EUROPSKA
KOMISIJA

Bruxelles, 27.11.2013.
COM(2013) 842 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

Europski sustav za praćenje financiranja terorizma (EU TFTS)

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

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

Europski sustav za praćenje financiranja terorizma (EU TFTS)

Ova Komunikacija, koja je uslijedila nakon Komunikacije od 13. srpnja 2011. (COM (2011) 429), ima za cilj informirati Europski parlament i Vijeće o rezultatima analize izvršene u pogledu izvedivosti uspostavljanja Europskog sustava za praćenje financiranja terorizma (EU TFTS).

1. KONTEKST

1.1. Temelj zahtjeva i definicija

Tijekom pregovora koji su prethodili sklapanju Sporazuma o Programu za praćenje financiranja terorizma (TFTP) između EU-a i SAD-a[1], raspravljalo se o najboljem načinu zaštite osobnih podataka i poštovanja temeljnih prava u kontekstu tog sporazuma. Neki su od sugovornika smatrali da će se uzimanjem podataka na europskom tlu ograničiti količina podataka koji se prenose u SAD te će se tako jamčiti bolja zaštita podataka. Neke su države članice bile mišljenja da se stvaranjem nezavisnog europskog sustava za praćenje financiranja terorizma dugoročno gledano može stvoriti dodana vrijednost. Europski je parlament od Vijeća i Komisije zatražio da poduzmu sve potrebne mjere kako bi se pronašlo trajno i pravno valjano europsko rješenje pitanja uzimanja traženih podataka na europskom tlu. Pri davanju suglasnosti TFTP-u između EU-a i SAD-a Vijeće i Europski parlament pozvali su Komisiju da u roku od godine dana nakon stupanja Sporazuma na snagu podnese tehnički i pravni okvir za uzimanje podataka na području EU-a te da u roku od tri godine nakon stupanja Sporazuma na snagu podnese izvješće o napretku u stvaranju ekvivalentnog sustava EU-a.[2] Osim toga, u članku 11. Sporazuma o TFTP-u između EU-a i SAD-a navodi se da će Komisija za vrijeme važenja Sporazuma provesti studiju o mogućem uvođenju ekvivalentnog sustava EU-a, kojim bi se omogućio preciznije usmjeren prijenos podataka.

Za potrebe ove Komunikacije treba razlikovati ekvivalentan sustav EU-a od okvira za uzimanje podataka na području EU-a. Pod *okvirom za uzimanje podataka* na području EU-a podrazumijeva se sustav kojim se omogućuje da se pretraživanje podataka koje EU trenutačno

[1] SL L 195, 27.7.2010., str. 5.
[2] Odluka Vijeća od 13. srpnja 2010., SL L 195, 27.7.2010., str. 3.

pruža SAD-u provodi na tlu EU-a. Za razliku od toga, *ekvivalentan sustav EU-a* bio bi neovisan europski sustav za praćenje financiranja terorizma pomoću pristupa podacima imenovanih davatelja podataka te za pretraživanje i analizu tih podataka. Uspostava bilo kakvog sustava EU-a zahtijevala bi izmjenu Sporazuma o TFTP-u između EU-a i SAD-a.

1.2. Poduzeti koraci

Komisija je u prosincu 2010. naručila *studiju*, koja je u srpnju 2011. proširena kako bi obuhvatila dodatnu mogućnost režima zadržavanja i uzimanja podataka. U okviru te studije Komisija je održala pet sastanaka stručnjaka na kojima su sudjelovali dionici poput Europola, Europskog nadzornika za zaštitu podataka, imenovanog davatelja podataka za TFTP[3] i brojni stručnjaci iz država članica koji su predstavljali zainteresirana ministarstva, tijela za provedbu zakona i obavještajne službe te tijela nadležna za zaštitu podataka.

Komisija je 13. srpnja 2011. u svojoj *Komunikaciji Europskom parlamentu i Vijeću („Komunikacija iz 2011.")* predstavila pet mogućnosti koje je utvrdila za Europski sustav za praćenje financiranja terorizma („EU TFTS"). Zaključeno je da su tri od njih izvedive. Cilj je Komunikacije iz 2011. bio pokrenuti raspravu o budućem radu i pružiti doprinos procjeni učinka koju treba provesti.

To je pitanje predstavljeno na zasjedanju Vijeća za pravosuđe i unutarnje poslove u listopadu 2011. te na Odboru Europskog parlamenta za građanske slobode.

