

Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Komisijos komunikato Europos Parlamentui ir Tarybai „Laisvės, saugumo ir teisingumo erdvė piliečių labui“

(2009/C 276/02)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

atsižvelgdamas į Europos bendrijos steigimo sutartį, ypač į jos 286 straipsnį,

atsižvelgdamas į Europos Sąjungos pagrindinių teisių chartiją, ypač į jos 8 straipsnį,

atsižvelgdamas į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo,

atsižvelgdamas į 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, ypač į jo 41 straipsnį,

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS

1. 2009 m. birželio 10 d. Komisija priėmė komunikatą Europos Parlamentui ir Tarybai „Laisvės, saugumo ir teisingumo erdvė piliečių labui“⁽¹⁾. Laikydamasis Reglamento (EB) Nr. 45/2001 41 straipsnio, Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) pateikia šią nuomonę.
2. Prieš priimdama Komunikatą, Komisija dėl jo neoficialiai 2009 m. gegužės 19 d. laišku konsultavosi su EDAPP. EDAPP atsakė 2009 m. gegužės 20 d. pateikdamas neoficialias pastabas Komunikato tekstui dar patobulinti. Be to, EDAPP aktyviai reagavo į 2009 m. sausio 14 d. Policijos ir teisingumo darbo grupės laišką dėl Daugiametės laisvės, saugumo ir teisingumo srities programos⁽²⁾.
3. Komunikate (1 punktas) pabrėžiama, kad Sąjunga „turi priimti naują daugiametę programą, kurioje, atsižvelgus į padarytą pažangą ir padarius išvadas dėl dabartinių trūkumų, būtų drąsiai žvelgiama į ateitį. Šioje naujojoje programoje turės būti nustatyti ateinančių penkerių metų

prioritetai.“ Ši daugiametė programa (vadinama „Stokholmo programa“) pratęs veiklą, vykdomą pagal Tamperės ir Hagos programas, kurios turi didelę politinę įtaką laisvės, saugumo ir teisingumo erdvei.

4. Komunikatas yra naujos daugiametės programos pagrindas. Todėl EDAPP pažymi, kad, nors daugiametės programos nėra privalomos priemonės, jos turi didelę įtaką būsimai atitinkamos srities institucijų politikai, kadangi daugelis konkrečių teisėkūros ir ne teisėkūros veiksmų remsis minėta programa.
5. Šio požiūrio į Komunikatą ir reikia laikytis. Tai yra dar vienas žingsnis debatuose, kurie prasidėjo maždaug 2008 m. birželio mėn. vadinamosioms „Ateities grupėms“, kurias idėjoms teikti įsteigė Tarybai pirmininkaujanti valstybė narė, pateikusi dvi ataskaitas: „Laisvė, saugumas, privatumas – Europos vidaus reikalai atvirame pasaulyje“⁽³⁾ ir „Siūlomi sprendimai dėl būsimos ES teisingumo programos“⁽⁴⁾.
6. Šioje nuomonėje EDAPP ne tik išdėstė požiūrį į Komunikatą, bet ir pateikė nuomonę dėl platesnių debatų dėl laisvės, saugumo ir teisingumo erdvės ateities, kuriais remiantis bus parengta nauja strateginė darbo programa (Stokholmo programa), kaip skelbia ES pirmininkaujanti Švedija⁽⁵⁾. Šioje nuomonėje taip pat aptariamos kai kurios galimo Lisabonos sutarties įsigaliojimo pasekmės.
7. III dalyje konkrečiai išdėstyti pagrindiniai nuomonės aspektai, o IV dalyje pateikiamas bendras Komunikato įvertinimas.
8. V dalyje aptariamas klausimas, kaip elgtis esant būtinybei nuolat užtikrinti privatumo ir asmens duomenų apsaugą, kai vis dažniau keičiamasi asmens duomenimis. Daugiausia dėmesio skiriama Komunikato 2.3 punktui „Asmens duomenų ir privatumo apsauga“, o bendresne prasme – papildomų teisėkūros ir ne teisėkūros veiksmų siekiant patobulinti duomenų apsaugos sistemą poreikiams.

⁽¹⁾ COM(2009) 262 galutinis („Komunikatas“).

⁽²⁾ Nepaskelbta. Policijos ir teisingumo darbo grupė įsteigė Europos duomenų apsaugos įgaliotinių konferencija, kad ji parengtų konferencijos pozicijas teisėsaugos srityje ir veiktų jos vardu sprendžiant neatidėliotinus klausimus.

⁽³⁾ Tarybos dok. Nr. 11657/08. Toliau – „Vidaus reikalų ataskaita“.

⁽⁴⁾ Tarybos dok. Nr. 11549/08 („Teisingumo ataskaita“).

⁽⁵⁾ Vyriausybės ES darbo programa, <http://www.regeringen.se>

9. VI dalyje aptariami informacijos, kaip teisėsaugos priemonės, o pagal Komunikatą – kaip saugios Europos užtikrinimo priemonės, saugojimo, galimybių naudotis ir keistis informacija poreikiai ir galimybės. Komunikato 4 punkte išdėstyti tikslai, susiję su informacijos srautu ir technologinėmis priemonėmis, visų pirma 4.1.2 punkte (Valdyti informaciją), 4.1.3 punkte (Sutelkti reikiamas technologines priemones) ir 4.2.3.2 punkte (Informacinės sistemos). Didžiausio užmojo pasiūlymu šiuo atveju galima laikyti Europos informacijos modelio kūrimą (4.1.2 punktas). EDAPP nuomonėje šis pasiūlymas nagrinėjamas nuodugniai.
10. VII dalyje trumpai aptariamas konkretus, su duomenų apsauga susijęs laisvės, saugumo ir teisingumo erdvės srities klausimas – teisė kreiptis į teismą ir e. teisingumas.

III. NUOMONĖS ASPEKTAI

11. Pagrindinė Komunikato nagrinėjimo kryptis šioje nuomonėje yra pagrindinių teisių apsaugos poreikis, o bendresne prasme – laisvės, saugumo ir teisingumo erdvės ateitis, kaip aprašyta naujoje daugiametėje programoje. Ji taip pat grindžiama EDAPP pastabomis dėl šios srities ES politikos plėtojimo, daugiausia kiek tai susiję su jo konsultuojamuoju vaidmeniu. Iki šiol EDAPP yra priėmęs daugiau kaip trisdešimt nuomonių ir pastabų dėl pagal Hagos programą parengtų iniciatyvų – visos jos pateiktos EDAPP tinklavietėje.
12. Vertindamas Komunikatą EDAPP atsižvelgia visų pirma į toliau išdėstytus keturis aspektus, kurie yra svarbūs laisvės, saugumo ir teisingumo erdvės ateičiai. Visi šie aspektai yra labai svarbūs ir Komunikate.
13. Pirmasis aspektas – proporcingas skaitmeninės informacijos apie piliečius kiekio didėjimas besivystant informacinėms ir ryšių technologijoms⁽⁶⁾. Visuomenė artėja prie reiškinio, kuris dažnai vadinamas „visuotiniu sekimu“, kai kiekvienas sandoris ir beveik kiekvienas piliečių žingsnis turėtų būti užfiksuotas skaitmeniniu įrašu. Vadinamasis „daiktų internetas“ ir „intelektualioji aplinka“ sparčiai vystosi naudojant radijo dažnių atpažinimo (RDA) žymenis. Vis dažniau naudojami skaitmeniniai žmogaus kūno duomenys (biometrika). Dėl to pasaulis tampa glaudžiau susijęs, ir
- jame visuomenės saugumo organizacijos gali turėti galimybę naudotis dideliais potencialiai naudingos informacijos kiekiais, o tai gali turėti tiesioginės įtakos atitinkamų asmenų gyvenimui.
14. Antrasis aspektas – internacionalizacija. Viena vertus, skaitmeniniame amžiuje keitimasis duomenimis neapsiriboja Europos Sąjungos išorės sienomis, kita vertus, vis labiau būtinas tarptautinis bendradarbiavimas vykdamas visą ES veiklą laisvės, saugumo ir teisingumo erdvės srityje: kovą su terorizmu, policijos ir teisminių bendradarbiavimą, civilinę teisėna ir sienų kontrolę – tai tik keli pavyzdžiai.
15. Trečiasis aspektas – duomenų naudojimas teisėsaugos tikslais: pastaruoju metu visuomenei iškilus grėsmėms, susijusioms ar nesusijusioms su terorizmu, teisėsaugos institucijoms buvo sudaryta daugiau galimybių rinkti ir saugoti asmens duomenis bei jais keistis (arba reikalauta tas galimybes suteikti). Daugeliu atvejų aktyviai dalyvauja privatieji subjektai, kaip *inter alia* numatyta Duomenų saugojimo direktyvoje⁽⁷⁾ ir įvairiose su PNR susijusiose priemonėse⁽⁸⁾.
16. Ketvirtasis aspektas – laisvas judėjimas. Laipsniškai plėtojant laisvės, saugumo ir teisingumo erdvę būtina toliau naikinti vidaus sienas ir galimas kliūtis laisvam judėjimui šioje erdvėje. Naujomis priemonėmis šioje erdvėje jokia būdu nereikėtų vėl sukurti kliūčių. Laisvas judėjimas šiuo atveju apima, viena vertus, laisvą asmenų judėjimą, kita vertus, laisvą (asmens) duomenų judėjimą.
17. Šie keturi aspektai rodo, kad informacijos naudojimo sąlygos greitai kinta. Tokiomis aplinkybėmis negalima abejoti tuo, koks svarbus yra patikimas piliečių pagrindinių teisių, visų pirma privatumo ir duomenų, apsaugos mechanizmas. Dėl šių priežasčių EDAPP, kaip minėta 11 punkte, nagrinėdamas Komunikatą, daugiausia atsižvelgia į apsaugos poreikį.

