EVROPSKA KOMISIJA

Bruselj, 13.7.2011
COM(2011) 429 konč.

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Evropski sistem za sledenje financiranja terorističnih dejavnosti: razpoložljive možnosti

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Evropski sistem za sledenje financiranja terorističnih dejavnosti: razpoložljive možnosti

1. UVOD

Svet je ob dogovoru o sklenitvi Sporazuma med Evropsko unijo in Združenimi državami Amerike o obdelavi in posredovanju podatkov o sporočilih glede finančnih plačil iz Evropske unije Združenim državam Amerike za namene programa za sledenje financiranja terorističnih dejavnosti (v nadaljnjem besedilu: sporazum TFTP med EU in ZDA)[1] pozval tudi Komisijo, naj Evropskemu parlamentu in Svetu v enem letu po začetku veljavnosti sporazuma (1. avgust 2010) predloži „pravni in tehnični okvir za vpogled v podatke na ozemlju EU“[2]. Evropski parlament je prav tako večkrat zahteval, da se dolgoročno najde trajna in pravno trdna evropska rešitev za vprašanje pridobivanja zahtevanih podatkov na evropskem ozemlju[3]. Tudi v sporočilu „Izvajanje strategije notranje varnosti EU: pet korakov k varnejši Evropi“ je bilo že navedeno, da bo Komisija leta 2011 razvila politiko EU za pridobivanje in analizo podatkov o finančnih transakcijah, ki se nahajajo na ozemlju EU[4]. Glede na dokazano učinkovitost ameriškega programa TFTP naj bi evropski sistem pomembno prispeval k prizadevanjem za prekinitev dostopa teroristov do financiranja in materialov ter spremljanje njihovih transakcij. Sklicevati se je mogoče tudi na člen 11 sporazuma TFTP med EU in ZDA, ki določa, da bo v času veljavnosti sporazuma Evropska komisija izvedla študijo glede možne uvedbe enakovrednega sistema EU, ki bo omogočal bolj usmerjeno posredovanje podatkov. To sporočilo je prva faza odziva Komisije na navedeni člen in na poziv Sveta. Opisuje različne ukrepe Komisije na poti k vzpostavitvi tovrstnega „pravnega in tehničnega okvira“ in predstavlja različne obravnavane možnosti za dosego tega cilja. Na tej stopnji ne izpostavlja ene najprimernejše možnosti, pač pa predstavlja pomembne točke, ki jih je treba upoštevati pri obravnavanih možnostih. Glede na politično pomembnost vprašanja ter njegovo pravno in tehnično zahtevnost želi Komisija Svet in Evropski parlament obvestiti o trenutnem stanju in sprožiti razpravo. Komisija meni, da bi bila takšna nadaljnja razprava koristna, preden se na podlagi ocene učinka predstavijo konkretni predlogi.

V tem okviru je treba poudariti, da to sporočilo ne vpliva na predlog, ki ga bo Komisija predložila. Kakršen koli prihodnji predlog bo upošteval omenjene razprave in oceno učinka, oblikovano na podlagi študije, ki jo je Komisija naročila v drugi polovici leta 2010. Glede na učinek, ki bi ga imel zakonodajni predlog na temeljne pravice, zlasti na varstvo podatkov, bo posebna pozornost pri oceni učinka namenjena nujnosti in sorazmernosti ukrepov, ki jih bo Komisija morda predlagala. V ta namen bo Komisija sledila usmeritvi iz svojega sporočila o strategiji za učinkovito izvajanje Listine o temeljnih pravicah v Evropski uniji[5].

---

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.
3 Glej na primer Resolucijo P7_TA(2010)0143 in Obrazložitveni memorandum k Priporočilu A7-0224/2010.
4 COM(2010) 673 konč. z dne 22. novembra 2010. Glej ukrep 2 pod ciljem 2, str. 8.
5 COM(2010) 573 konč. z dne 19. oktobra 2010.

Poleg tega bo ocena učinka omogočila potrebno tehnično podlago ter podrobno oceno vseh razpoložljivih možnosti. O teh vprašanjih so že potekale razprave s številnimi zainteresiranimi stranmi na tem področju, vključno z organi držav članic, organi za varstvo podatkov, Europolom in imenovanim ponudnikom. Končni rezultati omenjene študije bodo na voljo šele konec tega leta. Evropska komisija je v podporo pripravam na oceno učinka organizirala tri strokovna srečanja z istimi zainteresiranimi stranmi ter z organi ZDA, vključenimi v izvajanje programa TFTP. Možnosti, opisane v tem sporočilu, temeljijo na predhodnih rezultatih študije in razpravah na teh strokovnih srečanjih.

2. CILJI VZPOSTAVITVE SISTEMA EU ZA SLEDENJE FINANCIRANJA TERORISTIČNIH DEJAVNOSTI

Obstajata dva glavna razloga za vzpostavitev sistema EU za sledenje financiranja terorističnih dejavnosti (v nadaljnjem besedilu: sistem TFTS):

- sistem mora učinkovito prispevati k boju proti terorizmu in financiranju terorističnih dejavnosti znotraj Evropske unije;

- sistem mora prispevati k omejitvi količine osebnih podatkov, ki se prenesejo v tretje države. Omogočati bi moral obdelavo podatkov, potrebnih za njegovo delovanje na ozemlju EU, ob upoštevanju načel in zakonodaje EU s področja varstva podatkov.