Budući da se države članice i Europski parlament nisu izričito opredijelili ni za jednu od mogućnosti, odlučeno je da se sve od njih razmotre u Komisijinoj procjeni učinka te da se svaka od njih razradi tako što će se osmisliti različite podmogućnosti. Ova se Komunikacija temelji na Procjeni učinka[4].

[3] Udruženje za međunarodne međubankarske financijske telekomunikacije (SWIFT).
[4] SWD 2013 (xx) od

2. KOMISIJINA TEMELJNA NAČELA I UTVRĐENE MOGUĆNOSTI

2.1. Načela iz Strategije upravljanja informacijama donesene tijekom švedskog predsjedanja

U svojoj analizi predloženog budućeg rada Komisija uzima u obzir temeljna načela utvrđena u Strategiji upravljanja informacijama iz 2009.[5], koja su nakon toga u uključena u komunikacije Komisije: 2010. godine u Komunikaciju o pregledu upravljanja informacijama u području slobode, sigurnosti i pravde[6] te 2012. u Komunikaciju o Europskom modelu razmjene informacija[7].

U tom su pogledu od najveće važnosti načelo zaštite temeljnih prava te načela nužnosti, proporcionalnosti i isplativosti.

Komisija u izradi novih prijedloga u kojima je riječ o obradi osobnih podataka u području unutarnje sigurnosti posebno vodi računa o zaštiti *temeljnih prava* kako su sadržana u Povelji o temeljnim pravima Europske unije, posebno pravu na privatnost i zaštitu osobnih podataka. U člancima 7. i 8. Povelje naglašava se da svatko ima pravo na „poštovanje svojeg privatnog i obiteljskog života" i „zaštitu svojih osobnih podataka." U članku 16. Ugovora o funkcioniranju Europske unije, koji je obvezujući za države članice te institucije, agencije i tijela Unije potvrđuje se svačije pravo na „zaštitu svojih osobnih podataka." Prema članku 52. Povelje, uz poštovanje načela proporcionalnosti, ograničenja ostvarivanja prava i sloboda iz Povelje moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.

Narušavanje prava na privatnost smatra se *nužnim* ako odgovara hitnoj potrebi, ako je razmjerno cilju koji se nastoji postići te ako su razlozi koje tijelo javne vlasti navodi kako bi je opravdalo relevantni i dovoljni.

Premda je u financijskom smislu teško procijeniti sve troškove koje prouzroči terorizam, i dalje vrijedi načelo *isplativosti*. Pri primjeni pristupa u kojem se vodi računa o *isplativosti*, uzimaju se u obzir prethodna rješenja kako bi se na najmanju moguću mjeru svela preklapanja

[5] Zaključci Vijeća od 30. studenoga 2009. o strategiji upravljanja informacijama za unutarnju sigurnost EU-a 16637/09
[6] COM(2010) 385 od 20. srpnja 2010.
[7] COM(2012) 735 od 7. prosinca 2012.

i postigao maksimalan učinak sinergije. Potrebno je izvršiti procjenu kako bi se utvrdilo je li ciljeve prijedloga moguće postići boljim korištenjem postojećih instrumenata.

2.2. Pristup

U svjetlu navedenih načela Komisija je ispitala bi li EU TFTS bio potreban i razmjeran u pogledu njegovih troškova, koristi i učinka na temeljna prava u usporedbi sa sadašnjom situacijom.

Kada je riječ o *koristima*, sustavom EU-a mogla bi se povećati sposobnost EU-a i njegovih država članica za pristup relevantnim podacima te ojačati njihova analitička sposobnost praćenja i identificiranja terorista pomoću financijskih transakcija. Budući da se iz financijskih transakcija mogu dobiti dragocjeni obavještajni podaci koji nisu dostupni iz drugih izvora, ovaj bi alat bio iznimno značajan za otkrivanje terorističkih aktivnosti i subjekata koji u njima sudjeluju. Stoga bi EU TFTS mogao predstavljati dodatni alat za prikupljanje obavještajnih podataka i istrage u borbi protiv terorizma te za poboljšanje razine sigurnosti u EU-u, osobito ako bi takvim sustavom bili obuhvaćeni različiti davatelji financijskih podataka i različite vrste transakcija. Koristi od EU TFTS-a trebale bi se dovesti u ravnotežu s procijenjenim troškovima uvođenja i održavanja sustava, uključujući financijsko opterećenje EU-a, država članica te imenovane davatelje odgovarajućih podataka

