosti omejitve uresničevanja pravic in svoboščin, ki jih listina priznava, dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.

Poseganje v pravico do zasebnosti se šteje za *potrebno*, če rešuje nujno potrebo, če je sorazmerno s ciljem in če so razlogi, ki jih navaja javni organ kot utemeljitev, ustrezni in zadostni.

Čeprav je težko oceniti vse stroške terorizma v finančnem smislu, načelo *stroškovne učinkovitosti* še vedno velja. *Stroškovno učinkovit* pristop upošteva že obstoječe rešitve, da bi se kar najbolj zmanjšalo prekrivanje nalog in izboljšale mogoče sinergije. Potrebna je ocena, ali bi bilo mogoče doseči cilje predloga z boljšo uporabo obstoječih instrumentov.

⁵ Sklepi sveta z dne 30. novembra 2009 o strategiji upravljanja informacij na področju notranje varnosti EU 16637/09.

⁶ COM(2010) 385 z dne 20. julija 2010.

⁷ COM(2012) 735 z dne 7. decembra 2012.

2.2. Pristop

Ob upoštevanju zgoraj omenjenih načel je Komisija proučila, ali bi bil v primerjavi s sedanjim stanjem evropskega sistema TFTS potreben in sorazmeren glede na stroške, koristi in njegov učinek na temeljne pravice.

Korist evropskega sistema bi bila, da bi ta lahko povečal zmogljivosti EU in njenih držav članic za dostop do ustreznih podatkov in bi lahko okrepil njihove analitične zmogljivosti za sledenje in odkrivanje teroristov prek finančnih transakcij. Ker so lahko finančne transakcije vir dragocenih obveščevalnih podatkov, ki jih iz drugih virov morda ni mogoče pridobiti, bi bilo to orodje še posebej koristno za odkrivanje terorističnih dejavnosti in vpletenih akterjev. Zato bi lahko bil evropski sistem TFTS dodatno obveščevalno in preiskovalno orodje v boju proti terorizmu in pri krepitevi varnosti v EU, zlasti če bi takšen sistem zajemal različne ponudnike finančnih podatkov in vrste transakcij. Koristi evropskega sistema TFTS je treba uravnotežiti s predvidenimi stroški uvedbe in vzdrževanja takšnega sistema, vključno s finančno obremenitvijo za EU, države članice in zadevne imenovane ponudnike podatkov.

2.3. Predstavitev možnosti

Obravnavanih je bilo več možnosti tako za *okvir za pridobivanje* podatkov na ozemlju EU kot tudi za *enakovredni sistem EU*.

2.3.1. Okvir za pridobivanje podatkov na ozemlju EU

Okvir za pridobivanje podatkov na ozemlju EU bi se lahko izvajal prek sistema shranjevanja in pridobivanja podatkov, ki jih ima imenovani ponudnik, in z omogočanjem neposrednega dostopa do podatkov, ki se trenutno zagotavljajo ZDA v okviru programa TFTP. Neposreden dostop bi bil omogočen ameriškim analitikom ali strokovnjakom, pooblaščenim v ta namen.

Podatki bi se lahko za določeno obdobje shranjevali na strežniku imenovanega ponudnika, na katerem bi se omogočilo neposredno iskanje. Vendar je trenutni imenovani ponudnik v okviru sporazuma o evropskem sistemu TFTP med EU in ZDA vzpostavil visoko stopnjo varstva podatkov in stroge varnostne ukrepe, ki ne omogočajo identifikacije oseb, omenjenih v podatkih iz sporočil, ter zato njegova obstoječa podatkovna zbirka ne omogoča iskanja po osebnih podatkih. Zato bi bilo treba oblikovati ločeno podatkovno zbirko.

Lahko pa bi se podatki pridobivali in hranili na drugi varni lokaciji v EU. Analitiki ali strokovnjaki ZDA, pooblaščen za opravljanje poizvedb po podatkih, se lahko bodisi fizično nahajajo v prostorih imenovanega ponudnika ali lahko uporabljajo oddaljeni dostop do podatkov. V vsakem primeru bi bilo treba ne glede na lokacijo podatkov vzpostaviti celovite in trdne zaščitne ukrepe, ki so prilagojeni zasnovi sistema.