V Združenih državah se je izkazalo, da program za sledenje financiranja terorističnih dejavnosti (v nadaljnjem besedilu: program TFTP) pomeni precejšnjo dodano vrednost k boju proti terorizmu in financiranju terorističnih dejavnosti, od njega pa nimajo koristi le organi ZDA, temveč tudi organi v državah članicah Evropske unije in tretjih državah. Nedavni pregled sporazuma TFTP med EU in ZDA[6] je potrdil, da je bilo od vzpostavitve ameriškega programa TFTP več kot 2 500 poročil posredovanih organom tretjih držav, od tega velika večina (1 700) organom držav Evropske unije. Učinkovitost ameriškega programa in njegov pomen za boj proti terorizmu in financiranju terorističnih dejavnosti sta bila potrjena tudi v dveh poročilih, ki ju je predstavil sodnik Bruguière, ki ga je Evropska komisija leta 2008 imenovala za pregled programa. Informacije, pridobljene iz programa TFTP, ki so jih prejeli organi EU, so vsebovale pomembna opozorila v zvezi z vrsto nevarnih poskusov terorističnih napadov, na primer napadoma v Madridu in Londonu, načrtom sestrelitve čezatlantskih letov z uporabo tekočih eksplozivov leta 2006 in poskusom napada na lastnino in državljane ZDA v Nemčiji leta 2007. Skupina EU za pregled je sklenila tudi, da so ji bili predstavljeni „prepričljivi podatki o dodani vrednosti programa TFTP za prizadevanja za boj proti terorizmu in njegovemu financiranju“. Glede na te izkušnje obstajajo trdni razlogi za mnenje, da bo sistem TFTS v EU prinesel pomembno dodano vrednost k prizadevanjem EU in držav članic v boju proti terorizmu in financiranju terorističnih dejavnosti.

Čeprav ni dvoma o učinkovitosti ameriškega programa TFTP za boj proti terorizmu in financiranju terorističnih dejavnosti, so se pojavili resni pomisleki v zvezi z njegovimi posledicami za temeljne pravice državljanov. Ti pomisleki se večinoma osredotočajo na dejstvo, da izvajanje sporazuma TFTP med EU in ZDA vključuje zagotavljanje velike količine osebnih podatkov („neprečiščenih podatkov“) organom ZDA – velika večina teh podatkov zadeva državljane, ki nimajo nobene zveze s terorizmom ali financiranjem

[6] SEC(2011) 438 konč. z dne 30. marca 2011.

terorističnih dejavnosti. Podatki so dani na voljo v neprečiščeni obliki (na podlagi ustrezne kategorije podatkov) in ne na posamični osnovi (kot odgovor na zahtevo v zvezi z enim ali več posamezniki), saj ponudnik teh podatkov nima tehničnih zmogljivosti, da bi zagotovil podatke na posamični osnovi. Poleg tega bi moral ponudnik za posredovanje takšnih podatkov na posamični osnovi vzpostaviti posebni funkciji za iskanje in analizo, kar za njegove postopke delovanja ni potrebno in bi imelo precejšnje posledice v smislu sredstev. Poleg tega bi dostopanje do podatkov na posamični osnovi pomenilo, da bi ponudnik dejansko vedel, katere osebe so predmet preiskave v okviru terorizma in kakšna so njihova finančna razmerja. To bi lahko vplivalo na učinkovitost tovrstnih preiskav.

Za omilitev posledic zagotavljanja neprečiščenih podatkov so bili vzpostavljeni precejšnji zaščitni ukrepi proti njihovi zlorabi, tudi ta, da sta iskanje med poslanimi podatki in njihova uporaba dovoljena le za boj proti terorizmu in financiranju terorističnih dejavnosti. Nedavni pregled sporazuma TFTP med EU in ZDA je potrdil, da se ti zaščitni ukrepi dejansko izvajajo v skladu z določbami sporazuma.

Ne glede na to so se pojavile trditve, da posredovanje tako velikih količin osebnih podatkov tretji državi kljub upoštevanju nujnosti in sorazmernosti posega pomeni neupravičeno kršitev temeljnih pravic teh državljanov. Zato je Svet pozval Komisijo, naj predstavi predloge za vzpostavitev „sistema za ekstrakcijo podatkov na ozemlju EU“. Splošni cilj je zagotoviti, da bi obdelava tovrstnih podatkov potekala v skladu z zakonodajo in načeli EU o varstvu podatkov ter v skladu z Listino EU o temeljnih pravicah. V tem okviru je treba opozoriti, da zbiranje in obdelovanje finančnih podatkov s strani javnih organov vpliva na pravico do varstva osebnih podatkov, zapisano v členu 16 PDEU in členu 8 Listine.

V skladu s členom 52(1) Listine mora biti kakršno koli omejevanje teh temeljnih pravic predpisano z zakonom, dovolj natančno in kakovostno, da se lahko zagotovi predvidljivost, ter mora spoštovati bistveno vsebino teh pravic. Omejitve so dovoljene samo, če so potrebne in če ustrezajo upravičenim ciljem, ki jih priznava Unija. Načeli nujnosti in sorazmernosti morata biti torej upoštevani ne samo ob odločanju o morebitni vzpostavitvi sistema TFTS v EU, temveč tudi v zvezi z različnimi razpoložljivimi možnostmi za izvajanje sistema. Zato ti načeli enakovredno vplivata na prihodnje odločitve v zvezi z vprašanji, kot so obseg sistema, veljavna obdobja shranjevanja podatkov, pravice posameznikov glede dostopa in brisanja itd. Teh vprašanj to sporočilo ne obravnava podrobno. V celoti bodo analizirana v oceni učinka.

Seveda bi imela morebitna vzpostavitev sistema za pridobivanje podatkov na ozemlju EU posledice za veljavni sporazum TFTP med EU in ZDA, kakor priznava člen 11(3) sporazuma, ki pravi, da bi vzpostavitev sistema EU, če se bo EU odločila za vzpostavitev tega sistema, lahko bistveno spremenila okvir tega sporazuma, zato bi se morali pogodbenici posvetovati, da se odloči, ali bi bilo treba sporazum ustrezno prilagoditi. Vse možnosti bi torej vplivale tudi na prihodnje izvajanje in ustrezno prilagoditev veljavnega sporazuma TFTP med EU in ZDA.