2.3. Predstavljanje mogućnosti koje su na raspolaganju

U obzir je uzet niz mogućnosti za *okvir za uzimanje podataka* na području EU-a, kao i za *ekvivalentni sustav EU-a.*

2.3.1. Okvir za uzimanje podataka na teritoriju EU-a

Okvir za uzimanje podataka na teritoriju EU-a mogao bi se provesti pomoću sustava zadržavanja i dobivanja podataka koje posjeduje imenovani davatelj podataka tako da se omogući izravan pristup podacima, koji se u okviru PFTP-a trenutačno pružaju SAD-u. Takav bi se izravan pristup omogućio analitičarima ili stručnjacima iz SAD-a koji bi u tu svrhu dobili ovlasti.

Unutar ove mogućnosti jedna bi podmogućnost bila na određeno vrijeme zadržati podatke na poslužitelju imenovanog davatelja podataka i pretraživati ih izravno na tom poslužitelju. Međutim, imenovani davatelj podataka u okviru Sporazuma o TFPT-u između EU-a i SAD-a

primjenjuje stroge mjere zaštite i sigurnosti kojima se ne dopušta identificiranje osoba koje se spominju u podacima iz poruka, tako da se u njegovoj sadašnjoj bazi podataka ne mogu vršiti pretraživanja na osnovi osobnih podataka. Stoga bi bilo potrebno stvoriti posebnu bazu podataka.

Kao alternativa podaci bi se mogli uzimati i čuvati na drugom sigurnom mjestu u EU-u. Analitičari i stručnjaci iz SAD-a ovlašteni za vršenje pretraživanja mogli bi biti fizički prisutni u prostorijama imenovanog davatelja podataka ili bi podacima mogli imati pristup na daljinu. U oba slučaja i bez obzira na to gdje se nalaze podaci trebalo bi uspostaviti sveobuhvatne i čvrste zaštitne mehanizme koji bi bili prilagođeni posebnim značajkama sustava.

2.3.2. Ekvivalentni sustav EU-a

Izvršena je procjena niza mogućnosti za ekvivalentni sustav EU-a (kako su navedene u Komunikaciji iz 2011), uključujući potpuno centraliziran sustav na razini EU-a, decentralizirani sustav na razini država članica i tri mješovita sustava u kojima bi ulogu imali i EU i države članice.

Unutar svake mogućnosti postoje različite podmogućnosti u pogledu područja primjene sustava EU-a. Potrebno je donijeti odluke u pogledu vrste poruka i imenovanih davatelja podataka koji bi bili uključeni u sustav. U okviru ekvivalentnog sustava EU-a mogle bi se primjenjivati iste vrste poruka i koristiti usluge istog imenovanog davatelja podataka kao u trenutačnom Sporazumu o TFTP-u između EU-a i SAD-a, ali bi mogao uključivati i druge vrste poruka i davatelja.

- Mogućnost potpuno centraliziranog sustava na razini EU-a značilo bi da jedno tijelo EU-a vrši sve ključne funkcije sustava: podnošenje zahtjeva za uzimanje podataka, pohranu podataka, pretraživanje, obavještajnu analizu, zaštitu i nadzor sustava i distribuciju važnih obavještajnih podataka državama članicama. Ta mogućnost ne bi bila pravno valjana jer ne bi bila u skladu s člankom 72. Ugovora o funkcioniranju Europske unije, u kojem se potvrđuje da odgovornost za očuvanje javnog poretka i zaštitu unutarnje sigurnosti snose prvenstveno države članice. Takav sustav ne bi bio izvediv niti prihvatljiv državama članicama jer bi zahtijevao stvaranje jedne vrste centraliziranih obavještajnih kapaciteta na razini EU-a.

- Potpuno decentraliziran sustav na razini država članica značio bi da bi sustav vodila nadležna tijela država članica i da se nijedna funkcija ne vrši na razini EU-a. To bi značilo da bi se podaci mogli usporedno prenositi u svih 28 država članica i da bi ih one mogle pretraživati. Primjenom te mogućnosti višestruko bi se povećao broj tokova podataka, što bi imalo značajne posljedice u pogledu troškova. To bi isto tako dovelo do povećanog rizika od nedosljednog postupanja s podacima te stvaranja nejednakih mehanizama zaštite podataka. Stoga se ta mogućnost ne smatra održivom.