2.3.2. Enakovreden sistem EU

Proučena je bila vrsta možnosti za enakovreden sistem EU (kot je opisan v sporočilu iz leta 2011), vključno s popolnoma centraliziranim sistemom na ravni EU, decentraliziranim sistemom na ravni držav članic in tremi hibridnimi sistemi, v katerih bi imele svojo vlogo tako EU kot tudi države članice.

Pri vsaki možnosti je mogoče določiti različna področja uporabe sistema EU. Treba je izbrati vrste sporočil in imenovane ponudnike, ki bi bili vključeni. Enakovreden sistem EU bi lahko ostal pri vrstah finančnih sporočil in imenovanem ponudniku, ki jih trenutno zajema sporazum o evropskem sistemu TFTP med EU in ZDA, lahko pa bi to še nadgradil.

- Možnost popolnoma centraliziranega sistema na ravni EU bi pomenila, da bi en sam organ EU izvajal vse ključne naloge sistema: zahteval pridobivanje podatkov, shranjeval podatke, opravljal poizvedbe, izvajal analizo obveščevalnih podatkov, ščitil in spremljal sistem ter razširjal obveščevalne podatke po državah članicah. Ta možnost je pravno neustrezna, saj ne bi upoštevala člena 72 PDEU, ki potrjuje, da glavno odgovornost za vzdrževanje javnega reda in miru ter zagotavljanje notranje varnosti nosijo države članice. Tak sistem za države članice ne bi bil niti izvedljiv niti sprejemljiv, saj bi bilo treba vzpostaviti nekakšno obliko centralizirane obveščevalne zmogljivosti na ravni EU.
- Pri popolnoma decentraliziranem sistemu na ravni držav članic bi ta sistem vodili pristojni organi držav članic, pri čemer se nobena naloga ne bi izvajala na ravni EU. To bi pomenilo, da bi se podatki lahko prenesli v vseh 28 držav članic hkrati, ki bi lahko tudi opravljale poizvedbe. S to možnostjo bi se pomnožili prenosi podatkov, zaradi česar bi se zelo povečali stroški. Prav tako bi se povečalo tveganje nedosledne obdelave podatkov ter vzpostavitve neenakih mehanizmov za varstvo podatkov. Zato tudi ta možnost ne pride v poštev.

Ti dve možnosti se zato niso podrobneje proučile.

Preostale tri možnosti za enakovredni sistem EU vključujejo porazdelitev različnih nalog med različne organizacije na ravni EU in na nacionalnih ravneh (v nadaljevanju besedila: hibridni sistemi).

Pri vseh teh hibridnih sistemih bi bilo treba podatke zahtevati sproti in vsakič znova na zahtevo, naslovljeno na imenovanega ponudnika, jih pridobiti in shraniti v podatkovni zbirki na varni lokaciji v EU. Dejanske poizvedbe bi se nato opravljale po tej osrednji podatkovni zbirki. Pri vseh treh možnostih bi bilo treba sprejeti ustrezne zaščitne ukrepe za varstvo podatkov.

- A) V prvem hibridnem sistemu, tj. službi za koordinacijo in analizo v okviru evropskega sistema TFTS, bi bilo treba ustanoviti centralno enoto EU. Ta bi bila zadolžena za pošiljanje zahtev za podatke imenovanemu ponudniku, opravljanje poizvedb, analizo obveščevalnih podatkov in razširjanje rezultatov. Razlika med popolnoma centraliziranim sistemom in tem sistemom je, da bi imele države članice neposreden dostop do sistema in bi lahko zaprosile, da poizvedbe v njihovem imenu izvaja centralna enota ali njihovi analitiki.
- B) Tudi pri drugem hibridnem sistemu, tj. službi za pridobivanje podatkov v okviru evropskega sistema TFTS, bi bilo treba ustanoviti centralno enoto EU. Vendar bi pri tej možnosti organ EU opravljal poizvedbe na zaprosilo držav članic in razširjal rezultate državam članicam, pri čemer ne bi analiziral obveščevalnih podatkov. Vendar pa bi organ EU lahko izvajal lastne poizvedbe in analiziral njihove rezultate.
- C) V zadnjem hibridnem sistemu, tj. koordinacijski službi enot za finančni nadzor⁸, bi se ustanovila ad hoc platforma EU. To ne bi bil stalni organ, ampak skupina strokovnjakov za finančne podatke, ki sodelujejo na sestankih. V ta namen bi se lahko nadgradila platforma enot za finančni nadzor. Vsaka država članica bi imenovala enega predstavnika, ki bi jo zastopal. Ta ad hoc organ bi zbral zahteve enote za finančni nadzor vsake države članice in izdajal zahteve za podatke pri imenovanem ponudniku na podlagi teh zahtev držav članic. Vsak predstavnik države članice naj bi

