EUROPOS KOMISIJA

Briuselis, 2011.7.13
KOM(2011) 429 galutinis

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Europos terorizmo finansavimo sekimo sistema. Turimos galimybės

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Europos terorizmo finansavimo sekimo sistema. Turimos galimybės

1. ĮŽANGA

Taryba, pritardama Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimo dėl finansinių mokėjimų pranešimų duomenų tvarkymo ir perdavimo iš Europos Sąjungos į Jungtines Valstijas Terorizmo finansavimo sekimo programos tikslais (toliau – ES ir JAV TFSP susitarimas) sudarymui[1], paprašė Komisiją Europos Parlamentui ir Tarybai per vienus metus nuo susitarimo įsigaliojimo dienos (2010 m. rugpjūčio 1 d.) pateikti „teisinį ir techninį duomenų atrinkimo ES teritorijoje pagrindą“[2]. Europos Parlamentas taip pat nuolat ragino ilgesniu laikotarpiu numatyti tvarų ir teisiškai pagrįstą Europos sprendimą dėl prašomų duomenų atrinkimo Europos teritorijoje[3]. Komunikate „ES vidaus saugumo strategijos įgyvendinimas. Penki žingsniai kuriant saugesnę Europą“ jau nurodyta, kad Komisija 2011 m. suformuos ES teritorijoje turimų finansinių mokėjimų pranešimų duomenų atrinkimo ir analizavimo politiką[4]. Turint omenyje jau įrodytą JAV TFSP veiksmingumą, tikimasi, kad Europos sistema labai prisidėtų prie veiksmų, kuriais teroristams trukdoma gauti lėšų, medžiagų ir sekami jų sandoriai. Taip pat galima daryti nuorodą į ES ir JAV TFSP susitarimo 11 straipsnį, kuriame nurodoma, kad šio susitarimo laikotarpiu Europos Komisija atliks tyrimą dėl galimo lygiavertės ES sistemos, kuria būtų sudarytos tikslesnio duomenų perdavimo galimybės, kūrimo. Šis komunikatas yra pirmas Komisijos reakcijos į šią straipsnio nuostatą ir Tarybos raginimą etapas. Jame aprašomi įvairūs veiksmai, kurių Komisija ėmėsi, kad sukurtų tokį „teisinį ir techninį pagrindą“, ir pateikiamos įvairios svarstomos galimybės, kaip pasiekti šį tikslą. Šiame etape nenurodoma tinkamiausia galimybė, tačiau pateikiami argumentai, į kuriuos reikėtų atkreipti dėmesį svarstant galimybes. Atsižvelgdama į klausimo politinę svarbą ir teisinį bei techninį sudėtingumą, Komisija nori informuoti Tarybą ir Europos Parlamentą apie esamą padėtį ir paskatinti diskusijas. Komisija mano, kad tokios tolesnės diskusijos reikalingos prieš pateikiant konkrečius pasiūlymus (remiantis poveikio vertinimu).

Kartu reikėtų pabrėžti, kad šiuo komunikatu nėra iš anksto nusprendžiama dėl pasiūlymo, kurį pateiks Komisija. Bet kuriame būsimame pasiūlyme bus atsižvelgta į pirmiau minėtas diskusijas ir poveikio vertinimą, kuris bus pagrįstas tyrimu, kurį Komisija užsakė atlikti antrojoje 2010 m. pusėje. Atsižvelgiant į poveikį, kurį teisės akto pasiūlymas turėtų pagrindinėms teisėms ir pirmiausia duomenų apsaugai, poveikio vertinime ypatingas dėmesys bus skiriamas bet kurių priemonių, kurias gali pasiūlyti Komisija, būtinumui ir proporcingumui. Šiuo tikslu Komisija laikysis gairių, pateiktų Komunikate dėl veiksmingo Pagrindinių teisių chartijos įgyvendinimo strategijos[5].

---

1 OL L 195, 2010 7 27, p. 5.
2 2010 m. liepos 13 d. Tarybos sprendimas, OL L 195, 2010 7 27, p. 3.
3 Žr., pvz., Rezoliuciją P7_TA(2010)0143 ir Rekomendacijos A7-0224/2010 aiškinamąjį memorandumą.
4 COM(2010) 673 galutinis, 2010 11 22. Žr. 2 tikslo 2 veiksmą, p. 8.
5 COM(2010) 573 galutinis, 2010 10 19.

Be to, poveikio vertinime bus pateikta reikalinga techninio pobūdžio medžiaga, taip pat išsamus visų turimų galimybių vertinimas. Dėl šių klausimų jau diskutuota su daugeliu šios srities suinteresuotųjų subjektų, įskaitant valstybių narių valdžios institucijas, duomenų apsaugos institucijas, Europolą ir paskirtąjį paslaugų teikėją. Galutiniai pirmiau paminėto tyrimo rezultatai bus pateikti tik šių metų pabaigoje. Siekdama padėti parengti poveikio vertinimą, Europos Komisija surengė tris ekspertų posėdžius su tais pačiais suinteresuotaisiais subjektais, taip pat JAV valdžios institucijomis, valdančiomis TFSP. Šiame komunikate aptariamos galimybės grindžiamos preliminariais tyrimo rezultatais ir šių ekspertų posėdžių diskusijomis.

2. ES TERORIZMO FINANSAVIMO SEKIMO SISTEMOS SUKŪRIMO TIKSLAI

Yra dvi pagrindinės priežastys sukurti ES terorizmo finansavimo sekimo sistemą (TFSS):

- sistema turi veiksmingai prisidėti prie kovos su terorizmu ir jo finansavimu Europos Sąjungoje;

- sistema turi padėti sumažinti trečiosioms šalims perduodamų asmens duomenų kiekį. Sistema turėtų suteikti galimybę reikalaujamus duomenis tvarkyti ES teritorijoje, atsižvelgiant į ES duomenų apsaugos principus ir teisės aktus.