Zato te dvije mogućnosti nisu uzete u obzir za detaljniju procjenu.

Preostale tri mogućnosti za ekvivalentni sustav EU-a uključuju podjelu različitih funkcija između različitih organizacija na razini EU-a i nacionalnoj razini („mješoviti sustavi").

U svim tim mješovitim sustavima zahtjevi za podacima morali bi se podnositi imenovanim davateljima podataka kontinuirano i svaki put iznova, nakon čega bi se preuzimali i pohranjivali u bazu podataka na sigurnom mjestu u EU-u. Pretraživanja bi se nakon toga vršila u toj središnjoj bazi podataka. Slično kao i kod drugih mogućnosti, trebalo bi uspostaviti primjerene mehanizme zaštite podataka.

- A) U slučaju prvog mješovitog sustava, tj. službe za koordinaciju i analizu u okviru EU TFTS-a,trebalo bi osnovati središnju jedinicu na razini EU-a. Ona bi bila zadužena za traženje podataka od imenovanih davatelja podataka, pretraživanje, analizu obavještajnih podataka i dijeljenje rezultata. Razlika u odnosu na potpuno centralizirani sustav bila bi to da bi države članice imale izravan pristup sustavu i mogle tražiti od središnje jedinice da vrši pretraživanja u njihovo ime ili bi to mogli raditi njihovi vlastiti analitičari.
- B) Drugi mješoviti sustav, služba za uzimanje podataka u okviru EU TFTS-a, isto bi tako uključivao osnivanje središnje jedinice na razini EU-a. Međutim, u ovom bi slučaju tijelo EU-a vršilo pretraživanja na zahtjev država članica i rezultate dijelilo državama članicama bez analize obavještajnih podataka. Tijelo EU-a ipak bi moglo vršiti i svoja vlastita pretraživanja i analizu njihovih rezultata.

- C) Posljednji mješoviti sustav, osnovala bi se služba za koordinaciju Financijsko-obavještajnih jedinica[8] (FIU-ovi), *ad-hoc* platforma EU-a. To ne bi bilo stalno tijelo, nego skupina stručnjaka za financijske obavještajne podatke koji održavaju sastanke. U tu bi se svrhu mogla nadograditi platforma FIU-a. Svaka bi država članica kandidirala po jednog predstavnika koji bi je zastupao. To *ad hoc* tijelo prikupljalo bi zahtjeve iz FIU-ova svake države članice i na osnovi tih zahtjeva država članica podnosilo zahtjeve za podatke koje dostavljaju imenovani davatelji podataka. Predstavnik svake države članice u njezino bi ime bio odgovoran za pretraživanje i analizu te obradu rezultata. Nakon toga bi nadležna tijela država članica po svojem nahođenju koristila važne obavještajne podatke i dalje ih dijelila na nacionalnoj razini.

2.3.3. Status quo: Sporazum o TFTP-u između EU-a i SAD-a,

EU i države članice trenutačno mogu od SAD-a zatražiti da vrši pretraživanja na temelju Sporazuma o TFTP-u između EU-a i SAD-a, kojim se uređuje obrada i prijenos podataka iz financijskih poruka iz Europske unije Sjedinjenim Državama za namjene Programa za praćenje financiranja terorizma.

TFTP je alat za borbu protiv terorizma koji je SAD razvio nakon terorističkih napada 11. rujna 2001. Temelji se na pretraživanju podataka koje dostavlja imenovani davatelj podataka, uključujući podatke koji se prenose iz EU-a.

Sporazumom o TFTP-u između EU-a i SAD-a u potpunosti se uređuje postupak kojime tijela SAD-a podnose zahtjeve za podatke. Europol potvrđuje da su zahtjevi SAD-a u skladu sa Sporazumom te posebno da su što preciznije formulirani, kako bi količina podataka koji se prenose bila minimalna. Sigurnost postupanja s podacima te njihova pohranjivanja i brisanja uređuje se brojnim odredbama. Dostavljeni se podaci čuvaju u fizički sigurnom okruženju i pohranjuju odvojeno od drugih podataka. Sporazumom se propisuje razdoblje zadržavanja od pet godina te obveza redovite procjene potrebe za zadržavanjem podataka. Neovisni nadzornici nalaze se u SAD-u, a među njima su i dva nadzornika koja bira EU. Oni provode stalni nadzor načina na koji se upravlja sustavom i u mogućnosti su provjeravati svako pretraživanje koje vrši Ministarstvo financija SAD-a, kako bi se osiguralo da predmet pretraživanja bude povezan s terorizmom ili njegovim financiranjem.