⁽⁶⁾ Vidaus reikalų atskaitoje apie tai kalbama net kaip apie „skaitmeninį cunami“.

⁽⁷⁾ 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB (OL L 105, 2006 4 13, p. 54).

⁽⁸⁾ Žr., pvz., Europos Sąjungos ir Jungtinių Amerikos Valstijų Susitarimą dėl oro vežėjų atliekamo keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Jungtinių Valstijų vidaus saugumo departamentui (DHS) (2007 PNR susitarimas) (OL L 204, 2007 8 4, p. 18) ir Pasiūlymą dėl Tarybos pamatinio sprendimo dėl keleivio duomenų įrašo naudojimo teisėsaugoje (COM(2007) 654 galutinis).

IV. BENDRAS ĮVERTINIMAS

18. Komunikatu ir Stokholmo programa siekiama penkeriems ateinantiems metams nustatyti ES ketinimus, kurių poveikis galėtų būti jaučiamas ir ilgiau. EDAPP pažymi, kad Komunikatas parengtas laikantis neutralumo Lisabonos sutarties atžvilgiu principo. EDAPP visiškai supranta, kodėl Komisija laikėsi tokio požiūrio, tačiau apgailestauja, kad Komunikate nebuvo galima visapusiškai pasinaudoti Lisabonos sutartimi užtikrintomis papildomomis galimybėmis. Lisabonos sutarties aspektui šioje nuomonėje skiriama daugiau dėmesio.
19. Komunikatas grindžiamas pastaraisiais metais vykdytų ES veiksmų laisvės, saugumo ir teisingumo srityje rezultatais. Galima laikyti, kad šie rezultatai buvo paskatinti įvykių, akcentuojant priemones, kuriomis išplečiamos teisėsaugos institucijų galios ir kurios yra invazinio pobūdžio piliečių atžvilgiu. Tai iš tiesų būdinga toms sritims, kuriose asmens duomenys naudojami ir jais keičiamasi intensyviai ir kuriose dėl šios priežasties duomenų apsauga yra labai svarbi. Rezultatus lėmė įvykiai – išoriniai įvykiai, tokie kaip rugsėjo 11 d. įvykiai ir sprogdinimai Madride bei Londone, labai paskatino teisėkūros veiklą. Pavyzdžiui, keleivio duomenų perdavimą Jungtinėms Valstijoms⁽⁹⁾ galima laikyti rugsėjo 11 d. įvykių, o Duomenų saugojimo direktyvą 2006/24/EB⁽¹⁰⁾ – sprogdinimų Londone išdava. Buvo akcentuojamos labiau invazinės priemonės, kadangi ES teisėkūros institucija sutelkė dėmesį į tas priemones, kuriomis sudaromos palankesnės sąlygos duomenų naudojimui ir keitimuisi jais, o priemonių, kuriomis siekiama užtikrinti asmens duomenų apsaugą, svarstyti neskubėta. Pagrindinė apsaugos priemonė, priimta po trejus metus trukusių diskusijų Taryboje, buvo Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdančios policijos ir teisminių bendradarbiavimą baudžiamosiose bylose, apsaugos⁽¹¹⁾. Rezultatas – nevisiškai tenkinantis Tarybos pamatinis sprendimas (žr. 29–30 punktus).
20. Pastarųjų metų patirtis rodo, kad prieš patvirtinant naujas priemones būtina apsvaistyti pasekmes teisėsaugos institucijoms ir Europos piliečiams. Svarstant reikėtų deramai atsižvelgti į privatumo užtikrinimo išlaidas ir veiksmingumą teisėsaugos požiūriu, visų pirma tais atvejais, kai siūlomos ir svarstomos naujos priemonės, tačiau ir įgyvendinus tas priemones, periodiškai jas peržiūrint. Toks svarstymas yra būtinas ir prieš naujoje daugiametėje programoje nustatant pagrindines artimiausios ateities iniciatyvas.
21. EDAPP džiaugiasi, kad Komunikate pagrindinių teisių apsauga, visų pirma asmens duomenų apsauga, laikoma vienu iš svarbiausių laisvės, saugumo ir teisingumo erdvės ateities klausimu. Komunikato 2 punkte ES apibūdinama kaip unikali bendromis vertybėmis grindžiamos pagrindinių teisių apsaugos erdvė. Be to, labai gerai, kad Komunikate prisijungimas prie Europos žmogaus teisių konvencijos laikomas prioritetingu klausimu, net pačiu svarbiausiu prioritetingu klausimu. Prisijungimas prie šios konvencijos yra svarbus žingsnis užtikrinant suderintą ir nuoseklią pagrindinių teisių apsaugos sistemą. Paskutinis, bet ne mažiau svarbus dalykas yra tai, kad Komunikate reikšminga vieta skirta duomenų apsaugai.
22. Toks dėmesio sutelkimas Komunikate rodo tvirtą ketinimą užtikrinti piliečių teisių apsaugą ir tokiu būdu geriau išlaikyti pusiausvyrą. Vyriausybės turi turėti tinkamas priemones piliečių saugumui užtikrinti, tačiau Europos visuomenėje jos privalo visapusiškai gerbti piliečių pagrindines teises. Piliečių labai⁽¹²⁾ reikalinga, kad Europos Sąjunga užtikrintų šią pusiausvyrą.
23. EDAPP nuomone, Komunikate labai gerai atsižvelgiama į šios pusiausvyros poreikį, įskaitant asmens duomenų apsaugos poreikį. Jame pripažįstama, kad reikia kitur sutelkti dėmesį. Tai svarbu, kadangi laisvės, saugumo ir teisingumo erdvės politikoje nereikėtų skatinti laipsniško perėjimo prie visuotinio sekimo. EDAPP tikisi, kad Stokholmo programoje Taryba laikysis tokio paties požiūrio ir pripažins 25 punkte pateiktas gaires.
24. Tai yra tikrai svarbu, kadangi laisvės, saugumo ir teisingumo erdvė, kaip labai neseniai 2009 m. birželio 30 d. sprendime, susijusiame su Lisabonos sutartimi, pabrėžė Vokietijos konstitucinis teismas⁽¹³⁾, yra erdvė, kuri lemia piliečių gyvenimo aplinkybes, visų pirma asmeninę jų atsakomybės erdvę bei politinį ir socialinį saugumą, kurių apsauga užtikrinama pagrindinėmis teisėmis.

⁽⁹⁾ 2007 m. PNR susitarimas, nurodytas pirmiau išnašoje, ir ankstesni susitarimai.

⁽¹⁰⁾ 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB (OL L 105, 2006 4 13, p. 54). Nors teisinis pagrindas yra EB sutarties 95 straipsnis, tai buvo neatidėliotinas atsakas į sprogdinimus Londone.

⁽¹¹⁾ 2008 m. lapkričio 27 d. Tarybos pamatinis sprendimas 2008/977/TVR dėl asmens duomenų, tvarkomų vykdančios policijos ir teisminių bendradarbiavimą baudžiamosiose bylose, apsaugos (OL L 350, 2008 12 30, p. 60).

⁽¹²⁾ Žr. Komunikato pavadinimą.

⁽¹³⁾ 2009 m. birželio 30 d. Vokietijos federacinio konstitucinio teismo pranešimas spaudai Nr. 72/2009, 2 c. punktas.

25. EDAPP pabrėžia, kad tokioje erdvėje:

- Valstybių narių institucijos, atitinkamais atvejais Europos organai ar duomenų bazės, turėtų keistis informacija remdamosi tinkamais ir veiksmingais mechanizmais, kuriuos taikant visapusiškai gerbiamos piliečio pagrindinės teisės ir užtikrinamas abipusis pasitikėjimas.
- Tam reikalinga ne tik prieinama informacija ir valstybių narių (bei ES) teisinių sistemų savitarpio pripažinimas, bet ir suderinti informacijos apsaugos standartai, pavyzdžiui, bendra duomenų apsaugos sistema, ja neapsiribojant.
- Šie bendri standartai turėtų būti taikomi ne tik tarpvalstybinio pobūdžio aplinkybėmis. Savitarpio pasitikėjimas įmanomas tik tuo atveju, jei standartai yra pagrįsti ir jų visada laikomasi, jei nebijoma, kad jie nebus taikomi nesant tarpvalstybinio pobūdžio arba jam išnykus. Be to, informacijos naudojimo požiūriu „vidaus“ ir „tarpvalstybinių“ duomenų skirtumai praktiškai neįmanomi⁽¹⁴⁾.