Jau įrodyta, kad Jungtinėse Valstijose Terorizmo finansavimo sekimo programa (TFSP) turi didelę papildomą vertę kovojant su terorizmu ir jo finansavimu ir yra naudinga ne tik JAV valdžios institucijoms, bet ir Europos Sąjungos valstybių narių valdžios institucijoms bei trečiosioms šalims. Naujausioje ES ir JAV TFSP susitarimo peržiūroje[6] patvirtinta, kad nuo TFSP sukūrimo JAV su trečiųjų šalių valdžios institucijomis pasidalyta daugiau kaip 2 500 ataskaitų, daugiausia (1 700) – su Europos Sąjunga. JAV programos veiksmingumas ir jos vertė kovojant su terorizmu ir jo finansavimu taip pat patvirtinti teisėjo J. L. Bruguière, kurį 2008 m. Europos Komisija paskyrė peržiūrėti programą, pateiktose dviejose ataskaitose. Informacijoje, kurią ES valdžios institucijos gavo vykdant TFTP, buvo vertingų duomenų apie kelis didelio masto (bandymus įvykdyti) teroro aktus, kaip antai Madride ir Londone, 2006 m. sąmokslą susprogdinti transatlantinių skrydžių lėktuvus panaudojant skystus sprogmenis ir 2007 m. mėginimą pakenkti JAV interesams Vokietijoje. ES peržiūros grupė taip pat padarė išvadą, kad jai pateikta „įtikinamos informacijos apie TFSP pridėtinę vertę kovojant su terorizmu ir jo finansavimu“. Atsižvelgiant į šią patirtį yra tvirto pagrindo manyti, kad ES TFSS taip pat suteiks didelės papildomos vertės ES ir valstybių narių pastangoms kovoti su terorizmu ir jo finansavimu.

Nors JAV TFSP veiksmingumu kovojant su terorizmu ir jo finansavimu neabejojama, išreikštas didelis susirūpinimas dėl jos pasekmių piliečių pagrindinėms teisėms. Šis susirūpinimas labiausiai grindžiamas tuo, kad įgyvendinant ES ir JAV TFSP susitarimą JAV valdžios institucijoms teikiami dideli kiekiai asmens duomenų – didžioji šių duomenų dalis yra apie piliečius, kurie niekaip nesusiję su terorizmu ar jo finansavimu. Duomenys pateikiami dideliais kiekiais (remiantis atitinkamomis duomenų kategorijomis), o ne konkretūs duomenys kiekvienu atveju (reaguojant į prašymą dėl vieno ar daugiau asmenų), nes šių duomenų teikėjas neturi techninių galimybių pateikti konkrečių duomenų. Be to, siekiant, kad teikėjas suteiktų tokius konkrečius duomenis kiekvienu atveju, reikėtų sukurti

[6] SEC(2011) 438 galutinis, 2011 3 30.

specialią paieškos ir analizės funkciją, kuri verslo procesams nebūtina, ir tai reikštų dideles išlaidas. Be to, jeigu kiekvienu atveju būtų prašoma konkrečių duomenų, tai reikštų, kad teikėjas sužinotų asmenis, dėl kurių vykdomas su terorizmu susijęs tyrimas, ir jų finansinius ryšius. Tai galėtų turėti įtakos tokių tyrimų veiksmingumui.

Siekiant kompensuoti duomenų teikimą dideliais kiekiais, nustatytos svarbios apsaugos priemonės, kuriomis būtų užtikrinta, kad nebūtų įmanomas joks netinkamas duomenų naudojimas, įskaitant tai, kad atlikti pateiktų duomenų paiešką ir jais naudotis būtų galima tik kovos su terorizmu ir jo finansavimu tikslais. Naujausia ES ir JAV TFSP susitarimo peržiūra patvirtinta, kad šios apsaugos priemonės tikrai įgyvendintos laikantis susitarimo nuostatų.

Nepaisant to, pateikta argumentų, kad asmens duomenų teikimas tokiais dideliais kiekiais trečiajai šaliai yra nepateisinamas piliečių pagrindinių teisių pažeidimas, atsižvelgiant į šio pažeidimo būtinumą ir proporcingumą. Dėl šios priežasties Taryba paragino Komisiją pateikti pasiūlymus sukurti duomenų atrinkimo, vykdomo ES teritorijoje, sistemą – pagrindinis tikslas yra užtikrinti, kad tokie duomenys būtų tvarkomi laikantis ES duomenų apsaugos teisės aktų ir principų ir atsižvelgiant į ES pagrindinių teisių chartiją. Kartu reikėtų pabrėžti, kad valdžios institucijų vykdomas finansinių duomenų rinkimas ir tvarkymas turi įtakos teisei į asmens duomenų apsaugą, kuri įtvirtinta SESV 16 straipsnyje ir Chartijos 8 straipsnyje.

Pagal Chartijos 52 straipsnio 1 dalį bet koks šių pagrindinių teisių įgyvendinimo apribojimas turi būti numatytas įstatymo, būti pakankamai tikslus ir kokybiškas, kad užtikrintų numatomumą, ir nekeisti šių teisių esmės. Šis apribojimas turi būti būtinas ir proporcingas įgyvendintinam Sąjungos pripažintam teisėtam tikslui. Dėl šios priežasties į šiuos principus būtina atsižvelgti ne tik priimant sprendimą, ar reikėtų sukurti ES TFSS, bet ir svarstant įvairias turimas sistemos įgyvendinimo galimybes. Todėl šie principai taip pat turi įtaką priimant sprendimą dėl tokių klausimų kaip sistemos taikymo sritis, nustatytini saugojimo laikotarpiai, asmenų teisės susipažinti su duomenimis ir juos ištrinti ir pan. Šie klausimai dabartiniame komunikate išsamiai neaptarti. Juos reikės visapusiškai išanalizuoti poveikio vertinime.

Suprantama, galimas duomenų atrinkimo ES teritorijoje sistemos sukūrimas turėtų įtakos esamam ES ir JAV TFSP susitarimui, kaip pripažinta susitarimo 11 straipsnio 3 dalyje, kur nurodyta, kad sukūrus ES sistemą šio susitarimo aplinkybės galėtų gerokai pasikeisti, todėl Šalys turėtų konsultuotis ir nustatyti, ar šį susitarimą reikėtų atitinkamai patikslinti, jei Europos Sąjunga nuspręstų sukurti tokią sistemą. Todėl visos galimybės taip pat turėtų įtakos būsimam esamo ES ir JAV TFSP susitarimo įgyvendinimui ir vėlesniam patikslinimui.