[8] Odluka od 17. listopada 2000. o uređenju suradnje između financijsko-obavještajnih jedinica država članica vezano uz razmjenu informacija.

Sporazum sadržava i odredbe o pravu pristupa osobnim podacima i pravu na njihov ispravak te o postupcima traženja pravnog lijeka. U Sporazumu se predviđa da svaka osoba koja smatra da su se njezini osobni podaci obrađivali u suprotnosti s odredbama Sporazuma može tražiti učinkovit pravni lijek administrativnim ili sudskim putem, u skladu sa zakonodavstvom EU-a, njegovih država članica ili Sjedinjenih Američkih Država, ovisno o slučaju. U Sporazumu se definira kojim je osobama, neovisno o njihovu državljanstvu ili zemlji boravka, na raspolaganju postupak sudskog traženja pravnog lijeka u vezi sa štetnim administrativnim postupcima.

Mjerodavni pravni akti za traženje pravnog lijeka u odnosu na štetne administrativne postupke MInistarstva financija SAD-a u vezi s osobnim podacima dobivenima u skladu sa Sporazumom uključuju Zakon o upravnom postupku i Zakon o slobodi informiranja. Zakonom o upravnom postupku osobama koje su pretrpjele štetu uslijed postupaka Vlade SAD-a omogućuje se sudsko preispitivanje takvih postupaka. Zakonom o slobodi informiranja osobama koje traže pravni lijek administrativnim ili sudskim putem omogućuje se traženje državnih spisa. Postojeći jedinstveni postupci u pogledu pristupa osobnim podacima i/ili njihova ispravka, brisanja ili blokiranja, o kojima su se dogovorili Komisija i SAD, i postojanje Radne skupine iz članka 29. imaju za cilj građanima EU-a olakšati ostvarivanje tih prava. Provedba Sporazuma te njegovi zaštitni mehanizmi i provjere podliježu redovitim preispitivanjima u skladu s člankom 13. Sporazuma. Dva su takva preispitivanja provedena u 2011.[9] i 2012.[10] te je zaključeno da se Sporazum propisno provodi. Treće se preispitivanje planira za 2014. Iz Zajedničkog izvješća o vrijednosti dostavljenih podataka koje je sastavljeno u skladu s člankom 6. Sporazuma vidljive su prednosti TFTP-a u sprečavanju i borbi protiv terorizma te njegova financiranja, odnosno koristi koje je od Sporazuma imalo nekoliko država članica. Informacije dobivene u okviru TFTP-a zahvaljujući svojoj točnosti omogućuju identificiranje i praćenje terorista i njihovih mreža za potporu širom svijeta. Njima se pruža uvid u postojeće financijske strukture terorističkih organizacija i omogućuje utvrđivanje novih tokova financijske podrške i subjekata koji u njima sudjeluju.

[9] SEC (2011) 438 od 30. ožujka 2011.
[10] COM(2012) 454 od 14. prosinca 2012.

3. PROCJENA

Pri procjeni potrebe za predlaganjem osnivanja EU TFTS-a Komisija mora približiti različita stajališta i očekivanja u pogledu ambicioznosti sustava EU-a. Različiti dionici i donositelji odluka imaju različite predodžbe o ciljevima EU TFTS-a. Komisija je ispitala mogućnosti i moguće posljedice obaju scenarija u odnosu na načela razvoja i provedbu ranije opisanih novih inicijativa za vođenje politika. Svaka je od mogućnosti procijenjena posebno u odnosu na nužnost, proporcionalnost i isplativost.

3.1. Okvir za uzimanje podataka na teritoriju EU-a

Kako je opisano u odjeljku 2. 3. 1., mogućnost režima zadržavanja i uzimanja podataka poslužila bi kao način da se prikupljanje, pohrana i pretraživanje podataka, koji se trenutačno prenose u SAD u skladu sa Sporazumom o TFTP-u između EU-a i SAD-a, vrši na tlu EU-a. Na taj način u odnosu na sadašnje stanje za EU i države članice ne bi bili ostvareni dodatni pozitivni učinci u pogledu obavještajnih podataka. Naprotiv, uz pohranu podataka dobivenih u okviru TFTP-a u EU-u i SAD-u došlo bi do rascjepkanosti pretraživanja, koja se trenutačno vrše u odnosu na jedan skup podataka iz TFTP-a, što bi negativno utjecalo na kvalitetu i broj važnih obavještajnih podataka i pogoršalo ukupnu učinkovitost TFTP-a. Time bi se znatno usporio postupak analize jer bi za daljnji postupak u vezi s važnim obavještajnim podacima mogla biti potrebna uzastopna pretraživanja podataka iz TFTP-a pohranjenih na dva mjesta. U istragama o terorizmu brzina je često od iznimne važnosti.