3. GLAVNE NALOGE SISTEMA EU ZA SLEDENJE FINANCIRANJA TERORISTIČNIH DEJAVNOSTI

Eno od prvih vprašanj, ki se je pojavilo na razpravah s prej omenjenimi zainteresiranimi stranmi, je, da te zainteresirane strani v veliki večini menijo, da mora biti v primeru vzpostavitve sistema EU za sledenje financiranja terorističnih dejavnosti ta sistem vzpostavljen v interesu zagotavljanja varnosti državljanom EU. Sistema se ne bi smelo

vzpostaviti le zato, da bi zagotavljali koristne informacije organom ZDA – velik interes za rezultate, ki jih daje tovrsten sistem, imajo tudi organi držav članic. Ta pristop pomeni tudi, da bi se pri vzpostavitvi takega sistema sicer zagotovo lahko zgledovali po ameriškem programu TFTP, da pa enakovredni evropski sistem ne bi nujno posnemal vseh njegovih elementov. Prav tako bi moral biti sistem v EU oblikovan z upoštevanjem posebnosti pravnega in upravnega okvira EU, vključno s prej omenjenimi veljavnimi temeljnimi pravicami.

Toda vsak sistem, katerega namen bi bilo sledenje financiranja terorističnih dejavnosti v skladu z glavnimi prej opisanimi cilji, bi moral predvideti izvajanje naslednjih osnovnih nalog:

- pripravo in izdajanje (pravno veljavnih) zahtev imenovanemu ponudniku ali imenovanim ponudnikom storitev v zvezi s sporočili glede finančnih plačil za neobdelane podatke, ki jih je treba zagotoviti pooblaščenemu prejemniku ali prejemnikom. To vključuje določitev kategorij zahtevanih sporočil, pogostost pošiljanja teh sporočil in ohranjanje stikov s ponudniki o teh vprašanjih;

- spremljanje in avtorizacijo zahtev imenovanemu ponudniku ali imenovanim ponudnikom za tovrstne neobdelane podatke. To vključuje preverjanje, ali je bila zahteva za neobdelane podatke pripravljena v skladu z veljavnimi omejitvami;

- sprejemanje in shranjevanje (obdelavo) neobdelanih podatkov, prejetih od imenovanega ponudnika (ali imenovanih ponudnikov), vključno z izvajanjem ustreznega sistema fizične in elektronske varnosti podatkov;

- izvajanje dejanskih iskanj na poslanih podatkih v skladu z veljavnim pravnim okvirom; na podlagi zahtev za tovrstna iskanja, prejetih od organov držav članic, ZDA ali drugih tretjih držav na podlagi jasno opredeljenih pogojev in varnostnih ukrepov, ali na lastno pobudo organa (organov), zadolženega (zadolženih) za obdelavo podatkov;

- spremljanje in avtorizacijo izvajanja iskanj na poslanih podatkih;

- analizo rezultatov iskanj ob povezavi teh rezultatov z drugimi razpoložljivimi informacijami ali obveščevalnimi informacijami;

- distribucijo rezultatov iskanj (brez nadaljnje analize) ali rezultatov analiz pooblaščenim prejemnikom;

- izvajanje ustreznega režima varstva podatkov, vključno z veljavnimi obdobji shranjevanja podatkov, obveznostmi vpisovanja, obdelavo zahtev za dostop, popravek in izbris itd.

Te osnovne naloge bi morale biti določene v ustreznih pravnih aktih na ravni EU, na nacionalni ravni ali na obeh ravneh, odvisno od izbrane možnosti.

4. GLAVNA NAČELA PRI OBRAVNAVI RAZPOLOŽLJIVIH MOŽNOSTI

Poleg pomislekov v zvezi z opisanimi osnovnimi nalogami bo odločitev med razpoložljivimi možnostmi v veliki meri odvisna od tega, kako se obnesejo v zvezi s številnimi glavnimi vprašanji, ki so obravnavana v oceni učinka in nadaljnjem besedilu.

4.1. Učinkovitost

Ključen dejavnik je pričakovana učinkovitost različnih možnosti pri izpolnjevanju osnovnih ciljev boja proti terorizmu in financiranju terorističnih dejavnosti. S tega vidika je treba dati prednost možnostim, ki okrepijo priložnost za izmenjavo in analizo podatkov na mednarodni ravni, saj bosta tovrstni izmenjava in analiza povečali učinkovitost in omogočili večjo dodano vrednost. Zlasti izbira organizacije ali organizacij, ki jim bo zaupana analiza podatkov ter pošiljanje rezultatov analiz ustreznim organom, bo pomembno vplivala na splošno učinkovitost sistema ter na količino podatkov, ki bodo preneseni. Kljub temu bi morale v skladu s sedanjo prakso države članice še naprej obdržati popoln nadzor nad tem, ali se lahko njihove informacije in obveščevalne informacije posredujejo drugim organom.

4.2. Varstvo podatkov

Mednarodna izmenjava ter analiza informacij in obveščevalnih informacij lahko potekata samo v trdnem in dobro razvitem okviru varstva podatkov. Učinkovitost tovrstnega okvira ni odvisna samo od veljavnih pravnih določb, ki posameznikom, na katere se podatki nanašajo, omogočajo, da uveljavijo svoje pravice, na primer pravico do sodnega varstva, temveč tudi od razpoložljivosti izkušenega osebja, na primer neodvisne uradne osebe za varstvo podatkov in neodvisnega ter izkušenega organa za nadzor varstva podatkov. V nekaterih organizacijah, ki bi bile lahko vključene v vzpostavitev sistema TFTS v EU, že obstajajo tovrstne strukture, v drugih pa bi jih bilo treba še oblikovati. Zato je treba posledice vsake od različnih možnosti za varstvo podatkov pazljivo oceniti v skladu s prednostnimi načeli v zvezi s spoštovanjem temeljnih pravic iz dela 2 tega sporočila.