⁸ Sklep Sveta z dne 17. oktobra 2000 o dogovoru glede sodelovanja med enotami za finančni nadzor držav članic pri izmenjavi informacij.

bil odgovoren za opravljanje poizvedb, izvajanje analize in upravljanje rezultatov v imenu svoje države članice. Nato bi pristojni organi držav članic odločali o uporabi obveščevalnih podatkov in njihovem nadaljnjem razširjanju na nacionalni ravni.

2.3.3. Status quo: sporazum o evropskem sistemu TFTP med EU in ZDA

Trenutno lahko EU in države članice zahtevajo, da poizvedbe izvajajo ZDA v okviru sporazuma o evropskem sistemu TFTP med EU in ZDA, ki ureja obdelavo in prenos podatkov o sporočilih glede finančnih plačil iz Evropske unije v Združene države Amerike za namene programa za sledenje financiranja terorističnih dejavnosti (v nadaljnjem besedilu: program TFTP).

Program TFTP je orodje za boj proti terorizmu, ki so ga razvile ZDA po terorističnih napadih 11. septembra. Temelji na iskanju podatkov, ki jih je zagotovil imenovani ponudnik, vključno s podatki, prenesenimi iz EU.

Sporazum o evropskem sistemu TFTP med EU in ZDA natančno ureja postopek predložitve zahteve po podatkih, ki jo predložijo organi ZDA. Europol preveri, da so zahteve po podatkih, prejete iz ZDA, v skladu s sporazumom, in zlasti, da se v njihovem okviru prenesejo le najnujnejši podatki, da se čim bolj zmanjša obseg prenesenih podatkov. Številne določbe urejajo varno ravnanje s podatki ter njihovo shranjevanje in brisanje. Poslani podatki se hranijo v varnem fizičnem okolju in so shranjeni ločeno od vseh drugih podatkov. V sporazumu je obdobje hrambe podatkov omejena na pet let, ter določena obveznost, da se potreba po ohranitvi podatkov redno preverja. Med neodvisnimi nadzorniki, ki delujejo v ZDA, sta dva nadzornika, ki jih je izbrala EU. Ti nenehno nadzorujejo, kako se sistem upravlja, poleg tega pa imajo možnost preveriti vsako poizvedbo, ki jo opravi ministrstvo za finance Združenih držav, da se zagotovi, da je oseba, ki je predmet poizvedbe, povezana s terorizmom ali njegovim financiranjem.

Sporazum vsebuje tudi določbe o pravicah do dostopa do osebnih podatkov in o njihovih popravkih ter o postopku sodnega varstva. V sporazumu je določeno, da ima katera koli oseba, ki meni, da je bil pri obdelavi njenih osebnih podatkov ta sporazum kršen, pravico zahtevati uporabo učinkovitih pravnih sredstev v upravnih in sodnih postopkih v skladu z zakonodajo EU, njenih držav članic oziroma ZDA. V sporazumu je določeno, da je osebam ne glede na njihovo državljanstvo ali državo stalnega prebivališča po zakonodaji ZDA na voljo

postopek za uporabo pravnih sredstev v sodnem postopku zoper škodljivo dejanje upravnega organa.