Uzimanjem podataka na europskom tlu umjesto u SAD-u ne bi se sama po sebi mogla jamčiti bolja zaštita osobnih podataka. Zaštita pristupa podacima ključ je primjerenog postupanja s podacima, bez obzira na to gdje se nalaze. S tim bi ciljem trebalo uspostaviti niz čvrstih zaštitnih mehanizama kojima bi se jamčila sukladnost obrade podataka s važećim zahtjevima. U okviru sustava morala bi postojati kontrolna funkcija za provjeru zahtjeva za vršenje pretraživanja i njihove opravdanosti. Kako bi se osiguralo da se podaci koriste u ograničene svrhe koje se definiraju sporazumom o osnivanju, ključna bi bila uloga neovisnih nadzornika. Trebalo bi poduzeti mjere za sprečavanje neovlaštenog pristupa ili otkrivanja podataka, primjerice čuvanje podataka u sigurnom fizičkom okruženju. U sustav bi morali biti ugrađeni postupci za pristup osobnim podacima i njihov ispravak te odgovarajući postupci pravnog lijeka. Za osiguranje ispravnog funkcioniranja sustava bilo bi potrebno naručiti vanjsku reviziju.

U skladu Sporazuma o TFTP-u između EU-a i SAD-a, SAD nema pristup svim podacima imenovanog ddavatelja podataka, nego samo za skupove podataka koje SAD zatraži, a Europol odobri na temelju prethodnih i trenutačnih analiza rizika u vezi s terorizmom. Ako se ne uspostavi sličan mehanizam za početni uži odabir zahtjeva za dostavu podataka, omogućivanjem izravnog pretraživanja svih podataka imenovanog davatelja došlo bi do daljnjeg otkrivanja podataka, što bi imalo učinak na prava u vezi sa zaštitom podataka. To bi zahtijevalo znatne promjene u načinu rada imenovanog davatelja podataka i načinu pohrane njegovih podataka. Trenutačno se financijske poruke koje su obuhvaćene Sporazumom čuvaju u obliku koji ne dopušta utvrđivanje identiteta osoba koje se spominju u podacima iz poruka. Svaka se financijska poruka kodira i može se pretraživati samo prema metapodacima, tj. datumu slanja, vrsti poruke te banka pošiljatelj i banka primatelj. Imenovani davatelj podataka primjenjuje čvrste mehanizme sigurnosti i zaštite podataka kako bi zaštitio podatke svojih klijenata širom svijeta. Stoga, kako bi se omogućilo izravno pretraživanje na poslužitelju imenovanog davatelja podataka, sve se te poruke najprije moraju dekodirati. Takav bi postupak bio pretjeran i neproporcionalan jer se na poslužitelju imenovanog davatelja podataka nalaze i druge poruke uz one koje se traže u svrhu borbe protiv financiranja terorizma. Osim toga, izravan pristup u svrhu pretraživanja nedopušteno bi ometao svakodnevno funkcioniranje imenovanog davatelja podataka te bi na taj način došlo do znatnih operativnih, sigurnosnih i sistemskih rizika. Stoga bi u ovom slučaju trebalo stvoriti posebnu bazu podataka na teritoriju EU-a, koja bi sadržavala potrebne podatke dobivene od imenovanog davatelja podataka.

Za uspostavljanje sustava i jamčenje njegove pune sukladnosti sa zaštitnim mehanizmima bila bi potrebna znatna ulaganja. Trebalo bi prostorije imenovanog davatelja podataka ili neko drugo sigurno mjesto prilagoditi posebnim zahtjevima, isto bi tako trebalo razviti i održavati odgovarajuće IT i tehničke mehanizme te zaposliti i osposobiti kvalificirano osoblje koje bi nadziralo sustav i njime upravljalo.