3. ES TERORIZMO FINANSAVIMO SEKIMO SISTEMOS PAGRINDINĖS FUNKCIJOS

Vienas iš pirmųjų klausimų, iškilusių per pirmiau minėtas diskusijas su suinteresuotaisiais subjektais, buvo tas, kad, daugumos nuomone, jeigu būtų kuriama ES terorizmo finansavimo sekimo sistema (ES TFSS), tai turėtų būti daroma siekiant užtikrinti ES piliečių saugumą. Sistema neturėtų būti kuriama tik tam, kad suteiktų reikiamos informacijos JAV valdžios institucijoms, – valstybių narių valdžios institucijos taip pat suinteresuotos tokios sistemos rezultatais. Šis požiūris taip pat reiškia, kad, nors atsižvelgiant į JAV TFSP tikrai galėtų kilti idėjų, kaip būtų galima sukurti tokią sistemą, lygiavertė Europos sistema nebūtinai turėtų turėti visus JAV TFSP elementus. Be to, ES sistema turėtų būti sukurta, atsižvelgiant į ES teisinės ir administracinės sistemos specifiškumą, įskaitant taikomų pagrindinių teisių, kaip nurodyta pirmiau, laikymąsi.

Tačiau kuriant bet kokią sistemą, kurios tikslas – sekti terorizmo finansavimą atsižvelgiant į pagrindinius pirmiau nurodytus tikslus, reikėtų numatyti įgyvendinti tokias svarbiausias funkcijas:

- rengti ir teikti (teisiškai galiojančius) prašymus paskirtajam finansinių mokėjimų pranešimų paslaugų teikėjui teikti neapdorotus duomenis įgaliotam (-iems) gavėjui (-ams). Tai reiškia, kad reikia apibrėžti prašytinas pranešimų kategorijas, nustatyti, kaip dažnai tokie pranešimai turėtų būti siunčiami, ir palaikyti ryšius su teikėjais šiais klausimais;

- stebėti paskirtajam (-iesiems) teikėjui (-ams) teikiamus prašymus dėl tokių neapdorotų duomenų ir juos patvirtinti. Kartu reikia patikrinti, ar prašymas dėl neapdorotų duomenų parengtas laikantis taikomų apribojimų;

- gauti ir saugoti (tvarkyti) paskirtojo (-ųjų) teikėjo (-ų) pateiktus neapdorotus duomenis, taip pat įgyvendinti tinkamą fizinio ir elektroninio duomenų saugumo sistemą;

- atlikti faktines pateiktų duomenų paieškas, laikantis taikomos teisinės sistemos ir remiantis valstybių narių valdžios institucijų, JAV ar kitų trečiųjų valstybių pagal aiškiai nustatytas sąlygas ir apsaugos priemones arba asmenine institucijos (ar institucijų), atsakingos (-ų) už duomenų tvarkymą, iniciatyva pateiktais tokių paieškų prašymais;

- stebėti ir tvirtinti tokias pateiktų duomenų paieškas;

- analizuoti paieškų rezultatus, juos derinant su kita turima informacija ar žvalgybos informacija;

- pateikti paieškų rezultatus (be tolesnės analizės) arba analizių rezultatus įgaliotiems gavėjams;

- įgyvendinti tinkamą duomenų apsaugos režimą, įskaitant taikomus saugojimo terminus, registravimo įpareigojimus, prašymų susipažinti su informacija, ją pataisyti ir ištrinti tvarkymą ir pan.

Šias svarbiausias funkcijas reikėtų nustatyti tinkamais teisės aktais ES lygiu, nacionaliniu lygiu arba abiem lygiais, atsižvelgiant į pasirinktą galimybę.

4. PAGRINDINIAI PRINCIPAI, Į KURIUOS REIKIA ATSIŽVELGTI SVARSANT TURIMAS GALIMYBES

Be svarstymų dėl pirmiau nurodytų svarbiausių funkcijų, vienos iš turimų galimybių pasirinkimas didele dalimi priklausys nuo to, kaip jomis sprendžiami tam tikri pagrindiniai klausimai, kurie šiuo metu svarstomi rengiamame poveikio vertinime ir išsamiau aptariami toliau.

4.1. Veiksmingumas

Svarbiausias veiksnys yra tikėtinas skirtingų galimybių veiksmingumas siekiant svarbiausio kovos su terorizmu ir jo finansavimu tikslo. Pirmenybė turėtų būti teikiama galimybėms, kuriomis suteikiamos didesnės keitimosi duomenimis ir jų analizės galimybės tarptautiniu lygiu, nes toks dalijimasis duomenimis ir jų analizė padidins veiksmingumą ir suteiks daugiau pridėtinės vertės. Visų pirma organizacijos (-ų), kuriai (-ioms) bus patikėta analizuoti

duomenis ir teikti analizės rezultatus reikiamoms institucijoms, pasirinkimas turės didelę įtaką bendram sistemos veiksmingumui, taip pat duomenų, kurie bus perduodami, kiekiui. Net ir tokiu atveju pagal dabartinę praktiką valstybės narės turėtų toliau išlaikyti visapusišką kontrolę, kokia jų informacija ar žvalgybos informacija gali būti dalijamasi su kitomis valdžios institucijomis.

4.2. Duomenų apsauga

Tarptautinis dalijimasis informacija ir žvalgybos informacija bei jos analizė gali būti vykdomi tik turint patikimą ir tinkamai sukurtą duomenų apsaugos sistemą. Tokios sistemos veiksmingumas priklauso ne tik nuo taikomų teisės nuostatų, kuriomis suteikiama galimybė duomenų subjektams naudotis savo teisėmis, kaip antai žalos atlyginimu teismo tvarka, bet ir nuo to, ar yra patyręs personalas, kaip antai nepriklausomas duomenų apsaugos pareigūnas ir nepriklausoma ir patyrusi duomenų apsaugos kontrolės institucija. Kai kurios organizacijos, kurios galėtų būti įtrauktos, jeigu būtų kuriama ES TFSS, jau turi tokias struktūras, kitos turėtų jas sukurti. Todėl reikia atidžiai įvertinti kiekvienos iš skirtingų galimybių poveikį duomenų apsaugai, atsižvelgiant į bendrus principus, susijusius su pagrindinių teisių, kaip nurodyta šio komunikato 2 dalyje, laikymusi.