Postopek sodnega varstva zoper škodljivo upravno dejanje ministrstva za finance v zvezi z osebnimi podatki, prejetimi v skladu s sporazumom, med drugim urejata zakon o splošnem upravnem postopku (*Administrative Procedure Act*) in zakon o dostopu do informacij javnega značaja (*Freedom of Information act*). Zakon o upravnem postopku omogoča osebam, ki jim je bila povzročena škoda zaradi dejanja vlade ZDA, da zahtevajo sodno presojo navedenega dejanja. Zakon o dostopu do informacij javnega značaja omogoča uporabo upravnih in sodnih pravnih sredstev za vpogled v vladne evidence. Cilj obstoječih enotnih postopkov za dostop do osebnih podatkov in/ali njihovega popravka, izbrisa ali blokiranja, ki so bili dogovorjeni med Komisijo, ZDA in Delovno skupino iz člena 29, je državljanom EU olajšati uveljavljanje teh pravic. Izvajanje Sporazuma in v njem predvidenih zaščitnih ukrepov ter nadzora se redno pregleduje v skladu s členom 13 Sporazuma. Dva takšna pregleda sta bila opravljena v letih 2011⁹ in 2012¹⁰, v katerih je bilo ugotovljeno, da se je sporazum izvajal pravilno. Tretji pregled naj bi se izvedel spomladi 2014. Skupno poročilo v zvezi z vrednostjo poslanih podatkov, pripravljeno v skladu s členom 6 sporazuma, kaže prednosti programa TFTP pri preprečevanju terorizma in njegovega financiranja ter boju proti njima ter, da je program TFTP uporabljalo več držav članic. S točnimi informacijami iz programa TFTP je mogoče odkrivati teroriste in njihove podporne mreže po svetu in jim slediti. Program razkriva obstoječe finančne strukture terorističnih organizacij in omogoča identifikacijo novih tokov finančne podpore in vpletenih akterjev.

3. OCENA

Komisija mora pri oceni, ali bo predlagala vzpostavitev evropskega sistema TFTS, uskladiti različna stališča in pričakovanja glede ambicioznosti sistema EU. Zainteresirane strani in odločevalci imajo različna mnenja glede ciljev evropskega sistema TFTS. Komisija je proučila, kakšne bi bile možnosti in posledice obeh scenarijev glede na načela za razvoj in izvajanje zgoraj opisanih novih pobud politike. Zlasti je bila vsaka možnost proučena z vidika potrebnosti, sorazmernosti in stroškovne učinkovitosti.

⁹ SEC(2011) 438 z dne 30. marca 2011.

¹⁰ SWD(2012) 454 z dne 14. decembra 2012.

3.1. Okvir za pridobivanje podatkov na ozemlju EU

Kakor je opisano v oddelku 2.3.1., bi lahko na podlagi možnosti ureditve shranjevanja in pridobivanja podatkov na ozemlju EU zbirali, shranjevali in iskali podatke, ki so trenutno preneseni v ZDA v okviru sporazuma o evropskem sistemu TFTP med EU in ZDA. V primerjavi s sedanjim stanjem zato ne bi bilo dodatnih prednosti v zvezi z obveščevalnimi podatki za EU ali države članice. Nasprotno, če bi bili podatki iz programa TFTP shranjeni v ZDA in EU bi lahko razdrobljenost iskanja, ki trenutno poteka po enem samem sklopu podatkov iz programa TFTP, lahko negativno vplivala na kakovost in število obveščevalnih podatkov ter poslabšala splošno učinkovitost programa TFPT. Lahko tudi znatno upočasni postopek analize, ker se lahko zgodi, da bodo potrebna različna zaporedna iskanja po podatkih programa TFTP, shranjenih na dveh lokacijah, da bi se obveščevalni podatek lahko nadalje raziskalo. Hitrost je pogosto bistvena pri terorističnih preiskavah.