V. DUOMENŲ APSAUGOS PRIEMONĖS

V.1. Siekiant sukurti išsamią duomenų apsaugos sistemą

26. EDAPP pritaria strateginiam požiūriui duomenų apsaugą Komunikate laikyti svarbiu klausimu. Iš tiesų daug laisvės, saugumo ir teisingumo erdvėje vykdomų iniciatyvų priklauso nuo asmens duomenų naudojimo, todėl gera duomenų apsauga yra šių iniciatyvų sėkmės garantas. Privatumo užtikrinimas ir duomenų apsauga yra ne tik teisinė pareiga, kuri yra vis labiau pripažįstama ES lygiu, bet ir Europos piliečiams svarbus klausimas – tai rodo Eurobarometro apklausos rezultatai⁽¹⁵⁾. Be to, galimybių naudotis asmens duomenimis apribojimas taip pat labai svarbus užtikrinant teisės saugos įstaigų pasitikėjimą.
27. Komunikato 2.3 punkte teigiama, kad reikalinga visas ES kompetencijos sritis apimanti išsami duomenų apsaugos sistema⁽¹⁶⁾. EDAPP visapusiškai remia šį tikslą neatsižvelg-

damas į Lisabonos sutarties įsigaliojimą. Jis taip pat pažymi, kad tokia sistema nebūtina turi būti visam duomenų tvarkymui taikoma viena teisinė sistema. Pagal galiojančias sutartis galimybės priimti vieną išsamią teisinę sistemą, taikomą visam duomenų tvarkymui, yra ribotos dėl ramsčių struktūros ir dėl to, kad bent jau pirmojo ramsčio srityje Europos institucijų tvarkomų duomenų apsauga vykdoma remiantis atskiru teisiniu pagrindu (EB sutarties 286 straipsnis). Tačiau EDAPP nurodo, kad tam tikri patobulinimai gali būti atlikti visapusiškai išnaudojus galiojančiose sutartyse numatytas galimybes, kaip jau pabrėžė Komisija savo Komunikate „Hagos programos įgyvendinimas: ateities perspektyvos“⁽¹⁷⁾. Įsigaliojus Lisabonos sutarčiai, Sutarties dėl Europos Sąjungos veikimo 16 straipsnis bus reikiamas vienos visam duomenų tvarkymui taikomos išsamos teisinės sistemos teisinis pagrindas.

28. EDAPP pažymi, kad labai svarbu bet kuriuo atveju užtikrinti duomenų apsaugos teisinės sistemos nuoseklumą, prireikus derinant ir konsoliduojant įvairias teisines priemones, taikomas laisvės, saugumo ir teisingumo erdvėje.

Pagal galiojančias sutartis

29. Neseniai buvo žengtas pirmasis žingsnis priėmus Tarybos pamatinį sprendimą 2008/977/TVR⁽¹⁸⁾. Tačiau ši teisinė priemonė negali būti laikoma išsamia sistema iš esmės todėl, kad jos nuostatos nėra taikomos bendrai. Jos netaikomos vidaus situacijoms, kai asmens duomenys atsiranda toje valstybėje narėje, kuri juos naudoja. Šis apribojimas sumažina Tarybos pamatinio sprendimo pridėtinę vertę, nebent visos valstybės narės nuspręstų vidaus situacijas numatyti nacionaliniuose įgyvendinamuosiuose teisės aktuose, tačiau tai nėra tikėtina.
30. Kita priežastis, kodėl EDAPP mano, kad ilgainiui Tarybos pamatinis sprendimas 2008/977/TVR nustatytos duomenų apsaugos sistemos laisvės, saugumo ir teisingumo erdvėje nepakaks, yra ta, kad kelios esminės nuostatos neatitinka Direktyvos 95/46/EB. Pagal galiojančias sutartis antrasis žingsnis galėtų būti žengtas išplečiant Tarybos pamatinio sprendimo taikymo sritį ir jį suderinant su Direktyva 95/46/EB.
31. Dar vienas postūmis išsamią duomenų apsaugos sistemai įgyvendinti galėtų būti duotas nustatant aiškia ir ilgalaikę viziją. Šioje vizijoje galėtų būti numatytas visuotinis, suderintas požiūris, kaip apibrėžti duomenų rinkimą ir keitimąsiais bei esamų duomenų bazių eksploatavimą, taip pat duomenų apsaugos garantijas. Ši vizija turėtų užkirsti

⁽¹⁴⁾ Europos duomenų apsaugos priežiūros pareigūnas šį pastarąjį klausimą išsamią nagrinėjo 2005 m. gruodžio 19 d. nuomonėje dėl pasiūlymo dėl Tarybos pamatinio sprendimo dėl asmens duomenų, tvarkomų vykdamas policijos ir teisminių bendradarbiavimo baudžiamosiose bylose, apsaugos (COM(2005) 475 galutinis), OL C 47, 2006 2 25, p. 27, 30–32 punktai.

⁽¹⁵⁾ Duomenų apsauga Europos Sąjungoje – Piliečių supratimas – Analitinė ataskaita, *Flash Eurobarometer Series 225*, 2008 m. sausio mėn., http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

⁽¹⁶⁾ Taip pat žr. Komunikate nurodytus prioritetinius klausimus.

⁽¹⁷⁾ COM(2006) 331 galutinis, 2006 m. birželio 28 d.

⁽¹⁸⁾ Žr. 11 išnašą.

kelių priemonių (ir atitinkamai asmens duomenų tvarkymo pasikartojimui ir dubliavimuisi. Be to, ji turėtų paskatinti derinti ES politiką šioje srityje ir pasitikėti tuo, kaip valdžios institucijos tvarko piliečių duomenis. EDAPP rekomenduoja Tarybai Stokholmo programoje nurodyti, kad būtina aiški, ilgalaikė vizija.

32. Kita EDAPP rekomendacija yra įvertinti ir suformuoti naują požiūrį į šioje srityje jau patvirtintas priemones, jų konkretų įgyvendinimą ir veiksmingumą. Atliekant šį vertinimą reikėtų deramai atsižvelgti į privatumo užtikrinimo išlaidas ir veiksmingumą teisėsaugos požiūriu. Jei paaiškėtų, kad tam tikros priemonės neduoda numatytų rezultatų arba yra neproporcingos tikslams, kurių siekiama, reikėtų svarstyti, ar imtis šių veiksmų:

- pirma, iš dalies pakeisti arba panaikinti priemones, jei atrodo, kad jos nepakankamai pasiteisino kuriant konkrečią pridėtinę vertę teisėsaugos institucijoms ir Europos piliečiams,
- antra, įvertinti galimybes gerinti galiojančių priemonių taikymą,
- ir tik tada, trečia, pasiūlyti naujas teisės priemones, jei tikėtina, kad tokios naujos priemonės yra reikalingos numatytiems tikslams pasiekti. Naujas priemones reikėtų priimti tik tuo atveju, jei jos sukuria aiškią ir konkrečią pridėtinę vertę teisėsaugos institucijoms ir Europos piliečiams.

EDAPP rekomenduoja Stokholmo programoje padaryti nuorodą į galiojančių priemonių įvertinimo sistemą.

33. Paskutinis, bet ne mažiau svarbus dalykas yra tai, kad daug dėmesio reikėtų skirti geresniam galiojančių apsaugos priemonių įgyvendinimui, atsižvelgiant į Komisijos komunikatą dėl tolesnių veiksmų pagal Geresnio Duomenų apsaugos direktyvos įgyvendinimo darbo programą⁽¹⁹⁾ ir pasiūlymus, kuriuos EDAPP pateikė nuomonėje dėl to komunikato⁽²⁰⁾. Deja, trečiojo ramsčio srityje Komisija neturi pakankamai galimybių pradėti pažeidimo procedūrą.

Pagal Lisabonos sutartį

34. Lisabonos sutartimi praskinamas kelias realiai, išsamiai duomenų apsaugos sistemai. Sutarties dėl Europos Sąjungos

veikimo 16 straipsnio 2 dalyje reikalaujama, kad Taryba ir Europos Parlamentas nustatytų taisykles, susijusias su duomenų apsauga, kurią užtikrina Sąjungos institucijos, organai, biurai ir agentūros, valstybės narės, vykdydamos Sąjungos teisės taikymo sričiai priskiriamą veiklą, ir privatūs subjektai.

35. EDAPP supratimu, Komunikate akcentuojama išsami duomenų apsaugos sistema – tai Komisijos užmojis pasiūlyti visai duomenų tvarkymo veiklai taikomą teisės sistemą. Jis visiškai pritaria šiam užmojiui, kuriuo siekiama geriau suderinti sistemą, užtikrinti teisinį tikrumą ir tokiu būdu sustiprinti apsaugą. Visų pirma ateityje būtų išvengta sunkumų nustatant ribą tarp ramsčių sričių, kai privačiame sektoriuje komerciniais tikslais surinkti duomenys vėliau naudojami teisėsaugos tikslais. Tokia ramsčių sritis skirianti riba visapusiškai neatspindi realybės, kaip rodo svarbūs Teisingumo Teismo sprendimai dėl PNR⁽²¹⁾ ir dėl duomenų saugojimo⁽²²⁾.

36. EDAPP siūlo Stokholmo programoje pabrėžti tokį išsamios duomenų apsaugos sistemos pagrindimą. Jis rodo, kad tokia sistema nėra tik paprastas prioritetas, o yra besikeičiančios duomenų naudojimo praktikos nulemta būtinybė. Jis rekomenduoja į Stokholmo programą prioritetiniu klausimu įtraukti poreikį sukurti naują teisinę sistemą, *inter alia*, pakeičiančią Tarybos pamatinį sprendimą 2008/977/TVR.

37. EDAPP pabrėžia, kad išsamios duomenų apsaugos sistemos koncepcijoje, kuri grindžiama bendra teisės sistema, neatmetama galimybė priimti papildomas duomenų apsaugos taisykles, skirtas policijai ir teismų sektoriui. Tokiomis papildomomis taisyklėmis būtų galima atsižvelgti į konkrečius teisėsaugos poreikius, kaip numatyta prie Lisabonos sutarties pridedamoje 21 deklaracijoje⁽²³⁾.

V.2. Duomenų apsaugos principų performulavimas

38. Komunikate pažymima, jog dėl technologinių pokyčių kitaip palaikomi ryšiai tarp fizinių asmenų bei viešųjų ir privačiųjų organizacijų. Todėl, anot Komisijos, reikia performuluoti kai kuriuos pagrindinius duomenų apsaugos principus.

⁽¹⁹⁾ 2006 m. gegužės 30 d. Teismo sprendimas, Europos Parlamentas prieš Europos Sąjungos Tarybą (C-317/04) ir Europos Bendrijų Komisiją (C-318/04), Sujungtos bylos C-317/07 ir C-318/04, Rink. [2006], p. I-4721.