4.3. Duomenų saugumas

Patikimas duomenų apsaugos nuostatas reikia derinti su moderniausia duomenų saugumo infrastruktūra ir technologijomis. Svarstant duomenų saugumo klausimus linkstama prie nuomonės, kad reikia apriboti vietų, kuriose galima tvarkyti pateiktus duomenis, skaičių, taip pat bet kokią išorinės prieigos prie duomenų galimybę. Saugiausias sprendimas būtų saugoti duomenis vienoje vietoje be jokios išorinės prieigos. Dauguma organizacijų, kurios galėtų dalyvauti TFSS valdyme, jau turi saugaus duomenų tvarkymo technologijas, bet kol kas ne visos turi pajėgumų tvarkyti duomenis, kurių saugumo lygis aukštesnis nei „EU Restricted“.

4.4. Duomenų saugojimas

Duomenys galėtų būti saugomi nacionaliniu arba ES lygiu. ES lygiu iš paskirtojo (-ųjų) teikėjo (-ų) gautus duomenis būtų galima saugoti Europole ar kitoje ES įstaigoje, kaip antai dabar kuriamoje Didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūroje (IT agentūroje)[7]. Kadangi duomenų saugojimas neatskiriamai susijęs su duomenų apsaugos ir saugumo klausimais, už duomenų saugojimą atsakingos organizacijos pasirinkimas turėtų būti glaudžiai susietas su duomenų apsaugos ir saugumo režimu, kurį šios organizacijos gali taikyti.

4.5. Naudojimasis esamomis struktūromis ir priemonėmis

Pagal visas galimybes turėtų būti numatyta kuo geriau naudotis esamomis struktūromis. Taip apribojamos išlaidos ir suteikiama galimybė pasinaudoti įgyta patirtimi ir esama infrastruktūra. Kad būtų galima taip naudotis esamomis priemonėmis, reikia, kad esamai organizacijai paskirtos naujos užduotys visapusiškai atitiktų tos organizacijos turimus įgaliojimus. Pavyzdžiui, Europolas, Eurojustas ar nacionalinės teisėsaugos institucijos gali būti laikomos tinkamomis institucijomis tikrinti ir tvirtinti prašymus pateikti duomenis, skirtus paskirtajam (-iesiems) teikėjui (-ams).

---

[7] COM(2010) 93 galutinis, 2010 3 19.

4.6. Atsakingų institucijų bendradarbiavimas

Toliau nurodytos galimybės skiriasi nacionalinių valdžios institucijų tarpusavio, taip pat nacionalinių ir Europos institucijų bendradarbiavimo ir dalijimosi informacija bei žvalgybos informacija apimtimi. Skirtingos valstybės narės yra nustačiusios skirtingus būdus, kaip jų nacionalinės valdžios institucijos bendradarbiauja kovodamos su terorizmu, ir bet kokiais veiksmais Europos lygiu reikia tinkamai atsižvelgti į SESV 72 straipsnyje nustatytus apribojimus dėl valstybių narių išimtinių teisių, kiek tai susiję su viešosios tvarkos palaikymu ir vidaus saugumo užtikrinimu. Todėl bet kokia ES TFSS turėtų būti užtikrinama, jog valstybės narės tikrai galėtų kontroliuoti, kokia informacija ir žvalgybos informacija jos sutinka pasidalyti pagal tokią sistemą. Kai kurios toliau paminėtos organizacijos išreiškė skirtingą požiūrį į šį klausimą ir kai kurios jų idėjos galėtų būti tiesiogiai pritaikytos kuriant sistemą.

4.7. Skirtingų galimybių galimo finansinio poveikio pirmoji bendra apžvalga

Bendros ES TFSS sukūrimo išlaidos ir jų paskirstymas ES ir nacionaliniu lygiu didele dalimi priklausys nuo pasirinktos politikos galimybės. Bet kokiu atveju išlaidas sudarys:

- išlaidos, susijusios su saugiu duomenų, gautų iš paskirtojo (-ųjų) teikėjo (-ų), perdavimu ir saugojimu;
- išlaidos, susijusios su programinės įrangos, reikalingos paieškoms atlikti ir paieškų rezultatams pateikti, plėtote ir priežiūra;
- išlaidos, susijusios su paieškos rezultatų ar duomenų analizės pateikimu įgaliotiems gavėjams;
- išlaidos personalui, atliekančiam paieškas ir duomenų analizę ir pateikiančiam rezultatus;
- išlaidos personalui, vykdančiam stebėjimo ir audito funkcijas;
- išlaidos personalui, atsakingam už duomenų apsaugą ir piliečių teises.

Nors išsamių duomenų dėl išlaidų šiame etape dar neturima, iš pradinių skaičiavimų matyti, kad įgyvendinant išimtinai ES lygio metodą ar bet kurias kitas mišrias toliau aptariamas galimybes pradinės sukūrimo išlaidos sudarytų 33–47 mln. EUR, o valdymo išlaidos kasmet siektų papildomus 7–11 mln. EUR. Šio komunikato 6 dalyje aprašytos įvairios galimybės. 3 galimybė būtų pati brangiausia: sukūrimo išlaidos ES siektų 43 mln. EUR, valstybėms narėms – 3,7 mln. EUR (visoms bendrai), o metinės valdymo išlaidos ES sudarytų 4,2 mln. EUR ir 6,8 mln. EUR valstybėms narėms (visoms bendrai). 2 galimybė būtų pigiausia: sukūrimo išlaidos ES siektų 33 mln. EUR, metinės ES lygio valdymo išlaidos – 3,5 mln. EUR, o valstybių narių metinės valdymo išlaidos sudarytų 3,3 mln. EUR (visoms bendrai). Pagal 1 galimybę sukurti sistemą ES kainuotų 40,5 mln. EUR, metinės ES lygio valdymo išlaidos siektų 4 mln. EUR, o valstybių narių – 5 mln. EUR (visoms bendrai). Žinoma, išlaidas būtų galima sumažinti, jei pavyktų pasinaudoti jau veikiančiose organizacijose dirbančiu personalu arba esama infrastruktūra, taip pat programine ir techninę įranga. Išimtinai nacionalinės sistemos sukūrimo ir valdymo išlaidos būtų gerokai didesnės (390 mln. EUR sukūrimo išlaidų ir 37 mln. EUR metinių valdymo išlaidų), nes visos valstybės narės privalėtų sukurti labai saugias duomenų tvarkymo sistemas ir įdarbinti personalą toms sistemoms valdyti.