Pridobivanje podatkov na evropskih tleh namesto v ZDA samo po sebi ne bi zagotavljalo boljše zaščite osebnih podatkov. Zaščita dostopa do podatkov je ključnega pomena, da se zagotovi ustrezno ravnanje s podatki, ne glede na njihovo lokacijo. Zato bo treba sprejeti vrsto strogih zaščitnih ukrepov, ki bodo zagotovili skladnost obdelave in ravnanja s podatki s potrebnimi zahtevami. Sistem bi moral biti opremljen s kontrolno funkcijo za preverjanje zaprosil za iskanja in njihovih obrazložitev. Vloga neodvisnih nadzornikov bi bila bistvenega pomena za zagotovitev, da se podatki uporabljajo le za tiste namene, ki so določeni v kakršnem koli sporazumu o vzpostavitvi sistema. Treba bi bilo sprejeti ukrepe, da bi se preprečil nedovoljen dostop do podatkov ali njihovo razkritje, kot je shranjevanje podatkov v varnem fizičnem okolju. Vanje bi morali biti vključeni postopki za dostop do osebnih podatkov ter njihove popravke ter postopki sodnega varstva. Treba bi bilo naročiti zunanjo revizijo, da bi se zagotovilo pravilno delovanje sistema.

ZDA v okviru sporazuma o evropskem sistemu TFTP med EU in ZDA nimajo dostopa do vseh podatkov imenovanega ponudnika, ampak samo do sklopov podatkov, za katere so ZDA zaprosile in jih je Europol odobril na podlagi preteklih in sedanjih analiz tveganja v zvezi s terorizmom. Brez podobnega mehanizma začetnega omejevanja zaprosil za podatke bi omogočanje neposrednega iskanja po vseh podatkih imenovanega ponudnika še dodatno povečalo izpostavljenost podatkov in vplivalo na spoštovanje pravice do varstva podatkov. Imenovani ponudnik bi moral občutno spremeniti svoj način dela in postopke pri shranjevanju

podatkov. Zdaj se finančna sporočila, ki so predmet sporazuma, hranijo v obliki, ki ne omogoča identifikacije oseb, omenjenih v sporočilih. Vsa finančna sporočila so šifrirana, po njih pa je mogoče iskati le z metapodatki, tj. po datumu, ko je bilo sporočilo poslano, vrsti sporočila in bankah, ki so jih poslala ali prejela. Imenovani ponudnik je vzpostavil visoko stopnjo varstva podatkov in sprejel varnostne ukrepe za zaščito podatkov svojih strank po vsem svetu. Da bi se omogočilo iskanje neposredno na sedanjem strežniku imenovanega ponudnika, bi bilo zato treba vsa ta sporočila najprej dešifrirati. To pa bi bilo pretirano in nesorazmerno, saj na strežniku imenovanega ponudnika niso shranjena le sporočila, ki so potrebna za boj proti financiranju terorizma. Poleg tega bi bil neposredni dostop za namene iskanja nedopustno vsiljiv za dnevno poslovanje imenovanega ponudnika in bi povzročal precejšnja operativna, varnostna in sistemska tveganja. Zato bi bilo treba vzpostaviti ločeno bazo podatkov na tleh EU, v kateri bi bili shranjeni potrebni podatki imenovanega ponudnika.

Za vzpostavitev sistema in zagotovitev, da bo sistem popolnoma skladen z varnostnimi zaščitnimi ukrepi, bi bilo treba vložiti veliko. Prostori imenovanega ponudnika ali druga varna lokacija bi se morala prilagoditi posebnim zahtevam, treba bi bilo razviti in vzdrževati informacijsko tehnologijo in tehnične rešitve, poleg tega pa bi bilo treba zaposliti in usposobiti kvalificirano osebje, ki bi upravljalo in nadzorovalo sistem.

Pri tej možnosti bi morale EU in države članice reševati vse slabosti mehanizma, vzpostavljenega samo zaradi programa TFTP, tj. instrumenta, ki je v lasti tretje države, in kriti njegove stroške. Trenutno se ta možnost ne zdi potrebna, sorazmerna ali stroškovno učinkovita, saj ne bi prinesla dodatnih prednosti v zvezi z obveščevalnimi podatki, bila bi draga in njena vzpostavitev zahtevna, poleg tega pa bi lahko nastala tveganja v zvezi z varstvom osebnih podatkov.

3.2. Enakovreden sistem EU

Za popolnoma centraliziran evropski sistem TFTS podrobnejša ocena ni bila pripravljena, ker za to ni bilo pravne podlage in ker ni veliko možnosti, da bi države članice sprejele centralizirano vlogo EU na področju, ki je v pristojnosti držav članic. Tudi možnosti popolnoma decentraliziranega sistema je bila izključena, ker bi bila povezana z velikimi stroški in bi zelo vplivala na spoštovanje pravic do varstva podatkov. Trije ocenjeni hibridni sistemi omogočajo različne stopnje nadzora države članice nad iskanji, ki jih izvajajo same in centralizirani organ EU.

Razširitev področja uporabe enakovrednega sistema EU na avtomatizirane klirinške hiše, edenar in druge podatke, ki niso podatki FIN, bi bila koristna zaradi večje zmogljivosti EU pri sledenju plačil znotraj EU, poleg tega pa bi se lahko na ta način ustvaril varnejši sistem za prihodnost od tistega, ki bi obdeloval le finančna sporočila. Vendar bi se z vsakim novim dodanim ponudnikom povečalo tveganje kršitev pravic do varstva podatkov, zaradi česar bi bilo treba sprejeti vrsto strogih pogojev ter zaščitnih in kontrolnih ukrepov. To bi tudi povečalo upravno obremenitev imenovanih ponudnikov. S povečanjem števila ponudnikov podatkov in sporočil, katerega cilj bi bil vzpostaviti takšen kompleksen ter organizacijsko in tehnično zahteven sistem, bi se tudi bistveno povečali stroški.

Na podlagi te analize bi torej vsak izvedljivi evropski sistem TFTS lahko uporabil le podatke iz finančnih sporočil, saj Komisija meni, da prednosti, ki izhajajo iz uporabe več vrst podatkov in večjega števila ponudnikov, ne odtehtajo večjih stroškov za zasebna podjetja in morebitnih kršitev pravic do zasebnosti in varstva podatkov, do katerih bi v okviru takšnega sistema lahko prihajalo. Ker bi sistem EU vključeval samo istega imenovanega ponudnika in enako vrsto sporočila kot program TFTP, bi bila kakovost in količina prejetih obveščevalnih podatkov kot tudi izpostavljenost podatkov primerljiva z evropskim sistemom TFTS.

Kakor je opisano zgoraj, v okviru tega enakovrednega sistema EU obstajajo tri možnosti: A) služba za koordinacijo in analizo v okviru evropskega sistema TFTS, B) služba za pridobivanje podatkov v okviru evropskega sistema TFTS in C) koordinacijska služba enot za finančni nadzor.

Možnost A bi verjetno pozitivno vplivala na preprečevanje terorizma in povečanje varnosti v EU. Če bi iskanja opravljale in rezultate analizirale tako skupine na ravni EU kot tudi iz držav članic, bi se na nek način popolnoma upoštevale posebne obveščevalne zahteve EU in držav članic, sistem pa bi bil usmerjen k posebni „grožnji za EU“. Vendar je to izboljšanje pogojeno s povečanjem pripravljenosti in zmožnosti držav članic, da izmenjujejo informacije in analize v srednje- do dolgoročnem obdobju. Ni jasno, kako zanesljiv je lahko ta povečan pretok informacij. Ker bi države članice lahko še vedno zahtevale iskanja iz ZDA v okviru programa TFTP, bi morale države članice izvesti velika vlaganja in dobro sodelovati, da bi imele celovit pregled nad stanjem v EU.

Možnost B bi v določeni meri pozitivno vplivala na preprečevanje terorizma ter izboljšanje varnosti v EU. Sistem bi se bolje odzival na analize ogroženosti EU, saj bi se iskanja izvajala v skladu s posebnimi obveščevalnimi zahtevami držav članic. Vendar bi bila vloga centraliziranega organa EU omejena na izvajanje iskanj in prenos posredovanih podatkov državi članici, ki jih je zahtevala; njena vloga bi bila tako bolj kot ne omejena na nadzor dostopa do podatkov. Zaradi tega ne bi bilo nobene analize na ravni EU, sistem pa bi bil popolnoma odvisen od izmenjave analiz med državami članicami zunaj sistema, če bi bilo treba ustvariti celovito sliko v zvezi z grožnjami EU. Nezmožnost sistema, da bi zagotovil enoten pristop k opredelitvam iskanj, bi povečala tveganje lažno pozitivnih rezultatov, s tem pa ogrozila pravice do varstva podatkov in zasebnosti.