⁽²²⁾ 2009 m. vasario 10 d. Teismo sprendimas, Airija prieš Europos Parlamentą ir Europos Sąjungos Tarybą, Byla C-301/06, dar nepaskelbta.

⁽²³⁾ Žr. 21 deklaraciją dėl asmens duomenų apsaugos teismo bendradarbiavimo baudžiamosiose bylose ir policijos bendradarbiavimo srityse, pridedamą prie Lisabonos sutartį priėmusios tarpvyriausybinių konferencijos baigiamojo akto (OL C 115, 2008 5 9, p. 345).

⁽¹⁹⁾ 2007 m. kovo 7 d. COM(2007) 87 galutinis.

⁽²⁰⁾ 2007 m. liepos 25 d. nuomonė, OL C 255, 2007 10 27, p. 1, ypač 30 punktas.

39. EDAPP palankiai vertina tokius Komunikate nurodytus ketinimus. Nepaprastai naudinga įvertinti šių principų veiksmingumą atsižvelgiant į technologinius pokyčius. Pirmiausia, svarbu pažymėti, kad duomenų apsaugos principų reformulavimas ir pakartotinis patvirtinimas ne visada privalo būti susijęs su technologiniais pokyčiais. Jis gali būti reikalingas ir atsižvelgiant į kitus pirmiau (III dalyje) nurodytus aspektus – internacionalizaciją, augantį duomenų naudojimą teisės saugos tikslais ir laisvą judėjimą.

40. Be to, EDAPP nuomone, ši įvertinimą galima įtraukti į viešąją konsultaciją, apie kurią Komisija paskelbė 2009 m. gegužės 19–20 d. konferencijoje „Asmens duomenys – daugiau naudojami, labiau saugomi?“. Ši viešoji konsultacija galėtų suteikti vertingos informacijos⁽²⁴⁾. EDAPP siūlo Tarybai Stokholmo programos tekste, o Komisijai – jos viešuose pareiškimuose apie konsultaciją pabrėžti Komunikato 2.3 punkte nurodytų ketinimų ir viešosios konsultacijos dėl duomenų apsaugos ateities ryšį.

41. Pateikiant pavyzdžius, kas galėtų būti vertinama, paminėti toliau nurodyti punktai:

— Laisvės, saugumo ir teisingumo srities asmens duomenys turėtų būti ypač neskelbtino pobūdžio, pavyzdžiui, su baudžiamaisiais nuosprendžiais susiję duomenys, policijos duomenys ir biometriniai duomenys (pvz., pirštų atspaudai ir DNR analizės).

— Jų tvarkymas gali sukelti neigiamų pasekmių duomenų subjektams, visų pirma atsižvelgiant į teisės saugos institucijų prievartos galias. Be to, duomenų stebėseną ir analizę vis dažniau atliekama automatizuotai, dažnai be žmogaus įsikišimo. Technologijų dėka duomenų bazės, kuriose yra asmens duomenų, naudojamos bendroms paieškoms atlikti (duomenų gavyba, profilavimas ir t. t.). Reikėtų aiškiai nustatyti teisinius įsipareigojimus, kuriais būtų grindžiamas duomenų tvarkymas.

— Svarbiausia, kad duomenų apsaugos teisės akte būtų numatyta, jog asmens duomenys renkami nurodytais tikslais ir nenaudojami su tais tikslais nesuderinamais būdais. Su tikslais nesuderinamas naudojimas turėtų būti leidžiamas tik teisės aktuose nustatytais atvejais ir kai tai reikalinga konkrečių viešųjų interesų labui, kaip nustatyta Europos žmogaus teisių konvencijos 8 straipsnio 2 dalyje.

— Poreikis laikytis ribojimo pagal tikslą principo gali daryti poveikį dabartinėms duomenų naudojimui tendencijoms. Teisės saugos srityje naudojami privačių bendrovių komerciniais tikslais surinkti duomenys telekomunikacijų, transporto ir finansų sektoriuose. Be to, didelės

apimties informacinės sistemos sukurtos, pavyzdžiui, imigracijos ir sienų kontrolės srityse. Dar daugiau, galima tarpusavyje sujungti duomenų bazes ir leidžiama jomis naudotis, taip išplečiant tikslus, kuriais asmens duomenys buvo iš pradžių surinkti. Būtina apsvaistyti tokias dabartines tendencijas, prirėkus įskaitant visus galimus patikslinimus ir (arba) papildomas apsaugos priemones.

— Atliekant įvertinimą, reikėtų atkreipti dėmesį ne tik į Komunikate minėtus duomenų apsaugos principus, bet ir į skaidrumo poreikį tvarkant duomenis, kad duomenų subjektas galėtų pasinaudoti savo teisėmis. Skaidrumas yra ypač sunkus klausimas teisės saugos srityje, visų pirma todėl, kad skaidrumą reikia įvertinti atsižvelgiant į tyrimams kylančią riziką.

— Reikėtų surasti keitimosi informacija su trečiosiomis šalimis sprendimus.

42. Be to, atliekant šį įvertinimą, daug dėmesio reikėtų skirti galimybėms pagerinti duomenų apsaugos principų taikymo veiksmingumą. Šiuo požiūriu gali būti naudinga dėmesį sutelkti į priemones, kuriomis galima sustiprinti duomenų valdytojų atsakomybę. Šiomis priemonėmis turėtų būti sudarytos galimybės duomenų valdytojams prisiimti visišką atsakomybę už duomenų valdymą. Šiuo atveju naudinga sąvoka yra „duomenų valdymas“. Ji apima visas teises, technines ir organizacines priemones, kurias organizacijos taiko, kad užtikrintų visapusišką atsakomybę už duomenų tvarkymo būdą, pavyzdžiui, planavimą ir kontrolę, patikimos technologijos naudojimą, tinkamą personalo mokymą, atitikties auditus ir t. t.

V.3. Privatumo nepažeidžiančios technologijos

43. EDAPP džiaugiasi, kad Komunikato 2.3 punkte minimas sertifikavimas privatumui apsaugoti. Be to, galėtų būti padaryta nuoroda į „privatumą projektuojant“ ir poreikį nustatyti „geriausius technologijų būdus“, nepažeidžiant ES duomenų apsaugos sistemos.

44. EDAPP nuomone, „privatumas projektuojant“ ir privatumo nepažeidžiančios technologijos galėtų būti naudingos priemonės, padedančios geriau apsaugoti ir veiksmingiau naudoti informaciją. EDAPP siūlo du sprendimus, kurie gali būti taikomi ir kartu:

— privatumo ir duomenų apsaugos sertifikavimo sistema⁽²⁵⁾ – informacinių sistemų kūrėjams ir naudotojams (tiek gaunantiems, tiek negaunantiems ES finansavimą arba tiek besiremiantiems, tiek nesiremiantiems ES teisės aktais) skirta galimybė,

⁽²⁴⁾ 29 straipsnio duomenų apsaugos darbo grupė, kurios veikloje dalyvauja Europos duomenų apsaugos priežiūros pareigūnas, nusprendė aktyviai prisidėti prie šios viešosios konsultacijos.

⁽²⁵⁾ Tokios sistemos pavyzdys – Europos privatumo apsaugos ženklas (EuroPriSe).

- informacinių sistemų kūrėjų ir naudotojų teisinis įsipareigojimas naudoti sistemas nepažeidžiant privatumo projektuojant principo. Tam gali prireikti išplėsti esamą duomenų apsaugos teisės akto taikymo sritį, kad kūrėjai taptų atsakingi už jų kuriamas informacines sistemas ⁽²⁶⁾.

EDAPP siūlo šiuos galimus sprendimus nurodyti Stokholmo programoje.

V.4. Išorės aspektai

45. Kitas Komunikate minimas klausimas – duomenų apsaugos tarptautinių standartų rengimas ir propagavimas. Šiuo metu daug dirbama siekiant nustatyti įvykdomus visuotinai taikomus standartus, pavyzdžiui, šia veikla užsiima Tarptautinė privatumo ir duomenų apsaugos įgaliotinių konferencija. Artimiausioje ateityje gali būti susitarta dėl tarptautinio susitarimo. EDAPP siūlo šią veiklą paremti Stokholmo programa.
46. Komunikate taip pat minimas dvišalių susitarimų sudarymas, grindžiamas kartu su Jungtinėmis Valstijomis jau padaryta pažanga. EDAPP pritaria tam, kad reikia nustatyti aiškią duomenų perdavimo trečiosioms šalims teisinę sistemą, ir todėl palankiai įvertino ES ir JAV institucijų bendrą darbą aukšto lygio ryšių palaikymo grupėje, rengiant galimą transatlantinę duomenų apsaugos priemonę, ir paragino užtikrinti daugiau aiškumo ir atkreipti dėmesį į tam tikrus klausimus ⁽²⁷⁾. Šiuo požiūriu taip pat įdomu atkreipti dėmesį į mintis, pateikiamas vidaus reikalų srities ataskaitoje dėl euroatlantinės bendradarbiavimo laisvės, saugumo ir teisingumo srityse erdvės, dėl kurios, remiantis šia ataskaita, sprendimą ES turėtų priimti 2014 m. Tokia erdvė įmanoma tik nustačius tinkamas duomenų apsaugos garantijas.
47. EDAPP nuomone, Europos duomenų apsaugos standartais, kurie grindžiami Europos Tarybos konvencija 108 dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu ⁽²⁸⁾ ir Europos Teisingumo Teismo bei Europos žmogaus teisių teismo praktika, turėtų būti nustatytas apsaugos lygis bendrajame susitarime su Jungtinėmis Amerikos Valstijomis dėl duomenų apsaugos ir keitimosi duomenimis. Toks bendrasis susitarimas galėtų būti konkrečių keitimosi asmens duomenimis susitarimų

pagrindu. Tai dar svarbiau atsižvelgiant į Komunikato 4.2.1 punkte nurodytą ketinimą, kad Europos Sąjunga prireikus privalo sudaryti policijos bendradarbiavimo susitarimus.