Šios sumos yra preliminarios ir jas reikės toliau analizuoti ir išsamiau pateikti atsižvelgiant į poveikio vertinimo rezultatus.

5. SVARSTYTINI KLAUSIMAI

Nepaisant to, kuri iš visų skirtingų ES TFSS sukūrimo ir valdymo galimybių būtų pasirinkta, reikia apsvarstyti tam tikrus svarbius klausimus, susijusius su galimos ES TFSS taikymo sritimi. Šie klausimai aptariami toliau.

5.1. Terorizmas ir jo finansavimas ar daugiau?

Susipažinti su finansinių mokėjimų pranešimų duomenimis naudinga ne tik kovojant su terorizmu ir jo finansavimu. Beveik neabejojama, kad tokia prieiga būtų vertinga kovos su kitų rūšių sunkiais nusikaltimais, ypač organizuotu nusikalstamumu ir pinigų plovimu, priemonė. Tačiau ES ir JAV TFSP susitarimo atveju apsvarsčius proporcingumo klausimą tokių duomenų naudojimas galiausiai buvo labai tiksliai apribotas ir skirtas tik kovai su terorizmu ir jo finansavimu. Iš jau surengtų preliminarių diskusijų irgi matyti plataus masto sutarimas, kad dėl šių proporcingumo aspektų reikėtų taip pat apriboti lygiavertės Europos sistemos taikymo sritį, atsižvelgiant į bendrąsias pastabas dėl pagrindinių teisių laikymosi, kaip aptarta šio komunikato 2 dalyje.

5.2. Daugiau nei vienas paslaugos teikėjas?

ES ir JAV TFSP susitarime kol kas numatytas apribojimas, kad duomenų galima prašyti tik iš vieno tarptautinių finansinių mokėjimų pranešimų paslaugų teikėjo. Nors šis teikėjas tikrai yra pats svarbiausias pasaulinis tokių pranešimų paslaugų teikėjas, rinkoje veikia ir kiti paslaugų teikėjai. Svarstant veiksmingumo ir vienodų sąlygų visiems rinkos dalyviams sukūrimo klausimus linkstama prie nuomonės, kad reikėtų sukurti sistemą, kuri būtų taikoma visiems tarptautinių finansinių mokėjimų pranešimų paslaugų teikėjams. Bet kokiu atveju renkantis iš visų turimų galimybių būtina atsižvelgti į bendrovių, teikiančių finansinių mokėjimų pranešimų paslaugas, administracinę naštą.

5.3. Tik tarptautinės ar ir nacionalinės pranešimų paslaugos?

Dabar pagal ES ir JAV TFSP susitarimą duomenų galima prašyti tik iš tarptautinių finansinių mokėjimų pranešimų paslaugų, t. y. pranešimų paslaugų, teikiamų vykdant tarpvalstybinius sandorius, įskaitant tarp ES valstybių narių, teikėjų, išskyrus finansinių mokėjimų pranešimų duomenis, susijusius su bendra mokėjimų eurais erdve (SEPA). Kuriant ES TFSS taip pat reikės apsvarstyti galimybę, ar vertėtų įtraukti finansinių mokėjimų pranešimų, kuriais keičiamasi tarp valstybių narių, paslaugas, ar verčiau ji apimtų tik tarptautinį keitimąsi finansinių mokėjimų pranešimų paslaugomis. Išimtinai nacionalinės finansinių mokėjimų pranešimų paslaugos (kurios naudojamos tik vykdant nacionalinius finansinius sandorius) į ES ir JAV TFSS susitarimo taikymo sritį šiuo metu nepatenka. Prieiga prie tokių nacionalinių finansinių mokėjimų pranešimų paslaugų būtų naudinga kovojant su terorizmu ir kitomis nusikaltimų rūšimis. Tačiau net ir nenagrinėjant klausimo, ar prieiga prie tokių išimtinai nacionalinių sandorių turėtų būti reguliuojama Europos lygiu, iš preliminarių diskusijų paaiškėjo, kad, daugumos nuomone, tokia prieiga yra neproporcinga ir todėl neturėtų būti įtraukta į ES sistemos taikymo sritį.

5.4. Kokias finansinių mokėjimų pranešimų duomenų rūšis reikėtų įtraukti?

Tarptautinėje bankų sistemoje naudojami labai įvairūs finansinių mokėjimų pranešimų duomenys. ES ir JAV TFSP susitarime kol kas nustatyta tik viena konkreti finansinių mokėjimų pranešimų duomenų rūšis. Prieiga prie kitų rūšių finansinių mokėjimų pranešimų duomenų būtų naudinga kovojant su terorizmu ir jo finansavimu, galbūt ir su kitomis nusikaltimų rūšimis. Tačiau, kalbant apie tokį pasirinkimą, po svarstymų dėl proporcingumo ir piliečių pagrindinių teisių laikymosi linkstama apriboti į sistemą įtrauktinų pranešimų rūšis. Daugiau informacijos apie šį techninį aspektą bus pateikta poveikio vertinime.

6. ES TFSS GALIMYBĖS

Toliau aprašytas galimybes Komisija dabar nagrinėja rengiamame poveikio vertinime. Čia nebūtinai aptariamos visos įmanomos galimybės ir jokiu būdu nėra iš anksto nusprendžiama dėl galutinio poveikio vertinimo ar Komisijos pasirinkimo remiantis tuo poveikio vertinimu.