Z možnostjo C bi se lahko odzvali na posebne obveščevalne potrebe držav članic, zato bi v določeni meri pozitivno vplivala na preprečevanje terorizma in krepitev varnosti. Ker pa bi bile nacionalne enote za finančni nadzor odgovorne za raziskave in analize svojih držav članic, ima ta možnost enake slabosti kot možnost B – celovito sliko si je mogoče ustvariti zgolj z okrepljenim sodelovanjem držav članic zunaj sistema. Poleg tega se enote za finančni nadzor osredotočajo le na finančne podatke, vrzeli med temi informacijami in celovitim pregledom nad obveščevalnimi podatki pa lahko oteži odkrivanje povezav in financiranja terorizma. Pri tej možnosti je zelo malo sodelovanja na ravni EU, poleg tega pa bi se zmogljivosti povečale predvsem na nacionalni ravni.

Vse te možnosti bi pomenile znatne stroške za EU, države članice in imenovanega ponudnika, vključno s stroški razvoja infrastrukture informacijske tehnologije, zaščitnih objektov ter stroškov več deset ali celo več sto članov osebja, odgovornega za upravljanje sistema in izvajanje zaščitnih ukrepov in nadzora. Vendar lahko vsak od teh možnih sistemov prispeva k večji varnosti v Evropi, saj bi uporabljali ocene groženj, ki so specifične za evropske potrebe.

Z neodvisnim obveščevalnim in preiskovalnim orodjem na evropskih tleh podatkov ne bi bilo več treba prenašati v ZDA. Vendar bi bilo treba v okviru kakršnega koli evropskega sistema TFTS še vedno sprejeti obsežne zaščitne ukrepe za varstvo podatkov in vzpostaviti nadzor v podobnem obsegu, kot že velja v okviru sporazuma o evropskem sistemu TFTP med EU in ZDA in v vsakem primeru v skladu s pravnim redom EU in držav članic na področju varstva podatkov. Pri kakršnih koli zaprosilih za iskanje podatkov v sistemih v EU bi bilo treba preveriti, ali so skladna s strogo omejitvijo boja proti terorizmu in njegovega financiranja,

vkjučno s tem, ali je prenos podatkov upravičen. Zlasti usposobljeni neodvisni nadzorniki bi morali preveriti, da je bilo vsako iskanje EU in držav članic ustrezno odobreno in je bilo potrebno za namene boja proti terorizmu in njegovemu financiranju. Moralo bi biti zagotovljeno varno ravnanje s podatki in njihovo varno shranjevanje, poleg tega pa bi bilo treba preprečiti nedovoljen dostop do podatkov. Potrebna bi bila zunanja revizija pravnega delovanja sistema in vseh njegovih zaščitnih ukrepov. V sistem bi morali biti vključeni vsi potrebni postopki za dostop do osebnih podatkov ter njihove popravke ter postopki sodnega varstva.

Ugotavljamo, da je v skladu z zahtevama Evropskega parlamenta in Sveta Komisija ocenila možnosti delovanja evropskega sistema TFTS, vključno z ureditvijo shranjevanja in pridobivanja podatkov.

Ta ocena upošteva načela iz strategije upravljanja informacij, ki je bila sprejeta med švedskim predsedovanjem. Kateri koli vzpostavljeni sistem mora biti potreben, sorazmeren in stroškovno učinkovit ter spoštovati temeljne pravice. Analiza, ki jo je izvedla Komisija, kakor je opisano zgoraj in v oceni učinka, kaže, da imajo vse izvedljive možnosti prednosti in slabosti. Vendar Komisija ni upoštevala tistih možnosti, ki niso izvedljive.

Na podlagi zbranih informacij na tej stopnji ni jasno, ali bi bil predlog za evropski sistem TFTS potreben.

Komisija pozdravlja mnenja Evropskega parlamenta in Sveta o tem sporočilu.