48. EDAPP visiškai supranta, kad būtina stiprinti tarptautinį bendradarbiavimą, tam tikrais atvejais – ir su šalimis, kuriose pagrindinių teisių apsauga neužtikrinta. Vis dėlto ⁽²⁹⁾ yra labai svarbu atsižvelgti į tai, kad toks tarptautinis bendradarbiavimas turėtų labai padidinti duomenų rinkimą ir tarptautinį perdavimą. Todėl yra labai svarbu, kad sąžiningo ir teisėto duomenų tvarkymo principai – ir apskritai tinkamo proceso principai – būtų taikomi renkant asmens duomenis ir juos perduodant už Sąjungos teritorijos ribų, ir kad tie asmens duomenys būtų perduodami trečiosioms šalims ar tarptautinėms organizacijoms tik tuo atveju, jeigu tos atitinkamos trečiosios šalys garantuoja tinkamą apsaugos lygį ir kitas atitinkamas apsaugos priemones.
49. Galiausiai, EDAPP rekomenduoja Stokholmo programoje pabrėžti bendrųjų susitarimų dėl duomenų apsaugos ir keitimosi duomenimis, grindžiamų ES teritorijoje užtikrinamos apsaugos lygiu, su Jungtinėmis Valstijomis ir kitomis trečiosiomis šalimis svarbą. Platesne prasme EDAPP atkreipia dėmesį į tai, kad svarbu aktyviai skatinti gerbti pagrindines teises, visų pirma teisę į duomenų apsaugą, palaikant santykius su trečiosiomis šalimis ir tarptautinėms organizacijoms ⁽³⁰⁾. Be to, Stokholmo programoje galėtų būti paminėta bendra nuostata, kad keičiantis asmens duomenimis su trečiosiomis šalimis būtina užtikrinti tinkamą apsaugos lygį arba kitas atitinkamas apsaugos priemones tose trečiosiose šalyse.

VI. INFORMACIJOS NAUDOJIMAS

VI.1. Europos informacijos modelio kūrimas

50. Geresnis keitimasis informacija laisvės saugumo ir teisingumo erdvėje – vienas iš esminių Europos Sąjungos politikos tikslų. Komunikato 4.1.2 punkte pabrėžiama, kad Europos Sąjungos saugumas grindžiamas pažangiais nacionalinių valdžios institucijų ir Europos subjektų keitimosi informacija mechanizmais. Logiška, kad pabrėžiamas keitimasis informacija, nes nėra Europos policijos pajėgų,

⁽²⁶⁾ Informacijos naudotojams, taip pat duomenų valdytojams ar tvarkytojams, taikomas duomenų apsaugos teisės aktas.

⁽²⁷⁾ Žr. 2008 m. lapkričio 11 d. Europos duomenų apsaugos priežiūros pareigūno nuomonę dėl ES ir JAV aukšto lygio ryšių palaikymo grupės dėl keitimosi informacija, privatumo ir asmens duomenų apsaugos galutinės ataskaitos (OL C 128, 2009 6 6, p. 1).

⁽²⁸⁾ ETS Nr. 108, 1981 1 28.

⁽²⁹⁾ Žr. 2005 m. lapkričio 28 d. Europos duomenų apsaugos priežiūros pareigūno laišką dėl Komisijos komunikato dėl laisvės, saugumo ir teisingumo erdvės išorės aspekto, kuris pateikiamas Europos duomenų apsaugos priežiūros pareigūno tinklavietėje.

⁽³⁰⁾ Naujausia teisminė praktika, susijusi su teroristų sąrašais, patvirtina, kad reikalingos garantijos, taip pat ir palaikant santykius su Jungtinėmis Tautomis, siekiant užtikrinti, kad kovos su terorizmu priemonės atitiktų pagrindinėms teisėms taikomus ES standartus (Sujungtos bylos C-402/05 P ir C-415/05 P, *Kadi ir Al Barakaat Foundation prieš Tarybą*, 2008 m. rugsėjo 3 d. sprendimas, dar nepaskelbta).

Europos baudžiamojo teisingumo sistemos ir Europos sienų kontrolės. Todėl teikdama su informacija susijusias priemones Europos Sąjunga labai prisideda sudarant sąlygas valstybių narių valdžios institucijoms veiksmingai kovoti su tarpvalstybiniu nusikalstamumu ir tinkamai apsaugoti išorės sienas. Tačiau šios priemonės padeda užtikrinti ne tik piliečių saugumą, bet ir jų laisvę (vienu iš šios nuomonės aspektų pirmiau buvo nurodytas laisvas asmenų judėjimas) bei teisingumą.

51. Būtent dėl šių priežasčių Hagos programoje buvo nustatytas prieinamumo principas. Pagal šį principą ES valstybės narės turėtų netrukdomai keistis kovai su nusikalstamumu reikalinga informacija. Pastarųjų metų patirtis rodo, kad šį principą buvo sunku reglamentuoti teisinėmis priemonėmis. Taryba nepriėmė 2005 m. spalio 12 d. Komisijos pasiūlymo dėl Tarybos pamatinio sprendimo dėl keitimosi informacija pagal prieinamumo principą⁽³¹⁾. Valstybės narės nebuvo pasirengusios susitaikyti su visais prieinamumo principo padariniais. Vietoj šio pasiūlymo buvo priimti labiau ribotesni teisės aktai⁽³²⁾, pvz., 2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje (Priumo sprendimas)⁽³³⁾.
52. Prieinamumo principas buvo Hagos programos esmė, o dabar atrodo, kad Komisija laikosi kuklesnio požiūrio. Nustatydamą Europos informacijos modelį, ji numato toliau skatinti valstybių narių valdžios institucijas keistis informacija. ES pirmininkaujanti Švedija laikosi to paties požiūrio⁽³⁴⁾. Ji pateiks pasiūlymą dėl keitimosi informacija strategijos. Taryba jau pradėjo darbą, susijusį su šiuo plataus užmojo Europos Sąjungos informacijos valdymo strategijos projektu, kuris yra glaudžiai susijęs su Europos informacijos modeliu. EDAPP labai susidomėjęs seka šiuos įvykius ir pabrėžia, kad rengiant šiuos projektus atitinkamas dėmesys turėtų būti skirtas duomenų apsaugos elementams.

Europos informacijos modelis ir duomenų apsauga

53. Pirmiausia reikėtų pabrėžti, kad laisvės, saugumo ir teisingumo erdvės ateitis neturėtų priklausyti nuo technologijų; norima pasakyti, kad beveik neribotos naujų technologijų galimybės visada turėtų būti patikrintos atsižvelgiant į atitinkamus duomenų apsaugos principus ir naudojamos tik tada, jei jos atitinka tuos principus.
54. EDAPP atkreipia dėmesį į tai, kad Komunikate informacijos modelis pateikiamas ne tik kaip techninis modelis – galingi

strateginės analizės pajėgumai ir geresnis operatyvinės informacijos rinkimas bei tvarkymas. Taip pat pripažįstama, kad reikėtų atsižvelgti į su politika susijusius aspektus, tokius kaip informacijos rinkimo, keitimosi ja ir jos tvarkymo kriterijus, tuo pat metu laikantis duomenų apsaugos principų.

55. Informacinės technologijos ir teisinės sąlygos yra ir visada bus svarbios. EDAPP palankiai vertina Komunikatą, kurio pradžioje pateikiama prielaida, kad Europos informacijos modelio negalima sukurti remiantis techniniais motyvais. Svarbu, kad informacija būtų renkama, ja keičiamasi ir ji tvarkoma tik remiantis konkrečiais saugumo poreikiais ir atsižvelgiant į duomenų apsaugos principus. EDAPP taip pat visiškai pritaria tam, kad reikia nustatyti kontrolės mechanizmą, kad būtų galima įvertinti, kaip vyksta keitimasis informacija. Jis siūlo Tarybai toliau plėtoti šiuos elementus Stokholmo programoje.
56. Todėl EDAPP pabrėžia, kad neturėtų būti manoma, jog duomenų apsauga, kuria siekiama apsaugoti piliečius, trukdo veiksmingai valdyti duomenis. Ji užtikrina svarbias informacijos saugojimo, galimybių ja naudotis ir keistis gerinimo priemones. Duomenų subjekto teisės būti informuotam apie tai, kokia su juo susijusi informacija yra tvarkoma, ir ištaisyti neteisingą informaciją taip pat gali padidinti duomenų valdymo sistemose laikomų duomenų tikslumą.
57. Iš esmės pagal duomenų apsaugos teisės aktus duomenis galima naudoti, jei jų reikia konkrečiam teisėtam tikslui; asmens duomenų nereikėtų naudoti, jei jų nereikia aiškiai apibrėžtam tikslui. Pirmu atveju gali reikėti papildomų priemonių siekiant užtikrinti tinkamas apsaugos priemones.

58. Tačiau EDAPP kritiškai vertina tai, koku mastu Komunikate kaip informacijos modelio dalis minimas „būsimų poreikių nustatymas“. Jis pabrėžia, kad ir ateityje kuriant informacines sistemas reikėtų vadovautis ribojimo pagal tikslą principu⁽³⁵⁾. Tai viena iš pagrindinių garantijų, kurią duomenų apsaugos sistema suteikia piliečiui: jis turi iš anksto žinoti, kokiam tikslui renkami su juo susiję duomenys, ir kad jie bus naudojami tik tam tikslui, ypač ateityje. Ši garantija netgi įtvirtinta Sąjungos pagrindinių teisių chartijos 8 straipsnyje. Numatytos ribojimo pagal tikslą principo išimtys, o tai ypač aktualu laisvės, saugumo ir teisingumo erdvėje, tačiau tos išimtys neturėtų lemti sistemos sandaros.