4.3. Varnost podatkov

Trdne določbe o varstvu podatkov je treba dopolniti z najsodobnejšo infrastrukturo in tehnologijo varnosti podatkov. Pomisleki v zvezi z varnostjo podatkov vodijo k omejitvi števila mest, na katerih se lahko obdelujejo poslani podatki, ter omejitvi vseh oblik zunanjega dostopa do podatkov. Najvarnejša rešitev bi bilo shranjevanje na eni lokaciji brez zunanjega dostopa. Večina organizacij, ki bi lahko bile vključene v upravljanje sistema TFTS, je že vzpostavila varne tehnologije obdelave podatkov, vendar nimajo vse zmogljivosti za upravljanje podatkov, razvrščenih nad raven RESTREINT UE / EU RESTRICTED.

4.4. Shranjevanje podatkov

Shranjevanje podatkov bi lahko potekalo bodisi na nacionalni ravni bodisi na ravni EU. Na ravni EU bi lahko shranjevanje podatkov, prejetih od imenovanega ponudnika ali imenovanih ponudnikov, potekalo v Europolu ali drugem organu EU, na primer Agenciji za operativno upravljanje obsežnih informacijskih sistemov na področju svobode, varnosti in pravice (v nadaljnjem besedilu: agencija za IT)[7], ki se pravkar ustanavlja. Ker je shranjevanje podatkov neločljivo povezano z vprašanji varstva in varnosti podatkov, mora biti izbira organizacije, odgovorne za shranjevanje podatkov, tesno povezana z režimom varstva in varnosti podatkov, ki ga te organizacije lahko zagotovijo.

[7] COM(2010) 93 konč. z dne 19. marca 2010.

4.5. Uporaba obstoječih struktur in instrumentov

Vse možnosti bi morale kar najbolje izrabiti obstoječe strukture. S tem bi se omejili stroški in omogočile koristi od pridobljenih izkušenj ter obstoječe infrastrukture. Ob takšni uporabi obstoječih instrumentov morajo nove naloge, dodeljene obstoječi organizaciji, dobro ustrezati njenemu obstoječemu mandatu. Na primer, Europol, Eurojust ali nacionalni sodni organi bi bili lahko ustrezni organi za preverjanje in avtorizacijo zahtev za podatke, naslovljenih na imenovanega ponudnika ali imenovane ponudnike.

4.6. Sodelovanje med odgovornimi organi

V nadaljnjem besedilu opisane možnosti nudijo različne stopnje sodelovanja ter izmenjave informacij in obveščevalnih informacij med nacionalnimi organi ter med nacionalnimi in evropskimi organi. Različne države članice so vzpostavile različne načine sodelovanja njihovih nacionalnih organov v boju proti terorizmu, vsi ukrepi na evropski ravni pa morajo spoštovati omejitve, določene v členu 72 PDEU glede posebnih pravic držav članic v zvezi z ohranjanjem reda in miru ter varovanjem notranje varnosti. Kakršen koli sistem TFTS v EU mora torej omogočati, da države članice v precejšnji meri nadzorujejo informacije in obveščevalne informacije, ki so jih pripravljene izmenjati v okviru tovrstnega sistema. Številne organizacije, omenjene v nadaljnjem besedilu, so razvile različne pristope k temu vprašanju in nekateri od njih bi se lahko neposredno uporabili v prihodnjem vzpostavljenem sistemu.

4.7. Prvi splošni pregled možnih finančnih vplivov različnih možnosti

Skupni stroški vzpostavitve sistema TFTS v EU ter njihova porazdelitev med ravnjo EU in nacionalno ravnjo bodo v veliki meri odvisni od izbire možnosti politike. V vsakem primeru bodo stroški vključevali:

- stroške, povezane z varnim prenosom in shranjevanjem podatkov, prejetih od imenovanega ponudnika ali imenovanih ponudnikov;
- stroške, povezane z razvojem in vzdrževanjem informacijskih programov, potrebnih za izvajanje iskanj in zagotavljanje rezultatov iskanja;
- stroške, povezane z distribucijo rezultatov iskanja ali analiz pooblaščenim prejemnikom;
- stroške za osebje, ki bo izvajalo iskanja in analize ter distribuiralo rezultate;
- stroške za osebje, ki bo odgovorno za naloge spremljanja in revizije;
- stroške za osebje, ki bo odgovorno za varstvo podatkov in pravice državljanov.

Čeprav podrobne ocene stroškov še niso na voljo, začetni izračuni kažejo, da bi v nadaljnjem besedilu opisani pristop, omejen na EU, in različne mešane možnosti stali med 33 in 47 milijoni EUR za stroške vzpostavitve in med 7 in 11 milijoni EUR, potrebnih za letne stroške delovanja. Različne možnosti so opisane v delu 6 tega sporočila. Najdražja bi bila možnost 3, saj bi stroški vzpostavitve znašali 43 milijonov EUR za EU in 3,7 milijona EUR za države članice (skupaj), letni stroški delovanja pa 4,2 milijona EUR za EU in 6,8 milijona EUR za države članice (skupaj). Možnost 2 bi bila najcenejša, saj bi stroški vzpostavitve znašali 33 milijonov EUR za EU, letni stroški delovanja pa 3,5 milijona EUR na ravni EU ter 3,3

milijona EUR za države članice (skupaj). Možnost 1 bi zahtevala 40,5 milijona EUR v stroških vzpostavitve za EU in 4 milijone EUR v letnih stroških delovanja na ravni EU ter 5 milijonov EUR v letnih stroških delovanja za države članice (skupaj). Seveda bi se ti stroški zmanjšali, če bi se lahko uporabili osebje obstoječih organizacij, obstoječa infrastruktura ter programska in strojna oprema. Stroški vzpostavitve in delovanja izključno nacionalnega sistema bi bili bistveno višji (390 milijonov EUR v stroških vzpostavitve in 37 milijonov v letnih stroških delovanja), saj bi morale vse države članice vzpostaviti močno varovane sisteme za obdelavo podatkov in zaposliti osebje, da bi jih upravljalo.

Ti zneski so predhodne ocene ter bodo morali biti dodatno analizirani in podrobno proučeni glede na rezultate ocene učinka.

5. VPRAŠANJA, KI JIH JE TREBA UPOŠTEVATI

Ne glede na izbiro med različnimi možnostmi za vzpostavitev in delovanje sistema TFTS v EU je treba upoštevati številna pomembna vprašanja v zvezi z obsegom morebitnega sistema TFTS v EU. Ta so obravnavana v nadaljnjem besedilu.

5.1. Terorizem in financiranje terorističnih dejavnosti ali širši obseg?

Dostop do podatkov o sporočilih glede finančnih plačil ni uporaben samo v boju proti terorizmu in financiranju terorističnih dejavnosti. Skoraj zagotovo bi bil ta dostop dragoceno orodje tudi za boj proti drugim hudim oblikam kriminala, zlasti organiziranemu kriminalu in pranju denarja. Toda v okviru sporazuma TFTP med EU in ZDA so pomisleki glede sorazmernosti privedli do natančno vzdrževanih omejitev uporabe podatkov na namen boja proti terorizmu in financiranju terorističnih dejavnosti. Sodeč po predhodnih razpravah, ki so potekale do sedaj, se večina strani strinja, da tudi ti pomisleki glede sorazmernosti kažejo v smer vzpostavitve enakovrednega evropskega sistema v enakem omejenem obsegu in v skladu s splošnimi pomisleki v zvezi s spoštovanjem temeljnih pravic, obravnavanimi v delu 2 tega sporočila.

5.2. Več kot en ponudnik?

Sporazum TFTP med EU in ZDA je trenutno omejen na zahteve za podatke od samo enega ponudnika mednarodnih storitev sporočil glede finančnih plačil. Čeprav je ta ponudnik očitno najpomembnejši svetovni ponudnik tovrstnih sporočil, na trgu delujejo tudi drugi ponudniki. Pomisleki o učinkovitosti in oblikovanju enakih pogojev za vse udeležence na trgu kažejo v smer vzpostavitve sistema, ki bo uporaben za vse ponudnike mednarodnih storitev sporočil glede finančnih plačil. V vsakem primeru mora biti pri izbiri razpoložljivih možnosti upoštevano upravno breme podjetij, ki bodo opravljala storitve sporočil glede finančnih plačil.

5.3. Samo mednarodne storitve sporočil ali tudi nacionalne?

Sporazum TFTP med EU in ZDA je trenutno omejen na zahteve za podatke samo od ponudnikov mednarodnih storitev sporočil glede finančnih plačil, torej storitev sporočil, ki se uporabljajo za opravljanje nadnacionalnih transakcij, vključno s transakcijami med državami članicami EU, izključeni pa so podatki o sporočilih glede finančnih plačil v zvezi z enotnim območjem plačil v evrih (SEPA). Pri vzpostavitvi sistema TFTS v EU bo treba upoštevati tudi možnost vključitve ali izključitve storitev sporočil glede finančnih plačil med državami članicami in ali naj bo omejen na mednarodno izmenjavo sporočil glede finančnih plačil. Izključno nacionalne storitve sporočil (ki se uporabljajo samo v okviru nacionalnih finančnih

transakcij) so trenutno izključene iz področja uporabe sporazuma TFTP med EU in ZDA. Dostop do tovrstnih nacionalnih storitev sporočil bi bil lahko zanimiv za boj proti terorizmu in drugim oblikam kriminala. Toda tudi ob neupoštevanju vprašanja, ali bi moral biti dostop do tovrstnih izključno nacionalnih transakcij urejen na evropski ravni, so predhodne razprave potrdile stališče, da je tovrsten dostop po mnenju večine nesorazmeren in bi moral biti zato izločen iz obsega sistema v EU.

5.4. Kakšna vrsta podatkov o sporočilih glede finančnih plačil bi morala biti zajeta?

V mednarodnem bančnem sistemu se uporablja več različnih vrst podatkov o sporočilih glede finančnih plačil. Sporazum TFTP med EU in ZDA je trenutno omejen na eno določeno vrsto podatkov o sporočilih glede finančnih plačil. Dostop do drugih vrst podatkov o sporočilih glede finančnih plačil bi bil zanimiv za boj proti terorizmu in financiranju terorističnih dejavnosti ter morda proti drugim oblikam kriminala. Toda tudi v zvezi s to izbiro pomisleki glede sorazmernosti in spoštovanja temeljnih pravic državljanov kažejo, da je treba omejiti obseg vrst sporočil, vključenih v sistem. Dodatne podrobnosti o tem tehničnem vprašanju bodo zajete v oceni učinka.

6. MOŽNOSTI ZA SISTEM TFTS V EU

Komisija v nadaljnjem besedilu opisane možnosti proučuje v okviru ocene učinka, ki se trenutno izvaja. To ni nujno dokončen seznam možnosti in v nobenem primeru ne vpliva na končno oceno učinka ali izbiro, za katero bi se Komisija odločila na podlagi te ocene učinka.

Ena od možnosti, ki se vedno upošteva v postopku priprave novih pobud in njihovih spremnih ocen učinka, je možnost ohranitve nespremenjenega stanja, kar bi v tem primeru pomenilo, da bi se ohranil sporazum TFTP med EU in ZDA in se ne bi pripravil nov predlog za sistem TFTS v EU. S to možnostjo se ne bi odzvali na poziv Sveta in Evropskega parlamenta Komisiji, naj predstavi predlog za oblikovanje „pravnega in tehničnega okvira za vpogled v podatke na ozemlju EU“, kakor je navedeno v delu 1 tega sporočila. Poleg tega ta možnost ne bi prispevala k omejitvi količine osebnih podatkov, prenesenih v tretje države, in ne bi določala obdelave podatkov na ozemlju EU v skladu z načeli in zakonodajo EU s področja varstva podatkov. Druge možnosti, podrobneje obravnavane v nadaljnjem besedilu, vse predstavljajo možne načine vzpostavitve sistema TFTS v EU.