Viena iš galimybių, kuri visada svarstoma rengiant naujas iniciatyvas ir prie jų pateikiamus poveikio vertinimus, yra *status quo* galimybė, kuri šiuo atveju reikštų, kad bus toliau taikomas ES ir JAV TFSP susitarimas ir nebus teikiamas joks pasiūlymas dėl ES TFSS. Ši galimybė neatitiktų Tarybos ir Parlamento raginimo Komisijai pateikti pasiūlymą dėl „teisinio ir techninio duomenų atrinkimo ES teritorijoje pagrindo“, kaip nurodyta šio komunikato 1 dalyje. Be to, šia galimybe nebūtų prisidėta prie trečiosioms šalims perduodamų asmens duomenų kiekio apribojimo ir nebūtų numatyta galimybė tvarkyti duomenis ES teritorijoje, laikantis ES duomenų apsaugos principų ir teisės aktų. Visomis kitomis toliau išsamiau aptartomis galimybėmis pateikiami galimi ES TFSS sukūrimo būdai.

Teoriškai visos svarbiausios ES TFSS funkcijos, kaip nustatyta šio komunikato 3 dalyje, galėtų būti įgyvendinamos ES arba nacionaliniu lygiu. Funkcijos taip pat galėtų būti priskirtos vienai organizacijai arba kelioms skirtingoms, atsižvelgiant į jų dabartines pareigas, arba toms funkcijoms atlikti galėtų būti sukurtos naujos organizacijos. Tai galėtų būti Europos arba nacionalinės organizacijos. Tai reiškia (taip pat teoriškai), kad įmanomas ir išimtinai Europos metodas, t. y. visos svarbiausios funkcijos būtų paskirtos ES lygio organizacijoms, ir išimtinai nacionalinis metodas, t. y. visos funkcijos būtų atliekamos nacionaliniu lygiu. Iš esmės reikėtų turėti omenyje ir tai, kad centralizuotos, decentralizuotos ar mišrios sistemos pasirinkimas šiuo konkrečiu atveju nebūtinai atitiktų pasirinkimą, svarstant kitas su duomenų tvarkymu terorizmo ir organizuoto nusikalstamumo tikslais susijusias iniciatyvas: kiekvienos šios srities iniciatyvos privalumai turėtų būti įvertinti atskirai.

Tiek išimtinai centralizuotas, tiek išimtinai nacionalinis metodai turi didelių trūkumų. Pavyzdžiui, taikant išimtinai Europos metodą tikrai kiltų sunkumų dėl menkų sąsajų su valstybių narių teisėsaugos ir žvalgybos organizacijomis ir jų praktika, todėl jis nebūtų labai veiksmingas. Be šiuos klausimus sprendžiančių nacionalinių valdžios institucijų indėlio būtų beveik neįmanoma tiksliai nustatyti, kokių duomenų kategorijų reikėtų prašyti iš paskirtojo (-ųjų) teikėjo (-ų). Sistemos nauda taip pat sumažėtų, jei užklausos duomenų bazėje būtų pateikiamos tik remiantis ES lygiu turima žvalgybos informacija: turint omenyje dabartinį ES integracijos lygį tokia žvalgybos informacija didele dalimi prieinama tik nacionaliniu lygiu. Be to, valstybės narės vargu ar pritars tokiam išimtinai ES lygio metodui, nes tai nesuteiktų jokios pridėtinės vertės jų pačių pastangoms kovoti su terorizmu ir jo finansavimu. Per konsultacijas valstybės narės taip pat nurodė, kad priimti šią galimybę būtų sunku politiškai dėl teisinių ir su veikla susijusių priežasčių.

Kita vertus, taikant išimtinai nacionalinį metodą kiltų pavojus, kad skirtingose valstybėse narėse jis būtų įgyvendinamas nevienodai, ir padidėtų duomenų saugumo pažeidimų rizika dėl būtinybės turėti 27 skirtingas pateiktų duomenų kopijas. Be to, dėl išimtinai nacionalinio metodo kiltų sunkumų įgyvendinant suderintą duomenų apsaugos sistemą, taip pat suderintą požiūrį į kitus būtinus apribojimus (ir jų kontrolę), kaip antai jos taikymą tik terorizmo ir jo finansavimo tikslais. Be to, taikant išimtinai nacionalinį metodą būtų neaišku, kuri valstybė narė atsakinga už trečiųjų šalių pateiktų prašymų atlikti paieškas tvarkymą, ir nebeliktų paieškos rezultatų analizės Europos lygiu pridėtinės vertės. Be to, kaip nurodyta pirmiau, su šia galimybe susijusios išlaidos būtų gerokai didesnės, nes visos valstybės narės turėtų sukurti labai saugias duomenų tvarkymo sistemas ir įdarbinti personalą toms sistemoms valdyti.

Todėl per paruošiamąjį darbą su suinteresuotaisiais subjektais greitai nustatyta, kad kraštutiniams galimybių variantams nepritariama: pasiektas sutarimas, kad geriausius galimus rezultatus, siekiant dviejų pagrindinių tikslų, tikriausiai pavyktų pasiekti pasirinkus mišrų sprendimą, t. y. skirtingas funkcijas paskirsčius įvairioms organizacijoms ES ir nacionaliniu lygiu. Nors šis sutarimas padeda nustatyti tinkamiausią galimybę, net ir pasirinkus mišrų metodą dar reikia priimti labai daug papildomų sprendimų. Tolesniuose skirsniuose truputį išsamiau aprašomos trys mišrios galimybės, kurios per paruošiamąjį darbą įvertintos kaip labiausiai tikėtinos; be to, visos galimybės pateikiamos priedo lentelėje.

6.1. ES TFSS koordinavimo ir analitinė paslauga (1 galimybė)

Pagal šią galimybę būtų sukurtas centrinis ES TFSS skyrius ir dauguma užduočių ir funkcijų būtų atliekamos ES lygiu. Prašymų paskirtajam (-iesiems) teikėjui (-ams) pateikti neapdorotus duomenis teikimas, tokių prašymų tikrinimas, prašymų atlikti paieškas tvarkymas ir jų atlikimas, paieškos rezultatų valdymas ir ataskaitų perdavimas paprašiusiems atlikti paieškas – viskas būtų vykdoma ES lygiu. Tačiau prašymai paskirtajam (-iesiems) teikėjui (-ams) galėtų būti rengiami konsultuojantis su atsakingomis valstybių narių valdžios institucijomis, o valstybės narės taip pat galėtų deleguoti savo analitikus į centrinį skyrių, kad jie dalyvautų atliekant paieškas. Priešingai nei visiškai centralizuotos galimybės atveju, valstybės narės galėtų prašyti atlikti paieškas jų vardu, panašiai kaip dabar yra pagal JAV TFSP nustatytą tvarką, arba kad jas atliktų jų pačių analitikai.