⁽³¹⁾ COM(2005) 490 galutinis.

⁽³²⁾ Prieinamumo principo atžvilgiu; Priumo sprendime nustatytos plataus užmojo nuostos dėl biometrinių duomenų (DNR ir pirštų atspaudų) naudojimo.

⁽³³⁾ OL L 210, 2008 8 6, p. 1.

⁽³⁴⁾ Žr. Vyriausybės ES darbo programą, nurodytą 5 išnašoje, p. 23.

⁽³⁵⁾ Žr. taip pat 41 punktą.

Tinkamos architektūros parinkimas

59. Pirmiausia reikia parinkti tinkamą keitimosi informacija architektūrą. Komunikate pripažįstama, kad tinkama informacijos architektūra yra svarbus aspektas (4.1.3 punktas), tačiau tik sąveikos atžvilgiu.
60. EDAPP pabrėžia kitą aspektą: Europos informacijos modeliui taikomi duomenų apsaugos reikalavimai turėtų būti neatsiejama visos sistemos kūrimo dalis ir neturėtų būti manoma, kad jie būtini tik tam, kad sistema būtų teisėta⁽³⁶⁾. Turėtų būti vadovojamasi privatumo projektuojant ir poreikio nustatyti „geriausius technologijų būdus“⁽³⁷⁾ koncepcijomis, kaip nurodyta 4.3 punkte. Europos informacijos modelis turėtų būti grindžiamas šiomis koncepcijomis. Tiksliau, tai reiškia, kad informacinės sistemos, kurios sukurtos siekiant užtikrinti visuomenės saugumą, visada turėtų būti kuriamos laikantis privatumo projektuojant principo. EDAPP rekomenduoja Tarybai šiuos elementus įtraukti į Stokholmo programą.

Sistemų sąveika

61. EDAPP pabrėžia, kad sąveika nėra vien tik techninis klausimas, bet ir daro poveikį piliečių apsaugai – visų pirma duomenų apsaugai. Duomenų apsaugos atžvilgiu sistemų sąveika, jei gerai suderinta, turi aiškių privalumų, nes išvengiama dvigubo saugojimo. Tačiau taip pat akivaizdu, kad prieigą prie duomenų arba keitimąsi jais padarius techniškai įgyvendinamu dalyku dažnai atsiranda didelė paskata naudotis arba keistis tais duomenimis *de facto*. Kitaip tariant, sąveika ypač kelia pavojų, kad bus jungiamasi tarp duomenų bazių, kurių tikslai yra skirtingi⁽³⁸⁾. Taip gali būti nukrypta nuo griežtų duomenų bazių tikslų apribojimų.
62. Trumpai tariant, pats faktas, kad techniškai galima keistis skaitmenine informacija tarp sąveikių duomenų bazių arba sujungti šias duomenų bazes, nepateisina ribojimo pagal tikslą principo išimties taikymo. Konkrečiais atvejais sąveika

turėtų būti grindžiama aiškiais ir atsargiais politiniais sprendimais. EDAPP siūlo Stokholmo programoje patikslinti šią nuostatą.

VI.2. Kitiems tikslams surinktos informacijos naudojimas

63. Komunikate aiškiai neišnagrinėta viena iš svarbiausių pastarųjų metų tendencija, t. y. privačiajame sektoriuje komerciniais tikslais surinktų duomenų naudojimas teisėsaugoje. Ši tendencija susijusi ne tik su elektroninių ryšių šrauto duomenimis ir asmenų, skrendančių į (tam tikras) trečiasias šalis, keleivių duomenimis⁽³⁹⁾, bet ir su finansų sektoriumi. Pavyzdys yra 2005 m. spalio 26 d. Europos Parlamento ir Tarybos direktyva 2005/60/EB dėl finansų sistemos apsaugos nuo jos panaudojimo pinigų plovimui ir teroristų finansavimui⁽⁴⁰⁾. Kitas gerai žinomas ir daug diskusijų sukėlęs pavyzdys yra Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT)⁽⁴¹⁾ atliekamas asmens duomenų tvarkymas pagal JAV išdo departamento teroristų finansavimo sekimo programą.
64. EDAPP nuomone, Stokholmo programoje šioms tendencijoms reikia skirti ypatingą dėmesį. Šias tendencijas galima laikyti nukrypimu nuo ribojimo pagal tikslą principo; jos dažnai labai pažeidžia privatumą, nes naudojant šiuos duomenis galima labai daug sužinoti apie asmenų elgesį. Kiekvienu atveju, kai siūlomos tokios priemonės, turi būti pateikta labai tvirtų įrodymų, kad tokia invazinė priemonė yra reikalinga. Jei tokie įrodymai pateikiami, turi būti užtikrinta visapusiška asmenų teisių apsauga.
65. EDAPP nuomone, komerciniais tikslais surinktus asmens duomenis naudoti teisėsaugoje turėtų būti leidžiama tik nustatčius griežtas sąlygas, pavyzdžiui:

— duomenys turi būti naudojami tik konkrečiais kiekvienu atveju nustatytais tikslais, pvz., kovojant su terorizmu arba sunkiais nusikaltimais,

— duomenys turi būti perduodami taikant „eksporto“, o ne „importo“ sistemą⁽⁴²⁾,

⁽³⁶⁾ Žr. PRISE projekto metu parengtas „Privatumo didinimo saugumo technologijų kūrimo, diegimo ir naudojimo gaires bei kriterijus“ (*Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies*) (<http://www.prise.oew.ac.at>).

⁽³⁷⁾ Geriausi technologijų būdai – veiksmingiausia ir pažangiausia veiklos ir jos vykdymo metodų plėtojimo pakopa; tai reiškia, kad tam tikri technologijų būdai yra praktiškai tinkami iš esmės būti IT programų ir sistemų suderinimo su ES reglamentavimo sistemoje numatyto privatumo, duomenų apsaugos ir saugumo reikalavimo pagrindu.

⁽³⁸⁾ Žr. EDAPP pastabas dėl Komisijos komunikato dėl Europos duomenų bazių sąveikos, 2006 m. kovo 10 d.: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

⁽³⁹⁾ Žr., pvz., 15 punktą.

⁽⁴⁰⁾ OL L 309, 2005 11 25, p. 15.

⁽⁴¹⁾ Žr. 29 straipsnio darbo grupės nuomonę 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo.

⁽⁴²⁾ Pagal „eksporto“ sistemą duomenų valdytojas nusiunčia („eksportuoja“) duomenis prašančiai teisėsaugos institucijai. Pagal „importo“ sistemą teisėsaugos institucija turi prieigą prie duomenų valdytojo duomenų bazės ir gauna („importuoja“) informaciją iš šios duomenų bazės. Pagal „importo“ sistemą duomenų valdytojui sunkiau atgauti atsakomybę.

- prašymai pateikti duomenis turėtų būti proporcingi, susiję su konkrečiu tikslu ir iš esmės grįsti tam tikriems asmenims pateiktais įtarimais,
- turėtų būti vengiama atlikti einamąsias paieškas, duomenų gavybą ir profiliavimą,
- bet koks duomenų naudojimas teisėsaugoje turėtų būti registruojamas, kad savo teisėmis besinaudojantis duomenų subjektas, duomenų apsaugos institucijos ir teisminės institucijos galėtų atlikti veiksmingą jų naudojimo kontrolę.

VI.3. Informacinės sistemos ir ES organai

Centralizuoto arba decentralizuoto saugojimo informacinės sistemos ⁽⁴³⁾

66. Per pastaruosius metus laisvės, saugumo ir teisingumo erdvėje gerokai padaugėjo ES teise grindžiamų informacinių sistemų. Kartais primami sprendimai dėl centralizuoto duomenų saugojimo Europos lygiu sistemos sukūrimo, kitais atvejais teisės aktais numatomas tik keitimasis informacija tarp nacionalinių duomenų bazių. Šengeno informacinė sistema, ko gero, yra geriausias centralizuoto saugojimo sistemos pavyzdys. Tarybos sprendimas 2008/615/TVR (Priemo sprendimas) ⁽⁴⁴⁾ duomenų apsaugos atžvilgiu – pats geriausias decentralizuotos saugojimo sistemos pavyzdys, nes juo numatomas didžiulis keitimasis biometriniais duomenimis tarp valstybių narių valdžios institucijų.
67. Pagal Komunikatą galima spręsti, kad ši naujų sistemų kūrimo tendencija išliks. Pirmas pavyzdys, pateiktas 4.2.2 punkte, yra informacinė sistema, kuria išplečiama Europos nuosprendžių registru informacinė sistema (ECRIS) siekiant įtraukti šalių, kurios nėra ES narės, piliečius. Komisija jau pavedė atlikti Europos registro, skirto nuteistiems trečiųjų šalių piliečiams (EICTCN), tyrimą, kurį atlikus galbūt bus sukurta centralizuota duomenų bazė. Kitas pavyzdys – keitimasis informacija apie asmenis, įtrauktus į nemokumo registrus kitose valstybėse narėse, pagal e. teisingumo programą (Komunikato 3.4.1 punktas), netaikant centralizuoto saugojimo galimybes.
68. Duomenų apsaugos atžvilgiu decentralizuota sistema turėtų tam tikrų privalumų. Išvengiama dvigubo duomenų saugojimo – valstybės narės valdžios institucijoje ir centralizuotoje sistemoje; tokiu atveju yra aiški atsakomybė už duomenis, nes duomenų valdytojas yra valstybės narės valdžios institucija, o teisminės institucijos ir duomenų apsaugos institucijos gali vykdyti kontrolę valstybių narių lygiu. Tačiau ši sistema turi ir trūkumų, kai keičiamasi

duomenimis su kitomis jurisdikcijomis, pavyzdžiui, siekiant užtikrinti, kad tiek kilmės valstybė, tiek paskirties valstybė turėtų naujausią informaciją, ir užtikrinti veiksmingą kontrolę abiejose valstybėse. Dar sudėtingiau užtikrinti atsakomybę už techninę keitimosi sistemą. Šiuos trūkumus galima pašalinti pasirinkus centralizuotą sistemą, už kurią, bent jau už sistemos dalis (tokias kaip techninė infrastruktūra), būtų atsakingi Europos organai.