U slučaju primjene ove mogućnosti EU i države članice snosili bi sve negativne posljedice i troškove mehanizma uspostavljenog samo za potrebe TFTP-a, instrumenta u vlasništvu treće zemlje. Ova se mogućnost trenutačno ne čini nužnom, proporcionalnom ili isplativom jer ne bi dovela do pozitivnih učinaka u pogledu obavještajnih podataka, bila bi skupa i zahtjevna za realizaciju, a isto bi tako dovela do rizika za zaštitu osobnih podataka.

3.2. Ekvivalentni sustav EU-a

Potpuno centraliziran EU TFTS nije uzet u obzir za detaljniju procjenu zbog pravne neosnovanosti i male vjerojatnosti da bi države članice prihvatile središnju ulogu EU-a u području njihove nadležnosti. Potpuno decentraliziran sustav isključen je zato što bi prouzročio iznimno visoke troškove te višestruko povećao učinak na prava u vezi sa zaštitom podataka. Primjenom triju mješovitih sustava za koje je izvršena procjena omogućile bi se različite razine nadzora država članica nad pretraživanjima koja provode one same ili centralizirano tijelo EU-a.

Proširenjem područja primjene ekvivalentnog sustava EU-a na sustave tipa Automated Clearing House, elektronički novac i druge podatke koji nisu sadržani u FIN-porukama omogućili bi se pozitivni učinci tako što bi EU bio u stanju bolje pratiti plaćanja unutar EU-a te bi se tako stvorio napredniji sustav od onoga koji radi samo sa FIN-porukama. Međutim svakim novim dodavanjem imenovanog davatelja podataka povećao bi se rizik kršenja prava u vezi sa zaštitom podataka te bi stoga bio potreban kompaktan skup uvjeta, zaštitnih mehanizama i mjera nadzora. Time bi se imenovani davatelji podataka izložili dodatnom administrativnom opterećenju. Dodavanjem više davatelja podataka i poruka u cilju stvaranja složenog sustava koji bi organizacijski i tehnički zahtjevan došlo bi i do znatnog povećanja troškova.

Iz ove analize proizlazi da bi bilo kakav EU TFTS koristio samo podatke iz FIN-poruka jer Komisija smatra da pozitivni učinci korištenja više tipova podataka i davatelja podataka ne pravdaju znatne troškove za privatna poduzeća i narušavanje prava u pogledu privatnosti i zaštite podataka koje bi takav sustav podrazumijevao. Stoga, budući da bi sustav EU-a uključivao istog imenovanog davatelja podataka i istu vrstu poruka kao i TFTP, kvaliteta i količina dobivenih važnih obavještajnih informacija kao i razina otkrivanja informacija bile bi usporedive sa onima u okviru Sporazuma o TFTP-u između EU-a i SAD-a.

Kao što je prethodno naznačeno, postoje tri mogućnosti za takav ekvivalentni sustav EU-a. A) služba za koordinaciju i analizu u okviru EU TFTS-a, B) služba za uzimanje podataka u okviru EU TFTS-a i C) služba za koordinaciju Financijsko-obavještajnih jedinica.

Mogućnost A vjerojatno bi imala pozitivan učinak na sprečavanje terorizma i poboljšanje sigurnosti u EU-u. U slučaju da pretraživanja i analize rezultata vrše timovi EU-a i država

članica moglo bi se u izvjesnoj mjeri osigurati da se u obzir uzimaju posebni zahtjevi EU-a i država članica u vezi s obavještajnim podacima te da sustav bude više orijentiran na opasnosti koje prijete EU-u. Međutim, takva poboljšanja ovise o većoj spremnosti i sposobnosti država članica da srednjoročno i dugoročno dijele informacije. Nije sasvim jasno koliko se može računati na takav povećani priliv informacija. Uz to, budući da bi države članice zadržale pravo tražiti pretraživanja od SAD-a u okviru TFTP-a, bilo bi potrebno da države taj sustav u velikoj mjeri podupru i s njim surađuju kako bi se ostvarila dosljednija politika na razini EU-a.

Mogućnost B mogla bi imati pozitivan učinak na sprečavanje terorizma i poboljšanje sigurnosti u EU-a. Taj bi sustav bolje odgovarao potrebama analize prijetnji u EU-u, jer bi se pretraživanja vršila u skladu sa specifičnim potrebama država članica za obavještajnim podacima. Međutim, uloga centraliziranog tijela EU-a ograničila bi se na vršenje pretraživanja i prijenos dobivenih podataka u državu članicu koja ih traži; ta bi se uloga prvenstveno odnosila na čuvanje pristupa podacima. Kao rezultat toga ne bi postojala analiza na razini EU-a i sustav bi u potpunosti ovisio o tome koliko će države članice međusobno razmjenjivati analize izvan sustava kako bi se ostvarila dosljednija politika na razini EU-a. Nemogućnost sustava da jamči jedinstven pristup definiranju pretraga dovela bi do povećane opasnosti od dobivanja lažnih pozitivnih rezultata, što bi imalo negativan učinak na prava u području zaštite podataka i privatnosti.