Teoretično bi bile lahko vse osnovne naloge sistema TFTS v EU, navedene v delu 3 tega sporočila, izvedene bodisi na ravni EU bodisi na nacionalni ravni. Naloge se lahko dodelijo tudi eni organizaciji ali več različnim organizacijam, v skladu z njihovimi obstoječimi odgovornostmi, ali pa se ustanovijo nove organizacije, ki bi jih izvajale. Te organizacije bi lahko bile bodisi evropske bodisi nacionalne. To pomeni, da je – tudi teoretično – možen izključno evropski pristop, pri katerem bi bile vse osnovne naloge dodeljene organizacijam na ravni EU, in prav tako izključno nacionalen pristop, pri katerem bi se vse naloge izvajale na nacionalni ravni. Na splošno je treba prav tako opozoriti, da izbira med centraliziranim, decentraliziranim ali hibridnim sistemom v tem posebnem primeru ni enaka kot izbire v zvezi z drugimi pobudami, ki vključujejo obdelovanje podatkov za boj proti terorizmu in organiziranemu kriminalu – vsako pobudo na tem področju je treba presojati na podlagi njenih prednosti.

Tako izključno centralizirani kot izključno nacionalni pristopi imajo precejšnje pomanjkljivosti. Na primer, slabost izključno evropskega pristopa bi bila zagotovo njegova

izključitev iz organizacij kazenskega pregona in obveščevalnih organizacij ter praks držav članic, zato ne bi bil preveč učinkovit. Brez prizadevanj nacionalnih organov, odgovornih za obravnavo teh zadev, bi bilo skoraj nemogoče pravilno določiti, katere kategorije podatkov bi bilo treba zahtevati od imenovanega ponudnika ali imenovanih ponudnikov. Uporabnost sistema bi bila manjša tudi, če bi se iskanje po bazah podatkov izvajalo le na podlagi obveščevalnih informacij, ki so na voljo na ravni EU – na trenutni ravni povezave EU so tovrstne obveščevalne informacije namreč na voljo le na nacionalni ravni. Prav tako ni verjetno, da bi države članice sprejele takšen pristop izključno na ravni EU, saj ne bi ponudil dodane vrednosti k njihovim prizadevanjem za boj proti terorizmu in financiranju terorističnih dejavnosti. Med posvetovanji so države članice nakazale tudi, da bi bilo to možnost težko sprejeti iz pravnih in operativnih razlogov.

Pri drugi skrajnosti pa bi pri izključno nacionalnem pristopu obstajalo tveganje za razhajanja pri izvajanju v različnih državah članicah ter povečano tveganje za kršitve varnosti podatkov, saj bi moralo obstajati 27 različnih izvodov poslanih podatkov. Izključno nacionalen pristop bi vključeval tudi težave v zvezi z izvajanjem harmoniziranega okvira za varstvo podatkov ter harmoniziranega pristopa k nadzoru nad drugimi potrebnimi omejitvami, na primer omejitvijo na terorizem in financiranje terorističnih dejavnosti. Prav tako bi bilo pri izključno nacionalnem pristopu nejasno, katera država članica bi bila odgovorna za obravnavo zahtev za iskanje od tretjih držav, izgubljena pa bi bila tudi dodatna korist analize rezultatov iskanja na evropski ravni. Poleg tega bi se, kakor je bilo že navedeno, stroški s to možnostjo precej povišali, saj bi morale vse države članice vzpostaviti močno varovane sisteme za obdelavo podatkov in zaposliti osebje, da bi jih upravljalo.

Med pripravljalnim delom z zainteresiranimi stranmi smo torej hitro ugotovili, da rešitvi na skrajnih straneh velike izbire možnosti nimata podpore, zato se je oblikovalo soglasje, da bi najboljše možne rezultate za dva glavna cilja omogočila mešana rešitev z razdelitvijo različnih nalog med različne organizacije na ravni EU in na nacionalni ravni. Čeprav je to soglasje v pomoč pri iskanju najprimernejše možnosti, je znotraj mešanega pristopa še vedno treba izbrati med velikim številom možnosti. V naslednjih odstavkih so podrobneje opisane tri mešane možnosti, ki so se na podlagi trenutnega pripravljalnega dela izoblikovale kot najprimernejše – v Prilogi so možnosti predstavljene tudi v obliki razpredelnice.

6.1. Sistem TFTS v EU kot služba za koordinacijo in analizo (možnost 1)

Ta možnost bi vključevala vzpostavitev centralne enote sistema TFTS v EU in večina nalog bi se izvajala na ravni EU. Na ravni EU bi potekalo naslednje: izdajanje zahtev za neobdelane podatke imenovanemu ponudniku ali imenovanim ponudnikom, preverjanje teh zahtev, obravnava zahtev za iskanja in njihovo izvajanje, upravljanje rezultatov iskanja ter posredovanje poročil tistim, ki so zahtevali iskanja. Pripravljanje zahtev imenovanemu ponudniku ali imenovanim ponudnikom pa bi lahko potekalo v posvetovanju z odgovornimi organi držav članic in države članice bi lahko tudi ponudile napotitev svojih analitikov v centralno enoto, da bi sodelovali pri izvajanju iskanj. V nasprotju s popolnoma centraliziranо možnostjo bi države članice lahko zahtevale, da se iskanja izvajajo v njihovem imenu, podobno postopku, ki zdaj velja v ameriškem programu TFTP, ali da jih opravijo njihovi analitiki.

Države članice bi morale izmenjati podatke s centralno enoto sistema TFTS v EU, da bi „utemeljile“ zahtevo in njeno povezavo s terorizmom, preden bi se lahko začelo iskanje, ali pa bi morali njihove zahteve vnaprej dovoliti državni organi. Tovrstni državni organi bi bili lahko na primer nacionalni tožilci ali preiskovalni sodniki, ki se ukvarjajo z bojem proti

terorizmu – če bi dovoljenje za neko iskanje med poslanimi podatki prišlo od njih, potem bi lahko centralna enota sistema TFTS v EU privolila v izvajanje iskanj brez nadaljnjega preverjanja. Po tem predvidenem poteku ne bi bilo treba centralni enoti sistema TFTS v EU poslati nikakršnih nadaljnjih obveščevalnih informacij. Centralna enota sistema TFTS v EU bi posredovala rezultate iskanja in njihove analize ter bi lahko pošiljala informacije tudi na lastno pobudo. Tudi ZDA in druge tretje države bi morale zahtevati izvajanje iskanj na podlagi podobnega postopka.

Centralizirani bi bili tudi spremljanje spoštovanja zaščitnih ukrepov in nadzori, morda bi vključevali tudi nadzor s strani zunanjih zainteresiranih strani, na primer predstavnikov imenovanega ponudnika ali imenovanih ponudnikov, ter tistih, ki so imenovani za neodvisne nadzornike. Na centralni ravni bi bili zagotovljeni tudi varstvo, celovitost in varnost podatkov.

Glavna organa, vključena v sistem, bi bila lahko Europol in Eurojust. Naloge, ki bi jih izvajala Europol in Eurojust, morajo v tem primeru sovpadati z njunimi nalogami, kakor jih določa Pogodba o delovanju Evropske unije (PDEU). Treba bo tudi določiti, do kakšne mere bi bilo treba spremeniti pravne akte, ki trenutno urejajo njuno delovanje. Če bi bil za centralno enoto sistema TFTS v EU določen Europol, bi moral obravnavati tudi zahteve posameznikov, na katere se podatki nanašajo, za dostop, popravek in blokiranje, v skladu s svojim obstoječim pravnim okvirom in določbami v zvezi z varstvom podatkov. Centralna enota sistema TFTS v EU bi opravljala svojo vlogo v skladu z obstoječim pravnim okvirom, odškodninske zadeve in pritožbe pa bi bile prav tako obravnavane v skladu z veljavnimi pravnimi določbami. Na nacionalni ravni bi bili organi kazenskega pregona vključeni v preverjanje in avtorizacijo zahtev za iskanje. Predvidena bi bila lahko možnost ustanovitve novih nacionalnih organov, vendar bi bilo to odločitev najbolje prepustiti državam članicam na podlagi načela subsidiarnosti[8].

6.2. Sistem TFTS v EU kot služba za pridobivanje podatkov (možnost 2)

Tako kot prva možnost politike bi tudi druga vključevala vzpostavitev centralne enote sistema TFTS v EU, katere naloge bi zajemale izdajanje zahtev za neobdelane podatke imenovanemu ponudniku ali imenovanim ponudnikom, preverjanje teh zahtev, izvajanje iskanj in obravnavo zahtev za iskanja. Toda v okviru te možnosti centralna enota sistema TFTS v EU ne bi smela analizirati rezultatov iskanja in jih primerjati z drugimi razpoložljivimi informacijami ali obveščevalnimi informacijami, kadar bi se ta iskanja izvajala na zahtevo organov držav članic – v teh primerih bi bila njena naloga omejena na pripravljanje in pošiljanje rezultatov iskanja v primerni obliki.

Tako kot pri možnosti 1 bi bile zahteve za neobdelane podatke, ki bi bile izdane imenovanemu ponudniku ali imenovanim ponudnikom, pripravljene v tesnem sodelovanju z državami članicami, ki bi lahko sporočile svoje posebne potrebe centralni enoti sistema TFTS, ta pa bi jih analizirala in na podlagi te analize oblikovala eno ali več zahtev.

Organi držav članic bi zahtevali iskanja, ki bi se izvajala v njihovem imenu. Na nacionalni ravni bi se preverjalo in potrjevalo, ali so te zahteve utemeljene in ali obstaja povezava s terorizmom. Centralna enota sistema TFTS v EU bi izvedla iskanje in državam članicam poslala nazaj v primerni obliki urejen izčrpen seznam rezultatov. Organi držav članic bi bili

[8] Na tej stopnji še niso znane proračunske posledice za agencije EU, ki bi bile lahko udeležene pri izvajanju sistema.

edini, ki bi izvajali analizo rezultatov, in lahko bi se odločili tudi za pošiljanje informacij na lastno pobudo.

Centralna enota sistema TFTS v EU bi bila zadolžena za izvajanje iskanj in analizo rezultatov v imenu institucij EU, ZDA in drugih tretjih držav. Na tej podlagi bi lahko pošiljala informacije tudi na lastno pobudo.

Tako kot pri prejšnjih možnostih bi bili centralizirani tudi spremljanje spoštovanja zaščitnih ukrepov in nadzori, morda bi vključevali tudi nadzor s strani zunanjih zainteresiranih strani, na primer predstavnikov imenovanega ponudnika ali imenovanih ponudnikov, ter tistih, ki so imenovani za neodvisne nadzornike. Na centralni ravni bi bili zagotovljeni tudi varstvo, celovitost in varnost podatkov.

Spet tako kot pri prejšnji možnosti bi lahko bila glavna organa, vključena v sistem, Europol in Eurojust. Na nacionalni ravni bi bili ključni sodelujoči organi nacionalni organi kazenskega pregona ali obveščevalni organi. Kakor zgoraj bi bila ustanovitev novih nacionalnih organov prepuščena državam članicam na podlagi načela subsidiarnosti. Europol in/ali nacionalne enote bi obravnavali zahteve državljanov EU za dostop, popravek in izbris, kar bi vključevalo tako nacionalne organe za varstvo podatkov kot skupni nadzorni organ Europola. Odškodninske zadeve in pritožbe bi se obravnavale v skladu z veljavnimi pravnimi določbami na nacionalni ravni ali ravni EU[9].

6.3. Koordinacijska služba enot za finančni nadzor (možnost 3)

Ta možnost politike bi zajemala vzpostavitev posodobljenega foruma enot za finančni nadzor, ki bi ga sestavljale enote za finančni nadzor držav članic. Začasni organ na ravni EU bi izdajal zahteve za neobdelane podatke imenovanemu ponudniku ali imenovanim ponudnikom, tako da bi potrebe, ki jih določijo enote za finančni nadzor, zbral v eno samo zahtevo, ki bi bila prav tako preverjena in avtorizirana na centralni ravni.

Vsaka enota za finančni nadzor bi bila odgovorna za izvajanje iskanj in upravljanje rezultatov iskanja v imenu svoje države članice ter za izvajanje analiz in posredovanje poročil tistim, ki bi bili po njenem mnenju do njih upravičeni. Na nacionalni ravni ali na ravni EU bi se preverjalo in potrjevalo, v kolikšni meri so te zahteve utemeljene in ali obstaja povezava s terorizmom. Enote za finančni nadzor bi bile odgovorne tudi za pošiljanje informacij na lastno pobudo.

Posodobljeni forum enot za finančni nadzor bi lahko izvajal iskanja ter analiziral rezultate v imenu institucij EU in drugih tretjih držav, s katerimi bi EU sklenila sporazum. Lahko bi tudi pošiljal informacije na lastno pobudo.

Spremljanje spoštovanja zaščitnih ukrepov in nadzori bi bili centralizirani, morda bi vključevali tudi nadzor s strani zunanjih zainteresiranih strani, na primer predstavnikov imenovanega ponudnika ali imenovanih ponudnikov, ter tistih, ki so imenovani za neodvisne nadzornike. Na centralni ravni bi bili zagotovljeni tudi varstvo, celovitost in varnost podatkov.

Posodobljenemu forumu enot za finančni nadzor bi bil dodeljen uraden pravni status z jasno določenimi vlogami in odgovornostmi. Na nacionalni ravni bi bili ključni sodelujoči organi enote za finančni nadzor, nacionalni organi kazenskega pregona in obveščevalni organi.

---

[9] Glej opombo 8.

Organ na ravni EU bi obravnaval zahteve državljanov EU za dostop, popravek in izbris, medtem ko bi se odškodninske zadeve in pritožbe obravnavale v skladu z veljavnimi pravnimi določbami na nacionalni ravni ali ravni EU.

7. SKLEP

Na podlagi pripravljalnega dela, ki ga je do sedaj opravila Komisija, in v skladu z rezultati ocene učinka to sporočilo opisuje različne možnosti izbire za vzpostavitev „pravnega in tehničnega okvira za vpogled v podatke na ozemlju EU“ v okviru sistema za sledenje financiranja terorističnih dejavnosti. Različne možnosti, opisane v tem sporočilu, kažejo, da bodo še vedno potrebne pomembne izbire in odločitve, tudi v zvezi s spoštovanjem temeljnih pravic, precej podrobneje pa bo treba med prihodnjim pripravljalnim delom obravnavati tudi veliko pravnih, tehničnih, organizacijskih in finančnih vprašanj. Glede na te pomembne izzive Komisija meni, da bo za nadaljnje pripravljalno delo ter razpravo s Svetom in Parlamentom treba nameniti dovolj časa.

* * *

Priloga: Pregled mešanih možnosti v obliki razpredelnice

	Sistem TFTS v EU kot služba za koordinacijo in analizo (možnost 1)	Sistem TFTS v EU kot služba za pridobivanje podatkov (možnost 2)	Koordinacijska služba enot za finančni nadzor (možnost 3)
Priprava in izdajanje zahtev za neobdelane podatke	Centralna enota sistema TFTS v EU v koordinaciji z državami članicami	Centralna enota sistema TFTS v EU v koordinaciji z državami članicami	Posodobljeni forum enot za finančni nadzor
Spremljanje in avtorizacija zahtev za neobdelane podatke	Eurojust ali drug obstoječi organ	Eurojust ali drug obstoječi organ	Eurojust ali drug obstoječi organ
Sprejemanje in shranjevanje neobdelanih podatkov, varnost podatkov	Europol ali drug organ EU, na primer agencija za IT	Europol ali drug organ EU, na primer agencija za IT	Europol ali drug organ EU, na primer agencija za IT
Izvajanje iskanj na neobdelanih podatkih	Centralna enota sistema TFTS v EU, napoteni nacionalni analitiki ali kombinacija obojega	Centralna enota sistema TFTS v EU	Enote za finančni nadzor, posodobljeni forum enot za finančni nadzor
Spremljanje in avtorizacija izvajanja iskanj	Neodvisni nadzorniki, morda nacionalni organi	Neodvisni nadzorniki, nacionalni organi	Neodvisni nadzorniki
Analiza rezultatov iskanj	Centralna enota sistema TFTS v EU, napoteni nacionalni analitiki ali kombinacija obojega	Nacionalni organi za nacionalna iskanja, analitiki centralne enote sistema TFTS v EU za iskanja EU in tretjih držav	Posodobljeni forum enot za finančni nadzor, nacionalne enote za finančni nadzor
Distribucija rezultatov iskanj	Analitiki Europola ali napoteni analitiki držav članic	Nacionalni organi za nacionalna iskanja, analitiki centralne enote sistema TFTS v EU za iskanja EU in tretjih držav	Posodobljeni forum enot za finančni nadzor, nacionalne enote za finančni nadzor
Izvajanje ustreznega režima varstva podatkov	Europol ali drug organ EU, na primer agencija za IT	Europol ali drug organ EU, na primer agencija za IT	Europol ali drug organ EU, na primer agencija za IT