69. Todėl būtų naudinga parengti esminius centralizuotos ir decentralizuotos sistemos pasirinkimo kriterijus, konkrečiais atvejais užtikrinant aiškius ir atsargius politinius sprendimus. Šie kriterijai gali padėti užtikrinti sistemų veikimą ir piliečių duomenų apsaugą. EDAPP siūlo į Stokholmo programą įtraukti ketinimą parengti tokius kriterijus.

Didelės apimties informacinės sistemos

70. Komunikato 4.2.3.2 punkte trumpai aptariama didelės apimties informacinių sistemų ateitis, pagrindinį dėmesį skiriant Šengeno informacinei sistemai (SIS) ir Vizų informacinei sistemai (VIS).
71. 4.2.3.2 punkte taip pat nurodoma, kad bus sukurta elektroninio atvykimo į valstybių narių teritoriją ir išvykimo iš jos registravimo sistema bei keleivių registravimo programos. Komisija Pirmininko pavaduotojo F. Frattini iniciatyva apie šią sistemą pranešė jau anksčiau, pristatydamas dokumentų sienų valdymo srityje rinkinį ⁽⁴⁵⁾. Pateikdamas preliminarines pastabas ⁽⁴⁶⁾ EDAPP buvo gana kritiškai nusiteikęs dėl šio pasiūlymo, nes nebuvo aiškiai pagrįstas tokios intervencinės sistemos poreikis, atsižvelgiant į tai, kad jau veikia didelės apimties sistemos. EDAPP nežinoma apie jokių papildomus tokios sistemos reikalingumo įrodymus ir todėl jis siūlo Tarybai Stokholmo programoje apie tai neužsiminti.
72. Todėl EDAPP norėtų paminėti savo nuomones dėl įvairių iniciatyvų ES keitimosi informacija srityje ⁽⁴⁷⁾, kuriose gausiai pateikta pasiūlymų ir pastabų dėl didelių duomenų bazių naudojimo ES lygiu poveikio duomenų apsaugai. Be kitų klausimų, daug dėmesio buvo skirta griežtų ir specializuotų apsaugos priemonių, kurias reikėtų įdiegti, poreikiui,

⁽⁴³⁾ Čia centralizuotas saugojimas suprantamas kaip saugojimas centriniu Europos lygiu, o decentralizuotas saugojimas – kaip saugojimas valstybių narių lygiu.

⁽⁴⁴⁾ Žr. 33 išnašą.

⁽⁴⁵⁾ Komisijos komunikatas „Pasirengimas kitiems Europos Sąjungos sienų valdymo etapams“, 2008 2 13, COM(2008) 69.

⁽⁴⁶⁾ EDAPP preliminarios pastabos dėl trijų Komisijos komunikatų dėl sienų valdymo (COM(2008) 69, COM(2008) 68 ir COM(2008) 67), 2008 kovo 3 d.: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

⁽⁴⁷⁾ Konkrečiai: 2005 m. kovo 23 d. nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl Vizų informacinės sistemos (VIS) ir apsikeitimo duomenimis apie trumpalaikes vizas tarp valstybių narių (OL C 181, 2005 7 23, p. 13) ir 2005 m. spalio 19 d. nuomonė dėl trijų pasiūlymų dėl antrosios kartos Šengeno informacinės sistemos (SIS II) (OL C 91, 2006 4 19, p. 38).

taip pat poveikio vertinimo proporcingumui ir būtinybei prieš siūlant ar imantis bet kokių priemonių šioje srityje. EDAPP visada palaikė teisingą ir duomenų apsauga grįstą saugumo reikalavimų ir asmenų, kurių duomenys tvarkomi sistemoje, privatumo apsaugos pusiausvyrą. Jis laikėsi tokios pačios pozicijos veikdamas kaip sistemų centrinių dalių priežiūros pareigūnas.

73. Be to, EDAPP šia proga norėtų pabrėžti, kad reikia laikytis nuoseklaus požiūrio į ES keitimąsi informacija kaip į visumą, turint omenyje jau veikiančių ir kuriamų sistemų teisinį, techninį ir priežiūros nuoseklumą. Iš tiesų šiais laikais labiau nei anksčiau yra neabejotinai reikalinga drąsi ir visapusiška vizija, kaip turėtų atrodyti ES keitimasis informacija ir kokia turėtų būti didelės apimties informacinių sistemų ateitis. Tik tokios vizijos pagrindu galbūt galėtų būti iš naujo svarstoma elektroninio atvykimo į valstybių narių teritoriją ir išvykimo iš jos registravimo sistema.

74. EDAPP siūlo Stokholmo programoje nurodyti ketinimą parengti tokią viziją, atsižvelgiant į galimą Lisabonos sutarties įsigaliojimą ir jos poveikį pirmojo ir trečiojo ramsčių teisiniu pagrindu grindžiamoms sistemoms.

75. Galiausiai, Komunikate užsimenama apie naujos agentūros, kuri pagal Komunikatą taip pat turėtų būti kompetentinga elektroninės atvykimo ir išvykimo registravimo sistemos klausimais, įsteigimą. Komisija priėmė pasiūlymą dėl tokios agentūros įsteigimo⁽⁴⁸⁾. EDAPP iš principo pritaria šiam pasiūlymui, nes įsteigus tokią agentūrą gali padidėti šių sistemų ir duomenų apsaugos veiksmingumas. Jis reikiamu laiku pateiks nuomonę dėl šio pasiūlymo.

Europolas ir Eurojustas

76. Komunikate keliose vietose užsimenama apie Europolo vaidmenį ir pirmiausia pabrėžiama, kad Europolas turi atlikti svarbiausią vaidmenį koordinuojant veiklą, keičiantis informacija ir mokant specialistus. Be to, Komunikato 4.2.2 punkte nurodomi naujausi Eurojusto ir Europolo bendradarbiavimo teisinio pagrindo pakeitimai ir pranešama, kad toliau bus stiprinamas Eurojustas, ypač organizuoto tarpvalstybinio nusikalstamumo tyrimo srityje. EDAPP visiškai pritaria šiems tikslams, jei bus tinkamai laikomasi duomenų apsaugos užtikrinimo priemonių.

⁽⁴⁸⁾ 2009 m. birželio 24 d. Komisijos pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo įsteigiama Šengeno informacinės sistemos (SIS II), Vizų informacinės sistemos (VIS), EURODAC ir kitų didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra (COM(2009) 293/2).

77. Todėl EDAPP palankiai vertina naują susitarimo projektą, dėl kurio neseniai susitarė Europolas ir Eurojustas⁽⁴⁹⁾ ir kuriuo siekiama pagerinti ir sustiprinti abiejų organų tarpusavio bendradarbiavimą bei sudaryti sąlygas veiksmingai tarpusavyje keistis informacija. Vykdamas šią veiklą efektyvi ir veiksminga duomenų apsauga yra itin svarbi.

VI.4. Biometrinių duomenų naudojimas

78. EDAPP atkreipia dėmesį į tai, kad Komunikate nenagrinėjamas vis intensyvesnio biometrinių duomenų naudojimo įvairiuose Europos Sąjungos teisės aktuose dėl keitimosi informacija naudojimo, įskaitant aktus dėl didelės apimties informacinių sistemų sukūrimo, klausimas. Dėl to reikia apgailestauti, kadangi duomenų apsaugos ir privatumo atžvilgiu tai yra ypatingas svarbos ir opus reikalas.

79. EDAPP pripažįsta bendrus biometrinių duomenų naudojimo privalumus, tačiau jis nuolat pabrėžia, kad tokių duomenų naudojimas daro didžiulį poveikį asmenų teisėms, ir siūlo įtraukti griežtas biometrinių duomenų naudojimo kiekvienoje atitinkamoje sistemoje apsaugos priemones. Neseniai priimtas Europos žmogaus teisių teismo sprendimas byloje *S. ir Marper prieš Jungtinę Karalystę*⁽⁵⁰⁾ yra šiuo atveju naudingas šaltinis, visų pirma biometrinių duomenų naudojimo pagrindimo ir ribų klausimais. Visų pirma DNR informacijos naudojimas gali atskleisti neskelbtiną informaciją apie asmenis, taip pat atsižvelgiant į tai, kad vis didėja informacijos iš DNR gavimo techninės galimybės. Intensyvaus biometrinių duomenų naudojimo informacinėse sistemose atveju taip pat kyla problema dėl pasitaikančių netikslumų renkant biometrinius duomenis ir juos lyginant. Dėl šių priežasčių ES teisės aktų leidėjas turėtų užimti santūrią poziciją dėl šių duomenų naudojimo.