Mogućnost C bolje bi odgovarala specifičnim potrebama država članica za obavještajnim podacima te tako imao pozitivan učinak na sprečavanje terorizma i poboljšanje sigurnosti. Međutim, budući da bi nacionalni FIU-ovi bili odgovorni za vršenje pretraživanja i analiza dotičnih država članica, ta mogućnost pokazuje iste slabosti kao i mogućnost B – jasan bi se prikaz situacije mogao dobiti samo poboljšanom suradnjom između država članica, izvan sustava. Uz to, usmjerenost FIU-ova isključivo na financijske obavještajne podatke te podjela koja nastane između tih podataka i šireg područja obavještajnih podataka mogla bi otežati uočavanje veza i otkrivanje financiranja terorizma. U okviru ove mogućnosti isto tako postoji veoma niska razina uključivanja EU-a i sposobnost djelovanja prvenstveno bi se poboljšala na nacionalnoj razini.

Sve bi te mogućnosti uključivale znatne troškove za EU, države članice i imenovanog davatelja podataka, uključujući, između ostalog, troškove razvoja IT infrastrukture, sigurnih

objekata te troškove za desetke, ako ne i stotine, članova osoblja koje bi bilo odgovorno za upravljanje sustavom i provedbu zaštitnih mehanizama i kontrola. Međutim, svaki od tih mogućih sustava u stanju je pridonijeti poboljšanju sigurnosne situacije u Europi jer bi se u njihovu okviru vršile procjene rizika prema europskim potrebama.

Postojanjem neovisnog obavještajnog i istražnog mehanizma na europskom tlu prestala bi potreba za prijenosom podataka u SAD. Ali za bilo kakvu vrstu EU TFTS-a bili bi potrebni opsežni mehanizmi zaštite podataka i kontrole koji su već na snazi u okviru Sporazuma o TFTP-u između EU-a i SAD-a i koji su u svakom slučaju sukladni s pravnom stečevinom EU-a i država članica. Trebalo bi provjeravati sukladnost svakog zahtjeva za pretraživanje podataka u sustavima EU-a sa strogim ograničenjima primjene u svrhu borbe protiv terorizma i njegova financiranja, između ostalog i o tome je li prijenos podataka opravdan. Posebno bi bili potrebni neovisni nadzornici kako bi se provjerilo jesu li sva pretraživanja koja vrše EU i države članice propisno odobrena te jesu li potrebna u svrhu borbe protiv terorizma i njegova financiranja. Moralo bi se osigurati sigurno rukovanje podacima i njihova pohrana te spriječiti neovlašten pristup podacima. Bila bi potrebna vanjska revizija propisnog funkcioniranja sustava i svih njegovih zaštitnih mehanizama. U sustav bi morali biti uključeni svi potrebni postupci za pristup osobnim podacima i njihovo brisanje te odgovarajući postupci traženja pravnog lijeka.

Prema tome, Komisija je skladu sa zahtjevima Europskog parlamenta i Vijeća procijenila postojeće mogućnosti za uspostavljanje EU TFTS-a, uključujući režim uzimanja i zadržavanja podataka.

U procjeni se uzimaju u obzir načela iz Strategije upravljanja informacijama donesene tijekom švedskog predsjedanja. Svaki uspostavljeni sustav mora biti nužan, proporcionalan i isplativ, uz poštovanje temeljnih prava. Iz analize koju je izvršila Komisija, kako je podrobnije opisano u prethodnom tekstu i u Procjeni učinka, vidljivo je da svaka od izvedivih mogućnosti ima svoje prednosti i nedostatke. Komisija, međutim, nije uzela obzir mogućnosti koje nisu izvedive, kako je objašnjeno u tekstu.

U svjetlu prikupljenih informacija, nije jasno dokazana potreba da se u ovoj fazi iznese prijedlog za uspostavljanje EU TFTS-a.

Komisija poziva Europski parlament i Vijeće da iznesu mišljenje o ovoj Komunikaciji.