Valstybės narės turėtų dalytis informacija su centriniu ES TFSS skyriumi, kad prieš pradedant paiešką pagrįstų savo prašymą ir jo ryšį su terorizmu, arba jų prašymus galėtų iš anksto patvirtinti nacionalinės valdžios institucijos. Tokios nacionalinės institucijos galėtų būti, pavyzdžiui, už kovą su terorizmu atsakingi prokurorai ar tyrimui vadovaujantys teisėjai: jei jie patvirtintų konkrečią pateiktų duomenų paiešką, centrinis ES TFSS skyrius sutiktų atlikti tokias paieškas be papildomo patikrinimo. Šiuo atveju centriniam ES TFSS skyriui nereikėtų pateikti jokios papildomos žvalgybos informacijos. Centrinis ES TFSS skyrius perduotų paieškų ir atliktos analizės rezultatus, be to, galėtų teikti informaciją savo iniciatyva. JAV ir kitos trečiosios šalys taip pat turėtų prašyti atlikti paieškas ir būtų vykdomas panašus procesas.

Taip pat būtų centralizuotas atitikties apsaugos ir kontrolės priemonėms stebėjimas, galbūt įtraukiant išorės suinteresuotuosius subjektus, pavyzdžiui, atstovaujančius paskirtajam (-iesiems) teikėjui (-ams) ir paskirtus nepriklausomais prižiūrėtojais. Duomenų apsauga, vientisumas ir saugumas taip pat būtų užtikrinami centriniu lygiu.

Svarbiausios sistemoje dalyvaujančios įstaigos galėtų būti Europolas ir Eurojustas. Tokiu atveju užduotys, kurias atliktų Europolas ir Eurojustas, turėtų atitikti jų misijas, kaip nustatyta

Sutartyje dėl Europos Sąjungos veikimo (SESV). Taip pat reikės įvertinti, kiek reikės pakeisti teisines priemones, kuriomis šiuo metu reguliuojamas šių institucijų veikimas. Jei centrine ES TFSS institucija būtų pasirinktas Europolas, jis taip pat tvarkytų duomenų subjektų prašymus susipažinti su informacija, ją pataisyti ir užblokuoti, laikydamasis galiojančios teisinės sistemos ir duomenų apsaugos nuostatų. Centrinis ES TFSS skyrius atliktų savo vaidmenį pagal galiojančią teisinę sistemą, o prašymai atlyginti žalą ir skundai taip pat būtų nagrinėjami laikantis galiojančių teisės nuostatų. Nacionaliniu lygiu nacionalinės teisėsaugos institucijos tikrintų ir tvirtintų prašymus atlikti paieškas. Būtų galima numatyti galimybę sukurti naujas nacionalines įstaigas, bet šį pasirinkimą pagal subsidiarumo principą verčiau palikti valstybėms narėms[8].

6.2. ES TFSS atrinkimo paslauga (2 galimybė)

Pagal šią galimybę, kaip ir pagal pirmąją politikos galimybę, būtų sukurtas centrinis ES TFSS skyrius, kuris turėtų tokias užduotis: teikti prašymus dėl neapdorotų duomenų paskirtajam (-iesiems) teikėjui (-ams), tikrinti tokius prašymus, atlikti paieškas ir tvarkyti prašymus atlikti paieškas. Tačiau pagal šią galimybę ES TFSS skyrius neturėtų teisės analizuoti paieškos rezultatų ir jų lyginti su kita turima informacija ar žvalgybos informacija, kai tokios paieškos atliekamos paprašius valstybių narių valdžios institucijoms, – tokiais atvejais jo vaidmuo būtų ribotas ir apimtų tik paieškos rezultatų rengimą ir teikimą tinkama forma.

Kaip ir pagal 1 galimybę, paskirtajam (-iesiems) teikėjui (-ams) teiktini prašymai pateikti neapdorotus duomenis būtų rengiami glaudžiai konsultuojantis su valstybėmis narėmis, kurios centriniam TFSS skyriui nurodytų savo konkrečius poreikius, kad skyrius juos išanalizuotų ir pagal tai suformuluotų prašymą (-us).

Valstybių narių valdžios institucijos galėtų paprašyti atlikti paieškas jų vardu. Tokių prašymų pagrįstumas ir ryšys su terorizmu būtų tikrinamas ir tvirtinamas nacionaliniu lygiu. Centrinis ES TFSS skyrius atliktų paiešką ir visus rezultatus tinkama forma pateiktų valstybėms narėms. Tik valstybių narių valdžios institucijos galėtų atlikti paieškų analizę, be to, jos turėtų galimybę teikti informaciją savo iniciatyva.

Centrinis ES TFSS skyrius atliktų paieškas ir analizuotų rezultatus ES institucijų, JAV ar kitų trečiųjų šalių vardu. Tuo remdamasis jis taip pat galėtų teikti informaciją savo iniciatyva.

Kaip ir pagal ankstesnes galimybes, atitikties apsaugos ir kontrolės priemonėms stebėjimas būtų centralizuotas, galbūt įtraukiant išorės suinteresuotuosius subjektus, pavyzdžiui, atstovaujančius paskirtajam (-iesiems) teikėjui (-ams) ir paskirtus nepriklausomais prižiūrėtojais. Duomenų apsauga, duomenų vientisumas ir duomenų saugumas taip pat būtų užtikrinami centriniu lygiu.

Kaip ir pagal ankstesnę galimybę, svarbiausios sistemoje dalyvaujančios įstaigos galėtų būti Europolas ir Eurojustas. Pagrindinės nacionaliniu lygiu įtrauktos institucijos galėtų būti nacionalinės teisėsaugos ar žvalgybos institucijos. Kaip nurodyta pirmiau, pagal subsidiarumo principą dėl naujų nacionalinių įstaigų sukūrimo spręstų pačios valstybės narės. Europolas ir (arba) nacionaliniai skyriai tvarkytų ES piliečių prašymus susipažinti su informacija, ją pataisyti ir ištrinti, kartu įtraukdami nacionalines duomenų apsaugos institucijas ir Europolo

[8] Šiuo metu dar nežinoma, kokią įtaką tai turėtų ES agentūrų, kurios gali dalyvauti įgyvendinant sistemą, biudžetui.

jungtinę priežiūros instituciją. Prašymai atlyginti žalą ir skundai būtų tvarkomi laikantis taikomų teisės nuostatų nacionaliniu ar ES lygiu[9].

6.3. Finansinės žvalgybos padalinių (FŽP) koordinavimo paslauga (3 galimybė)

Pagal šią politikos galimybę būtų sukurta patobulinta FŽP platforma, kurią sudarytų visi valstybių narių FŽP. ES lygio *ad hoc* valdžios institucija pateiktų prašymus dėl neapdorotų duomenų paskirtajam (-iesiems) teikėjui (-ams), visus FŽP nurodytus poreikius sudėdama į vieną prašymą, kuris taip pat būtų patikrintas ir patvirtintas centriniu lygiu.

Kiekvienas FŽP atliktų paieškas ir valdytų paieškos rezultatus savo valstybės narės vardu, taip pat vykdytų analizes ir perduotų ataskaitas tiems, kam, jo nuomone, jos būtų svarbios. Tokių paieškų pagrįstumas ir ryšys su terorizmu būtų tikrinamas ir tvirtinamas nacionaliniu arba ES lygiu. FŽP taip pat teiktų informaciją savo iniciatyva.

Patobulinta FŽP platforma galėtų atlikti paieškas ir analizuoti rezultatus ES institucijų ir kitų trečiųjų šalių, su kuriomis ES bus sudariusi susitarimą, vardu. Ji taip pat galėtų teikti informaciją savo iniciatyva.

Atitikties apsaugos ir kontrolės priemonėms stebėjimas būtų centralizuotas, galbūt įtraukiant išorės suinteresuotuosius subjektus, pavyzdžiui, atstovaujančius paskirtajam (-iesiems) teikėjui (-ams) ir paskirtus nepriklausomais prižiūrėtojais. Duomenų apsauga, vientisumas ir saugumas taip pat būtų užtikrinami centriniu lygiu.

Patobulintai FŽP platformai būtų suteiktas oficialus teisinis statusas ir aiškiai nustatytos jos funkcijos ir atsakomybės sritys. Pagrindinės nacionaliniu lygiu įtrauktos institucijos galėtų būti FŽP ir nacionalinės teisėsaugos ir žvalgybos institucijos.

Bet kuri ES lygio valdžios institucija tvarkytų ES piliečių prašymus susipažinti su informacija, ją pataisyti ir ištrinti, o prašymai atlyginti žalą ir skundai būtų nagrinėjami laikantis nacionaliniu ar ES lygiu taikomų teisės nuostatų.

7. IŠVADA

Remiantis Komisijos iki šiol atliktu paruošiamuoju darbu ir nedarant įtakos poveikio vertinimo rezultatams, šiame komunikate aprašomos įvairios „teisinio ir techninio duomenų atrinkimo ES teritorijoje pagrindo“, t. y. terorizmo finansavimo sekimo sistemos, sukūrimo galimybės. Šiame komunikate pateiktomis įvairiomis galimybėmis parodoma, kad reikės pasirinkti ir nuspręsti dėl svarbių klausimų, įskaitant pagrindinių teisių laikymosi aspektą, be to, reikės gerokai išsamiau įvertinti daug teisinių, techninių, organizacinių ir finansinių klausimų atliekant tolesnį paruošiamąjį darbą. Turėdama omenyje šiuos svarbius uždavinius, Komisija mano, kad tolesniam paruošiamajam darbui ir diskusijoms su Taryba ir Parlamentu reikia skirti pakankamai laiko.

* * *

[9] Žr. 8 išnašą.

Priedas. Mišrių galimybių apžvalga

	ES TFSS koordinavimo ir analitinė paslauga (1 galimybė)	ES TFSS atrinkimo paslauga (2 galimybė)	Finansinės žvalgybos padalinių (FŽP) koordinavimo paslauga (3 galimybė)
Prašymų pateikti neapdorotus duomenis rengimas ir teikimas	Centrinis ES TFSS skyrius, koordinuojantis veiksmus su VN	Centrinis ES TFSS skyrius, koordinuojantis veiksmus su VN	Patobulinta FŽP platforma
Prašymų pateikti neapdorotus duomenis stebėjimas ir tvirtinimas	Eurojustas ar kita veikianti įstaiga	Eurojustas ar kita veikianti įstaiga	Eurojustas ar kita veikianti įstaiga
Neapdorotų duomenų gavimas ir saugojimas, duomenų saugumas	Europolas arba kita ES įstaiga, kaip antai IT agentūra	Europolas arba kita ES įstaiga, kaip antai IT agentūra	Europolas arba kita ES įstaiga, kaip antai IT agentūra
Neapdorotų duomenų paieškos	Centrinis ES TFSS skyrius, VN deleguoti analitikai arba abu kartu	Centrinis ES TFSS skyrius	FŽP, patobulinta FŽP platforma
Paieškų atlikimo stebėjimas ir tvirtinimas	Nepriklausomi prižiūrėtojai, galbūt nacionalinės institucijos	Nepriklausomi prižiūrėtojai, nacionalinės institucijos	Nepriklausomi prižiūrėtojai
Paieškų rezultatų analizė	Centrinis ES TFSS skyrius, VN deleguoti analitikai arba abu kartu	Nacionalinės institucijos (nacionalinės paieškos), centrinio ES TFSS skyriaus analitikai (ES ir trečiųjų šalių paieškos)	Patobulinta FŽP platforma, nacionaliniai FŽP
Paieškų rezultatų teikimas	Europolo analitikai arba VN deleguoti analitikai	Nacionalinės institucijos (nacionalinės paieškos), centrinio ES TFSS skyriaus analitikai (ES ir trečiųjų šalių paieškos)	Patobulinta FŽP platforma, nacionaliniai FŽP

Tinkamo duomenų apsaugos režimo įgyvendinimas	Europolas arba kita ES įstaiga, kaip antai IT agentūra	Europolas arba kita ES įstaiga, kaip antai IT agentūra	Europolas arba kita ES įstaiga, kaip antai IT agentūra