80. Kitas pastaraisiais metais nuolat kylantis klausimas yra vaikų ir vyresnio amžiaus asmenų pirštų atspaudų naudojimas, nes biometrinių duomenų sistemos pačios savaime turi trūkumų šių amžiaus grupių atžvilgiu. EDAPP paprašė atlikti išsamų tyrimą siekiant tinkamai nustatyti šių sistemų tikslumą⁽⁵¹⁾. Jis pasiūlė vaikams nustatyti 14 metų amžiaus ribą, nebent šiuo tyrimu būtų įrodyta kitaip. EDAPP rekomenduoja Stokholmo programoje paminėti šį klausimą.

⁽⁴⁹⁾ Tarybos patvirtintas susitarimo projektas, kurį turi pasirašyti abi šalys. Žr. Tarybos dokumentų registrą:

<http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf>
<http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf>

⁽⁵⁰⁾ Jungtinė paraiška 30562/04 ir 30566/04, *S. ir Marper prieš Jungtinę Karalystę*, 2008 m. gruodžio 4 d. sprendimas, ETT, dar nepaskelbta.

⁽⁵¹⁾ 2008 m. kovo 26 d. nuomonė dėl pasiūlymo dėl reglamento, iš dalies keičiančio Tarybos reglamentą (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų (OL C 200, 2008 8 6, p. 1).

81. Todėl EDAPP mano, kad būtų naudinga parengti esminius biometrinių duomenų naudojimo kriterijus. Šiais kriterijais turėtų būti užtikrinama, kad duomenys būtų naudojami tik esant būtinybei, tinkamai bei proporcingai ir kai teisės aktų leidėjas nurodo aiškų, tiksliai apibrėžtą ir teisėtą tikslą. Konkrečiau, biometriniai duomenys ir visų pirma DNR duomenys neturėtų būti naudojami, jei tą patį rezultatą galima pasiekti naudojanti kitą, ne tokią konfidencialią informaciją.

VII. TEISĖ KREIPTIS Į TEISMĄ IR E. TEISINGUMAS

82. Technologijos taip pat bus naudojamos kaip geresnio teismo bendradarbiavimo priemonė. Komunikato 3.4.1 punkte nurodoma, kad e. teisingumas suteikia daugiau galimybių piliečiams kreiptis į teismą. E. teisingumas – tai portalas, kuriame pateikiama informacija ir vaizdo konferencijos kaip teisinės procedūros dalis. Be to, greitai teisinės procedūros galės būti atliekamos internetu ir numatoma tarpusavyje sujungti nacionalinius registrus, pavyzdžiui, nemokumo registrus. EDAPP atkreipia dėmesį į tai, kad Komunikate neminimos naujos su e. teisingumu susijusios iniciatyvos, tačiau sustiprinami veiksmai, kurių jau imtasi. EDAPP dalyvauja kai kuriuose iš tų veiksmų vykdydamas su savo 2008 m. gruodžio 19 d. nuomone dėl Komisijos komunikato „Europos e. teisingumo strategijos link“⁽⁵²⁾ susijusią tolesnę veiklą.

83. E. teisingumas – platus užmojo projektas, kurį reikia visapusiškai remti. Šis projektas gali veiksmingai patobulinti Europos teisingumo sistemą ir piliečių teisminę apsaugą. Tai reikšmingas žingsnis į priekį kuriant Europos teisingumo erdvę. Atsižvelgiant į šį teigiamą įvertinimą galima padaryti kelias pastabas:

- e. teisingumo technologinės sistemos turėtų būti kuriamos laikantis privatumo projektuojant principo. Kaip jau minėta, kuriant Europos informacijos modelį pirmiausia reikia parinkti tinkamą architektūrą,
- sistemų sujungimas ir sąveika neturėtų pažeisti ribojimo pagal tikslą principo,
- turėtų būti tiksliai nustatyta įvairių subjektų atsakomybė,
- turėtų būti iš anksto išnagrinėtos nacionalinių registru, kuriuose saugomi konfidencialūs asmens duomenys, pvz., nemokumo registru, sujungimo pasekmės asmenims.

VIII. IŠVADOS

84. EDAPP pritaria, kad Komunikate pagrindinių teisių apsauga, visų pirma asmens duomenų apsauga, laikoma vienu iš

svarbiausių laisvės, saugumo ir teisingumo erdvės ateities klausimų. EDAPP nuomone, Komunikate tinkamai skatinama išlaikyti tinkamų piliečių saugumą užtikrinančių priemonių poreikio ir jų pagrindinių teisių apsaugos pusiausvyrą. Pripažįstama, kad daugiau dėmesio reikėtų skirti asmens duomenų apsaugai.

85. EDAPP visiškai pritaria Komunikato 2.3 punktui, kuriame raginama sukurti išsamią duomenų apsaugos sistemą, kuri apimtų visas ES kompetencijos sritis, neatsižvelgiant į Lisabonos sutarties įsigaliojimą. Todėl jis rekomenduoja:

- Stokholmo programoje nurodyti, kad būtina aiški ir ilgalaikė tokios išsamos sistemos vizija,
- įvertinti priemones, kurios jau buvo patvirtintos šioje srityje, jų konkretų įgyvendinimą ir veiksmingumą, atsižvelgiant į privatumo užtikrinimo išlaidas ir veiksmingumą teisėsaugos požiūriu,
- į Stokholmo programą kaip prioritetą įtraukti poreikį sukurti naują teisinę sistemą, *inter alia*, pakeičiančią Tarybos pamatinį sprendimą 2008/977/TVR.

86. EDAPP palankiai vertina Komisijos ketinimus dar kartą patvirtinti duomenų apsaugos principus; ši veikla turėtų būti atliekama po viešosios konsultacijos, apie kurią Komisija paskelbė 2009 m. gegužės 19–20 d. vykusioje konferencijoje „Asmens duomenys – daugiau naudojami, labiau saugomi?“. Dėl klausimo esmės EDAPP pabrėžia, kad ribojimo pagal tikslą principas, kaip duomenų apsaugos teisės aktų kertinis akmuo, yra labai svarbus ir svarbu daug dėmesio skirti galimybėms pagerinti duomenų apsaugos principų taikymo veiksmingumą, naudojant priemones, kuriomis galima sustiprinti duomenų valdytojų atsakomybę.

87. Privatumo projektuojant principas ir privatumo nepažeidžiančios technologijos galėtų būti skatinamos nustatant:

- privatumo ir duomenų apsaugos sertifikavimo sistemą – informacinių sistemų kūrėjams ir naudotojams skirtą galimybę,
- informacinių sistemų kūrėjų ir naudotojų teisinį išpaigojimą naudoti sistemas nepažeidžiant privatumo projektuojant principo.

88. Dėl duomenų apsaugos išorės aspektų EDAPP rekomenduoja:

- Stokholmo programoje pabrėžti bendrųjų susitarimų dėl duomenų apsaugos ir keitimosi duomenimis su Jungtinėmis Valstijomis ir kitomis trečiosiomis šalimis svarbą,

⁽⁵²⁾ 2008 m. gruodžio 19 d. EDAPP nuomonė dėl Komisijos komunikato „Europos e. teisingumo strategijos link“, OL C 128, 2009 6 6, p. 13.

- aktyviai skatinti gerbti pagrindines teises, visų pirma teisę į duomenų apsaugą, palaikant santykius su trečiojomis šalimis ir tarptautinėmis organizacijomis,
 - Stokholmo programoje paminėti, kad keičiantis asmens duomenimis su trečiosiomis šalimis būtina užtikrinti tinkamą apsaugos lygį arba kitas atitinkamas apsaugos priemones tose trečiojoiose šalyse.
89. EDAPP labai susidomėjęs atkreipia dėmesį į Europos Sąjungos informacijos valdymo strategijos ir Europos informacijos modelio kūrimo procesą ir pabrėžia, kad šiuose projektuose tinkamas dėmesys turėtų būti skirtas duomenų apsaugos elementams, kurie bus toliau plėtojami Stokholmo programoje. Keitimosi informacija architektūra turėtų būti grindžiama privatumo projektuojant principu ir geriausiais technologijų būdais.
90. Pats faktas, kad techniškai galima keistis skaitmenine informacija tarp sąveikių duomenų bazių arba sujungti šias duomenų bazes, nepateisina ribojimo pagal tikslą principo išimties taikymo. Konkrečiais atvejais sąveika turėtų būti grindžiama aiškiais ir atsargiais politiniais sprendimais. EDAPP siūlo Stokholmo programoje patikslinti šią nuostatą.
91. EDAPP nuomone, komerciniais tikslais surinktus asmens duomenis naudoti teisėsaugoje turėtų būti leidžiama tik nustačius griežtas sąlygas, nurodytas šios nuomonės 65 punkte.
92. Kiti pasiūlymai dėl asmeninės informacijos naudojimo:
- parengti esminius centralizuotos ir decentralizuotos sistemos pasirinkimo kriterijus bei įtraukti į Stokholmo programą ketinimą parengti tokius kriterijus,
 - Stokholmo programoje nereikėtų minėti, kad bus sukurta elektroninio atvykimo į valstybių narių teritoriją ir išvykimo iš jos registravimo sistema bei keleivių registravimo programos,
 - remti Europolo ir Eurojusto stiprinimą ir naują neseniai parengtą Europolo ir Eurojusto susitarimą,
 - parengti esminius biometrinių duomenų naudojimo kriterijus užtikrinant, kad duomenys būtų naudojami tik esant būtinybei, tinkamai bei proporcingai ir kai teisės aktų leidėjas nurodo aiškų, tiksliai apibrėžtą ir teisėtą tikslą. DNR duomenys neturėtų būti naudojami, jei tą patį rezultatą galima pasiekti naudojanti kitą, ne tokią konfidencialią informaciją.
93. EDAPP pritaria e. teisingumo projektui ir pateikė kelias pastabas dėl šio projekto pagerinimo (žr. 83 punktą).

Priimta Briuselyje 2009 m. liepos 10 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas