ISSN 1725-521X

Europos Sąjungos oficialusis leidinys

C 128

Leidimas
lietuvių kalba

52 tomas
2009 m. birželio 6 d.

Informacija ir pranešimai

Pranešimo Nr. Turinys Puslapis

LT

(Tęsinys antrajame viršelyje)

IV *Pranešimai*

EUROPOS SĄJUNGOS INSTITUCIJŲ IR ORGANŲ PRANEŠIMAI

Komisija

Klaidų ištaisymas

LT

I

(Rezoliucijos, rekomendacijos ir nuomonės)

NUOMONĖS

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl ES ir JAV aukšto lygio ryšių palaikymo grupės dėl keitimosi informacija, privatumo ir asmens duomenų apsaugos galutinės ataskaitos

(2009/C 128/01)

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 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 – SU NUOMONE SUSIJUSI BENDRA INFORMACIJA

1. 2008 m. gegužės 28 d. Europos Sąjungos Tarybai pirmininkaujanti valstybė narė, atsižvelgdama į 2008 m. birželio 12 d. ES aukščiausiojo lygio susitikimą, pranešė Nuolatinių atstovų komitetui, kad ES ir JAV aukšto lygio ryšių palaikymo grupė (toliau – HLCG) dėl keitimosi informacija, privatumo ir asmens duomenų apsaugos parengė galutinę ataskaitą. Ši ataskaita paskelbta 2008 m. birželio 26 d. ([1]).

2. Ataskaita siekiama apibrėžti bendrus privatumo ir duomenų apsaugos principus, kurie yra pirmas žingsnis siekiant keistis informacija su Jungtinėmis Amerikos Valstijomis kovai su terorizmu ir sunkiais tarptautiniais nusikaltimais.

3. Pranešime Tarybai pirmininkaujanti valstybė narė nurodo, kad ji pageidautų sužinoti nuomonių dėl tolesnių veiksmų, susijusių su šia ataskaita, visų pirma gauti pastabų dėl rekomendacijų dėl ataskaitoje nurodytų tolesnių veiksmų. Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) reaguodamas į šį kvietimą pateikia toliau išdėstytą nuomonę, parengtą remiantis dabartine padėtimi ir neturinčią įtakos jokiai kitai pozicijai, kurią jis galėtų pareikšti atsižvelgdamas į su šiuo klausimu susijusius pokyčius.

4. EDAPP pažymi, kad HLCG darbas buvo atliekamas tokiu metu, kai JAV ir ES pradėjo intensyviau keistis duomenims remdamosi tarptautiniais ar kitokiais susitarimais, ypač nuo 2001 m. rugsėjo 11 d. Tarp jų yra Europolo ir Eurojusto susitarimai su Jungtinėmis Amerikos Valstijomis, taip pat susitarimai dėl keleivio duomenų įrašo (PNR) bei SWIFT atvejis, dėl kurio ES ir JAV pareigūnai pasikeitė laiškais siekdamos nustatyti būtiniausias duomenų apsaugos garantijas ([2]).

([1]) Tarybos dokumentas Nr. 9831/08 pateiktas šioje tinklavietėje adresu http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — 2001 m. gruodžio 6 d. Jungtinių Amerikos Valstijų ir Europos policijos biuro susitarimas bei Papildomas Europolo ir JAV susitarimas dėl keitimosi asmens duomenimis ir susijusia informacija, paskelbti Europolo tinklavietėje;
— 2006 m. lapkričio 6 d. Jungtinių Amerikos Valstijų ir Eurojusto susitarimas dėl teisminio bendradarbiavimo, paskelbtas Eurojusto tinklavietėje;
— Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimas dėl oro vežėjų atliekamo keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Jungtinių Valstijų Vidaus saugumo departamentui (DHS) (2007 PNR susitarimas), pasirašytas 2007 m. liepos 23 d. Briuselyje ir 2007 m. liepos 26 d. Vašingtone (OL L 204, 2007 8 4, p. 18);
— JAV ir ES valdžios institucijų pasikeitimas laiškais dėl Terorizmo finansavimo sekimo programos, 2007 m. birželio 28 d.

5. Be to, ES veda derybas ir pritaria panašiems susitarimams, kuriuose numatytas keitimasis asmens duomenimis su kitomis trečiosiomis šalimis. Europos Sąjungos ir Australijos susitarimas dėl oro vežėjų atliekamo Europos Sąjungos pateiktų keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Australijos muitinės tarnybai ([3]) yra naujausias tokių susitarimų pavyzdys.

6. Todėl akivaizdu, kad trečiųjų šalių teisėsaugos institucijos prašo vis didesnės apimties asmens duomenų, prašydamos ne tik duomenų iš įprastų valstybės duomenų bazių, bet ir iš kitų bylų, visų pirma privačiojo sektoriaus surinktų duomenų.

7. EDAPP taip pat primena svarbų susijusį aspektą – asmens duomenų perdavimo trečiosioms šalims vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose klausimas yra aptartas Tarybos pamatiniame sprendime dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos ([4]), kuris turėtų būti priimtas iki 2008 m. pabaigos.

8. Šis transatlantinis keitimasis informacija galėtų tik suintensyvėti ir apimti papildomus sektorius, kurie susiję su asmens duomenų tvarkymu. Todėl dialogas „transatlantinės teisėsaugos klausimais“ taip pat yra pageidautinas ir labai svarbus. Jis pageidautinas ta prasme, kad jis galėtų suteikti aiškesnį pagrindą duomenų keitimuisi, kuris šiuo metu vyksta ar vyks. Jis taip pat labai svarbus, nes toks pagrindas įteisintų didelės apimties duomenų perdavimą srityje (teisėsauga), kurioje jis daro ypač didelį poveikį asmenims ir kurioje patikimos apsaugos priemonės ir garantijos yra dar labiau reikalingos ([5]).

9. Kitame šios nuomonės skyriuje bus aptarta dabartinė padėtis ir galimi tolesni veiksmai. III skyriuje bus aptarta susitarimo, kuris suteiktų galimybę keistis informacija, taikymo sritis ir pobūdis. Nuomonės IV skyriuje bus nagrinėjami su galimo susitarimo turiniu susiję teisiniai klausimai atsižvelgiant į bendrą perspektyvą. Jame bus aptarti klausimai, pavyzdžiui, Jungtinėse Amerikos Valstijose užtikrinamo apsaugos lygio vertinimo sąlygos, ir aptartas ES reglamentavimo sistemos taikymas kaip kriterijus vertinant tokios apsaugos lygį. Šiame skyriuje taip pat bus išdėstyti pagrindiniai reikalavimai, kurie turi būti įtraukti į tokį susitarimą. Galiausiai, nuomonės V skyriuje bus pateikta prie ataskaitos pridedamų privatumo principų analizė.

([3]) OL L 213, 2008 8 8, p. 49.

([4]) Tarybos pamatinis sprendimas dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos, 2008 m. birželio 24 d. redakcija; jis pateiktas tinklavietėje adresu http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371.

([5]) Dėl aiškaus teisinio pagrindo būtinybės žr. šios nuomonės III ir IV skyrius.

II. DABARTINĖ PADĖTIS IR GALIMI TOLESNI VEIKSMAI

10. EDAPP dabartinę padėtį vertina taip: buvo padaryta tam tikra pažanga siekiant apibrėžti bendrus keitimosi informacija, privatumo ir asmens duomenų apsaugos standartus.

11. Tačiau parengiamasis darbas, susijęs su bet kokio pobūdžio ES ir JAV susitarimu, dar nebaigtas. Reikia atlikti papildomą darbą. Pačioje HLCG ataskaitoje paminėta daug neišspręstų klausimų, iš kurių žalos atlyginimo klausimas yra pats aktualiausias. Vis dar nesutariama dėl žalos atlyginimo teismo tvarka taikymo srities ([6]). Penki kiti neišspręsti klausimai nurodyti ataskaitos 3 skyriuje. Be to, šioje nuomonėje pažymima, kad yra dar daugelis kitų neišspręstų klausimų, pavyzdžiui, dėl keitimosi informacija susitarimo taikymo srities ir pobūdžio.

12. Kadangi ataskaitoje nurodyta, kad pageidautina galimybė yra privalomas susitarimas, ir EDAPP pritaria tokiai nuomonei, atsargumas yra dar reikalingesnis. Reikia tęsti nuodugnų ir išsamų pasirengimą, kad būtų galima pasiekti susitarimą.

13. Galiausiai, pasak EDAPP, būtų geriausia, jei susitarimas būtų sudarytas pagal Lisabonos sutartį, žinoma, jei ji įsigalios. Iš tiesų pagal Lisabonos sutartį nebūtų teisinio netikrumo dėl ES ramsčių skiriamosios ribos. Be to, būtų užtikrintas visiškas Europos Parlamento dalyvavimas bei teisminė kontrolė, kurią vykdytų Teisingumo Teismas.

14. Tokiomis aplinkybėmis geriausias būdas būtų parengti veiksmų planą galimam susitarimui pasiekti vėlesniame etape. Tokiame veiksmų plane būtų pateikti šie elementai:

— HLCG (ar kurios nors kitos grupės) tolesnio darbo gairės bei tvarkaraštis;

— pradiniame etape – esminių klausimų, pavyzdžiui, dėl susitarimo taikymo srities ir pobūdžio, aptarimas ir galimas susitarimas dėl jų;

— remiantis bendru šių esminių klausimų supratimu, tolesnis duomenų apsaugos principų rengimas;

— suinteresuotųjų subjektų dalyvavimas įvairiuose procedūros etapuose;

— Europos atveju – su instituciniais apribojimais susijusių klausimų sprendimas.

([6]) Ataskaitos 5 puslapis, C dalis.

III. **SUSITARIMO DĖL KEITIMOSI INFORMACIJA TAIKYMO SRITIS IR POBŪDIS**

15. EDAPP nuomone, itin svarbu, kad galimo susitarimo, kuriame būtų numatyti duomenų apsaugos principai, taikymo sritis ir pobūdis būtų aiškiai apibrėžti, ir tai būtų pirmas žingsnis toliau rengiant tokį susitarimą.

16. Taikymo srities klausimu reikia atsakyti į šiuos svarbius klausimus:

— kas yra susiję subjektai teisėsaugos ir kitos srityse;

— ką reiškia „teisėsaugos tikslas“ ir kokia jo sąsaja su kitais tikslais, pavyzdžiui, nacionaliniu saugumu, o konkrečiau su sienų kontrole bei visuomenės sveikata;

— kaip susitarimas būtų suderinamas su visuotinės transatlantinės saugumo erdvės perspektyva.

17. Pobūdžio sąvokos apibrėžtis padėtų paaiškinti šiuos klausimus:

— jei būtina, pagal kurį ramstį bus vedamos derybos dėl susitarimo;

— ar susitarimas bus privalomas ES ir JAV;

— ar jis turės tiesioginį poveikį ta prasme, kad jame bus apibrėžtos asmenų teisės ir pareigos, kurios gali būti vykdomos teisminėje institucijoje;

— ar pats susitarimas numatys galimybę keistis informacija ar nustatys būtiniausią keitimosi informacija standartą, kurį papildytų konkretūs susitarimai;

— kaip susitarimas bus siejamas su galiojančiais susitarimais: ar jis atitiks, pakeis ar papildys juos?

III.1. **Susitarimo taikymo sritis**

Susiję subjektai

18. Nors HLCG ataskaitoje nėra aiškiai nurodyta, kokia turėtų būti tiksli būsimo susitarimo taikymo sritis, remiantis joje paminėtais principais galima daryti išvadą, kad susitarimas turėtų būti taikomas duomenų perdavimui tiek tarp privačiojo ir valstybės sektorių subjektų ([7]), tiek tarp valstybės institucijų.

— Privačiojo ir valstybės sektorių subjektų atveju:

19. EDAPP supranta, kodėl pagal kokį principą būsimas susitarimas turėtų būti taikomas duomenų perdavimui tarp privačiojo ir valstybės sektorių subjektų. Toks susitarimas rengiamas atsižvelgiant į pastaraisiais metais JAV teikiamus prašymus privačiojo sektoriaus subjektams teikti informaciją. EDAPP iš tiesų pažymi, kad privačiojo sektoriaus subjektai tampa sistemingu informacijos šaltiniu teisėsaugos srityje tiek ES, tiek tarptautiniu lygiu ([8]). SWIFT atvejis buvo svarbus precedentas, kai privačios bendrovės buvo prašoma sistemingai perduoti didelės apimties duomenis trečiosios valstybės teisėsaugos institucijoms ([9]). PNR duomenys iš aviakompanijų renkami pagal tokį pat principą. EADDP nuomonėje dėl pamatinio sprendimo projekto dėl europinės PNR sistemos jau pareiškė abejonę dėl tokios tendencijos teisėtumo ([10]).

20. Yra dar dvi priežastys, dėl kurių duomenų perdavimo tarp privačiojo ir valstybės sektorių subjektų nereikėtų įtraukti į būsimo susitarimo taikymo sritį.

21. Pirma, tokių subjektų įtraukimas galėtų padaryti nepageidaujamą poveikį pačios ES teritorijoje. EADDP yra labai susirūpinęs dėl to, kad tuo atveju, jeigu privačių bendrovių (pvz., finansų įstaigų) duomenys iš esmės būtų perduodami trečiosioms šalims, atsirastų didelis spaudimas tokius ES turimus duomenis taip pat teikti teisėsaugos institucijoms. PNR sistema – tokios nepageidautinos tendencijos, kuri atsirado JAV pradėjus dideliais kiekiais rinkti keleivių duomenis ir kuri tokiu būdu atsirastų ir Europoje ([11]), pavyzdys, nors sistemos būtinumas ir proporcingumas nėra aiškiai pagrįsti.

22. Antra, savo nuomonėje dėl Komisijos pasiūlymo dėl ES PNR EADDP taip pat iškėlė duomenų apsaugos sistemos (pirmojo ar antrojo ramsčio), taikytinos valstybės ir privačiojo sektorių subjektų bendradarbiavimo sąlygoms, klausimą: ar taisyklės turėtų būti grindžiamos duomenų valdytojo (privačiojo sektoriaus) kokybe ar siektinu tikslu (teisėsauga)? Pirmojo ir trečiojo ramsčių skiriamoji linija yra labai neaiški tais atvejais, kai įpareigojimai tvarkyti asmens duomenis teisėsaugos tikslais nustatomi privačiojo sektoriaus subjektams. Todėl šiuo atžvilgiu palankiai vertinama tai, kad Generalinis advokatas Bot neseniai pateiktoje

([7]) Visų pirma žr. ataskaitos 3 skyriaus „Su transatlantiniais santykiais susiję neišspręsti klausimai“ 1 punktą: „Privačiojo sektoriaus subjektų įpareigojimų suderinamumas vykdant duomenų perdavimą“.

([8]) Šiuo klausimu žr. 2007 m. gruodžio 20 d. EADDP nuomonę dėl pasiūlymo dėl Tarybos pamatinio sprendimo dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teisėsaugoje, OL C 110, 2008 5 1, p. 1. „Tradiciškai teisėsaugos ir privačiojo sektoriaus veikla yra aiškiai atskirta: su teisėsauga susijusį darbą atlieka specialiai tam paskirtos institucijos, būtent policijos pajėgos, o privačių subjektų kiekvienu konkrečiu atveju prašoma perduoti asmens duomenis šioms teisėsaugos institucijoms. Šiuo metu esama tendencijos privatiems subjektams primesti sistemingą bendradarbiavimą teisėsaugos tikslais“.

([9]) Žr. pagal 29 straipsnio darbo grupės 2006 m. lapkričio 22 d. Nuomonę 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo, DG 128.

([10]) 2007 m. gruodžio 20 d. nuomonė, op. cit.

([11]) Žr. 8 išnašoje paminėtą pasiūlymą dėl Tarybos pamatinio sprendimo dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teisėsaugoje, kuris šiuo metu svarstomas Taryboje.

nuomonėje byloje dėl duomenų saugojimo ([12]) pasiūlė tokiems atvejams skiriamosios linijos apibrėžimą, tačiau EDAPP taip pat teigia, kad: „šią skiriamąją liniją tikrai galima įvertinti kritiškai ir kai kuriais aspektais ji gali atrodyti dirbtinai apibrėžta“. EDAPP taip pat pažymi, kad Teismo sprendime dėl PNR ([13]) nėra visiškai atsakyta į klausimą dėl taikytino teisinio pagrindo. Pavyzdžiui, tai, kad Direktyva 95/46/EB netaikoma tam tikroms veiklos rūšims automatiškai nereiškia, kad šios veiklos rūšys gali būti reglamentuojamos pagal trečiąjį ramstį. Todėl taikytinos teisės požiūriu gali būti palikta spraga ir kiekvienu atveju atsiranda teisinis netikrumas dėl duomenų subjektams užtikrinamų teisinių garantijų.

23. Atsižvelgdamas į tai, EDAPP pabrėžia, kad būtina užtikrinti, jog galimas būsimas susitarimas, kuriame būtų išdėstyti bendri duomenų apsaugos principai, negali automatiškai įteisinti transatlantinio asmens duomenų perdavimo tarp privačiojo ir valstybės sektorių subjektų. Toks perdavimas būsimame susitarime gali būti numatytas tik tuo atveju, jeigu:

— būsimame susitarime būtų numatyta, kad perduoti duomenis leidžiama tik tuo atveju, jeigu įrodyta, kad tai visiškai būtina konkrečiam tikslui, o sprendžiama kiekvienu konkrečiu atveju;

— pats perdavimas atliekamas taikant aukšto lygio duomenų apsaugos priemones (kaip nurodyta šioje nuomonėje).

Be to, EDAPP pažymi, kad yra netikrumas dėl taikytino teisinio duomenų apsaugos pagrindo, ir todėl prašo bet kokiu atveju nenumatyti asmens duomenų perdavimo tarp privačiojo ir valstybės sektorių subjektų pagal galiojančią ES teisę.

— Valstybės institucijų atveju:

24. Tiksli keitimosi informacijos taikymo sritis nėra aiški. Tolesniame darbe rengiant bendrą susitarimą pirmiausia reikėtų tiksliai apibrėžti numatomą tokio susitarimo taikymo sritį. Visų pirma reikia išspręsti šiuos klausimus:

— ar dėl ES veikiančių duomenų bazių – susitarimas apimtų centralizuotas duomenų bazes, kurias (iš dalies) tvarko ES, pavyzdžiui, Europolo ir Eurojusto duomenų bazes arba valstybių narių tvarkomas decentralizuotas duomenų bazes, arba abiejų rūšių duomenų bazes;

— ar susitarimo taikymo sritis apimtų tarpusavyje sujungtus tinklus, t. y. ar numatytos garantijos būtų taikomos duomenims, kuriais keičiasi valstybės narės ar agentūros ES bei JAV;

— ar susitarimas būtų taikomas keičiantis tik duomenų bazių duomenimis teisėsaugos (policijos, teisingumo, galbūt muitinės) srityse ir kitų duomenų bazių, pavyzdžiui, mokesčių, duomenimis;

— ar susitarimas taip pat apimtų nacionalinių saugumo agentūrų duomenų bazes ar sudarytų galimybę toms agentūroms turėti prieigą prie teisėsaugos duomenų bazių kitos susitariančiosios šalies teritorijoje (Europos Sąjungai – Jungtinėse Amerikos Valstijose ir atvirkščiai);

— ar susitarimas kiekvienu konkrečiu atveju apimtų informacijos perdavimą ar nuolatinę prieigą prie veikiančių duomenų bazių. Dėl pastarosios prielaidos tikrai kils su proporcingumu susijusių klausimų, kaip toliau aptariama V skyriaus 3 punkte.

Teisėsaugos tikslas

25. Dėl galimo susitarimo tikslo apibrėžimo taip pat yra netikrumo. Teisėsaugos tikslai yra aiškiai nurodyti įvade bei ataskaitos dalyje, kur išdėstytas pridedamas pirmasis principas, ir bus toliau nagrinėjami šios nuomonės IV skyriuje. EDAPP pažymi, kad remiantis šia informacija galima manyti, jog keitimasis duomenimis daugiausia būtų vykdomas trečiojo ramsčio klausimais, tačiau gali kilti klausimas, ar tai yra tik pirmas žingsnis siekiant suintensyvinti keitimąsi duomenimis. Atrodo aišku, kad ataskaitoje nurodyti „visuomenės saugumo“ tikslai apima kovą su terorizmu, organizuotu nusikalstamumu ir kitais nusikaltimais. Tačiau ar tai irgi reiškia, kad gali būti leidžiama keistis duomenimis kitų viešų interesų labui, pavyzdžiui, galbūt siekiant išvengti rizikos visuomenės sveikatai?

26. EDAPP rekomenduoja numatyti, kad tikslas – tai tiksliai nustatytas duomenų tvarkymas, ir pagrįsti pasirinktus politinius sprendimus, kuriais remiantis taip apibrėžtas tikslas.

([12]) Generalinio advokato Bot 2008 m. spalio 14 d. nuomonė *Airija prieš Europos Parlamentą ir Tarybą* (Byla C- 301/06), 108 punktas.

([13]) 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.

Visuotinė transatlantinė saugumo erdvė

27. Plati šios ataskaitos taikymo sritis turėtų būti vertinama atsižvelgiant į visuotinę transatlantinės saugumo erdvės perspektyvą, kurią aptarė „Ateities grupė“ ([14]). 2008 m. birželio mėn. paskelbtoje šios grupės ataskaitoje šiek tiek dėmesio skirta vidaus reikalų politikos išorės aspektui. Joje nurodoma, kad *„iki 2014 m. Europos Sąjunga turėtų apsispręsti dėl politinio tikslo – sukurti euroatlantinę bendradarbiavimo su Jungtinėmis Valstijomis laisvės, saugumo ir teisingumo srityse erdvę“*. Bendradarbiaujama būtų ne tik saugumo klausimais siaurąja prasme, bet bent jau tose srityse tokiais klausimais, kurie numatyti dabartinėje EB sutarties IV antraštinėje dalyje, t. y. imigracijos, vizų, prieglobsčio ir bendradarbiavimo civilinės teisės srityse, klausimais. Būtina kelti klausimą, kaip susitarimas dėl pagrindinių duomenų apsaugos principų, pavyzdžiui, paminėtų HLCG ataskaitoje, galėtų ir turėtų būti keitimosi informacija tokioje plačioje srityje pagrindas.

28. Iš esmės iki 2014 m. ramsčių struktūros nebeliks, o bus vienas teisinis duomenų apsaugos pagrindas pačios ES viduje (pagal Lisabonos sutartį, Sutarties 16 straipsnis dėl Europos Sąjungos veikimo). Tačiau iš tiesų tai, kad duomenų apsaugos *reglamentavimas* yra suderintas ES lygiu, nereiškia, kad bet kokiame susitarime su trečiąja šalimi būtų numatyta galimybė *perduoti* asmens duomenis bet kokiu tikslu. Atsižvelgiant į duomenų tvarkymo aplinkybes ir sąlygas, tam tikrose srityse, pavyzdžiui, teisėsaugos, gali reikėti keisti duomenų apsaugos garantijas. EDAPP rekomenduoja rengiant būsimą susitarimą atsižvelgti į tokių skirtingų aspektų padarinius.

III.2. **Susitarimo pobūdis**

Europos institucinė struktūra

29. Bet kokiu atveju trumpalaikiu laikotarpiu itin svarbu nustatyti, pagal kurį ramstį bus vedamos derybos dėl susitarimo. To ypač reikia asmens duomenų apsaugos vidaus reglamentavimo sistemos, kuriai toks susitarimas turės įtakos, atžvilgiu. Ar tai bus pirmasis ramstis-pagrindas – iš esmės Direktyva 95/46/EB, kurioje numatyta speciali duomenų perdavimo trečiosioms šalims tvarka, – ar tai bus trečiasis ramstis-pagrindas, kuriame būtų numatyta ne tokia griežta duomenų perdavimo trečiosioms šalims tvarka? ([15])

30. Nors, kaip jau minėta, teisėsaugos tikslai yra pagrindiniai, HLCG ataskaitoje taip pat nurodytas duomenų rinkimas iš privačiojo sektoriaus subjektų, o tikslai taip pat gali būti aiškinami plačiąja prasme, įtraukiant ne tik saugumo, bet ir imigracijos ir sienų kontrolės klausimus, o galbūt ir visuomenės sveikatos klausimus. Atsižvelgiant į tokį netikrumą, būtų labai pageidautina palaukti ramsčių suderinimo pagal ES teisę, kaip numatyta Lisabonos sutartyje, kad būtų aiškiai nustatytas teisinis derybų pagrindas ir tiksliai apibrėžtas Europos institucijų, ypač Europos Parlamento ir Komisijos, vaidmuo.

Privalomas susitarimo pobūdis

31. Reikėtų aiškiai nustatyti, ar remiantis diskusijų išvadomis bus sudarytas susitarimo memorandumas arba kitoks neprivalomas susitarimas, ar tai bus privalomas tarptautinis susitarimas.

32. EDAPP pritaria ataskaitoje pateiktai nuomonei, kad reikalingas privalomas susitarimas. EDAPP nuomone, oficialus privalomas susitarimas būtinas tam, kad būtų vykdomas duomenų perdavimas už ES ribų, nesvarbu, kokiu tikslu duomenys perduodami. Duomenys trečiajai šaliai negali būti perduodami, jei nesilaikoma atitinkamų sąlygų ir apsaugos priemonių, numatytų konkrečiame (ir privalomame) teisiniame pagrinde. Kitaip tariant, susitarimo memorandumas ar kitoks neprivalomas susitarimas gali būti naudingas derybų dėl kitų privalomų susitarimų gairėms nustatyti, tačiau jokiu būdu negali pakeisti būtino privalomo susitarimo.

Tiesioginis poveikis

33. Susitarimo nuostatos turėtų būti privalomos tiek JAV, tiek ES bei jos valstybėms narėms.

34. Be to, reikėtų užtikrinti, kad asmenys turėtų teisę naudotis savo teisėmis ir ypač gauti žalos atlyginimą pagal susitartus principus. EDAPP nuomone, šį rezultatą galima geriausiai pasiekti, jei esminės susitarimo nuostatos yra taip suformuluotos, kad jos turi tiesioginį poveikį Europos Sąjungos gyventojams ir gali būti taikomos teisme. Todėl susitarime turi būti aiškiai nurodytas tiesioginis tarptautinio susitarimo nuostatų poveikis bei jų perkėlimo į Europos ir nacionalinę teisę siekiant užtikrinti priemonių veiksmingumą sąlygos.

Sąsaja su kitais dokumentais

35. Kitas esminis klausimas – kiek susitarimas gali būti taikomas atskirai arba kiekvienu konkrečiu atveju papildytas kitais susitarimais dėl konkretaus keitimosi duomenimis. Iš tiesų kyla klausimas, ar atskiras susitarimas, kuriame nustatyti bendri standartai, galėtų tinkamai aprėpti daugybę duomenų tvarkymo trečiojo ramsčio klausimais ypatumų. Dar daugiau abejonių kyla dėl to, ar be papildomų diskusijų ir nenumačius apsaugos priemonių būtų galima taip paprastai patvirtinti asmens duomenų perdavimą, neatsižvelgiant į atitinkamų asmenų tikslą ir pobūdį. Be to, susitarimai su trečiosiomis šalimis nebūtinai yra

([14]) Europos vidaus reikalų politikos ateities neoficialios aukšto lygio patariamosios grupės ataskaita „Laisvė, saugumas, privatumas – Europos vidaus reikalai atvirame pasaulyje“, 2008 m. birželio mėn., pateikta tinklavietėje adresu register.consilium.europa.eu

([15]) Žr. šios nuomonės 7 punkte paminėto sprendimo (DAPS) 11 ir 13 straipsnius.

nuolatiniai, nes jie gali būti susiję su tam tikromis grėsmėmis, peržiūrimi arba jiems taikomos nuostatos dėl laikino galiojimo. Kita vertus, privalomame susitarime pripažinti bendri būtiniausi standartai galėtų sudaryti palankesnes sąlygas toliau diskutuoti dėl asmens duomenų perdavimo, susijusio su konkrečia duomenų baze ar duomenų tvarkymo veiksmais.

36. Todėl EDAPP pritartų tam, kad būtų parengti būtiniausi duomenų apsaugos kriterijai, kuriuos kiekvienu konkrečiu atveju papildytų papildomos konkrečios nuostatos, kaip paminėta HLCG ataskaitoje, o nebūtų vadovaujamasi vienu atskiru susitarimu. Šios papildomos konkrečios nuostatos yra būtinos tam, kad būtų numatyta galimybė perduoti duomenis konkrečiu atveju. Tai paskatintų taikyti suderintą duomenų apsaugos metodą.

Galiojančių susitarimų taikymas

37. Reikėtų taip pat nagrinėti, kaip galimas bendras susitarimas būtų suderintas su jau galiojančiais ES ir JAV sudarytais susitarimais. Reikėtų pažymėti, kad šie galiojantys susitarimai neturi tokio pat privalomo pobūdžio: visų pirma, pažymėtinas PNR susitarimas (suteikiantis daugiau teisinio tikrumo), Europolo ir Eurojusto susitarimai arba SWIFT pasikeitimas laiškais ([16]). Ar šie nauji bendri teisės aktai papildytų šiuos galiojančius susitarimus, ar jie liktų nepakitę, ir nauji teisės aktai būtų taikomi tik keitimuisi asmens duomenimis ateityje? EDAPP nuomone, siekiant teisinio suderinamumo reikėtų parengti suderintas taisykles, taikomas tiek galiojantiems, tiek būsimiems privalomiems susitarimams dėl duomenų perdavimo ir juos papildantiems.

38. Bendro susitarimo taikymas galiojantiems susitarimams turėtų privalumą – sustiprintų jų privalomą pobūdį. Visų pirma tai būtų pageidautina teisiškai neprivalomų susitarimų, pavyzdžiui, SWIFT pasikeitimo laiškais, atžvilgiu, nes taip būtų nustatytas reikalavimas laikytis bendrų privatumo principų.

IV. **BENDRO POBŪDŽIO TEISINIS ĮVERTINIMAS**

39. Šiame skyriuje bus nagrinėjama, kokiu būdu turi būti įvertintas konkrečia sistema ar dokumentu užtikrinamos apsaugos lygis, įskaitant taikytinus kriterijus ir būtinus pagrindinius reikalavimus.

([16]) Žr. 2 išnašą.

Tinkamas apsaugos lygis

40. Anot EDAPP, turėtų būti akivaizdu, jog vienas iš būsimų susitarimo pagrindinių pasiekimų – užtikrinimas, kad asmens duomenys Jungtinėms Valstijoms būtų perduodami tik tuo atveju, jei Jungtinių Amerikos Valstijų institucijos garantuoja tinkamą apsaugos lygį (ir atvirkščiai).

41. EDAPP nuomone, asmens duomenų apsaugos lygį tinkamai garantuotų tik realus tinkamumo testas. Jis teigia, kad bendrasis susitarimas, kurio taikymo sritis būtų tokia pat plati, kaip HLCG parengtos ataskaitos, pats savaime vargu ar išlaikytų realų tinkamumo testą. Bendrasis susitarimas galėtų būti pripažintas tinkamu tik tuo atveju, jei jis būtų susietas su kiekvienu konkrečiu atveju sudarytais tinkamais specialiais susitarimais.

42. Trečiųjų šalių užtikrinamos apsaugos lygio įvertinimas nėra neįprasta užduotis, visų pirma Europos Komisijai: pagal pirmąjį ramstį tinkamumas yra vienas iš perdavimui taikytinų reikalavimų. Remiantis konkrečiais kriterijais tinkamumas buvo keletą kartų įvertintas pagal Direktyvos 95/46/EB 25 straipsnį – tai patvirtinta Europos Komisijos sprendimais ([17]). Pagal trečiąjį ramstį tokia sistema nėra aiškiai numatyta: vertinti apsaugos tinkamumą įpareigojama tik pamatinio sprendimo dėl duomenų apsaugos (dar nepriimtas) 11 ir 13 straipsniuose apibrėžtais konkrečiais atvejais ([18]) ir ši pareiga yra skirta valstybėms narėms.

43. Šiuo atveju užduotis susijusi su teisėsaugos tikslais, o diskusijas rengia Komisija prižiūrint Tarybai. Aplinkybės lyginant su „saugaus uosto“ privatumo principų ar Kanados teisės aktų tinkamumo vertinimu skiriasi ir labiau siejamos su derybomis dėl PNR duomenų tvarkymo, kurios neseniai buvo surengtos su JAV ir Australija pagal trečiajam ramsčiui priskiriamus teisės aktus. Tačiau HLCG principai buvo paminėti ir diskutuojant dėl vizų režimo netaikymo programos, kuri susijusi su sienų apsaugos ir imigracijos klausimais – taigi, pirmojo ramsčio klausimais.

44. EDAPP rekomenduoja visus tinkamumo vertinimus pagal galimą būsimą susitarimą atlikti remiantis patirtimi

([17]) Komisijos sprendimai dėl asmens duomenų apsaugos tinkamumo trečiosiose šalyse, įskaitant Argentiną, Kanadą, Šveicariją, Jungtines Valstijas, Gernsiu, Meno salą ir Džersį (pateikiami tinklavietėje adresu http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm).

([18]) Tik tuo atveju, jei valstybė narė perduoda trečiajai šaliai ar tarptautinei organizacijai kitos valstybės narės kompetentingos institucijos pateiktus duomenis.

minėtose įvairiose srityse. Jis rekomenduoja galimame būsimame susitarime dar labiau išplėsti „tinkamumo“ sąvoką remiantis panašiais kriterijais, kurie buvo taikomi apibrėžiant ankstesnes tinkamumo sąvokas.

Abipusis pripažinimas – abipusiškumas

45. Dar vienas apsaugos lygio aspektas siejamas su abipusiu ES ir JAV sistemų pripažinimu. HLCG ataskaitoje šiuo klausimu nurodyta, kad tikslas – „siekti viena kitos privatumo ir duomenų apsaugos sistemų veiksmingumo pripažinimo srityse, kurioms taikomi minėti principai“ ([19]) ir užtikrinti „lygiavertį ir abipusį privatumo ir asmens duomenų apsaugos teisės aktų taikymą“.

46. EDAPP akivaizdu, kad abipusis pripažinimas (arba abipusiškumas) įmanomas tik tuo atveju, jei yra užtikrintas tinkamas apsaugos lygis. Kitaip tariant, būsimame susitarime turėtų būti suderintos nuostatos dėl būtiniausio apsaugos lygio (atliekant tinkamumo vertinimą, atsižvelgiant į specialių susitarimų poreikį kiekvienu konkrečiu atveju). Abipusis pripažinimas yra įmanomas tik laikantis šios būtinos sąlygos.

47. Pirmasis elementas, į kurį reikia atsižvelgti – esminių nuostatų dėl duomenų apsaugos abipusiškumas. EDAPP nuomone, susitarime esminių nuostatų dėl duomenų apsaugos abipusiškumo sąvoka turėtų būti nagrinėjama taip, jog būtų užtikrinta, kad, viena vertus, tvarkant duomenis ES teritorijoje (ir JAV) būtų visiškai laikomasi vietos teisės aktų dėl duomenų apsaugos ir, kita vertus, kad tvarkant susitarimo taikymo sričiai priklausančius duomenis ne kilmės šalyje būtų laikomasi tame susitarime numatytų duomenų apsaugos principų.

48. Antrasis aspektas – žalos atlyginimo mechanizmų abipusiškumas. Turėtų būti užtikrinta, kad Europos piliečiams būtų garantuojamos tinkamos žalos atlyginimo priemonės, kai su jais susiję duomenys tvarkomi Jungtinėse Valstijoje (neatsižvelgiant į tokiam duomenų tvarkymui taikomą teisės aktą), ir kad lygiai taip pat Europos Sąjunga ir jos valstybės narės suteiktų lygiavertes teises JAV piliečiams.

49. Trečiasis aspektas – abipusis teisėsaugos institucijų teisės susipažinti su asmens duomenimis užtikrinimas. Jei kokiu nors dokumentu Jungtinių Valstijų institucijoms būtų suteikta prieiga prie ES duomenų, abipusiškumas reikštų, kad tokia pati prieiga prie JAV duomenų turėtų būti suteikta ES institucijoms. Abipusiškumas neturi pakenkti duomenų subjekto apsaugos veiksmingumui. Tai viena iš teisėsaugos institucijoms suteikiamos „transatlantinės“ prieigos būtinų sąlygų. Konkrečiai tai reiškia, kad:

— Jungtinių Valstijų institucijoms tiesioginė prieiga prie duomenų ES teritorijoje (ir atvirkščiai) neturėtų būti suteikta. Prieiga turėtų būti suteikta tik netiesiogiai pagal aktyviąją sistema („*push*“ sistema).

— Tokios prieigos sąlygas turėtų kontroliuoti šalies, kurioje tvarkomi duomenys, duomenų apsaugos institucijos ir teisminės institucijos.

— Jungtinių Valstijų institucijų prieigą prie ES turimų duomenų bazių turėtų reglamentuoti esminės nuostatos dėl duomenų apsaugos (žr. aukščiau) ir tokios prieigos atžvilgiu duomenų subjektui turėtų būti užtikrintos visapusiškos žalos atlyginimo priemonės.

Susitarimo tikslumas

50. Labai svarbu tiksliai apibrėžti įvertinimo (tinkamumo, lygiavertiškumo, abipusio pripažinimo) sąlygas, nes tai lemia apsaugos turinį tikslumo, teisinio tikrumo ir veiksmingumo požiūriu. Būsimo dokumento turinys turi būti tikslus ir išsamus.

51. Be to, turėtų būti akivaizdu, kad vėlesniame etape sudarytuose specialiuose susitarimuose taip pat reikės išsamiai ir visapusiškai apibrėžti apsaugos priemones dėl duomenų apsaugos, taikytinas numatomo keitimosi duomenimis objektui. Tik tokie dviejų lygių konkretaus pobūdžio duomenų apsaugos principai užtikrintų būtiną bendrojo susitarimo ir specialių susitarimų „glaudžią sąsają“, kaip jau nurodyta šios nuomonės 35 ir 36 punktuose.

Kitoms trečiosioms šalims skirto modelio nustatymas

52. Ypatingą dėmesį reikėtų skirti tam, kiek susitarimas su JAV gali būti pavyzdžiu kitų trečiųjų šalių atžvilgiu. EDAPP pažymi, kad pirmiau minėtoje Ateities grupės ataskaitoje strateginėmis ES partnerėmis įvardyta net tik JAV, bet ir Rusija. Atsižvelgiant į tai, kad principai yra neutralūs ir atitinka esmines ES apsaugos priemones, jie galėtų sudaryti vertingą precedentą. Tačiau ypatumai, susiję, pavyzdžiui, su duomenis gaunančios šalies teisine sąranga arba duomenų perdavimo tikslu, trukdytų vien tik perkelti susitarimo nuostatas. Vienodai lemiamas veiksnys bus demokratijos padėtis trečiosiose šalyse: reikėtų įsitikinti, kad principai, dėl kurių bus susitarta, bus veiksmingai garantuojami ir įgyvendinami duomenis gaunančioje šalyje.

Kokie kriterijai taikomi siekiant įvertinti apsaugos lygį?

53. Tačiau vertinant numanomą ar aiškų tinkamumą reikėtų laikytis tarptautinių bei europinių teisės aktų ir visų pirma apsaugos priemonių duomenų apsaugos srityje, dėl kurių bendrai susitarta. Jie yra nustatyti Jungtinių Tautų

([19]) A skyrius. Privalomas tarptautinis susitarimas, p. 8.

gairėse, Europos Tarybos konvencijoje Nr. 108 ir jos papildomame protokole, OECD gairėse ir pamatinio sprendimo dėl duomenų apsaugos projekte, o pirmojo ramsčio aspektais – Direktyvoje 95/46/EB ([20]). Visuose šiuose dokumentuose nustatyti panašūs principai, kurie iš esmės pripažinti kaip pagrindiniai duomenų apsaugos principai.

54. Atsižvelgiant į galimo susitarimo, pavyzdžiui, numatytojo HLCG ataskaitoje, poveikį, labai svarbu tinkamai atsižvelgti į pirmiau nurodytus principus. Dokumentas, kuris apimtų visą trečiosios šalies *vykdymo užtikrinimo* sektorių, iš tiesų reikštų precedento neturinčią situaciją. Galiojantys sprendimai dėl tinkamumo pirmojo ramsčio srityje ir su trečiosiomis šalimis sudaryti susitarimai ES trečiojo ramsčio srityje (Europolas, Eurojustas) visuomet buvo susiję su konkrečiu duomenų perdavimu, tačiau atsižvelgiant į visapusišką siektiną tikslą (kova su nusikalstamumu, nacionalinis bei visuomenės saugumas, sienų saugumo užtikrinimas) ir tai, kad nežinomas atitinkamų duomenų bazių skaičius, šiuo metu kalbame apie galimybę perduoti duomenis daug didesniu mastu.

Pagrindiniai reikalavimai

55. Sąlygos, kurių būtina laikytis perduodant asmens duomenis trečiosioms šalims, nustatytos 29 straipsnio darbo grupės darbiniame dokumente ([21]). Visi susitarimai dėl būtiniausių privatumo principų turėtų užtikrinti atitikties testo reikalavimus, užtikrinančius apsaugos priemonių dėl duomenų apsaugos veiksmingumą.

— Dėl esmės: duomenų apsaugos principai turėtų numatyti aukšto lygio apsaugą ir atitikti su ES principais suderintus standartus. HLCG ataskaitoje nustatyti 12 principų bus šiuo atžvilgiu toliau analizuojami šio nuomonės V skyriuje.

— Dėl specifiškumo: atsižvelgiant į susitarimo pobūdį ir visų pirma tuo atveju, jei tai oficialus tarptautinis susitarimas, taisyklės ir procedūros turėtų būti pakankamai išsamios, kad susitarimą būtų galima veiksmingai įgyvendinti.

— Dėl priežiūros: siekiant užtikrinti atitiktį taisyklėms, dėl kurių susitarta, turėtų būti įdiegti konkretūs kontrolės mechanizmai vidaus kontrolės (auditas) ir išorės kontrolės (peržiūros) srityse. Šie mechanizmai turi būti vienodai prieinami abiem susitarimo šalims. Priežiūra apima mechanizmus, kuriais siekiama užtikrinti atitiktį makro lygiu, pavyzdžiui, bendros peržiūros mechanizmai, ir atitiktį mikro lygiu, pavyzdžiui, atskiros žalos atlyginimo priemonės.

56. Be šių trijų pagrindinių reikalavimų ypatingą dėmesį reikėtų skirti specifiškumui, siejamam su asmens duomenų tvarkymu teisėsaugos tikslais. Tai iš tiesų yra sritis, kurioje pagrindinės teisės gali būti šiek tiek apribotos. Todėl kompensuojant asmens teisių apribojimus ir atsižvelgiant į poveikį asmeniui turėtų būti patvirtintos apsaugos priemonės visų pirma toliau nurodytais aspektais:

— Skaidrumas: informacija apie asmens duomenis ir teisė su jais susipažinti gali būti suteikta tik teisėsaugos tikslais, pavyzdžiui, atsižvelgiant į vykdomų slaptų tyrimų poreikius. Nors ES tradiciškai nustatomi papildomi mechanizmai tokiam pagrindinių teisių apribojimui kompensuoti (dažnai pasitelkiant nepriklausomas duomenų apsaugos institucijas), vis dėlto turi būti užtikrinta, kad informaciją perdavus trečiajai šaliai bus galima naudotis panašiais kompensavimo mechanizmais.

— Žalos atlyginimo priemonės: dėl pirmiau nurodytų priežasčių asmenims turėtų būti užtikrintos alternatyvios galimybės apginti savo teises, visų pirma naudojantis nepriklausomos priežiūros institucijos paslaugomis ir teisme.

— Duomenų saugojimas: duomenų saugojimo laikotarpio pagrindimas nebūtinai gali būti skaidrus. Turi būti imtasi priemonių užtikrinti, kad tai duomenų subjektams ar priežiūros institucijoms netrukdytų veiksmingai naudotis teisėmis.

([20]) — 1990 m. gruodžio 14 d. Generalinės Asamblėjos priimtos Jungtinių Tautų gairės dėl kompiuterizuotų asmens duomenų bylų, pateikiamos tinklavietėje adresu www.unhchr.ch/html/menu3/b/71.htm
— 1981 m. sausio 28 d. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, pateikiama tinklavietėje adresu www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— 1980 m. rugsėjo 23 d. EOCD gairės dėl privatumo apsaugos ir asmens duomenų tarpvalstybinių srautų, pateikiama tinklavietėje adresu www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Tarybos pamatinio sprendimo dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos, projektas, pateikiamas tinklavietėje adresu http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).

([21]) 1998 m. liepos 24 d. darbinis dokumentas dėl asmens duomenų perdavimų trečiosioms šalims: ES duomenų apsaugos direktyvos 25 ir 26 straipsnių taikymas; DG 12.

— Teisėsaugos institucijų atskaitomybė: tuo atveju, jei skaidrumas nėra veiksmingas, asmenų arba institucinių subjektų taikomi kontrolės mechanizmai negali būti visapusiški. Vis dėlto labai svarbu turėti patikimai veikiančius kontrolės mechanizmus atsižvelgiant į neskelbtiną tokių duomenų pobūdį ir prievartos priemones, kurias galima taikyti asmenims duomenų tvarkymo pagrindu. Atskaitomybė yra lemiamas klausimas duomenis gaunančios šalies nacionalinių kontrolės mechanizmų atžvilgiu bei duomenų kilmės šalyje ar regione esamų peržiūros galimybių atžvilgiu. Tokie peržiūros mechanizmai numatyti specialiuose susitarimuose, pavyzdžiui, susitarime dėl PNR duomenų, ir EDAPP primygtinai rekomenduoja juos taip pat įtraukti į bendrąjį susitarimą.

V. **PRINCIPŲ ANALIZĖ**

Įvadas

57. Šiame skyriuje atsižvelgiant į toliau nurodytus principus nagrinėjami HLCG dokumente numatyti 12 principų:

— Šie principai rodo, kad JAV ir ES laikosi tam tikro bendro požiūrio dėl principų apimties, nes galima įžvelgti panašumų su Konvencijoje Nr. 108 nustatytais principais.

— Tačiau sutarimo dėl principų apimties nepakanka. Siekiant užtikrinti atitiktį, reikalingas pakankamai griežtas teisinis dokumentas.

— EDAPP apgailestauja, kad prie principų nėra pridėtas aiškinamasis memorandumas.

— Turėtų būti akivaizdu, kad dar prieš apibrėždamos principus abi šalys turi vienodai aiškinti vartojamas formuluotes, pavyzdžiui, dėl asmens duomenų ar saugomų asmenų. Todėl būtų palankiai įvertintas sprendimas pateikti sąvokų apibrėžtis.

1. Išsamus tikslo apibūdinimas

58. Pirmasis HLCG ataskaitos priede nurodytas principas – asmens duomenys tvarkomi teisėtais teisėsaugos tikslais. Kaip nurodyta pirmiau, ES tai reiškia nusikaltimų prevenciją, nustatymą, tyrimą ar patraukimą baudžiamojon atsakomybėn. Tačiau Jungtinėse Valstijose teisėsaugos sąvoka aiškinama plačiau, ją siejant ne vien su nusikaltimų sritimi, bet ir „sienų saugumo, visuomenės saugumo ir nacionalinio saugumo tikslais“. Tokių ES ir JAV nurodytų tikslų neatitikimo pasekmės neaiškios. Nors ataskaitoje minima, kad iš principo šie tikslai gali didžia dalimi sutapti, ir toliau yra labai svarbu tiksliai žinoti, kiek šie tikslai *ne*sutampa. Teisėsaugos srityje atsižvelgiant į asmenims taikomų priemonių poveikį būtina griežtai laikytis tikslo ribojimo principo, o nurodyti principai privalo būti aiškūs ir apriboti. Atsižvelgiant į ataskaitoje numatytą abipusiškumą, taip pat būtų labai svarbu suderinti šiuos tikslus. Trumpai, būtina patikslinti tai, kaip šis principas suprantamas.

2. Vientisumas/duomenų kokybė

59. EDAPP palankiai vertina nuostatą, pagal kurią reikalaujama laiku pateikti tikslius, aktualius ir išsamius asmens duomenis, kurie reikalingi teisėto tvarkymo tikslais. Toks principas yra viena iš pagrindinių veiksmingo duomenų tvarkymo sąlygų.

3. Būtinumas/proporcingumas

60. Pagal šį principą turi būti aiški surinktos informacijos ir šios informacijos būtinumo įstatymu nustatytam teisėsaugos tikslui įvykdyti sąsaja. Šis teisinio pagrindo reikalavimas yra teigiamas veiksnys tvarkymo teisėtumui nustatyti. Tačiau EDAPP teigia, kad nors tai ir sustiprina tvarkymo teisinį tikrumą, tokio tvarkymo teisinis pagrindas yra įtvirtintas trečiosios šalies įstatyme. Trečiosios šalies įstatymas pats savaime nesukuria teisėto pagrindo asmens duomenų perdavimui ([22]). Remiantis HLCG ataskaita, reikėtų daryti prielaidą, kad trečiosios šalies, t. y. Jungtinių Valstijų, įstatymo teisėtumas iš principo pripažįstamas. Vertėtų atkreipti dėmesį į tai, kad nors tokie motyvai gali būti vertinami kaip pagrįsti, atsižvelgiant į tai, kad Jungtinės Valstijos yra demokratinė valstybė, tokia pati schema santykiuose su kita trečiąja šalimi būtų negaliojanti ir jos santykiuose su ta šalimi perkelti negalima.

61. HLCG ataskaitos priede teigiama, kad bet koks asmens duomenų perdavimas turi būti tikslingas, būtinas ir tinkamas. EDAPP pabrėžia, kad siekiant išlaikyti tikslo proporcingumą, tvarkant duomenis neturi būti pernelyg kišamasi į asmens privatumą, o tvarkymo sąlygos turi būti subalansuotos atsižvelgiant į duomenų subjektų teises ir interesus.

62. Dėl šios priežasties teisė susipažinti su informacija turėtų būti suteikiama kiekvienu atveju atskirai, atsižvelgiant į konkretaus tyrimo praktinius poreikius. Trečiųjų šalių teisėsaugos institucijų nuolatinė prieiga prie ES esančių duomenų bazių būtų vertinama kaip neproporcinga tikslui ir nepakankamai pagrįsta priemonė. EDAPP primena, kad

([22]) Žr. visų pirma Direktyvos 95/46/EB 7 straipsnio c ir e punktus. 2002 m. spalio 24 d. nuomonėje 6/2002 dėl oro linijų bendrovių Jungtinėms Valstijoms perduodamų keleivio duomenų ir kitų duomenų 29 straipsnio darbo grupė nurodė, jog negalima sutikti su tuo, kad viešąjį interesą turinčiai trečiajai šaliai priėmus vienašališką sprendimą, būtų reguliariai perduodami išsamūs duomenys, kurie saugomi pagal direktyvą.

net remiantis galiojančiais susitarimais dėl keitimosi duomenimis, pavyzdžiui, susitarimu dėl PNR duomenų, duomenimis turi būti keičiamasi konkrečiomis aplinkybėmis ir susitarimas sudaromas tik ribotam laikui ([23]).

63. Vadovaujantis ta pačia logika, duomenų saugojimo laikotarpis turėtų būti reglamentuotas: atsižvelgiant į konkretų tikslą duomenys turėtų būti saugomi tik tol, kol jie būtini. Jeigu duomenys nustatytam tikslui nebeaktualūs, jie turėtų būti ištrinti. EDAPP griežtai prieštarauja pasiūlymui įsteigti duomenų saugyklas, kuriose būtų saugoma informacija apie neįtariamus asmenis, kad ateityje šia informacija prireikus būtų galima pasinaudoti.

4. Informacijos saugumas

64. Principuose apibrėžiamos priemonės ir procedūros, skirtos apsaugoti duomenis nuo panaudojimo netinkamais tikslais, duomenų pakeitimo ir kitų pavojų, taip pat nuostata, pagal kurią prieiga suteikiama tik įgaliotiems asmenims. EDAPP nuomone, tokios nuostatos pakanka.

65. Šį principą taip pat galėtų papildyti nuostata, kad turėtų būti vedami asmenų, turinčių teisę susipažinti su duomenimis, žurnalai. Tai sustiprintų apsaugos priemonių, skirtų apriboti teisę susipažinti su šiais duomenimis ir užkirsti kelią jų panaudojimui netinkamais tikslais, veiksmingumą.

66. Be to, reikėtų numatyti abipusį keitimąsi informacija saugumo pažeidimo atveju: duomenų gavėjai JAV ir ES būtų atsakingi už kolegų kitoje šalyje informavimą tuo atveju, jei duomenys, kurie jiems buvo pateikti, būtų neteisėtai atskleisti. Tai užtikrins didesnę atsakomybę, taigi, didesnį duomenų tvarkymo saugumą.

5. Specialios asmens duomenų kategorijos

67. EDAPP nuomone, principą, pagal kurį draudžiama tvarkyti neskelbtinus duomenis, labai susilpnina išimtis, suteikianti galimybę tvarkyti tuos neskelbtinus duomenis, kurių atžvilgiu šalies vidaus teisėje yra nustatytos „tinkamos apsaugos priemonės“. Būtent dėl neskelbtino duomenų pobūdžio bet kokia nuostata, leidžianti nukrypti nuo draudimo principo, turi būti tinkamai ir tiksliai pagrįsta, nustatant tikslų ir aplinkybių, kuriomis galima tvarkyti nustatytos rūšies neskelbtinus duomenis, sąrašą bei nurodant duomenų valdytojų, turinčių teisę tvarkyti tokių rūšių duomenis, kompetenciją. Išskyrus apsaugos priemones, kurias būtina patvirtinti, EDAPP nuomone, neskelbtini duomenys patys savaime nėra veiksnys, dėl kurio būtų galima pradėti tyrimą. Jais galėtų būti pasinaudota konkrečiomis aplinkybėmis, bet tik kaip papildoma informacija apie duomenų subjektą, kurio atžvilgiu jau atliekamas tyrimas. Ribotas tokių apsaugos priemonių ir sąlygų sąrašas turi būti pateiktas principą apibūdinančiame tekste.

6. Atskaitomybė

68. Šios nuomonės 55–56 punktuose teigiama, kad būtina veiksmingai užtikrinti asmens duomenis tvarkančių valstybės sektoriaus subjektų atskaitomybę ir susitarime nustatyti garantijas, kaip ši atskaitomybė bus užtikrinta. Tai juolab svarbiau atsižvelgiant į tai, kad trūksta skaidrumo, tradiciškai siejamo su asmens duomenų tvarkymu teisėsaugos srityje. Todėl paminėjimas (kaip yra dabartiniame priede), kad valstybės sektoriaus subjektai yra atskaitingi, nepateikiant jokių papildomų paaiškinimų dėl tokios atskaitomybės sąlygų ir padarinių, nėra pakankama garantija. EDAPP rekomenduoja tokį paaiškinimą pateikti susitarimo tekste.

7. Nepriklausoma ir veiksminga priežiūra

69. EDAPP visiškai pritaria tam, kad būtų įtraukta nuostata, numatanti nepriklausomą ir veiksmingą priežiūrą, kurią vykdytų viena ar kelios valstybės priežiūros institucijos. Jo nuomone, turėtų būti aišku, kaip turėtų būti aiškinamas nepriklausomumas, visų pirma nuo kokių institucijų šios institucijos yra nepriklausomos ir kam jos turi teikti ataskaitas. Šioje srityje būtina nustatyti kriterijus, kuriais turėtų būti atsižvelgta į institucijų ir funkcijų nepriklausomumą vykdomosios valdžios ir teisėkūros organų atžvilgiu. EDAPP primena, kad tai yra labai svarbus veiksnys siekiant užtikrinti veiksmingą atitiktį principams, dėl kurių susitarta. Be to, kaip nurodyta pirmiau, atsižvelgiant į valstybės sektoriaus subjektų atskaitomybės klausimą, itin svarbu minėtoms institucijoms suteikti intervencijos ir vykdymo užtikrinimo įgaliojimus. Duomenų subjektai turi būti aiškiai informuoti apie tai, kad tokios institucijos veikia ir kokią kompetenciją jos turi, kad jos galėtų naudotis joms suteiktomis teisėmis, ypač jei kompetencija atsižvelgiant į duomenų tvarkymo aplinkybes suteikta kelioms institucijoms.

70. Be to, EDAPP rekomenduoja būsimame susitarime taip pat numatyti priežiūros institucijų bendradarbiavimo mechanizmus.

8. Individuali prieiga ir taisymas

71. Teisėsaugos tikslais suteikiant prieigą prie duomenų ir juos taisyti būtinos specialios garantijos. Ta prasme EDAPP palankiai vertina principą, nurodantį, kad asmenims suteikiama/turėtų būti suteikta teisė susipažinti su savo asmens duomenimis ir užtikrintos priemonės siekti, kad „jų asmens duomenys būtų ištaisyti ir (arba) ištrinti“. Tačiau kai kurių neaiškumų vis dar yra dėl asmenų sąvokos apibrėžties (turėtų būti užtikrinta ne tik atitinkamos šalies piliečių, bet ir visų duomenų subjektų duomenų apsauga) ir sąlygų,

([23]) Susitarimas nustos galioti ir nebebus taikomas praėjus septyneriems metams nuo jo pasirašymo, nebent Šalys tarpusavyje susitartų jį pakeisti kitu susitarimu.

kuriomis asmenys galėtų prieštarauti duomenų apie juos tvarkymui. Būtina patikslinti „atitinkamus atvejus“, kuriais galima ir negalima prieštarauti. Duomenų subjektai turėtų būti aiškiai informuoti apie tai, kokiomis aplinkybėmis, atsižvelgiant, pavyzdžiui, į įgaliojimų rūšį, tyrimo rūšį ar kitus kriterijus, jie galės naudotis savo teisėmis.

72. Be to, jei nėra tiesioginės galimybės prieštarauti tvarkymui dėl pagrįstų priežasčių, turėtų būti numatyta galimybė paprašyti už tvarkymo priežiūrą atsakingos nepriklausomos institucijos atlikti netiesioginį patikrinimą.

9. Skaidrumas ir pranešimas

73. EDAPP dar kartą pabrėžia, kaip svarbu užtikrinti veiksmingą skaidrumą, kad asmenys galėtų naudotis savo teisėmis ir būtų prisidėta prie asmens duomenis tvarkančių valstybinių institucijų bendros atskaitomybės didinimo. Jis pritaria parengtiems principams ir primygtinai reikalauja visų pirma nustatyti reikalavimą pateikti asmeniui bendrą *ir* atskirą pranešimą. Tai nurodyta priedo 9 punkte apibrėžtame principe.

74. Tačiau ataskaitos 2 skyriaus B dalyje („Principai, dėl kurių susitarta“) paminėta, kad Jungtinėse Valstijose skaidrumo sąvoka gali apimti „atskirą arba bendrą paskelbimą Federaliniame registre bei atskirą pranešimą ir duomenų atskleidimą teismo procese“. Turi būti akivaizdu, kad vien tik paskelbimo Oficialiajame leidinyje nepakanka, kad būtų užtikrintas duomenų subjekto tinkamas informavimas. EDAPP primena, jog be to, kad duomenų subjektui turi būti pateiktas atskiras pranešimas, informacija jam turi būti pateikta lengvai suprantama forma ir kalba.

10. Žalos atlyginimas

75. Norėdami veiksmingai pasinaudoti jiems suteiktomis teisėmis, asmenys turi turėti galimybę pateikti skundą nepriklausomai duomenų apsaugos institucijai, taip pat siekti žalos atlyginimo nepriklausomame ir nešališkame teisme. Abi galimybės siekti žalos atlyginimo turėtų būti vienodai prieinamos.

76. Teisė kreiptis į nepriklausomą duomenų apsaugos instituciją yra būtina, nes tai yra lanksti ir pigesnė pagalbos priemonė teisėsaugos sąlygomis, kurios asmenims gali atrodyti gana neaiškios. Duomenų apsaugos institucijos taip pat gali suteikti pagalbą duomenų subjektams, norintiems pasinaudoti teisėmis susipažinti su savo asmens duomenimis, kai išimtys pastariesiems draudžia tiesioginę prieigą prie asmens duomenų.

77. Teisė kreiptis į teismus yra papildoma ir būtina garantija, užtikrinanti, kad duomenų subjektai galėtų siekti žalos atlyginimo per instituciją, priklausančią demokratinės struktūros padaliniui, kuri nėra faktiškai duomenis apie juos tvarkanti valstybinė institucija. Šią veiksmingą teisės gynimo priemonę Europos Teisingumo Teismas ([24]) įvertino kaip būtiną priemonę, kuri asmeniui užtikrina veiksmingą jo teisės apsaugą. (...) [Ji] atspindi bendrąjį Bendrijos teisės principą, kuris yra valstybėms narėms bendrų konstitucinių tradicijų pagrindas ir kuris buvo įtvirtintas Europos konvencijos dėl žmogaus teisių ir pagrindinių laisvių apsaugos 6 ir 13 straipsniuose. Apie teisės gynimo priemonių taikymą taip pat aiškiai užsimenama Europos Sąjungos pagrindinių teisių chartijos 47 straipsnyje ir Direktyvos 95/46/EB 22 straipsnyje, nepažeidžiant jokių administracinių teisės gynimo priemonių.

11. Sprendimai atskirais automatizuoto duomenų tvarkymo atvejais

78. EDAPP palankiai vertina nuostatą, numatančią atitinkamas apsaugos priemones automatizuoto asmens duomenų tvarkymo atvejais. Jis pažymi, kad bendras supratimas apie tai, kas laikoma „atitinkamiems asmens interesams ypač nepalankiu veiksmu“, patikslintų šio principo taikymo sąlygas.

12. Tolesni duomenų perdavimai

79. Kai kurių tolesnių perdavimų nustatytos sąlygos yra neaiškios. Visų pirma, kai atliekant tolesnį perdavimą būtina laikytis tarptautinių susitarimų ir duomenis siunčiančių bei gaunančių šalių susitarimų, turėtų būti nurodyta, ar tai taikytina pirmąjį perdavimą inicijavusių dviejų šalių susitarimams ar su tolesniu perdavimu susijusių dviejų šalių susitarimams. Pasak EDAPP, bet kuriuo atveju būtini pirmąjį perdavimą inicijavusių dviejų šalių susitarimai.

80. EDAPP taip pat atkreipia dėmesį į labai plačią „teisėtų viešųjų interesų“, kuriais vadovaujantis galima toliau perduoti duomenis, sąvokos apibrėžtį. Visuomenės saugumo sritis tebėra neaiški, o perdavimų išplėtimas etikos pažeidimo atveju ar reglamentuojamų profesijų srityje yra nepagrįsta ir neadekvati priemonė teisėsaugos srityje.

VI. **IŠVADA**

81. EDAPP palankiai vertina bendrą ES ir JAV institucijų darbą teisėsaugos srityje, kai labai svarbu užtikrinti duomenų apsaugą. Vis dėlto, jis primygtinai pabrėžia, kad tai yra labai sudėtingas klausimas, visų pirma tikslios taikymo

([24]) Byla 222/84 *Johnston* [1986] Rink. 1651; Byla 222/86 *Heylens* [1987] Rink. 4097; Byla C-97/91 *Borelli* [1992] Rink. I-6313).

srities ir pobūdžio požiūriu, todėl jį būtina atidžiai ir išsamiai nagrinėti. Tarpvalstybinio susitarimo dėl duomenų apsaugos poveikį reikėtų atidžiai svarstyti remiantis galiojančiais teisės aktais ir atsižvelgiant į padarinius piliečiams.

82. EDAPP reikalauja daugiau aiškumo ir konkrečių nuostatų visų pirma dėl šių aspektų:

— turi būti patikslintas dokumento pobūdis; siekiant užtikrinti pakankamą teisinį tikrumą, tai turėtų būti teisiškai privalomas dokumentas;

— turi būti atliktas išsamus tinkamumo įvertinimas, pagrįstas būtiniausiais reikalavimais dėl schemos esmės, specifiškumo ir priežiūros aspektų. EDAPP nuomone, bendrojo dokumento tinkamumą galima pripažinti tik tuo atveju, jei toks dokumentas yra susietas su kiekvienam konkrečiam atvejui skirtais specialiais susitarimais;

— turi būti nustatyta apribota taikymo sritis, pateikiant aiškią ir bendrą teisėsaugos tikslų, kuriems kyla pavojus, sąvokos apibrėžtį;

— turi būti tiksliai apibrėžtos sąlygos, kuriomis privačius subjektus galima įtraukti į duomenų perdavimo schemas;

— turi būti laikomasi proporcingumo principo, numatant, kad duomenimis turi būti keičiamasi kiekvienu atveju, kai tam yra konkretus poreikis;

— turi būti nustatyti griežti priežiūros mechanizmai ir duomenų subjektams prieinami žalos atlyginimo mechanizmai, įskaitant administracines ir teismines teisės gynimo priemones;

— turi būti nustatytos veiksmingos priemonės, garantuojančios, kad savo teisėmis galės naudotis visi duomenų subjektai, neatsižvelgiant į jų pilietybę;

— turi būti numatyta galimybė dalyvauti nepriklausomoms duomenų apsaugos institucijoms, visų pirma priežiūros ir duomenų subjektams teikiamos pagalbos srityse.

83. EDAPP primygtinai reikalauja vengti skubos rengiant principus, nes tokiu būtų patvirtinti tik netinkami sprendimai, o tai turėtų neigiamų pasekmių tiems, kuriems jie skirti duomenų apsaugos srityje. Todėl šiame etape geriausia būtų parengti veiksmų planą, kuriuo vadovaujantis būtų siekiama galimo susitarimo vėlesniame etape.

84. EDAPP taip pat reikalauja daugiau skaidrumo duomenų apsaugos principų rengimo procese. Demokratiškos diskusijos dėl dokumento būtų naudingos ir dokumentu būtų užsitikrinta būtina parama ir pripažinimas tik tuo atveju, jei diskusijose dalyvautų visi suinteresuoti subjektai, įskaitant Europos Parlamentą.

Priimta Briuselyje, 2008 m. lapkričio 11 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas

Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Komisijos komunikato Tarybai, Europos Parlamentui ir Europos ekonomikos ir socialinių reikalų komitetui „Europos e. teisingumo strategijos link“

(2009/C 128/02)

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 ([1]),

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 ([2]), ypač į jo 41 straipsnį,

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS

1. 2008 m. gegužės 30 d. buvo priimtas Komisijos komunikatas Tarybai, Europos Parlamentui ir Europos ekonomikos ir socialinių reikalų komitetui „Europos e. teisingumo strategijos link“ (toliau – Komunikatas). Laikydamasis Reglamento (EB) Nr. 45/2001 41 straipsnio, EDAPP pateikia šią nuomonę.

2. Komunikatu siekiama pasiūlyti e. teisingumo strategiją, kuria ketinama stiprinti piliečių pasitikėjimą Europos teisingumo erdve. Pagrindinis e. teisingumo tikslas turėtų būti padėti veiksmingiau administruoti teisingumą piliečių naudai visoje Europoje. ES veiksmais turėtų būti sudaryta galimybė piliečiams gauti informaciją, nesudarant kalbinių, kultūrinių ir teisinių barjerų, kurie atsiranda dėl sistemų įvairovės. Prie Komunikato pridedamas veiksmų plano ir tvarkaraščio projektas.

3. Šioje EDAPP nuomonėje aptariami Komunikato aspektai, susiję su asmens duomenų tvarkymu, privatumo apsauga elektroninių ryšių sektoriuje ir laisvu duomenų judėjimu.

([1]) OL L 281, 1995 23 11, p. 31.
([2]) OL L 8, 2001 1 12, p. 1.

II. BENDRA INFORMACIJA IR KONTEKSTAS

4. 2007 m. birželio mėn. TVR taryba ([3]) nustatė kelias e. teisingumo plėtojimo prioritetines sritis:

— sukurti Europos sąsają (e. teisingumo portalą);

— sudaryti sąlygas kelių registrų, pavyzdžiui, nuosprendžių registrų, nemokumo registrų, komercinių ir verslo registrų bei žemės registrų, sujungimui į tinklą;

— pradėti rengtis naudoti IRT vykdant Europos mokėjimo orderio procedūrą;

— pagerinti vaizdo konferencijų technologijos naudojimą tarpvalstybiniuose procesuose, visų pirma renkant įrodymus;

— sukurti pagalbines priemones vertimui raštu ir žodžiu.

5. Nuo to laiko darbo e. teisingumo srityje pažanga buvo stabili. Komisijos nuomone, dirbant šiuo klausimu reikia užtikrinti, kad pirmenybė būtų teikiama veiklos projektams ir decentralizuotoms struktūroms, tuo pat metu numatant koordinavimą Europos lygiu, remtis galiojančiais teisiniais dokumentais ir naudoti IT priemones jų veiksmingumui gerinti. Europos Parlamentas taip pat pareiškė pritariantis e. teisingumo projektui ([4]).

6. Komisija nuolat ragina naudoti šiuolaikines informacines technologijas civilinės ir baudžiamosios teisės srityse. Todėl buvo sukurtos tokios priemonės, kaip Europos mokėjimo orderis. Nuo 2003 m. Komisija administruoja Europos teisminio tinklo civilinėse ir komercinėse bylose „portalą“, kuriuo piliečiai gali naudotis 22 kalbomis. Komisija taip pat sukūrė ir įdiegė Europos teisminį atlasą. Šios priemonės yra parengtiniai būsimos Europos e. teisingumo sistemos elementai. Baudžiamosios teisės srityje Komisija rengė priemonę, kuri sudarytų sąlygas keistis informacija iš valstybių narių nuosprendžių registrų ([5]). Ne tik Komisija, bet ir Eurojustas parengė saugias ryšių su nacionalinėmis institucijomis sistemas.

([3]) Dok. 10393/07 JURINFO 21.
([4]) Žr. Europos Parlamento Teisės reikalų komiteto ataskaitos projektą.
([5]) Visų pirma žr. toliau nurodytą ECRIS sistemą.

7. E. teisingumo projektu ketinama pasiūlyti daugiau galimybių, kad per ateinančius metus Europos teisingumo erdvė įgytų konkretesnį pavidalą piliečiams. Siekdama parengti bendrą strategiją šiuo svarbiu klausimu Komisija priėmė šį Komunikatą dėl e. teisingumo. Komunikate išdėstyti objektyvūs prioritetų nustatymo kriterijai, visų pirma būsimų Europos lygio projektų srityje, kad per pagrįstą laiką būtų pasiekta konkrečių rezultatų.

8. Komisijos tarnybų darbiniame dokumente – Komunikato lydimajame dokumente, kuriame išdėstyta poveikio vertinimo santrauka – taip pat pateikta tam tikros bendros informacijos ([6]). Poveikio vertinimo ataskaita buvo parengta atsižvelgiant į valstybių narių, teisminių institucijų, teisinių profesijų atstovų, piliečių ir įmonių atsiliepimus. Su EDAPP konsultuotasi nebuvo. Poveikio vertinimo ataskaitoje prioritetas buvo suteiktas politikos pasirinkimui problemoms, kurios apima europinį aspektą ir nacionalinę kompetenciją, spręsti. Komunikate buvo pasinaudota šiuo politikos pasirinkimu. Strategijoje daugiausia dėmesio bus skiriama vaizdo konferencijų naudojimui, e. teisingumo portalo sukūrimui, vertimo priemonių gerinimui parengiant automatinio vertimo internete priemones, teisinių institucijų tarpusavio ryšių gerinimui, geresnei nacionalinių registrų ir Europos procedūrų (pavyzdžiui, Europos mokėjimo orderis) sąveikai.

9. EDAPP pritaria, kad pirmiau nurodytai veiklai būtų skiriama daugiausia dėmesio. Iš esmės jis pritaria e. teisingumo visapusiškam požiūriui. Jis patvirtina, kad esama trejopos būtinybės gerinti galimybes kreiptis į teismus, Europos teisinių institucijų bendradarbiavimą ir pačios teisingumo sistemos veiksmingumą. Šiuo požiūriu daromas poveikis kelioms institucijoms ir asmenims:

— valstybės narėms, kurios visų pirma atsakingos už veiksmingų ir patikimų sistemų sukūrimą;

— Europos Komisijai, kuriai tenka sutarčių sergėtojos vaidmuo;

— valstybių narių teisminėms institucijoms, kurioms reikia modernesnių priemonių ryšiams palaikyti, ypač tarpvalstybinių bylų atveju;

— teisinių profesijų atstovams, piliečiams ir įmonėms, kurie visi pasisako už geresnį IT priemonių panaudojimą siekiant, kad būtų geriau patenkinti jų poreikiai, susiję su teisingumu.

10. Komunikatas yra glaudžiai susijęs su Tarybos sprendimu dėl Europos nuosprendžių registrų informacinės sistemos (ECRIS) sukūrimo. 2008 m. rugsėjo 16 d. EDAPP priėmė nuomonę dėl šio pasiūlymo ([7]). EDAPP pritarė pasiūlymui, jei bus atsižvelgta į keletą aspektų. Visų pirma jis pažymėjo, kad papildomos duomenų apsaugos garantijos turėtų užpildyti dabartinę spragą, kai nėra išsamios teisinės sistemos dėl duomenų apsaugos policijos ir teisminių institucijų bendradarbiavimo srityje. Todėl jis pabrėžė, kad atliekant sistemos duomenų apsaugos priežiūrą, būtinas veiksmingas koordinavimas dalyvaujant valstybių narių institucijoms ir Komisijai, kuri užtikrina bendrą ryšių infrastruktūrą.

11. Kai kurie šios nuomonės elementai, kuriuos naudinga priminti, yra šie:

— turėtų būti nurodyta, kad aukšto lygio duomenų apsauga yra būtina sąlyga įgyvendinamosioms priemonėms patvirtinti;

— siekiant teisinio tikrumo, Komisijos atsakomybė už bendrą ryšių infrastruktūrą ir už Reglamento (EB) Nr. 45/2001 taikymą, turėtų būti aiškiai nurodyta;

— Komisija – o ne valstybės narės – taip pat turėtų būti atsakinga už sąsają užtikrinančią programinę įrangą, siekiant gerinti keitimosi informacija veiksmingumą ir sudaryti sąlygas geresnei sistemos priežiūrai.

— Turėtų būti aiškiai apibrėžtas automatinio vertimo naudojimas ir nustatytos jo ribos, kad būtų skatinamas abipusis baudžiamųjų veikų supratimas nedarant įtakos perduodamos informacijos kokybei.

12. Šios rekomendacijos tebėra vertingos kontekstui, į kurį atsižvelgiant bus nagrinėjamas šis Komunikatas.

III. KOMUNIKATE NUMATYTAS KEITIMASIS INFORMACIJA

13. E. teisingumo taikymo sritis yra labai plati, iš esmės apimanti IRT naudojimą teisingumo administravimo srityje

([6]) Komisijos tarnybų darbinis dokumentas – Komunikato Tarybai, Europos Parlamentui ir Europos ekonomikos ir socialinių reikalų komitetui „Europos e. teisingumo strategijos link“ lydimasis dokumentas. Poveikio vertinimo santrauka, 2008 m. gegužės 30 d. SEC (2008) 1944.

([7]) Žr. EDAPP nuomonę dėl Tarybos sprendimo dėl Europos nuosprendžių registrų informacinės sistemos (ECRIS) sukūrimo pagal Pamatinio sprendimo 2008/XX/TVR 11 straipsnį, kuri pateikiama EDAPP tinklavietėje www.edps.europa.eu („consultation“, „opinions“, „2008“).

Europos Sąjungoje. Tai taikoma daugeliui klausimų, pavyzdžiui, projektams, skirtiems informacijos procese dalyvaujančioms bylos šalims veiksmingesniam teikimui. Tai apima informaciją internete apie teisines sistemas, teisės aktus ir teisminę praktiką, elektronines ryšių sistemas, susiejančias procese dalyvaujančias bylos šalis ir teismus bei visiškai elektroninių procedūrų nustatymą. Tai taip pat taikoma Europos projektams, pavyzdžiui, elektroninių priemonių naudojimui bylos nagrinėjimui įrašyti ir projektams, susijusiems su keitimusi informacija ar sąveika.

14. Net jei ši taikymo sritis ir yra labai plati, EDAPP pastebėjo, kad e. teisingumo portale bus pateikiama informacija apie baudžiamąsias bylas ir civilines bei komercines teismines sistemas, tačiau ne apie administracines teismines sistemas. Taip pat bus pateiktas saitas į Baudžiamąjį ir į Civilinį atlasą, bet ne į Administracinį atlasą, nors galbūt būtų geriau suteikti piliečiams ir įmonėms prieigą prie teisminių administracinių sistemų, pavyzdžiui, administracinės teisės ir skundų procedūros. Taip pat turėtų būti numatytas saitas į valstybės tarybų asociaciją. Toks informacijos papildymas būtų naudingas piliečiams, mėginantiems rasti kelią džiunglėse – tokia dažnai yra administracinė teisė su visais teismais – kad jie būtų geriau informuoti apie administracines teismines sistemas.

15. Todėl EDAPP rekomenduoja įtraukti administracines procedūras į e. teisingumą. Vienas iš šio naujo elemento aspektų turėtų būti e. teisingumo projektų inicijavimas siekiant didinti duomenų apsaugos taisyklių bei nacionalinių duomenų apsaugos institucijų matomumą, visų pirma duomenų, tvarkomų e. teisingumo projektuose, atžvilgiu. Tai atitiktų vadinamąją Londono iniciatyvą, kurią 2006 m. lapkričio mėn. pradėjo vykdyti duomenų apsaugos institucijos ir kuria siekiama „informuoti apie duomenų apsaugą ir padidinti jos veiksmingumą“.

IV. **NAUJAS PAMATINIS SPRENDIMAS DĖL ASMENS DUOMENŲ, TVARKOMŲ VYKDANT POLICIJOS IR TEISMINĮ BENDRADARBIAVIMĄ BAUDŽIAMOSIOSE BYLOSE, APSAUGOS**

16. Dėl Komisijos komunikate numatyto augančio teisminių institucijų keitimosi asmens duomenimis, taikoma duomenų apsaugos teisinė sistema tampa dar svarbesnė. Atsižvelgdamas į tai EDAPP pažymi, kad praėjus trejiems metams nuo pirminio Komisijos pasiūlymo, lapkričio 27 d. Europos Sąjungos Taryba priėmė pamatinį sprendimą dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos ([8]). Šiame naujame teisės akte numatoma bendra duomenų apsaugos teisinė sistema „trečiojo ramsčio“ srityje, papildant Direktyvos 95/46/EB duomenų apsaugos nuostatas „pirmojo ramsčio“ srityje.

17. EDAPP palankiai vertina šį teisinį dokumentą, kuris yra pirmas svarbus žingsnis duomenų apsaugos vykdant policijos ir teisminį bendradarbiavimą srityje. Tačiau galutinėje teksto redakcijoje numatytas duomenų apsaugos lygis nėra visiškai patenkinamas. Visų pirma, pamatinis sprendimas apima tik policijos ir teisminius duomenis, kuriais keičiasi valstybės narės, ES institucijos ir sistemos, bet neapima šalies duomenų. Be to, priimtame pamatiniame sprendime nėra numatytas įpareigojimas skirstyti duomenų subjektus į kategorijas, pavyzdžiui, įtariamieji, nusikaltėliai, liudytojai ir nukentėjusieji, siekiant užtikrinti, kad jų duomenys būti tvarkomi taikant tinkamesnę apsaugą. Jame nenumatytas visiškas suderinimas su Direktyvos 95/46/EB nuostatoms, visų pirma dėl tikslų, kuriais asmens duomenys gali būti toliau tvarkomi, apribojimo. Taip pat jame nenumatyta nepriklausoma atitinkamų nacionalinių ir ES duomenų apsaugos institucijų grupė, kuri galėtų užtikrinti geresnį duomenų apsaugos institucijų koordinavimą bei reikšmingai prisidėti prie vienodo pamatinio sprendimo taikymo.

18. Tai reiškia, kad net jei ir dedama daug pastangų parengti bendras tarpvalstybinio keitimosi asmens duomenimis sistemas, vis dar esama neatitikimų, susijusių su taisyklėmis, pagal kurias tvarkomi šie duomenys, o piliečiai gali pasinaudoti savo teisėmis skirtingose ES valstybėse.

19. EDAPP dar kartą primena, kad aukšto lygio duomenų apsaugos užtikrinimas policijos ir teisminio bendradarbiavimo srityje bei derėjimas su Direktyvos 95/46/EB nuostatomis turi papildyti kitas priemones, kurios yra įdiegtos ar numatytos siekiant sudaryti palankesnes sąlygas tarpvalstybiniam keitimuisi asmens duomenimis teisėsaugos srityje. Ši būtinybė susijusi ne tik su piliečių teise į tai, kad būtų gerbiama pagrindinė teisė į duomenų apsaugą, bet ir su teisėsaugos institucijų poreikiu užtikrinti duomenų, kuriais keičiamasi, kokybę – kaip patvirtinta Komunikato priede dėl elektroninio teistumo duomenų sujungimo – įvairių šalių institucijų tarpusavio pasitikėjimu ir galiausiai įrodymų, surinktų tarpvalstybinėje byloje, teisine galia.

20. Todėl EDAPP ragina ES institucijas ypač atsižvelgti į šiuos aspektus ne tik įgyvendinant Komunikate numatytas priemones, bet taip pat siekiant kuo greičiau pradėti svarstyti, kaip galima toliau tobulinti duomenų apsaugos teisinę sistemą teisėsaugos srityje.

V. **E. TEISINGUMO PROJEKTAI**

E. teisingumo priemonės Europos lygiu

21. EDAPP pripažįsta, kad keitimasis asmens duomenimis yra labai svarbus elementas kuriant laisvės, saugumo ir teisingumo erdvę. Dėl šios priežasties EDAPP pritaria pasiūlymui

([8]) Sprendimas dar nėra paskelbtas OL.

dėl el. teisingumo strategijos, pabrėždamas duomenų apsaugos svarbą šiuo požiūriu. Iš tiesų, pagarba duomenų apsaugai nėra vien teisinė prievolė, bet taip pat vienas iš svarbiausių elementų, kad numatytos sistemos, pavyzdžiui, keitimosi duomenimis kokybės užtikrinimas, būtų sėkmingos. Tai taip pat taikytina institucijoms ir organams, kai jie tvarko asmens duomenis bei kai rengiamos naujos politikos kryptys. Taisyklės ir principai turi būti taikomi bei jų laikomasi praktikoje, visų pirma atsižvelgiant į informacinių sistemų kūrimo ir diegimo etapą. Privatumas ir duomenų apsauga yra iš esmės „svarbiausieji sėkmės veiksniai“ siekiant klestinčios ir subalansuotos informacinės visuomenės. Todėl tikslinga į juos investuoti ir padaryti tai kuo anksčiau.

22. Atsižvelgdamas į tai EDAPP pabrėžia, kad Komunikate nenumatoma centrinė Europos duomenų bazė. Jis palankiai vertina tai, kad pirmenybė teikiama decentralizuotoms struktūroms. EDAPP primena, kad jis paskelbė nuomonę dėl ECRIS ([9]) ir dėl Priumo iniciatyvos ([10]). Nuomonėje dėl ECRIS EDAPP pareiškė, kad decentralizuota sistema išvengiama asmens duomenų dubliavimosi centrinėje bazėje. Nuomonėje dėl Priumo iniciatyvos jis rekomendavo aptariant duomenų bazių tarpusavio ryšį tinkamai atsižvelgti į sistemos mastą. Visų pirma turėtų būti nustatyti duomenų perdavimo konkretūs formatai, pavyzdžiui, užklausos internetu dėl informacijos iš nuosprendžių registro, be kita ko, atsižvelgiant į kalbų skirtumus, ir turėtų būti nuolat stebima, ar užtikrinamas keitimosi duomenimis tikslumas. Į šiuos elementus taip pat turėtų būti atsižvelgta rengiant iniciatyvas, susijusias su e. teisingumo strategija.

23. Europos Komisija ketina prisidėti prie e. teisingumo priemonių stiprinimo ir vystymo Europos lygiu glaudžiai bendradarbiaudama su valstybėmis narėmis ir kitais partneriais. Be valstybių narių pastangų rėmimo, Komisija ketina tuo pat metu pati parengti tam tikras kompiuterines priemones, kuriomis būtų didinamas sistemų sąveikumas, sudaromos palankesnės sąlygos visuomenei kreiptis į teismą, o teisminėms institucijoms palaikyti ryšius, bei užtikrinama didelė masto ekonomija Europos lygiu. Atsižvelgiant į valstybių narių naudojamos programinės įrangos sąveikumą, ne visos valstybės narės privalo naudoti tokią pat programinę įrangą – nors tai būtų praktiškiausia – tačiau jų programinė įranga turėtų būti visapusiškai sąveiki.

24. EDAPP rekomenduoja sistemų sujungimo ir sąveikumo srityje deramai atsižvelgti į tikslų apribojimo principą bei remtis duomenų apsaugos standartais („į privatumą atsižvelgiama projektuojant“). Kiekviena skirtingų sistemų sąveikos forma turėtų būti išsamiai pagrindžiama dokumentais. Dėl sąveikos niekada neturėtų susidaryti padėtis, kad valdžios institucija, kuriai nesuteikta prieigos prie tam tikrų duomenų teisė arba teisė juos naudoti, galėtų įgyti šią prieigą per kitą informacinę sistemą. EDAPP dar kartą nori pabrėžti, kad sąveikumu savaime neturėtų būti grindžiamas tikslų apribojimo principo netaikymas ([11]).

25. Be to, labai svarbu užtikrinti, kad sustiprintas tarpvalstybinis keitimasis asmens duomenimis būtų vykdomas apsaugos institucijoms taikant sustiprintą duomenų priežiūrą ir joms bendradarbiaujant. 2006 m. gegužės 29 d. nuomonėje dėl pamatinio sprendimo dėl keitimosi informacija iš nuosprendžių registro ([12]) EDAPP jau pabrėžė, kad pasiūlyme dėl pamatinio sprendimo turėtų reglamentuojamas ne tik centrinių institucijų bendradarbiavimas, bet ir įvairių kompetentingų duomenų apsaugos institucijų bendradarbiavimas. Šis poreikis dar padidėjo, nes atsižvelgiant į derybų dėl neseniai priimto pamatinio sprendimo dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos ([13]), rezultatus, buvo išbraukta nuostata dėl darbo grupės, vienijančios ES duomenų apsaugos institucijas ir koordinuojančios jų veiksmus duomenų tvarkymo vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose srityje. Todėl siekiant užtikrinti veiksmingą priežiūrą bei duomenų iš nuosprendžių registrų kokybišką tarpvalstybinį perdavimą reikėtų nustatyti veiksmingus duomenų apsaugos institucijų veiklos koordinavimo mechanizmus ([14]). Taikant tokius mechanizmus taip pat reikėtų atsižvelgti į EDAPP priežiūros kompetenciją s-TESTA infrastruktūros atžvilgiu ([15]). E. teisingumo priemonės galėtų prisidėti prie šių mechanizmų, kurie gali būti parengti glaudžiai bendradarbiaujant su duomenų apsaugos institucijomis.

26. Komunikato 4.2.1 dalyje nurodyta, kad keičiantis duomenimis iš nuosprendžių registrų bus svarbu taikyti platesnį, nei teisminį bendradarbiavimą, kad būtų atsižvelgta į kitus tikslus, pavyzdžiui, kontroliuoti asmens galimybę užimti tam tikras pareigas. EDAAP pabrėžia, kad tvarkant asmens duomenis kitais tikslais, nei tais, kuriems jie buvo surinkti, turėtų būti laikomasi konkrečių sąlygų, nustatytų galiojančiuose duomenų apsaugos teisės aktuose. Visų pirma, tvarkyti asmens duomenis papildomais tikslais turi būti leidžiama tik jeigu tai yra būtina siekiant Bendrijos

([9]) Žr. 4 išnašą 18 dalyje.
([10]) OL C 89, 2008 4 10, p. 4.
([11]) OL C 91, 2006 4 19, p. 53. Taip pat žr. EDAPP pastabas dėl Komisijos komunikato dėl Europos duomenų bazių sąveikos, Briuselis, 2006 3 10.
([12]) OL C 313, 2006 12 20, p. 26.
([13]) Žr. pirmiau nurodytą dokumentą, IV skyrių.
([14]) Žr. EDAPP nuomonę dėl ECRIS, 8 punktą ir 37–38 punktus.
([15]) Šiuo klausimu žr. pirmiau nurodyti dokumento 27–28 dalis.

duomenų apsaugos teisės aktuose nustatytų tikslų ([16]) ir jeigu šie tikslai įtvirtinti teisėkūros priemonėmis.

27. Atsižvelgiant į nuosprendžių registrų sujungimą Komunikate teigiama, kad rengdamasi pamatinio sprendimo dėl keitimosi informacija iš nuosprendžių registro įsigaliojimui Komisija vykdys dvi galimybių įvertinimo studijas, kad bevystant projektą jis būtų organizuojamas, ir išplės keitimosi informacija mastą įtraukdama ir duomenis apie trečiųjų šalių piliečius, nuteistus už nusikalstamas veikas. 2009 m. Komisija valstybėms narėms pateiks programinę įrangą, suprojektuotą taip, kad per trumpą laiką būtų galima keistis visais nuosprendžių registrų duomenimis. Ši konsultavimosi sistema, ją naudojant kartu su s-TESTA informacijos keitimosi tikslais, sukurs masto ekonomiją, nes valstybėms narėms nebereikės pačioms atlikti kūrimo darbų. Taip pat dėl to projektą bus lengviau valdyti.

28. Todėl EDAPP palankiai vertina s-TESTA infrastruktūros naudojimą, kuri, kaip buvo įrodyta, yra patikima keitimosi duomenimis sistema, ir rekomenduoja išsamiai apibrėžti su numatomomis duomenų keitimosi sistemomis susijusius statistinius elementus bei deramai atsižvelgti į poreikį užtikrinti duomenų apsaugos priežiūrą. Pavyzdžiui, statistiniai duomenys akivaizdžiai galėtų apimti tokius elementus, kaip, pavyzdžiui, prašymų gauti ar ištaisyti asmens duomenis skaičių, atnaujinimo proceso trukmę ir užbaigtumą, teisę gauti tokius duomenis turinčių asmenų statusą bei saugumo pažeidimo atvejus. Be to, statistiniai duomenys ir jais grindžiamos ataskaitos turėtų būti teikiami kompetentingoms duomenų apsaugos institucijoms.

Automatinis vertimas ir vertėjų duomenų bazė

29. Automatinio vertimo naudojimas – naudinga priemonė, galinti padėti atitinkamiems subjektams valstybėse narėse pasiekti abipusio supratimo. Tačiau dėl automatinio vertimo naudojimo neturėtų sumažėti informacijos, kuria keičiamasi, kokybė, ypač jeigu ši informacija naudojama priimant sprendimus, turinčius teisines pasekmes atitinkamiems asmenims. EDAPP nurodo, kad svarbu aiškiai apibrėžti automatinio vertimo naudojimą ir nustatyti jo ribas. Tačiau naudojant automatinį vertimą informacijai, kurios pirminis vertimas buvo netikslus, pavyzdžiui, atskirais atvejais pridedamų papildomų pastabų ar instrukcijų atveju, perduoti, gali būti padarytas poveikis perduodamos informacijos – ir ja remiantis priimamų sprendimų – kokybei, ir iš esmės automatinis vertimas šiuo atveju turėtų būti nenaudojamas ([17]). EDAPP siūlo atsižvelgti į šią rekomendaciją rengiant priemones, kurios numatytos Komunikate.

30. Komunikate nustatytas siekis sukurti teisės srities vertėjų raštu ir žodžiu duomenų bazę, tuo siekiant pagerinti teisinių tekstų vertimo raštu ir žodžiu kokybę. EDAPP remia šį tikslą, tačiau primena, kad šiai duomenų bazei bus taikomi atitinkami asmens duomenų apsaugos teisės aktai. Visų pirma, jeigu duomenų bazėje pateikiami vertėjų darbo įvertinimo duomenys, gali būti taikomas išankstinis duomenų apsaugos institucijų patikrinimas.

Europos e. teisingumo veiksmų plano link

31. 5 dalyje Komisija nurodo, kad reikia aiškiai paskirstyti Komisijos, valstybių narių ir kitų teisminiame bendradarbiavime dalyvaujančių subjektų pareigas. Komisija vykdys bendras koordinavimo funkcijas skatindama keitimąsi geriausios praktikos pavyzdžiais ir sukurs, parengs ir koordinuos informaciją e. teisingumo portale. Be to, Komisija tęs darbą tarpusavyje sujungdama nuosprendžių registrus ir toliau prisiims tiesioginę atsakomybę už teisinį tinklą civilinėje srityje bei rems teisinį tinklą baudžiamojoje srityje. Valstybės narės turės atnaujinti e. teisingumo tinklavietėje pateiktą informaciją apie jų teismines sistemas. Kiti subjektai – teisiniai tinklai civilinėje ir baudžiamojoje srityse ir Eurojustas. Jie glaudžiai bendradarbiaudami su Komisija plėtos veiksmingesniam teisminiam bendradarbiavimui reikalingas priemones, visų pirma automatinio vertimo priemones ir saugią keitimosi informacija sistemą. Prie Komunikato pridedamas veiksmų plano projektas ir įvairių projektų tvarkaraštis.

32. Todėl EDAPP pabrėžia, kad ECRIS sistemoje, viena vertus, nėra įdiegta viena centrinė Europos duomenų bazė ir nenumatoma tiesioginė prieiga prie, pavyzdžiui, tokių duomenų bazių, kuriose yra kitų valstybių narių nuosprendžių registrai, o kita vertus, nacionaliniu lygiu pareigos užtikrinti teisingą informaciją yra centralizuotai pavestos valstybių narių pagrindinėms institucijoms. Pagal šį mechanizmą valstybės narės atsako už nacionalinių duomenų bazių veikimą ir už veiksmingą keitimąsi informacija. Neaišku, ar jos yra atsakingos už sujungimo programinę įrangą. Komisija valstybėms narėms pateiks programinę įrangą, suprojektuotą taip, kad per trumpą laiką būtų galima keistis visais nuosprendžių registrų duomenimis. Ši konsultavimosi sistema bus naudojama kartu su s-TESTA siekiant keistis informacija.

33. EDAPP supranta, kad ir analoginėse e. teisingumo iniciatyvose gali būti įgyvendinamos panašios sistemos ir Komisija

([16]) Visų pirma žr. Direktyvos 95/46/EB 13 straipsnį ir Reglamento (EB) Nr. 45/2001 20 straipsnį.

([17]) Žr. EDAPP nuomonės dėl ECRIS 39–40 dalis.

bus atsakinga už bendrą infrastruktūrą, nors tai konkrečiai nenurodyta Komunikate. EDAPP siūlo siekiant teisinio tikrumo aiškiai nurodyti tokią atsakomybę už priemones, numatytas Komunikate.

E. teisingumo projektai

34. Priede išdėstyti projektai, kurie bus vystomi per kitus penkerius metus. Pirmasis projektas – e. teisingumo puslapių kūrimas, yra susijęs su e. teisingumo portalu. Šiam veiksmui reikia atlikti galimybių įvertinimo studiją ir sukurti portalą. Be to, reikia įdiegti valdymo metodus ir pateikti informaciją internete visomis ES kalbomis. Antrasis ir trečiasis projektai yra susiję su nuosprendžių registrų sujungimu. 2 projektas yra susijęs su nacionalinių nuosprendžių registrų sujungimu. 3 projektu numatoma, atlikus galimybių įvertinimo studiją ir pateikus pasiūlymą dėl teisės akto, sukurti nuteistųjų trečiųjų šalių piliečių Europos registrą. EDAPP pažymi, kad pastarasis projektas nebeminimas Komisijos darbo programoje ir klausia, ar tai atspindi Komisijos numatomų projektų pokyčius, ar šis konkretus projektas tik atidedamas.

35. Taip pat Komunikate išvardyti trys projektai elektroninio keitimosi informacija srityje ir trys projektai pagalbinių priemonių vertimui srityje. Bandomasis projektas bus pradėtas palaipsniui kaupiant lyginamąjį daugiakalbį teisės žodyną. Kiti atitinkami projektai yra susiję su dinamiškomis formomis, kurios naudojamos greta Europos teisėkūros tekstų, bei teisminių institucijų skatinimui naudotis vaizdo konferencijomis. Galiausiai, kaip viena e. teisingumo forumų, kasmet bus rengiami posėdžiai e. teisingumo temomis ir vystomi teisės specialistų mokymai teisminio bendradarbiavimo srityje. EDAPP teigia, kad tokiuose susitikimuose ir mokymuose būtų skiriama pakankamai dėmesio duomenų apsaugos įstatymams ir praktikai.

36. Todėl priede numatomas platus Europos priemonių spektras, siekiant sudaryti palankesnes sąlygas keistis informacija tarp subjektų skirtingose valstybėse narėse. Kaip viena šių priemonių svarbų vaidmenį atliks e. teisingumo portalas, už kurį pirmiausia atsakinga Komisija.

37. Bendras daugelio šių priemonių bruožas tas, kad informacija ir asmens duomenimis keisis ir juos valdys skirtingi subjektai nacionaliniu ir ES lygiu, kuriems taikomos duomenų apsaugos prievolės ir kuriuos prižiūri priežiūros institucijos, įsteigtos remiantis Direktyva 95/46/EB arba Reglamentu (EB) Nr. 45/2001. Šiuo požiūriu EDAPP jau yra aiškiai pareiškęs savo nuomonėje dėl Vidaus rinkos informacijos (IMI) sistemos ([18]), kad būtina užtikrinti, jog su duomenų apsaugos taisyklių laikymųsi susijusios pareigos būtų užtikrinamos veiksmingai ir sklandžiai.

38. Iš esmės tam reikia, viena vertus, aiškiai apibrėžti ir paskirstyti asmens duomenų šiose sistemose tvarkymo pareigas; kita vertus, prireikus reikia nustatyti atitinkamus koordinavimo mechanizmus – visų pirma susijusius su priežiūra.

39. Naujų technologijų naudojimas yra vienas e. teisingumo iniciatyvų kertinių akmenų: nacionalinių registrų sujungimas, elektroninio parašo plėtojimas, saugūs tinklai, virtualios keitimosi informacija platformos ir platesnis naudojimasis vaizdo konferencijomis kitus kelerius metus bus esminiai e. teisingumo iniciatyvų elementai.

40. Todėl kuo ankstesniame etape būtina atsižvelgti į duomenų apsaugos klausimus ir juos integruoti į kuriamų priemonių architektūrą. Visų pirma, labai svarbūs yra ir sistemos architektūra, ir tinkamų saugumo priemonių įdiegimas. Šis „į privatumą atsižvelgiama projektuojant“ požiūris sudarytų sąlygas atitinkamomis e. teisingumo iniciatyvomis numatyti veiksmingą asmens duomenų valdymą kartu užtikrinant duomenų apsaugos principų laikymąsi ir skirtingų institucijų keitimosi duomenimis saugumą.

41. Be to, EDAPP pabrėžia, kad technologijų priemonės turėtų būti naudojamos ne tik siekiant užtikrinti keitimąsi informacija, bet taip pat sutvirtinti susijusių asmenų teises. Šiuo požiūriu EDAPP palankiai vertina tai, kad Komunikate piliečiams numatyta galimybė internetu savo pasirinkta kalba pateikti prašymus gauti informacijos iš nuosprendžių registro ([19]). Atsižvelgdamas į šį klausimą, EDAPP primena, kad savo nuomonėje dėl Komisijos pasiūlymo dėl keitimosi informacija iš nuosprendžių registrų jis palankiai vertino tai, kad atitinkamam asmeniui nustatyta galimybė valstybės narės centrinės institucijos prašyti informacijos iš nuosprendžių registro apie to asmens teistumą, jeigu asmuo gyvena, gyveno arba yra ar buvo prašymą gavusios ar prašymą teikiančios valstybės narės pilietis. Koordinavimo ir socialinės apsaugos sistemų srityje EDAPP pateikė idėją, kad institucija, kuri yra prieinamesnė atitinkamam asmeniui, galėtų veikti pagal „vieno langelio principą“. Todėl EDAPP ragina Komisiją tęsti darbą skatinant

([18]) OL C 270, 2008 10 25, p. 1.
([19]) Žr. Komunikato 6 p.

technologijų priemones – visų pirma prieigą internetu – suteikiant piliečiams galimybę geriau valdyti savo asmens duomenis net tuomet, kai jie juda tarp skirtingų valstybių narių.

VI. **IŠVADOS**

42. EDAPP pritaria nagrinėjamam pasiūlymui dėl e. teisingumo sukūrimo ir rekomenduoja atsižvelgti į šioje nuomonėje pareikštas pastabas, būtent:

— atsižvelgti į neseniai priimtą pamatinį sprendimą dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos – įskaitant į jo trūkumus – ir ne tik įgyvendinti Komunikate numatytas priemones, bet ir siekiant kuo greičiau pradėti svarstyti, kaip galima labiau patobulinti duomenų apsaugos teisinę sistemą teisėsaugos srityje;

— įtraukti į e. teisingumą administracines procedūras. Vienas iš šio naujo elemento aspektų turėtų būti e. teisingumo projektų inicijavimas siekiant didinti duomenų apsaugos taisyklių bei nacionalinių duomenų apsaugos institucijų matomumą, visų pirma duomenų, tvarkomų e. teisingumo projektuose, atžvilgiu;

— teikti pirmenybę decentralizuotai architektūrai;

— užtikrinti, kad sistemų sujungimo ir sąveikumo srityje būtų tinkamai atsižvelgta į tikslų apribojimo principą;

— visiems asmens duomenis numatomose programose tvarkantiems subjektams paskirstyti aiškias pareigas ir nustatyti veiksmingus duomenų apsaugos institucijų koordinavimo mechanizmus;

— užtikrinti, kad tvarkant asmens duomenis kitais tikslais, nei tais, kuriems jie buvo surinkti, turėtų būti laikomasi konkrečių sąlygų, nustatytų galiojančiuose duomenų apsaugos teisės aktuose;

— aiškiai apibrėžti automatinio vertimo naudojimą ir nustatyti jo ribas, kad būtų skatinamas abipusis baudžiamųjų veikų supratimas nedarant įtakos perduodamos informacijos kokybei;

— patikslinti Komisijos atsakomybę už bendrą infrastruktūrą, pavyzdžiui, s-TESTA;

— atsižvelgiant į naujų technologijų naudojimą užtikrinti, kad į duomenų apsaugos klausimus būtų atsižvelgta kuo ankstesniame etape („į privatumą atsižvelgiama projektuojant“), bei būtų skatinamas technologijos priemonių naudojimas, sudarant piliečiams galimybę geriau kontroliuoti savo asmens duomenis net tuomet, kai jie juda tarp skirtingų valstybių narių.

Priimta Briuselyje, 2008 m. gruodžio 19 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas

Europos duomenų apsaugos priežiūros pareigūno nuomonės dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos dėl pacientų teisių į sveikatos priežiūros paslaugas kitose valstybėse narėse įgyvendinimo projektas

(2009/C 128/03)

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,

atsižvelgdamas į 2008 m. liepos 2 d. EDAPP pateiktą prašymą pateikti nuomonę pagal Reglamento (EB) Nr. 45/2001 28 straipsnio 2 dalį,

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS

Pasiūlymas dėl direktyvos dėl pacientų teisių į sveikatos priežiūros paslaugas kitose valstybėse narėse įgyvendinimo

1. 2008 m. liepos 2 d. Komisija priėmė pasiūlymą dėl Europos Parlamento ir Tarybos direktyvos dėl pacientų teisių į sveikatos priežiūros paslaugas kitose valstybėse narėse įgyvendinimo (toliau – pasiūlymas) [1]. Pagal Reglamento (EB) Nr. 45/2001 28 straipsnio 2 dalį Komisija, norėdama pasikonsultuoti, nusiuntė pasiūlymą EDAPP.

2. Pasiūlymu siekiama nustatyti tarpvalstybinio sveikatos priežiūros paslaugų teikimo ES Bendrijos sistemą tiems atvejams, kai sveikatos priežiūros paslaugos, kurias pacientas nori gauti, yra teikiamos ne jo gyvenamosios vietos šalyje, o kitoje valstybėje narėje. Ši sistema kuriama reglamentuojant tris pagrindines sritis:

— nustatomi visų ES sveikatos sistemų bendri principai, aiškiai apibrėžiant valstybių narių atsakomybę;

— kuriama konkreti tarpvalstybinio sveikatos priežiūros paslaugų teikimo sistema, aiškiai reglamentuojant pacientų teises gauti sveikatos priežiūros paslaugas kitoje valstybėje narėje;

— skatinamas ES bendradarbiavimas sveikatos priežiūros srityje, tokiais klausimais kaip kitose šalyse išduotų receptų pripažinimas, Europos pavyzdiniai tinklai, sveikatos srities technologijų vertinimas, duomenų rinkimas, kokybė ir sauga.

3. Šios sistemos tikslai dvejopi: pakankamai aiškiai reglamentuoti teises į kitose valstybėse narėse suteiktų sveikatos priežiūros paslaugų išlaidų apmokėjimą ir užtikrinti, kad būtini kokybiškų, saugių bei efektyvių sveikatos priežiūros paslaugų reikalavimai būtų taikomi kitose valstybėse narėse gaunamoms priežiūros paslaugoms.

4. Tam, kad būtų įgyvendinama tarpvalstybinio sveikatos priežiūros paslaugų teikimo sistema reikia, kad skirtingų valstybių narių įgaliotos organizacijos bei sveikatos priežiūros srities specialistai keistųsi atitinkamais su pacientų sveikata susijusiais asmens duomenimis (toliau – sveikatos duomenys). Šie duomenys laikomi konfidencialiais, todėl jiems taikomos griežtesnės duomenų apsaugos taisyklės, nustatytos Direktyvos 95/46/EB 8 straipsnyje dėl ypatingų duomenų kategorijų.

Konsultavimasis su EDAPP

5. EDAPP palankiai vertina tai, kad vadovaujantis Reglamento (EB) Nr. 45/2001 28 straipsniu su juo konsultuojamasi šiuo klausimu ir kad tai yra nurodyta pasiūlymo preambulėje.

6. Dėl pasiūlymo dėl direktyvos sveikatos priežiūros srityje su EDAPP oficialiai konsultuotasi pirmą kartą. Todėl šioje nuomonėje kai kurios pateiktos pastabos yra platesnio pobūdžio, skirtos bendriems asmens duomenų apsaugos sveikatos priežiūros sektoriuje klausimams, bei galėtų būti taikomos ir kitiems atitinkamiems teisės aktams (privalomiems ar neprivalomiems).

[1] COM(2008) 414 galutinis. Pažymėtina, kad tą pačią dieną buvo priimtas ir papildomas komunikatas dėl pacientų teisių į sveikatos priežiūros paslaugas kitose valstybėse narėse įgyvendinimo Bendrijos sistemos (COM(2008) 415 galutinis). Tačiau kadangi šis komunikatas tėra gana bendro pobūdžio, EDAPP nusprendė daugiau dėmesio skirti siūlomai direktyvai.

7. Jau nuomonės pradžioje EDAPP norėtų pareikšti, kad pritaria iniciatyvoms, kuriomis gerinamos tarpvalstybinio sveikatos priežiūros paslaugų teikimo sąlygos. Iš tiesų šį pasiūlymą reikėtų nagrinėti bendros EB programos, skirtos gerinti piliečių sveikatą informacinėje visuomenėje, kontekste. Kitos iniciatyvos šioje srityje yra Komisijos numatyta direktyva ir komunikatas dėl žmogaus organų donorystės ir persodinimo ([1]), rekomendacija dėl elektroninių sveikatos įrašų sistemų suderinamumo ([2]) ir numatytas komunikatas dėl telemedicinos ([3]). Tačiau EDAPP yra susirūpinęs dėl to, kad visos šios susijusios iniciatyvos nėra glaudžiai susietos ir (arba) susijusios tarpusavyje privatumo ir duomenų saugumo srityje, ir dėl to atsiranda trukdžių taikyti vienodą duomenų apsaugos metodą sveikatos priežiūros srityje, visų pirma naujų IRT technologijų naudojimo atžvilgiu. Kaip pavyzdį šiame pasiūlyme galima paminėti tai, kad nors telemedicina yra aiškiai paminėta siūlomos direktyvos 10 konstatuojamojoje dalyje, nėra jokios nuorodos į atitinkamo Europos Komisijos komunikato duomenų apsaugos aspektą. Be to, nors elektroniniai sveikatos įrašai yra vienas iš galimų būdų vykdyti tarpvalstybinį sveikatos duomenų perdavimą, nėra pateikta jokios nuorodos į privatumo užtikrinimo klausimus, nagrinėtus atitinkamoje Komisijos rekomendacijoje ([4]). Dėl to susidaro įspūdis, kad bendra privatumo užtikrinimo sveikatos priežiūros srityje perspektyva tebėra neaiškiai apibrėžta, o kai kuriais atvejais jos iš viso nėra.

8. Tai akivaizdu ir šiame pasiūlyme, todėl EDAPP apgailestauja, kad duomenų apsaugos aspektai nėra konkrečiai reglamentuoti. Be abejo, galima rasti nuorodų į duomenų apsaugą, tačiau jos yra daugiausia bendro pobūdžio ir tinkamai neatspindi specifinių su privatumu susijusių poreikių bei reikalavimų tarpvalstybinio sveikatos priežiūros paslaugų teikimo srityje.

9. EDAPP nori pabrėžti, kad vienodas ir patikimas duomenų apsaugos metodas visuose siūlomuose sveikatos priežiūros srities teisės aktuose ne tik užtikrins piliečių pagrindinę teisę į jų asmens duomenų apsaugą, bet ir padės toliau plėtoti tarpvalstybinį sveikatos priežiūros paslaugų teikimą ES.

II. **DUOMENŲ APSAUGA TEIKIANT SVEIKATOS PRIEŽIŪROS PASLAUGAS KITOSE VALSTYBĖSE NARĖSE**

Bendras kontekstas

10. Plačiausiai žinomas Europos bendrijos tikslas buvo sukurti vidaus rinką – erdvę be vidaus sienų, kurioje būtų užtikrintas laisvas prekių, asmenų, paslaugų ir kapitalo judėjimas. Akivaizdu, tai, kad buvo sudarytos galimybės piliečiams lengviau atvykti ir apsigyventi ne savo kilmės, o kitose valstybėse narėse, nulėmė tai, kad kilo su sveikatos priežiūra susijusių klausimų. Todėl dešimtajame dešimtmetyje Teisingumo Teismas vidaus rinkos kontekste susidūrė su klausimais dėl kitoje valstybėje narėje patirtų medicininių išlaidų galimo kompensavimo. Teisingumo Teismas pripažino, kad laisvė teikti paslaugas, nustatyta EB sutarties 49 straipsnyje, apima asmens laisvę atvykti į kitą valstybę narę tam, kad gautų gydymą ([5]). Todėl pacientams, norintiems gauti sveikatos priežiūros paslaugas kitoje valstybėje narėje, nebegalėjo būti taikomos kitokios sąlygos nei savo kilmės šalyje esantiems piliečiams, gavusiems tokį patį gydymą nekirtus sienos.

11. Šie teismo sprendimai yra esminiai šio pasiūlymo atžvilgiu. Kadangi Teismo praktika grindžiama atskiromis bylomis, šiuo pasiūlymu siekiama aiškiau reglamentuoti šią sritį siekiant bendriau ir veiksmingiau įgyvendinti laisvę gauti ir teikti sveikatos paslaugas. Tačiau, kaip jau minėta, šis pasiūlymas taip pat yra platesnio užmojo programos, kuria siekiama gerinti piliečių sveikatą informacinėje visuomenėje, dalis, o ES mato plačias galimybes gerinti tarpvalstybinį sveikatos priežiūros paslaugų teikimą pasitelkiant informacines technologijas.

12. Dėl akivaizdžių priežasčių tarpvalstybinį sveikatos priežiūros paslaugų teikimą reglamentuojančių taisyklių nustatymas yra opus klausimas. Jis susijęs su opia sritimi, kurioje valstybės narės yra nustačiusios skirtingas nacionalines sistemas, pavyzdžiui, draudimo ir išlaidų kompensavimo ar sveikatos priežiūros infrastruktūros organizavimo atžvilgiu, įskaitant sveikatos priežiūros informacinius tinklus ir taikomąsias programas. Nors Bendrijos teisės aktų leidėjas šiame pasiūlyme reglamentuoja tik *tarpvalstybinį* sveikatos priežiūros paslaugų teikimą, šios taisyklės turės įtakos bent tam, kaip organizuojamos nacionalinės sveikatos priežiūros sistemos.

13. Tarpvalstybinio sveikatos priežiūros paslaugų teikimo sąlygų gerinimas bus naudingas piliečiams. Tačiau dėl to tuo pat metu kils ir tam tikra rizika piliečiams. Reikia išspręsti daug praktinių problemų, atsirandančių žmonėms iš skirtingų šalių, kalbantiems skirtingomis kalbomis, bendradarbiaujant tarpvalstybiniu lygiu. Kadangi gera sveikata kiekvienam piliečiui yra itin svarbi, reikėtų panaikinti bet kokią riziką, kad gali kilti bendravimo sunkumų ir dėl to atsirasti netikslumų. Neabejotina, kad tarpvalstybinio sveikatos priežiūros paslaugų teikimo sąlygų gerinimas kartu pasitelkiant informacinių technologijų laimėjimus, turi

([1]) Paskelbta Komisijos darbo programoje.
([2]) 2008 m. liepos 2 d. Komisijos rekomendacija dėl tarpvalstybinio elektroninių sveikatos įrašų sistemų suderinamumo (pranešta dokumentu Nr. C(2008) 3282), OL L 190, 2008 7 18, p. 37.
([3]) Paskelbta Komisijos darbo programoje.
([4]) Šiuo atveju kaip pavyzdį galima nurodyti tai, kad 1 išnašoje nurodytame komunikate, kuriuo siekiama nustatyti pacientų teisių į sveikatos priežiūros paslaugas kitose valstybėse narėse įgyvendinimo Bendrijos sistemą, nėra jokios nuorodos į privatumo užtikrinimą ar duomenų apsaugą.
([5]) Žr. bylą 158/96, *Kohll*, [1998] Rink. I-1931, 34 punktas. Taip pat žr. bylą C-147/99, *Smits ir Peerbooms* [2001] Rink. I-5473 ir bylą C-385/99, *Müller-Fauré ir Van Riet* [2003] Rink. I-12403.

labai didelę reikšmę asmens duomenų apsaugai. Dėl veiksmingesnio ir todėl intensyvėjančio keitimosi sveikatos duomenimis, didėjančio atstumo tarp žmonių ir atitinkamų instancijų, skirtingų nacionalinių teisės aktų, kuriais įgyvendinamos duomenų apsaugos taisyklės, kyla klausimų dėl duomenų saugumo ir teisinio tikrumo.

Sveikatos duomenų apsauga

14. Reikia pabrėžti, kad sveikatos duomenys laikomi ypatinga duomenų kategorija, kurią reikia labiau saugoti. Kaip neseniai nurodė Europos žmogaus teisių teismas Europos žmogaus teisių konvencijos 8 straipsnio kontekste: „Asmens duomenų, visų pirma medicininių duomenų, apsauga yra esminės svarbos tam, kad asmuo galėtų naudotis savo teise į tai, kad būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, kaip užtikrinta Konvencijos 8 straipsnyje“ ([1]). Prieš aiškinant direktyvoje 95/46/EB nustatytas griežtesnes sveikatos duomenų tvarkymo taisykles, bus pateikti keli pastebėjimai dėl sąvokos „sveikatos duomenys“.

15. Direktyvoje 95/46/EB nėra pateiktos aiškios sveikatos duomenų sąvokos apibrėžties. Paprastai šį sąvoka aiškinama plačiai, dažnai sveikatos duomenis apibrėžiant kaip „asmens duomenis, kurie yra aiškiai ir glaudžiai susiję su asmens sveikatos būklės apibūdinimu“ ([2]). Šiuo atžvilgiu sveikatos duomenys paprastai apima medicininius duomenis (pvz., gydytojo nukreipimai ir receptai, sveikatos patikrinimo išvados, laboratoriniai tyrimai, radiogramos ir pan.) ir su sveikata susijusius administracinius bei finansinius duomenis (pvz., dokumentai, susiję su hospitalizacija, socialinio draudimo numeris, registracijos konsultacijoms laikas, sąskaitos už suteiktas sveikatos priežiūros paslaugas ir pan.). Pažymėtina, kad sąvoka „medicininiai duomenys“ ([3]), kaip ir sąvoka „duomenys apie sveikatos priežiūros paslaugas“ ([4]), taip pat kartais naudojama su sveikata susijusiems duomenims apibūdinti. Visoje šioje nuomonėje bus vartojama sąvoka „sveikatos duomenys“.

16. Naudinga sąvokos „sveikatos duomenys“ apibrėžtis nustatyta ISO 277799: „bet kokia informacija, susijusi su asmens fizine ar psichine sveikata arba su sveikatos priežiūros paslaugų teikimu asmeniui, kuri gali būti: a) informacija apie asmens registraciją, kad būtų suteiktos sveikatos priežiūros paslaugos; b) su tuo asmeniu susijusi informacija apie mokėjimus ar reikalavimų sveikatos priežiūros paslaugoms gauti atitiktį; c) numeris, simbolis ar detalė, priskirti asmeniui, kad sveikatos tikslais būtų galima nustatyti būtent jo tapatybę; d) bet kokia informacija apie asmenį, surinkta teikiant jam sveikatos priežiūros paslaugas; e) informacija, gauta atlikus kūno dalies ar organizmo medžiagos tyrimus ar patikrinimą; ir f) asmens (sveikatos priežiūros srities specialisto), teikiančio atitinkamam asmeniui sveikatos priežiūros paslaugas, tapatybės nustatymas“.

17. EDAPP itin palankiai vertintų tai, kad šiame pasiūlyme būtų priimta konkreti sąvokos „sveikatos duomenys“ apibrėžtis, kuri taip pat galėtų būti naudojama ateityje kituose atitinkamuose EB teisės aktų tekstuose (žr. III skirsnį).

18. Direktyvos 95/46/EB 8 straipsnyje nustatytos ypatingų duomenų kategorijų tvarkymo taisyklės. Šios taisyklės yra griežtesnės nei kitų duomenų tvarkymo taisyklės, nustatytos Direktyvos 95/46/EB 7 straipsnyje. Tai paaiškėja jau iš 8 straipsnio 1 dalies, kurioje aiškiai nurodyta, kad valstybės narės *uždraudžia* tvarkyti, *inter alia*, duomenis apie asmens sveikatą. Kitose šio straipsnio dalyse suformuluota keletas šiam draudimui taikomų išimčių, tačiau šios išimtys yra siauresnės nei 7 straipsnyje nustatyti įprastų duomenų tvarkymo pagrindai. Pavyzdžiui, šis draudimas netaikomas, jeigu duomenų subjektas yra davęs savo *aiškų* sutikimą (Direktyvos 95/46/EB 8 straipsnio 2 dalies a punktas), o 95/46/EB 7 straipsnio a punkte reikalaujama, kad duomenų subjektas būtų *nedviprasmiškai* davęs sutikimą. Be to, valstybės narės įstatymai gali numatyti, kad tam tikrais atvejais šio draudimo negalima panaikinti duomenų subjekto duotu sutikimu. 8 straipsnio 3 dalis reglamentuojamas tik su sveikata susijusių duomenų tvarkymas. Vadovaujantis šia dalimi, 1 dalyje numatytas draudimas netaikomas, kai duomenis reikia tvarkyti teikiant profilaktines medicinos, medicininės diagnostikos, medicinos priežiūros, gydymo, sveikatos apsaugos paslaugas ir kai tokius duomenis tvarko sveikatos apsaugos darbuotojas, kuriam pagal nacionalinius įstatymus arba nacionalinių kompetentingų institucijų nustatytas taisykles galioja profesinės paslapties saugojimo pareiga, arba kitas asmuo, kuriam irgi galioja lygiavertė paslapties saugojimo prievolė.

19. Direktyvos 95/46/EB 8 straipsnyje itin akcentuojama tai, kad valstybės narės turėtų numatyti tinkamas ar pakankamas apsaugos priemones. 8 straipsnio 4 dalyje, pavyzdžiui, nustatyta, kad dėl svarbių visuomenės interesų valstybės narės gali numatyti ir kitas draudimui tvarkyti konfidencialius duomenis taikomas išimtis, bet turi užtikrinti tinkamas apsaugos priemones. Šia nuostata bendrai akcentuojama valstybių narių atsakomybė ypatingą dėmesį skirti konfidencialių, pavyzdžiui, su sveikata susijusių, duomenų tvarkymui.

Sveikatos duomenų apsauga vykdant tarpvalstybinį keitimąsi šiais duomenimis

Bendra valstybių narių atsakomybė

20. Valstybės narės turėtų ypač gerai suvokti šią bendrą atsakomybę, kadangi kalbama apie tarpvalstybinį keitimąsi sveikatos duomenimis. Kaip nurodyta pirmiau, vykdant tarpvalstybinį keitimąsi sveikatos duomenimis didėja pavojus, kad duomenys bus tvarkomi neteisingai ar neteisėtai. Akivaizdu, tai gali turėti itin didelių neigiamų

([1]) Žr. EŽTT, 2008 m. liepos 17 d., *I prieš Suomiją* (paraiška Nr. 20511/03), 38 punktas.

([2]) Žr. 29 straipsnio darbo grupės 2007 m. vasario mėn. 131-o darbinio dokumento dėl su sveikata susijusių asmens duomenų tvarkymo elektroniniuose sveikatos įrašuose II dalies 2 punktą. Taip pat dėl sąvokos „asmens duomenys“ plačios reikšmės žr. 29 straipsnio darbo grupės Nuomonę 4/2007 dėl asmens duomenų sąvokos, išdėstytą 136-ame darbiniame dokumente.

([3]) Europos Tarybos rekomendacija Nr. R(97)5 dėl medicininių duomenų apsaugos.

([4]) ISO 27799:2008 „Sveikatos informatika – informacijos saugumo valdymas sveikatos srityje vadovaujantis ISO/IEC 27002“.

pasekmių duomenų subjektui. Kadangi šiame procese dalyvauja ir valstybė narė, kurioje pacientas apdraustas (kurioje pacientas yra apdraustas asmuo), ir valstybė narė, kurioje teikiamos sveikatos priežiūros paslaugos (kurioje faktiškai teikiamos sveikatos priežiūros paslaugos pacientams iš kitų valstybių narių), jos abi dalijasi šia atsakomybe.

21. Sveikatos duomenų saugumas šiame kontekste yra svarbus klausimas. Pirmiau cituotoje neseniai svarstytoje byloje Europos žmogaus teisių teismas ypač daug dėmesio skyrė sveikatos duomenų konfidencialumui: „Sveikatos duomenų konfidencialumo užtikrinimas yra vienas iš esminių visų Konvencijos Susitariančiųjų Šalių teisės sistemų principas. Labai svarbu ne tik gerbti paciento privatumo jausmą, bet ir išsaugoti jo pasitikėjimą gydytojo profesija bei apskritai sveikatos priežiūros paslaugomis“ ([1]).

22. Direktyvoje 95/46/EB nustatytose duomenų apsaugos taisyklėse taip pat reikalaujama, kad valstybė narė, kurioje pacientas apdraustas, pacientui suteiktų tinkamą, tikslią ir atnaujintą informaciją apie paciento asmens duomenų perdavimą kitai valstybei narei, tuo pat metu užtikrindama, kad duomenų perdavimas šiai valstybei narei būtų saugus. Valstybė narė, kurioje teikiamos sveikatos priežiūros paslaugos, pagal savo nacionalinę duomenų apsaugą reglamentuojančią teisę taip pat turėtų užtikrinti, kad šie duomenys būtų gauti saugiai, ir tinkamą apsaugos lygį tuomet, kai jie yra iš tiesų tvarkomi.

23. EDAPP norėtų, kad pasiūlyme būtų aiškiai apibrėžta valstybių narių bendra atsakomybė, be kita ko atsižvelgiant į duomenų perdavimą elektroninėmis priemonėmis, ypač naujų IRT taikomųjų programų kontekste, kaip aptarta toliau šioje nuomonėje.

Sveikatos duomenų perdavimas elektroninėmis priemonėmis

24. Iš esmės nustatyta, kad tarpvalstybinis keitimasis sveikatos duomenimis gerinamas pasitelkiant informacines technologijas. Nors keitimasis duomenimis tarpvalstybinio sveikatos priežiūros paslaugų teikimo sistemoje vis dar gali vykti naudojantis popieriuje surašytais dokumentais (pvz., pacientas atvyksta į kitą valstybę narę su savimi pasiimdamas visus atitinkamus savo sveikatos duomenis, tokius kaip laboratoriniai tyrimai, gydytojo nukreipimai ir pan.), aiškiai ketinama vietoje to naudotis elektroninėmis priemonėmis. Perduodant sveikatos duomenis elektroninėmis priemonėmis bus pasitelkiamos sveikatos priežiūros informacinės sistemos, sukurtos (ar kurios turi būti sukurtos ateityje) valstybėse narėse (ligoninėse, klinikose ir pan.), naujos technologijos, pavyzdžiui, elektroninių sveikatos priežiūros įrašų taikomosios programos (galbūt veikiančios internete), ir kitos priemonės, pavyzdžiui, pacientų ir gydytojo sveikatos kortelės. Žinoma, taip pat įmanoma, kad priklausomai nuo valstybių narių sveikatos priežiūros sistemų bus naudojamos kartu ir popierinės, ir elektroninės keitimosi duomenimis formos.

25. E. sveikatos ir telemedicinos taikomosios programos, kurios patenka į siūlomos direktyvos taikymo sritį, bus grindžiamos išimtinai keitimusi elektroniniais sveikatos duomenimis (pvz., gyvybinių funkcijų duomenimis, vaizdais ir kt.), paprastai kartu naudojant kitas esamas valstybės narės, kurioje asmeniui teikiamos sveikatos priežiūros paslaugos, ir valstybės narės, kurioje jis apdraustas, elektronines sveikatos priežiūros informacines sistemas. Tai apima sistemas, kurios veikia palaikant paciento ir gydytojo ryšį (pvz., nuotolinės stebėsenos ir diagnozavimo sistemas), taip pat gydytojų tarpusavio ryšį (pvz., sveikatos priežiūros specialistų tarpusavio telekonsultacijas norint gauti specialistų nuomonę konkrečiais sveikatos priežiūros klausimais). Kitos labiau specialiems poreikiams skirtos sveikatos priežiūros taikomosios programos, naudojamos bendram tarpvalstybiniam sveikatos priežiūros paslaugų teikimui, taip pat gali būti grindžiamos išimtinai keitimusi duomenimis elektroninėmis priemonėmis, pvz., e. receptų arba e. nukreipimo programos, kurios kai kuriose valstybėse narėse jau yra įgyvendinamos nacionaliniu lygiu ([2]).

Susirūpinimą keliančios sritys tarpvalstybinio keitimosi sveikatos duomenimis srityje

26. Atsižvelgiant į pirmiau nurodytus klausimus, taip pat į esamą valstybių narių sveikatos priežiūros sistemų įvairovę ir į vis didesnę e. sveikatos taikomųjų programų plėtrą, išryškėja šios dvi pagrindinės su asmens duomenų apsauga teikiant sveikatos priežiūros paslaugas kitose valstybėse narėse susijusios susirūpinimą keliančios sritys: a) skirtingi saugumo lygiai, kuriuos valstybės narės gali taikyti asmens duomenų apsaugai (techninės ir organizacinės priemonės), ir b) privatumo integravimas į e. sveikatos taikomąsias programas, ypač naujausių pokyčių atveju. Be to, taip pat gali reikėti skirti ypatingą dėmesį kitiems aspektams, pavyzdžiui, antriniam sveikatos duomenų naudojimui, ypač statistikos rengimo srityje. Šie klausimai toliau analizuojami likusioje šio skirsnio dalyje.

Duomenų saugumas valstybėse narėse

27. Nepaisant to, kad direktyvos 95/46/EB ir 2002/58/EB Europoje yra taikomos vienodai, tam tikrų nuostatų aiškinimas ir įgyvendinimas skirtingose šalyse gali skirtis, ypač tose srityse, kuriose teisinės nuostatos yra bendro pobūdžio ir valstybėms narėms paliekama veikimo laisvė. Šiuo požiūriu svarbiausia sritis yra duomenų tvarkymo saugumas, t. y. priemonės (techninės ir organizacinės), kurių valstybės narės imasi, kad užtikrintų sveikatos duomenų saugumą.

([1]) Žr. EŽTT, 2008 m. liepos 17 d., *I prieš Suomiją* (paraiška Nr. 20511/03), 38 punktas.

([2]) *eHealth ERA Report, Towards the Establishment of a European eHealth Research Area*, Europos Komisija, Informacinė visuomenė ir žiniasklaida, 2007 m. kovas, http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Nors už griežtą sveikatos duomenų apsaugą atsako visos valstybės narės, šiuo metu nėra bendrai pripažintos „tinkamo“ ES sveikatos priežiūros saugumo lygio apibrėžties, kuri galėtų būti taikoma teikiant sveikatos priežiūros paslaugas kitose valstybėse narėse. Todėl, pavyzdžiui, vienos valstybės narės ligoninė pagal nacionaliniu lygiu nustatytas duomenų apsaugos taisykles gali privalėti taikyti konkrečias saugumo priemones (pavyzdžiui, nustatyti saugumo politiką ir elgesio kodeksus, konkrečias naudojimosi išorės paslaugų teikėjų ir rangovų paslaugomis taisykles, audito reikalavimus ir kt.), o kitose valstybėse narėse to gali nebūti. Šis nenuoseklumas gali turėti įtakos tarpvalstybiniam keitimuisi duomenimis, ypač elektroniniu būdu, kadangi negali būti garantuojama, kad duomenys skirtingose valstybėse narėse duomenys vienodai saugūs (techniniu ir organizaciniu požiūriu).

29. Todėl reikia toliau derinti nuostatas šioje srityje nustatant sveikatos priežiūros srityje taikomus bendrus saugumo reikalavimus, kuriuos turėtų vienodai taikyti valstybių narių sveikatos priežiūros paslaugų teikėjai. Šis poreikis tikrai atitinka bendrą poreikį nustatyti ES sveikatos sistemų bendrus principus, kaip nurodyta pasiūlyme.

30. Tai turėtų būti daroma bendro pobūdžio priemonėmis, nenustatant valstybėms narėms konkrečių privalomų techninių sprendimų, tačiau nustatant tarpusavio pripažinimo ir priėmimo pagrindą, pvz., saugumo politikos nustatymo, pacientų ir sveikatos priežiūros specialistų tapatybės nustatymo bei atpažinimo ir kt. srityse. Šio mėginimo gairėmis galėtų tapti galiojantys Europos ir tarptautiniai standartai (pvz., ISO ir CEN) sveikatos priežiūros ir saugumo srityje, taip pat tinkamai pripažintos ir teisiniu požiūriu pagrįstos techninės koncepcijos (pvz., elektroniniai parašai ([1])).

31. EDAPP pritaria sveikatos priežiūros saugumo suderinimo ES lygiu idėjai ir laikosi nuomonės, kad Komisija jau šiame pasiūlyme turėtų imtis atitinkamų iniciatyvų (žr. III skirsnį).

Privatumas naudojant e. sveikatos taikomąsias programas

32. Privatumo ir saugumo aspektai turėtų būti įtraukiami rengiant sistemų projektus ir įgyvendinant bet kurią sveikatos priežiūros sistemą, ypač šiame pasiūlyme minimas e. sveikatos taikomąsias programas („atsižvelgimas į privatumą rengiant projektus“). Šiam neginčytinam reikalavimui jau pritarta kituose atitinkamuose politikos dokumentuose ([2]), tiek bendro pobūdžio, tiek skirtuose konkrečiai sveikatos priežiūrai ([3]).

33. Pasiūlyme aptariamos e. sveikatos sąveikos srityje kaip visos numatomos raidos pagrindas dar kartą turėtų būti pabrėžiama atsižvelgimo į privatumą rengiant projektus sąvoka. Ši sąvoka taikoma keliais skirtingais lygiais: organizaciniu, semantiniu, techniniu.

— Organizaciniu lygiu į privatumą turėtų būti atsižvelgiama apibrėžiant valstybių narių sveikatos priežiūros organizacijų keitimosi sveikatos duomenimis būtinas procedūras. Tai gali turėti tiesioginės įtakos keitimosi rūšiai ir perduodamų duomenų detalumui (pvz., kai tai įmanoma, identifikavimo numerių naudojimas vietoj pacientų tikrųjų pavardžių).

— Semantiniu lygiu privatumo ir saugumo reikalavimai turėtų būti įtraukti į naujus standartus ir sistemas, pvz., nustatant elektroninio recepto formą, kuri aptariama pasiūlyme. Tai darant galėtų būti remiamasi galiojančiais techniniais standartais šioje srityje, pvz., duomenų konfidencialumo ir skaitmeninio parašo standartais, ir galėtų būti patenkinami konkrečiai sveikatos priežiūrai būdingi poreikiai, pavyzdžiui, kvalifikuotų sveikatos priežiūros specialistų atpažinimas pagal jų darbo pobūdį.

— Techniniu lygiu sistemų architektūra ir vartotojams skirtos taikomosios programos turėtų pritaikyti privatumo didinimo technologijas, taip įgyvendinant pirmiau nurodytą semantinę apibrėžtį.

34. EDAPP mano, kad elektroninių receptų sritis galėtų būti pirmoji, kurioje privatumo ir saugumo reikalavimai būtų įtraukiami pačiame pradiniame kūrimo etape (žr. III skirsnį).

Kiti aspektai

35. Papildomas aspektas, į kurį galėtų būti atsižvelgiama vykdant tarpvalstybinį keitimąsi sveikatos duomenimis, yra antrinis sveikatos duomenų naudojimas, visų pirma duomenų naudojimas statistikos tikslais, kaip jau nurodyta šiame pasiūlyme.

36. Kaip nurodyta 18 punkte, Direktyvos 95/46 8 straipsnio 4 dalyje numatyta antrinio sveikatos duomenų naudojimo galimybė. Tačiau šis tolesnis tvarkymas turėtų vykti tik dėl su svarbių visuomenės interesais susijusių priežasčių ir jam turi būti taikomos nacionalinėje teisėje arba priežiūros institucijos sprendimu nustatytos „tinkamos apsaugos priemonės“ ([4]). Be to, statistinio duomenų tvarkymo atveju, kaip minėta ir EDAPP nuomonėje dėl siūlomo reglamento

([1]) 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos, OL L 13, 2000 1 19, p. 12–20.

([2]) EDAPP ir ES moksliniai tyrimai bei technologinė plėtra, politikos dokumentas, EDAPP, 2008 m. balandžio mėn., http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

([3]) 2008 m. liepos 2 d. Komisijos rekomendacija dėl tarpvalstybinio elektroninių sveikatos įrašų sistemų suderinamumo (pranešta dokumentu Nr. C(2008) 3282), OL L 190, 2008 7 18, p. 37.

([4]) Žr. taip pat Direktyvos 95/46 34 konstatuojamąją dalį. Šiuo klausimu žr. taip pat 8 išnašoje minėtą 29 straipsnio darbo grupės nuomonę dėl elektroninių sveikatos įrašų, p. 16.

dėl Bendrijos statistikos apie visuomenės sveikatą ir darbuotojų sveikatą bei saugą ([1]), dėl galimos skirtingos sąvokų „konfidencialumas“ ir „duomenų apsauga“ prasmės taikant, viena vertus, duomenų apsaugos teisės aktus ir, kita vertus, statistikos teisės aktus, esama papildomos rizikos.

37. ESAPP norėtų pabrėžti pirmiau išvardytus aspektus nagrinėjant šį pasiūlymą. Turėtų būti aiškiau nurodyti duomenų apsaugos reikalavimai, susiję su vėlesniu sveikatos duomenų naudojimu (žr. III skirsnį).

III. **IŠSAMI PASIŪLYMO ANALIZĖ**

Pasiūlymo nuostatos dėl duomenų apsaugos

38. Įvairiose pasiūlymo dalyse ne kartą nurodyta duomenų apsauga ir privatumas, konkrečiau:

— 3 konstatuojamojoje dalyje, be kita ko, nurodyta, kad direktyva turi būti įgyvendinama ir taikoma tinkamai gerbiant teisę į privatų gyvenimą ir teisę į asmens duomenų apsaugą;

— 11 konstatuojamojoje dalyje pagrindinė teisė į privatumą tvarkant asmens duomenis ir konfidencialumas nurodyti kaip du visos Bendrijos sveikatos sistemoms bendri veiklos principai;

— 17 konstatuojamojoje dalyje teisė į asmens duomenų apsaugą apibūdinama kaip asmenų pagrindinė teisė, kuri turėtų būti saugoma, skiriant ypač daug dėmesio asmenų teisei gauti su sveikata susijusius duomenis, taip pat teikiant sveikatos priežiūros paslaugas kitose valstybėse narėse, kaip nustatyta Direktyvoje 65/46/EB;

— 3 straipsnio, kuriame apibūdintas direktyvos ryšys su kitomis Bendrijos nuostatomis, 1 dalies a punkte nurodytos direktyvos 95/46/EB ir 2002/58/EB;

— 5 straipsnio dėl valstybės narės, kurioje teikiamos sveikatos priežiūros paslaugos, atsakomybės 1 dalies f punkte teisės į privatumą apsauga nurodyta kaip viena iš šių atsakomybės sričių, laikantis nacionalinių priemonių, kuriomis įgyvendinamos direktyvos 95/46/EB ir 2002/58/EB;

— 6 straipsnio dėl kitoje valstybėje narėje teikiamų sveikatos priežiūros paslaugų 5 dalyje pabrėžiama pacientų, kurie vyksta į kitą valstybę narę gauti sveikatos priežiūros paslaugų arba nori gauti kitoje valstybėje narėje teikiamų sveikatos priežiūros paslaugų, teisė susipažinti su savo medicininiais dokumentais, taip pat laikantis nacionalinių priemonių, kuriomis įgyvendinamos direktyvos 95/46/EB ir 2002/58/EB;

— 12 straipsnio dėl sveikatos priežiūros paslaugų kitose valstybėse nacionalinių kontaktinių punktų 2 dalies a punkte nurodyta, kad šie kontaktiniai punktai, be kita ko, turėtų būti atsakingi už informacijos apie asmens duomenų apsaugos kitoje valstybėje narėje garantijas teikimą ir platinimą pacientams;

— 16 straipsnyje dėl e. sveikatos nurodyta, kad nustatant priemones informacinių ir ryšių technologijų sistemų sąveikai užtikrinti turėtų būti gerbiama pagrindinė teisė į asmens duomenų apsaugą pagal taikomus teisės aktus;

— Galiausiai 18 straipsnio 1 dalyje, be kita ko, paminėta, kad statistikos ir stebėsenos tikslais duomenys turėtų būti kaupiami laikantis nacionalinių ir Bendrijos teisės aktų dėl asmens duomenų apsaugos.

39. EDAPP palankiai vertina tai, kad rengiant pasiūlymą buvo atsižvelgta į duomenų apsaugą ir kad mėginama pademonstruoti bendrą privatumo poreikį teikiant tarpvalstybines sveikatos priežiūros paslaugas. Tačiau esamos pasiūlymo nuostatos dėl duomenų apsaugos yra pernelyg bendro pobūdžio arba valstybių narių pareigos nurodomos gana selektyviai ir išbarstytai:

— Visų pirma, 3 ir 11 konstatuojamosiose dalyse, jas siejant su 3 straipsnio 1 dalies a punktu, 16 straipsniu ir 18 straipsnio 1 dalimi, faktiškai nurodyta bendra duomenų apsaugos teisinė sistema (pastaraisiais dviem atvejais e. sveikatos ir statistinių duomenų rinkimo kontekste, tačiau nenustatant konkrečių su privatumu susijusių reikalavimų).

— Valstybių narių atsakomybės klausimu pateikiama bendra nuoroda 5 straipsnio 1 dalies f punkte.

— 17 konstatuojamojoje dalyje ir 6 straipsnio 5 dalyje konkrečiau nurodyta pacientų prieigos teisė valstybėje narėje, kurioje teikiamos sveikatos priežiūros paslaugos.

— Galiausiai 12 straipsnio 2 dalies a punkte yra nuostata dėl pacientų teisės gauti informaciją valstybėje narėje, kurioje jie apdrausti (vykdant nacionalinių kontaktinių punktų veiklą).

Be to, kaip minėta šios nuomonės įvade, nėra sąsajų su kitais EB teisiniais dokumentais (privalomais ar neprivalomais) sveikatos priežiūros srityje ir (arba) nuorodų į juos, ypač naujų IRT taikomųjų programų (pvz., telemedicinos arba elektroninių sveikatos įrašų) naudojimo atvejais.

([1]) OL C 295, 2007 12 7, p. 1.

40. Tokiu būdu, nors privatumas bendrai nurodytas kaip tarpvalstybinio sveikatos priežiūros paslaugų teikimo reikalavimas, vis dėlto nėra bendro vaizdo, nei valstybių narių pareigų, nei dėl tarpvalstybinio sveikatos priežiūros paslaugų teikimo pobūdžio ypatumų (lyginant su nacionaliniu sveikatos priežiūros paslaugų teikimu) požiūriu. Konkrečiau:

— valstybių narių atsakomybė nėra nurodyta kaip darni visuma, kadangi kai kurios pareigos (prieigos teisės ir informacija) pabrėžiamos (skirtingose pasiūlymo dalyse), o kitos visiškai nenurodomos, pavyzdžiui, tvarkymo saugumas.

— Nenurodyti susirūpinimą keliantys klausimai dėl valstybių narių nenuoseklumo saugumo priemonių srityje ir poreikis, kad teikiant tarpvalstybines sveikatos priežiūros paslaugas sveikatos duomenų saugumas būtų suderintas Europos lygiu.

— Nenurodytas privatumo integravimas e. sveikatos taikomosiose programose. Tai nėra tinkamai nurodyta ir e. receptų atveju.

41. Be to, kyla konkrečių susirūpinimą keliančių klausimų dėl 18 straipsnio, kuriame aptariamas duomenų rinkimas statistikos ir stebėsenos tikslais. Pirmoje dalyje nurodyti „statistiniai ir *kiti papildomi duomenys*“; be to, joje daugiskaita nurodyti stebėsenos tikslai ir vėliau išvardytos sritys, kuriose taikomi šie stebėsenos tikslai, t. y. tarpvalstybinis sveikatos priežiūros paslaugų teikimas, suteiktos priežiūros paslaugos, paslaugų teikėjai ir pacientai, išlaidos ir rezultatai. Šiame kontekste, kuris ir taip pakankamai neaiškus, bendrai nurodyti duomenų apsaugos teisės aktai, tačiau nenustatyti jokie konkretūs reikalavimai, taikomi vėlesniam su sveikata susijusių duomenų naudojimui, kaip nustatyta Direktyvos 95/46/EB 8 straipsnio 4 dalyje. Be to, antroje dalyje nustatyta besąlygiška pareiga bent kartą per metus perduoti daug duomenų Komisijai. Kadangi nėra aiškiai nurodytas būtinybės perduoti šiuos duomenis įvertinimas, atrodo, kad Bendrijos teisės aktų leidėjas pats yra nustatęs šio perdavimo Komisijai būtinybę.

EDAPP rekomendacijos

42. Norėdamas, kad būtų tinkamai išspręsti pirmiau nurodyti klausimai, EDAPP pateikia keletą toliau išvardytų rekomendacijų, kurios išdėstytos kaip penki pagrindiniai pakeitimų etapai.

1 etapas. Sveikatos duomenų apibrėžtis

43. Pagrindiniai pasiūlyme vartojami terminai apibrėžti 4 straipsnyje. EDAPP primygtinai rekomenduoja įtraukti į šį straipsnį sveikatos duomenų sąvokos apibrėžtį. Turėtų būti taikomas platus sveikatos duomenų aiškinimas, pavyzdžiui, kaip apibūdinta šios nuomonės II skirsnyje (14 ir 15 punktai).

2 etapas. Konkrečiai duomenų apsaugai skirto straipsnio įtraukimas

44. EDAPP taip pat primygtinai rekomenduoja įtraukti į pasiūlymą konkretų straipsnį dėl duomenų apsaugos, kuriame aiškiai ir lengvai suprantamai galėtų būti išdėstytas visas privatumo aspektas. Šiame straipsnyje turėtų būti a) apibūdintos valstybių narių, kuriose asmenys yra apdrausti, ir valstybių narių, kuriose teikiamos sveikatos priežiūros paslaugos, pareigos, įskaitant, be kita ko, poreikį užtikrinti tvarkymo saugumą, ir b) nustatytos pagrindinės tolesnės plėtros sritys, t. y. suderinimas saugumo srityje ir privatumo integravimas e. sveikatos srityje. Gali būti įtrauktos konkrečios šiems klausimams skirtos nuostatos (siūlomame straipsnyje), kaip išdėstyta 3 ir 4 etapuose.

3 etapas. Konkrečios suderinimui saugumo srityje skirtos nuostatos

45. Atsižvelgdamas į 2 etapo pakeitimą, EDAPP rekomenduoja, kad Komisija patvirtintų mechanizmą, pagal kurį apibrėžiamas bendrai priimtinas nacionalinis sveikatos priežiūros duomenų saugumo lygis, atsižvelgdama į esamus techninius standartus šioje srityje. Pasiūlymas turėtų tai atspindėti. Tai galėtų būti įgyvendinama taikant komitologijos procedūrą, kaip jau nurodyta 19 straipsnyje ir taikoma kitoms pasiūlymo dalims. Be to, atitinkamoms gairėms parengti galėtų būti naudojamos papildomos priemonės, įtraukiant visus suinteresuotuosius subjektus, pavyzdžiui, 29 straipsnio darbo grupę ir EDAPP.

4 etapas. Privatumo integravimas į e. recepto formą

46. 14 straipsnyje dėl kitoje valstybėje narėje išrašytų receptų pripažinimo numatytas Bendrijos receptų formos parengimas, taip padedant užtikrinti e. receptų sąveiką. Ši priemonė patvirtinama taikant komitologijos procedūrą, kaip apibrėžta pasiūlymo 19 straipsnio 2 dalyje.

47. EDAPP rekomenduoja, kad siūloma e. recepto forma apimtų privatumą ir saugumą, net ir labiausiai baziniu lygiu semantiškai apibrėžiant šią formą. Tai turėtų būti aiškiai nurodyta 14 straipsnio 2 dalies a punkte. Ir šiuo atveju labai svarbus visų suinteresuotųjų subjektų dalyvavimas. EDAPP norėtų būti informuojamas apie tolesnius su šiuo klausimu susijusius veiksmus taikant siūlomą komitologijos procedūrą ir juose dalyvauti.

5 etapas. Vėlesnis sveikatos duomenų naudojimas statistikos ir stebėsenos tikslais

48. Kad būtų išvengta nesusipratimų, EDAPP ragina paaiškinti 18 straipsnio 1 dalyje vartojamą sąvoką „kiti papildomi duomenys“. Be to, šis straipsnis turėtų būti iš dalies pakeistas, kad jame būtų aiškiau nurodyti vėlesnio duomenų naudojimo reikalavimai, kaip nustatyta Direktyvos 95/46/EB 8 straipsnio 4 dalyje. Be to, 2 dalyje nurodyta pareiga perduoti visus duomenis Komisijai, turėtų būti vertinama siekiant nustatyti, ar toks perdavimas būtinas atsižvelgiant į iš anksto deramai nurodytus teisėtus tikslus.

IV. **IŠVADOS**

49. EDAPP norėtų pareikšti, kad pritaria iniciatyvoms, kuriomis gerinamos tarpvalstybinio sveikatos priežiūros paslaugų teikimo sąlygos. Tačiau jam kelia susirūpinimą tai, kad su sveikatos priežiūra susijusios EB iniciatyvos ne visuomet gerai derinamos IRT naudojimo, privatumo ir saugumo požiūriu, o tai kliudo visuotinai laikytis vienodo požiūrio į duomenų apsaugą sveikatos priežiūros srityje.

50. EDAPP palankiai vertina tai, kad pasiūlyme yra nurodytas privatumas. Tačiau reikia keleto pakeitimų, kurie paaiškinti šios nuomonės III skirsnyje, kad būtų numatyti aiškūs reikalavimai, taikomi tiek valstybėms narėms, kuriose teikiamos sveikatos priežiūros paslaugos, tiek valstybėms narėms, kuriose asmenys yra apdrausti, taip pat kad būtų tinkamai sprendžiami su tarpvalstybinio sveikatos priežiūros paslaugų teikimo duomenų apsaugos aspektu susiję klausimai:

— 4 straipsnyje turėtų būti įtraukta sveikatos duomenų apibrėžtis – tai turėtų būti visi asmens duomenys, kurie gali būti aiškiai ir glaudžiai susiję su asmens sveikatos būklės apibūdinimu. Jie iš esmės turėtų apimti medicininius duomenis, taip pat administracinius ir finansinius su sveikata susijusius duomenis.

— Primygtinai rekomenduojama įtraukti konkretų straipsnį dėl duomenų apsaugos. Šiame straipsnyje turėtų būti aiškiai išdėstytas bendras vaizdas: apibūdinta valstybių narių, kuriose asmenys yra apdrausti, ir valstybių narių, kuriose teikiamos sveikatos priežiūros paslaugos, atsakomybė ir nurodytos pagrindinės tolesnės plėtros sritys, t. y. suderinimas saugumo srityje ir privatumo integravimas, ypač e. sveikatos taikomosiose programose.

— Rekomenduojama, kad Komisija pagal šį pasiūlymą patvirtintų mechanizmą, pagal kurį apibrėžiamas bendrai priimtinas nacionalinis sveikatos priežiūros apsaugos lygis, atsižvelgdama į esamus techninius standartus šioje srityje. Taip pat turėtų būti skatinamos papildomos ir (arba) papildančios iniciatyvos, pagal kurias įtraukiami visi suinteresuotieji subjektai, 29 straipsnio darbo grupė ir EDAPP.

— Rekomenduojama, kad į siūlomą e. recepto Bendrijos formą (taip pat ir semantiniu lygiu) būtų įtraukta „atsižvelgimo į privatumą rengiant projektus“ sąvoka. Tai turėtų būti aiškiai nurodyta 14 straipsnio 2 dalies a punkte. EDAPP norėtų būti informuojamas apie tolesnius su šiuo klausimu susijusius veiksmus taikant siūlomą komitologijos procedūrą ir juose dalyvauti.

— Rekomenduojama konkrečiau suformuluoti 18 straipsnį ir aiškiau nurodyti konkrečius reikalavimus, taikomus su sveikata susijusių duomenų vėlesniam naudojimui, kaip nustatyta Direktyvos 95/46/EB 8 straipsnio 4 dalyje.

Priimta Briuselyje, 2008 m. gruodžio 2 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas

Europos duomenų apsaugos priežiūros pareigūno antra nuomonė dėl Europos Parlamento ir Tarybos direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) peržiūros

(2009/C 128/04)

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 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje,

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

Bendra informacija

1. 2007 m. lapkričio 13 d. Europos Komisija priėmė pasiūlymą, iš dalies keičiantį, be kita ko, Direktyvą dėl privatumo ir elektroninių ryšių, paprastai vadinamą E. privatumo direktyva [1] (toliau – pasiūlymas arba Komisijos pasiūlymas). 2008 m. balandžio 10 d. EDAPP priėmė nuomonę dėl Komisijos pasiūlymo, kurioje pateikė rekomendacijų dėl pasiūlymo tobulinimo, siekdamas užtikrinti, kad siūlomais pakeitimais būtų kuo geriau apsaugomas asmenų privatumas ir asmens duomenys (toliau – EDAPP pirma nuomonė) [2].

2. EDAPP palankiai įvertino tai, kad Komisija pasiūlė sukurti privalomo pranešimo apie saugumo pažeidimus sistemą, pagal kurią bendrovės privalėtų pranešti asmenims apie atvejus, kai kilo pavojus jų asmens duomenims. Be to, jis taip pat palankiai įvertino naują nuostatą, kuri sudaro sąlygas juridiniams asmenims (*pvz.*, vartotojų asociacijoms ir interneto paslaugų teikėjams) imtis veiksmų prieš nepageidaujamų e. laiškų siuntėjus ir kuria siekiama papildyti turimas kovos su nepageidaujamu e. laiškų siuntimu priemones.

3. Prieš Europos Parlamento pirmąjį svarstymą vykusių parlamentinių diskusijų metu EDAPP pateikė papildomų rekomendacijų ir pastabų tam tikrais klausimais, iškeltais Europos Parlamento komitetų, kurių kompetencijai priklauso peržiūrėti Universaliųjų paslaugų [3] ir E. privatumo direktyvas, parengtose ataskaitose (toliau – pastabos) [4]. Pastabose pirmiausia buvo nagrinėjami klausimai, susiję su srauto duomenų tvarkymu ir intelektinės nuosavybės teisių apsauga.

4. 2008 m. rugsėjo 24 d. Europos Parlamentas (toliau – EP) priėmė teisėkūros rezoliuciją dėl E. privatumo direktyvos (toliau – per pirmąjį svarstymą priimta rezoliucija) [5]. EDAPP teigiamai įvertino keletą EP pakeitimų, kuriuos EP priėmė išnagrinėjęs pirmiau nurodytą EDAPP nuomonę ir pastabas. Vienas iš svarbių pakeitimų – pareigos pranešti apie saugumo pažeidimus taikymas ir informacinės visuomenės paslaugų teikėjams (*t. y.* internetu veikiančioms bendrovėms). EDAPP taip pat palankiai įvertino pakeitimą, kuriuo sudaromos sąlygos juridiniams ir fiziniams asmenims imtis teisinių veiksmų bet kurios E. privatumo

[1] E. privatumo direktyvos peržiūra – dalis didesnio peržiūros proceso, kuriuo siekiama sukurti ES telekomunikacijų instituciją, peržiūrėti Direktyvas 2002/21/EB, 2002/19/EB, 2002/20/EB, 2002/22/EB bei 2002/58/EB ir peržiūrėti Reglamentą (EB) Nr. 2006/2004 (visi toliau – telekomunikacijų reguliavimo paketo peržiūra).

[2] 2008 m. balandžio 10 d. nuomonė dėl pasiūlymo dėl Direktyvos, iš dalies keičiančios, be kita ko, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), OL C 181, 2008 7 18, p. 1.

[3] Direktyva 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (Universaliųjų paslaugų direktyva), OL L 108, 2002 4 24, p. 51.

[4] 2008 m. rugsėjo 2 d. EDAPP pastabos dėl tam tikrų klausimų, iškeltų Vidaus rinkos ir vartotojų apsaugos komiteto (IMCO) ataskaitoje dėl Direktyvos 2002/22/EB (Universaliosios paslaugos) ir Direktyvos 2002/58/EB (e. privatumas) peržiūros. Pateikiama adresu: www.edps.europa.eu

[5] 2008 m. rugsėjo 24 d. Europos Parlamento teisėkūros rezoliucija dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos, iš dalies keičiančios Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl bendradarbiavimo vartotojų apsaugos srityje (COM(2007) 698 – C6-0420/2007 – 2007/248(COD)).

direktyvos nuostatos pažeidimo atveju (ne tik nuostatų dėl nepageidaujamo e. laiškų siuntimo pažeidimo atveju, kaip siūlyta pradiniame Komisijos pasiūlyme). Parlamentui per pirmąjį svarstymą priėmus rezoliuciją Komisija priėmė iš dalies pakeistą pasiūlymą dėl E. privatumo direktyvos (toliau – iš dalies pakeistas pasiūlymas) ([6]).

5. 2008 m. lapkričio 27 d. Taryba pasiekė politinį susitarimą dėl telekomunikacijų reguliavimo paketo, įskaitant E. privatumo direktyvą, taisyklių peržiūros, kuris taps Tarybos bendrąja pozicija (toliau – bendroji pozicija) ([7]). Apie bendrąją poziciją bus pranešta EP pagal Europos bendrijos steigimo sutarties 251 straipsnio 2 dalį, o EP gali pateikti pasiūlymą dėl pakeitimų.

Bendra nuomonė apie Tarybos poziciją

6. Taryba pakeitė esminius pasiūlymo teksto aspektus ir nepritarė daugeliui EP priimtų pakeitimų. Bendrojoje pozicijoje, be abejo, yra teigiamų nuostatų, tačiau iš esmės EDAPP susirūpinimą kelia jos turinys, visų pirma dėl to, kad į bendrąją poziciją neįtraukti kai kurie teigiami EP pasiūlyti pakeitimai, iš dalies pakeisto pasiūlymo ar nuomonių, kurias pateikė EDAPP ir Europos duomenų apsaugos institucijos per 29 straipsnio darbo grupę ([8]), nuostatos.

7. Priešingai, nemažai vietų išbrauktos ar iš esmės susilpnintos iš dalies pakeisto pasiūlymo ir EP pakeitimų nuostatos, suteikiančios apsaugos priemonių piliečiams. Todėl bendrąja pozicija asmenims suteikiama apsauga yra labai sumažinama. Dėl šių priežasčių EDAPP dabar skelbia antrą nuomonę, tikėdamasis, kad teisėkūros procese nagrinėjant E. privatumo direktyvą bus priimta naujų pakeitimų, kurie atkurs duomenų apsaugos priemones.

8. Šioje antrojoje nuomonėje daugiausia dėmesio skiriama kai kuriems esminiams susirūpinimą keliantiems klausimams ir nekartojami visi EDAPP pirmojoje nuomonėje ar pastabose nurodyti klausimai, kurie visi tebėra aktualūs. Visų pirma šioje nuomonėje nagrinėjami šie klausimai:

— nuostatos dėl pranešimo apie saugumo pažeidimus;

— E. privatumo direktyvos taikymas privatiesiems ir viešai prieinamiems privatiesiems tinklams;

— srauto duomenų tvarkymas apsaugos tikslais;

— galimybė juridiniams asmenims imtis veiksmų E. privatumo direktyvos pažeidimų atveju.

9. Šioje nuomonėje nagrinėjant pirmiau nurodytus klausimus analizuojama Tarybos bendroji pozicija, ji taip pat lyginama su EP per pirmąjį svarstymą priimta rezoliucija ir Komisijos iš dalies pakeistu pasiūlymu. Nuomonėje pateikiama rekomendacijų, kuriomis siekiama supaprastinti E. privatumo direktyvos nuostatas ir užtikrinti, kad direktyva ir toliau tinkamai saugotų asmenų privatumą ir asmens duomenis.

II. NUOSTATOS DĖL PRANEŠIMO APIE SAUGUMO PAŽEIDIMUS

10. EDAPP pritaria tam, kad nustatyta pranešimo apie saugumo pažeidimus sistema, pagal kurią institucijoms ir asmenims bus pranešama apie atvejus, kai kilo pavojus jų asmens duomenims ([9]). Pranešimais apie saugumo pažeidimus galima padėti asmenims imtis būtinų priemonių, kad būtų sumažinta žala, kuri gali kilti dėl pavojaus duomenims. Be to, pareiga pranešti apie saugumo pažeidimus skatins bendroves gerinti duomenų saugumą ir didinti su asmens duomenimis, už kuriuos jos atsakingos, susijusią atskaitomybę.

11. Komisijos iš dalies pakeistas pasiūlymas, Europos Parlamento per pirmąjį svarstymą priimta rezoliucija ir Tarybos bendroji pozicija atspindi tris skirtingus požiūrius į nagrinėjamą pranešimo apie saugumo pažeidimus klausimą. Visi trys požiūriai turi teigiamų aspektų. Tačiau EDAPP mano, kad juos visus galima dar pagerinti, ir pataria atsižvelgti į toliau pateiktas rekomendacijas galutinai nustatant pranešimo apie saugumo pažeidimus sistemą.

([6]) Iš dalies pakeistas pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos, iš dalies keičiančios Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl bendradarbiavimo vartotojų apsaugos srityje, Briuselis, 2008 11 6, COM(2008) 723 galutinis.

([7]) Ji pateikiama viešoje Tarybos interneto svetainėje.

([8]) Nuomonė 2/2008 dėl Direktyvos 2002/58/EB dėl privatumo ir elektroninių ryšių (E. privatumo direktyva) peržiūros, kuri pateikiama 29 straipsnio darbo grupės interneto svetainėje.

([9]) Šioje nuomonėje vartojama frazė „kilo pavojus“ reiškia bet kokį asmens duomenų apsaugos pažeidimą, atsiradusį atsitiktinai arba neteisėtai sunaikinus, praradus, pakeitus, be leidimo atskleidus perduodamus, saugomus arba kitaip tvarkomus asmens duomenis arba su jais susipažinus.

12. Nagrinėjant tris pranešimo apie saugumo pažeidimus sistemas reikia apsvarstyti šiuos penkis pagrindinius klausimus: *i*) saugumo pažeidimo sąvokos apibrėžtis; *ii*) subjektai, kuriems taikoma pareiga pranešti (subjektai, kuriems taikoma pareiga); *iii*) standartas, kuriuo remiantis atsiranda pareiga pranešti; *iv*) subjekto, kuris turi nustatyti, ar saugumo pažeidimas atitinka standartą, nustatymas ir *v*) pranešimo gavėjai.

Komisijos, Tarybos ir EP požiūrių apžvalga

13. Europos Parlamentas, Komisija ir Taryba laikosi skirtingų požiūrių į pranešimo apie saugumo pažeidimus sistemą. Per pirmąjį svarstymą priimtoje EP rezoliucijoje pakeista pradinė Komisijos pasiūlyme nustatyta pranešimo apie saugumo pažeidimus sistema ([10]). EP laikosi požiūrio, kad pareiga pranešti taikoma ne tik viešųjų elektroninių ryšių paslaugų teikėjams, bet ir informacinės visuomenės paslaugų teikėjams (toliau – PPECS ir ISSP). Be to, laikantis šio požiūrio, apie visus asmens duomenų apsaugos pažeidimus turėtų būti pranešama nacionalinei reguliavimo institucijai arba kompetentingoms institucijoms (visos toliau – institucijos). Institucijos, nustačiusios, kad pažeidimas yra *rimtas*, reikalautų, kad PPECS ir ISSP nedelsdami apie tai praneštų su pažeidimu susijusiam asmeniui. Pažeidimų, kurie kelia neišvengiamą ir tiesioginį pavojų, atveju PPECS ir ISSP apie juos praneštų asmenims prieš informuodami institucijas ir nelauktų oficialaus įvertinimo. Pareigos pranešti vartotojams išimtis taikoma subjektams, kurie gali įrodyti institucijoms, kad „*taikomos tokios technologinės apsaugos priemonės*“, kuriomis užtikrinama, kad duomenų negali perskaityti nė vienas leidimo neturintis asmuo.

14. Taryba taip pat laikosi požiūrio, kad pranešti apie saugumo pažeidimus reikia tiek abonentams, tiek institucijoms, tačiau tik tais atvejais, kai, *subjekto, kuriam taikoma pareiga*, nuomone, pažeidimas kelia *rimtą pavojų* abonento privatumui (*t. y*. tapatybės vagystės ar su tapatybe susijusio sukčiavimo, fizinės žalos, didelio pažeminimo ar žalos reputacijai atvejais).

15. Komisijos iš dalies pakeistame pasiūlyme palikta EP numatyta pareiga pranešti institucijoms apie visus pažeidimus. Tačiau, priešingai nei EP požiūryje, į iš dalies pakeistą pasiūlymą įtraukta reikalavimo pranešti išimtis, susijusi su atitinkamais asmenimis tais atvejais, kai PPEC įrodo kompetentingai institucijai, kad i) „*nėra pagrindo manyti*“, jog dėl pažeidimo bus padaryta žala (*pvz*., ekonominiai nuostoliai, socialinė žala ar tapatybės vagystė), arba *ii*) su pažeidimu susijusiems duomenims buvo taikomos „*tinkamos technologinės apsaugos priemonės*“. Taigi Komisijos požiūris apima analizę, pagrįstą su atskirais pranešimais susijusia žala.

([10]) Su šiuo klausimu susiję visų pirma EP 187, 124–127, 27, 21 ir 32 pakeitimai.

16. Svarbu pažymėti, kad remiantis EP ([11]) ir Komisijos požiūriais *institucijos* galiausiai turi nustatyti, ar pažeidimas yra rimtas arba ar yra pagrindo manyti, kad bus padaryta žala. O remiantis Tarybos požiūriu sprendimą priima *atitinkami subjektai*.

17. Tiek Tarybos, tiek Komisijos požiūris taikomas tik PPECS, o ne, priešingai nei EP požiūris, ISSP.

Saugumo pažeidimo sąvokos apibrėžtis

18. EDAPP palankiai vertina tai, kad trijuose pasiūlymuose dėl teisės akto pateikiama ta pati pranešimo apie saugumo pažeidimus sąvokos apibrėžtis: „*saugumo pažeidimas, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami asmens duomenys arba atsiranda galimybė naudotis tais duomenimis, kai jie buvo perduodami, saugomi arba kitaip tvarkomi […]*“ ([12]).

19. Kaip nurodyta toliau, ši sąvokos apibrėžtis vertinama palankiai, kadangi ji pakankamai plati ir apima daugumą svarbių situacijų, kai reikėtų pranešti apie saugumo pažeidimus.

20. Pirma, į sąvoką įtraukti atvejai, kai trečioji šalis *be leidimo pasinaudojo* asmens duomenimis, pvz., įsilaužimas į serverį, kuriame laikomi asmens duomenys, ir tokios informacijos gavimas.

21. Antra, ši sąvoka taip pat apimtų situacijas, kai asmens duomenys prarasti ar atskleisti, tačiau dar reikia įrodyti, kad jais pasinaudota be leidimo. Tai apimtų tokias situacijas, kai asmens duomenys galėjo būti prarasti (pvz., naudojant pastoviosios atminties kompaktinius diskus, USB atmintines ar kitus nešiojamus prietaisus) arba viešai prieinami paprastiems paslaugų gavėjams (darbuotojų duomenų rinkmena netyčia ir laikinai viešai prieinama internete). Dažnai neturima duomenų, įrodančių, kad su tokiais duomenimis kažkuriuo metu galėjo susipažinti arba pasinaudoti leidimo tam neturinčios trečiosios šalys, todėl atrodo tikslinga šiuos atvejus įtraukti į sąvokos apibrėžtį. Todėl EDAPP siūlo palikti šią sąvokos apibrėžtį. EDAPP taip pat rekomenduoja saugumo pažeidimo sąvokos apibrėžtį įtraukti į E. privatumo direktyvos 2 straipsnį, kadangi tai labiau atitiktų bendrą direktyvos struktūrą ir suteiktų daugiau aiškumo.

([11]) Išskyrus neišvengiamo ir tiesioginio pavojaus atvejus, kai subjektai, kuriems taikoma pareiga, pirmiausia privalo pranešti vartotojams.

([12]) Bendrosios pozicijos ir iš dalies pakeisto pasiūlymo 2 straipsnio i punktas ir per pirmąjį svarstymą priimtos EP rezoliucijos 3 straipsnio 3 dalis.

Subjektai, kuriems turėtų būti taikoma pareiga pranešti

22. Pagal EP požiūrį pareiga pranešti taikoma ir PPECS, ir ISSP. Tačiau remiantis Tarybos ir Komisijos pasiūlymais tik PPECS, pvz., telekomunikacijų bendrovės ir interneto paslaugų teikėjai, privalės pranešti asmenims apie atvejus, kai padaromi saugumo pažeidimai, dėl kurių kyla pavojus asmens duomenims. Ši pareiga neprivaloma kitų veiklos sektorių subjektams, pavyzdžiui, internetiniams bankams, internetiniams mažmeniniams prekybininkams, internetiniams sveikatos paslaugų teikėjams ir kitiems. Dėl toliau nurodytų priežasčių EDAPP mano, kad atsižvelgiant į viešosios politikos aspektą labai svarbu užtikrinti, kad informacinės visuomenės paslaugų teikėjams, įskaitant internetines įmones, internetinius bankus, internetinius sveikatos paslaugų teikėjus ir t. t., taip pat būtų taikomas reikalavimas pranešti.

23. Pirma, EDAPP pažymi, kad saugumo pažeidimais, apie kuriuos reikia pranešti, be abejo, taikomasi ne tik į telekomunikacijų bendroves, bet ir kitų tipų bendroves/paslaugų teikėjus. Internetiniai mažmeniniai prekybininkai, internetiniai bankai ir internetinės vaistinės, taip pat kaip ir telekomunikacijų bendrovės, net ir labiau, gali nukentėti dėl saugumo pažeidimų. Todėl dėl pavojaus neverta pranešimo apie pažeidimus reikalavimo taikyti tik PPECS. Poreikį laikytis platesnio požiūrio įrodo kitų šalių patirtis. Pavyzdžiui, Jungtinėse Valstijose beveik visose valstijose (šiuo metu daugiau negu 40) galioja įstatymai dėl pranešimo apie saugumo pažeidimus, kurių taikymo sritis yra platesnė, apimanti ne tik PPECS, bet ir visus subjektus, laikančius atitinkamus asmens duomenis.

24. Antra, nors asmens duomenų, kuriuos paprastai tvarko PPECS, pažeidimas, aišku, gali turėti įtakos asmens privatumui, tai taip pat, gal net labiau, aktualu ir ISSP tvarkomai asmeninei informacijai. Akivaizdu, kad bankai ir kitos finansų įstaigos gali turėti labai konfidencialios informacijos (*pvz.*, banko sąskaitos duomenys), kurią atskleidus galėtų būti sudarytos sąlygos ja pasinaudoti tapatybės vagystės tikslais. Panašiai, internetiniams sveikatos paslaugų teikėjams atskleidus neskelbtiną su sveikata susijusią informaciją gali būti padaryta daug žalos asmenims. Todėl dėl tam tikrų rūšių asmens duomenų, kuriems gali kilti pavojus, reikia plačiau taikyti reikalavimą pranešti apie saugumo pažeidimus, įtraukiant bent ISSP.

25. Buvo iškelta keletas teisinių argumentų prieš šio straipsnio taikymo srities (*t. y.* subjektai, kuriems taikomas šis reikalavimas) išplėtimą. Visų pirma kaip viena iš kliūčių pareigą pranešti taikyti ir ISSP buvo nurodyta tai, kad E. privatumo direktyva iš esmės taikoma tik PPECS.

26. Atsižvelgdamas į šiuos argumentus, EDAPP norėtų priminti, kad: *i)* nėra jokių teisinių kliūčių tam tikras direktyvos nuostatas taikyti ir kitiems subjektams, ne tik PPECS. Bendrijos teisės aktų leidėjas šiuo klausimu turi visišką kompetenciją; *ii)* yra kitų precedentų, kai galiojanti E. privatumo direktyva taikoma kitiems, ne tik PPECS, subjektams.

27. Pavyzdžiui, 13 straipsnis taikomas ne tik PPECS, bet ir bet kuriai neužsakytus pranešimus siunčiančiai bendrovei, reikalaujant išankstinio abonentų sutikimo. Be to, E. privatumo direktyvos 5 straipsnio 3 dalis, kurioje draudžiama, *inter alia*, saugoti informaciją, pavyzdžiui, slapukus, paslaugos gavėjo galiniame įrenginyje, yra privaloma ne tik PPECS, bet visiems, kurie bando saugoti informaciją asmenų galiniuose įrenginiuose arba ja pasinaudoti. Be to, šio teisėkūros proceso metu Komisija net pasiūlė 5 straipsnio 3 dalį taikyti ir tais atvejais, kai panašios technologijos (slapukai/šnipinėjimo programos) yra įdiegiamos ne tik per elektroninių ryšių sistemas, bet ir kitais galimais metodais (atsisiuntus iš interneto ar per išorines duomenų saugojimo laikmenas, pavyzdžiui, pastoviosios atminties kompaktinius diskus, USB raktus, didelės atminties diskus ir t. t.). Visi šie aspektai yra sveikintini ir turėtų būti išlaikyti, taip pat jie turėtų būti laikomi tinkamais precedentais dabartinėse diskusijose dėl taikymo srities.

28. Dabartinio teisėkūros proceso metu Komisija, EP ir, be abejo, Taryba pasiūlė naują toliau nagrinėjamą 6 straipsnio 6 dalies a punktą, kuris taikomas ne PPECS, bet kitiems subjektams.

29. Galiausiai atsižvelgiant į visapusiškus su pareiga pranešti apie saugumo pažeidimus susijusius privalumus labai tikėtina, kad piliečiai tikėsis šių privalumų ne tik tais atvejais, kai jų asmens duomenims kilo pavojus dėl PPECS, bet ir dėl ISSP. Piliečių lūkesčiai gali likti nepatenkinti, jeigu, pavyzdžiui, jiems nepranešama, kad internetinis bankas prarado jų banko sąskaitos informaciją.

30. Apskritai EDAPP yra įsitikinęs, kad visais pranešimo apie saugumo pažeidimus sistemos privalumais bus galima geriau pasinaudoti tik šią pareigą taikant ir PPECS, ir ISSP.

Standartas, kuriuo remiantis atsiranda pareiga pranešti

31. Priežasties, dėl kurios atsiranda pareiga pranešti, klausimu, kaip nurodyta toliau, EDAPP mano, kad iš dalies pakeistame pasiūlyme nurodytas standartas *„yra pagrindo manyti, kad bus padaryta žala“* yra tinkamiausias iš visų trijų siūlomų standartų. Tačiau svarbu užtikrinti, kad „žalos“ sąvoka būtų pakankamai plati ir apimtų visus atitinkamus neigiamo poveikio privatumui ar kitiems teisėtiems asmenų interesams atvejus. Priešingu atveju būtų pageidautina sukurti naują standartą, pagal kurį pranešti būtų privaloma tais atvejais, *„jeigu yra pagrindo manyti, kad pažeidimas turės neigiamą poveikį asmenims“*.

32. Kaip nurodyta ankstesniame skirsnyje, EP, Komisijos ir Tarybos požiūriai į sąlygas, kuriomis remiantis privaloma pranešti asmenims („priežastis“ arba „standartas“), skiriasi. Akivaizdu, kad pranešimų, kuriuos gaus asmenys, skaičius didžiąja dalimi priklausys nuo pranešimui nustatytos priežasties ar standarto.

33. Pagal Tarybos ir Komisijos sistemas pranešti reikia, jeigu pažeidimas yra *„rimtas abonento privatumo pažeidimas“* (Taryba) ir jeigu *„yra pagrindo manyti, kad dėl pažeidimo vartotojo interesams bus padaryta žala“* (Komisija). Pagal EP sistemą priežastis, dėl kurios atsiranda pareiga pranešti asmenims, yra *„pažeidimo rimtumas“* (*t. y.* asmenims pranešti reikia, jeigu pažeidimas laikomas *„rimtu“*). Pranešti nereikia, jeigu pažeidimas mažesnis ([13]).

34. EDAPP suvokia, kad jeigu asmens duomenims kilo pavojus, galima teigti, kad asmenys, kuriems tie duomenys priklauso, turi teisę visada sužinoti apie tokius atvejus. Tačiau tikslinga apsvarstyti, ar tai yra tinkamas sprendimas atsižvelgiant į kitus interesus ir klausimus.

35. Buvo pasiūlyta, kad pareiga pranešti visais atvejais, kai asmens duomenims kilo pavojus, arba, kitaip tariant, be jokių apribojimų, gali lemti pernelyg didelį pranešimų skaičių ir „nuovargį dėl pranešimų“, kuris sumažintų budrumą. Kaip nurodyta toliau, EDAPP atsižvelgia į šį argumentą, tačiau tuo pat metu nori pabrėžti savo susirūpinimą, kad pernelyg didelis pranešimų skaičius galėtų būti apskritai prastai taikomos informacijos saugumo tvarkos rodiklis.

([13]) Žr. 11 išnašą dėl šios taisyklės išimties.

36. Kaip nurodyta pirmiau, EDAPP suvokia galimas neigiamas pernelyg didelio pranešimų skaičiaus pasekmes ir norėtų padėti užtikrinti, kad priimta pranešimo apie saugumo pažeidimus teisinė sistema to nesukeltų. Jeigu asmenys dažnai gautų pranešimus apie pažeidimus net ir tais atvejais, kai nebuvo padaryta neigiamo poveikio, žalos ar nekilo pavojus, gali kilti grėsmė vienam iš pagrindinių pranešimų teikimo tikslų, nes asmenys, nors ir paradoksalu, gali ignoruoti pranešimus tais atvejais, kai iš tiesų jiems reikėtų imtis priemonių apsisaugoti. Todėl svarbu pasiekti teisingą pusiausvyrą teikiant reikšmingus pranešimus, nes asmenims nereaguojant į gaunamus pranešimus pranešimo sistemų veiksmingumas labai sumažėja.

37. Siekiant priimti tinkamą standartą, kuris nelemtų pernelyg didelio pranešimų skaičiaus, reikia apsvarstyti ne tik pranešimo priežastį, bet ir kitus veiksnius, visų pirma saugumo pažeidimo sąvokos apibrėžtį ir informaciją, dėl kurios taikoma pareiga pranešti. Šiuo klausimu EDAPP pažymi, kad pagal tris pasiūlytus požiūrius pranešimų skaičius gali būti didelis dėl plačios pirmiau išnagrinėtos saugumo pažeidimo sąvokos apibrėžties. Šį susirūpinimą keliantį klausimą dėl pernelyg didelio pranešimų skaičiaus paryškina ir tai, kad saugumo pažeidimo sąvokos apibrėžtis apima visų rūšių asmens duomenis. Nors, EDAPP nuomone, tai teisingas požiūris (nenustatyti apribojimų asmens duomenų rūšims, dėl kurių taikoma pareiga pranešti) lyginant su kitais požiūriais, pvz., JAV įstatymais, kurių reikalavimuose daugiausia dėmesio yra skiriama informacijos skelbtinumui, vis dėlto reikia atsižvelgti į šį veiksnį.

38. Atsižvelgdamas į visa tai ir į visus skirtingus apsvarstytus kintamuosius, EDAPP mano, kad tikslinga numatyti ribą ar standartą, kai pranešti neprivaloma.

39. Panašu, kad abu siūlomi standartai, *t. y.* pažeidimas, kuris kelia „rimtą *pavojų privatumui*“ arba dėl kurio *„yra pagrindo manyti, kad bus padaryta žala“*, apima, pavyzdžiui, socialinę žalą ar žalą reputacijai ir ekonominius nuostolius. Pavyzdžiui, šie standartai apimtų atvejus, kai sudaromos sąlygos tapatybės vagystei atskleidžiant neviešus identifikatorius, tokius kaip paso numeriai, ir sudaromos sąlygos gauti informacijos apie asmens privatų gyvenimą. EDAPP palankiai vertina šį požiūrį. Jis įsitikinęs, kad būtų pasinaudota ne visais pranešimo apie saugumo pažeidimus sistemos privalumais, jeigu ji būtų taikoma tik ekonominę žalą darantiems pažeidimams.

40. Iš dviejų pasiūlytų standartų EDAPP pirmenybę teikia Komisijos standartui *„yra pagrindo manyti, kad bus padaryta žala“*, nes juo būtų užtikrinta tinkamesnio lygio asmenų apsauga. Labiau tikėtina, kad dėl pažeidimų bus taikomas reikalavimas pranešti, jeigu *„yra pagrindo manyti, kad bus padaryta žala“* asmenų privatumui, negu kai jie kelia *„rimtą“* tokios žalos *„pavojų“*. Todėl reikalavimą taikant tik pažeidimų, kurie kelia rimtą pavojų asmenų privatumui, atveju žymiai sumažėtų pažeidimų, apie kuriuos turi būti pranešta, skaičius. Reikalavimo pranešti taikymas tik tokiems pažeidimams suteiktų pernelyg didelę veiksmų laisvę PPECS ir ISSP sprendžiant, ar reikia pranešti, nes jiems būtų daug lengviau pagrįsti išvadą, kad nėra *„rimto“* žalos *„pavojaus“*, negu kad *„nėra pagrindo manyti, kad nebus padaryta“* žala. Nors, žinoma, reikia vengti pernelyg didelio pranešimų skaičiaus, apkritai būtina apsaugoti asmenų privatumo interesus, o asmenys turėtų būti apsaugoti bent tais atvejais, kai yra pagrindo manyti, kad pažeidimas jiems gali padaryti žalos. Be to, sąvoka *„yra pagrindo manyti“* bus veiksmingesnė praktiškai tiek subjektų, kuriems taikoma ši pareiga, tiek kompetentingų institucijų atžvilgiu, nes reikia objektyviai įvertinti kiekvieną atvejį ir bendras jo aplinkybes.

41. Be to, asmens duomenų apsaugos pažeidimai gali padaryti žalos, kurią sunku įvertinti ir kuri gali būti skirtinga. Iš tiesų, tos pačios rūšies duomenų atskleidimas, priklausomai nuo asmeninių aplinkybių, gali padaryti didelę žalą vienam asmeniui ir mažesnę kitam. Standartas, kuris reikalautų, kad žala būtų materialinė, svarbi arba rimta, būtų netinkamas. Pavyzdžiui, Tarybos požiūris, kuriame reikalaujama, kad pažeidimas turėtų *rimtos* įtakos asmens privatumui, suteiktų netinkamą asmenų apsaugą, nes tokiu standartu reikalaujama, kad poveikis privatumui būtų „rimtas“. Be to, taip sudaromos sąlygos subjektyviam vertinimui.

42. Kaip nurodyta pirmiau, atrodytų, kad kriterijus *„yra pagrindo manyti, kad bus padaryta žala“* yra tinkamas pranešimui apie saugumo pažeidimus taikytinas standartas, tačiau EDAPP vis dar kelia susirūpinimą tai, kad jis gali apimti ne visas situacijas, kai asmenims reikia pranešti, *t. y.* ne visas situacijas, kai yra pagrindo manyti, kad padaryta neigiamos įtakos asmenų privatumui ar kitoms teisėtoms teisėms. Dėl šios priežasties būtų galima apsvarstyti standartą, pagal kurį būtų reikalaujama pranešti, *„jeigu yra pagrindo manyti, kad bus padaryta neigiamos įtakos asmenims“*.

43. Šis alternatyvus standartas, be kita ko, atitiktų ES duomenų apsaugos teisės aktus. Duomenų apsaugos direktyvoje dažnai daroma nuoroda į neigiamą įtaką duomenų subjektų teisėms ir laisvėms. Pavyzdžiui, pagal 18 straipsnį ir 49 konstatuojamąją dalį, kuriuose nurodyta pareiga pranešti duomenų apsaugos institucijoms apie duomenų tvarkymo operacijas, valstybėms narėms leidžiama taikyti šios pareigos išimtis tais atvejais, kai tvarkant duomenis *„galėtų būti pakenkta duomenų subjektų teisėms ir laisvėms“*. Panaši formuluotė vartojama bendrosios pozicijos 16 straipsnio 6 dalyje, kad juridiniai asmenys galėtų imtis teisinių veiksmų prieš nepageidaujamų e. laiškų siuntėjus.

44. Be to, atsižvelgiant į tai, kas nurodyta pirmiau, taip pat tikėtina, kad subjektai, kuriems taikoma ši pareiga, ir visų pirma institucijos, kurių kompetencijai priklauso užtikrinti duomenų apsaugos teisės aktų vykdymą, būtų geriau susipažinę su pirmiau nurodytu standartu ir jiems būtų lengviau vertinti, ar tam tikras pažeidimas atitinka privalomą standartą.

Subjektas, kuris turi nustatyti, ar saugumo pažeidimas atitinka standartą

45. Pagal EP požiūrį (išskyrus neišvengiamo pavojaus atvejus) ir Komisijos iš dalies pakeistą pasiūlymą valstybių narių institucijos priima sprendimą, ar saugumo pažeidimas atitinka standartą, kuriuo remiantis atsiranda pareiga pranešti atitinkamiems asmenims.

46. EDAPP nuomone, institucijos dalyvavimas vaidina svarbų vaidmenį nustatant atitiktį standartui, nes ji tam tikru mastu užtikrina teisingą teisės taikymą. Tokia sistema gali užkirsti kelią bendrovėms netinkamai įvertinti, kad pažeidimas nedaro žalos ar nėra rimtas, ir taip išvengti pareigos pranešti, kai iš tiesų toks pranešimas būtinas.

47. Kita vertus, EDAPP yra susirūpinęs dėl to, kad tvarką, pagal kurią institucijos turi atlikti įvertinimą, gali būti praktiškai sunku taikyti arba gali paaiškėti, kad praktiškai ji neveiksminga. Taip galėtų net sumažėti duomenų apsaugos priemonių poveikis asmenims.

48. Remiantis tokiu požiūriu tikėtina, kad duomenų apsaugos institucijos gaus labai daug pranešimų apie saugumo pažeidimus ir gali patirti rimtų sunkumų atlikdamos būtinus įvertinimus. Svarbu prisiminti, kad vertindamos, ar pažeidimas atitinka standartą, institucijos turės gauti pakankamai viešai neatskleistos informacijos, kuri dažnai bus techniškai sudėtinga ir kurią jos turės tvarkyti labai greitai. Atsižvelgdamas į vertinimo sudėtingumą ir į tai, kad kai kurios institucijos turi ribotus išteklius, EDAPP būgštauja, kad institucijoms bus labai sunku vykdyti šią pareigą ir kad joms gali tekti pasitelkti kitiems svarbiems prioritetams skirtus išteklius. Be to, tokia sistema institucijoms gali daryti netinkamą spaudimą: jeigu jos nuspręstų, kad pažeidimas nėra rimtas, o asmenims vis tiek būtų padaryta žala, institucijos galėtų būti patrauktos atsakomybėn.

49. Pirmiau nurodytą sunkumą dar pabrėžia ir tai, kad laikas yra vienas iš pagrindinių veiksnių mažinant dėl saugumo pažeidimų atsirandantį pavojų. Išskyrus tuos atvejus, kai institucijos gali atlikti vertinimus per labai trumpą laiką, dėl papildomo laiko, kurio institucijoms reikia atlikti tokius vertinimus, gali padidėti žala, kurią patiria atitinkami asmenys. Todėl ši papildoma priemonė, kuria siekiama numatyti didesnę asmenų apsaugą, gali paradoksaliai suteikti mažesnę apsaugą nei tiesioginiu pranešimu pagrįstos sistemos.

50. Dėl pirmiau nurodytų priežasčių EDAPP mano, kad pageidautina nustatyti sistemą, pagal kurią atitinkami subjektai turėtų vertinti, ar pažeidimas atitinka standartą, kaip numatyta Tarybos požiūryje.

51. Tačiau siekiant išvengti galimo piktnaudžiavimo rizikos, pavyzdžiui, atvejų, kai subjektai atsisako pranešti susidarius tokioms aplinkybėms, kai pranešti aiškiai būtina, labai svarbu įtraukti toliau nurodytas tam tikras duomenų apsaugos priemones.

52. Pirma, subjektams, kuriems taikoma pareiga nustatyti, ar jie privalo pranešti, žinoma, taip pat turi būti taikoma privaloma pareiga pranešti institucijoms apie visus pažeidimus, kurie atitinka reikalaujamą standartą. Tais atvejais iš atitinkamų subjektų turėtų būti reikalaujama informuoti institucijas apie pažeidimą, pažeidimo nustatymo priežastis ir pateikto pranešimo turinį.

53. Antra, institucijoms turi būti patikėta faktinės priežiūros funkcija. Šiai funkcijai atlikti institucijoms turi būti sudarytos sąlygos, tačiau jų tam neįpareigojant, tirti pažeidimo aplinkybes ir reikalauti, kad būtų imtasi tinkamų veiksmų padėčiai ištaisyti ([14]). Tai turėtų apimti ne tik pranešimą asmenims (jeigu tai dar nepadaryta), bet ir teisę nustatyti pareigą imtis veiksmų siekiant užkirsti kelią tolesniems pažeidimams. Šiuo atžvilgiu institucijoms turėtų būti suteikti veiksmingi įgaliojimai bei ištekliai ir suteikta būtina veiksmų laisvė spręsti, kada imtis veiksmų dėl pranešimo apie saugumo pažeidimą. Kitaip tariant, tai sudarytų sąlygas institucijoms veikti selektyviai ir vykdyti, pavyzdžiui, didelių ir tikrai daug žalos padariusių saugumo pažeidimų tyrimus tikrinant, kaip laikomasi teisės reikalavimų, ir užtikrinant jų vykdymą.

54. Siekiant pirmiau išdėstytų tikslų, EDAPP rekomenduoja ne tik suteikti E. privatumo direktyvoje, pavyzdžiui, 15a straipsnio 3 dalyje, ir Duomenų apsaugos direktyvoje pripažintus įgaliojimus, bet ir įtraukti šį sakinį: *„jeigu abonentui ar atitinkamam asmeniui dar nepranešta, kompetentinga nacionalinė institucija, išnagrinėjusi pažeidimo pobūdį, gali pareikalauti, kad PPECS arba ISSP tai padarytų.“*

55. Be to, EDAPP rekomenduoja EP ir Tarybai patvirtinti EP pasiūlytą subjektų pareigą (122 pakeitimas, 4 straipsnio 1 dalies a punktas) atlikti rizikos vertinimą ir nustatyti sistemas bei asmens duomenis, kuriuos ketinama tvarkyti. Remdamiesi šia pareiga, subjektai parengs pritaikytą ir tikslią saugumo priemonių, kurios bus jiems taikomos ir kuriomis galėtų naudotis institucijos, sąvokos apibrėžtį. Saugumo pažeidimo atveju ši pareiga padės subjektams, kuriems taikoma ši pareiga, ir galiausiai priežiūros funkciją vykdančioms institucijoms nustatyti, ar tokiai informacijai kilęs pavojus gali turėti neigiamo poveikio ar žalos asmenims.

56. Trečia, subjektams, kuriems taikoma pareiga nustatyti, ar jie privalo pranešti asmenims, taip pat turi būti taikoma pareiga tiksliai ir išsamiai registruoti vidaus audito istoriją apibūdinant visus padarytus pažeidimus ir pranešimus apie juos bei priemones, kurių imtasi siekiant išvengti pažeidimų ateityje. Institucijos vykdydamos peržiūrą ir galimus tyrimus turi turėti galimybę pasinaudoti šia vidaus audito istorija. Tai sudarys sąlygas institucijoms vykdyti priežiūros funkciją. Tai būtų galima pasiekti vartojant tokią formuluotę: *„PPECS ir ISSP renka bei saugo išsamius duomenis apie visus padarytus saugumo pažeidimus, su jais susijusią atitinkamą techninę informaciją ir veiksmus, kurių imtasi padėčiai ištaisyti. Šiuose įrašuose taip pat daroma nuoroda į visus abonentams ar atitinkamiems asmenims ir kompetentingoms nacionalinėms institucijoms pateiktus pranešimus, įskaitant jų datą ir turinį. Šie įrašai pateikiami kompetentingai nacionalinei institucijai, jai pateikus prašymą.“*

57. Žinoma, kad būtų užtikrintas nuoseklumas įgyvendinant šį standartą ir kitus atitinkamus pranešimo apie saugumo pažeidimus sistemos aspektus, tokius kaip pranešimo formatas ir procedūros, būtų tikslinga, kad Komisija, pasikonsultavusi su EDAPP, 29 straipsnio darbo grupe ir atitinkamais suinteresuotaisiais subjektais, priimtų techninės įgyvendinamąsias priemones.

([14]) 15a straipsnio 3 dalyje pripažįstami šie priežiūros įgaliojimai nustatant, kad *„valstybės narės užtikrina, kad kompetentingos nacionalinės institucijos ir, kai tinka, kitos nacionalinės įstaigos turėtų visus įgaliojimus ir išteklių tyrimui atlikti, įskaitant galimybę gauti visą reikiamą informaciją, būtinus pagal šią direktyvą priimtų nacionalinių nuostatų vykdymui stebėti ir užtikrinti.“*

Pranešimo gavėjai

58. EDAPP pirmenybę teikia EP ir Komisijos, o ne Tarybos, nuostatų dėl pranešimų gavėjų formuluotei. EP pakeitė žodį „abonentai“ į žodį „paslaugų gavėjai“. Komisija vartoja terminus „abonentai“ ir „atitinkami asmenys“. Tiek EP, tiek Komisijos vartojamos formuluotės dėl pranešimų gavėjų apimtų ne tik dabartinius abonentus, bet ir buvusius abonentus bei trečiąsias šalis, pavyzdžiui, paslaugų gavėjus, kurie turi ryšių su kai kuriais subjektais, kuriems taikoma pareiga pranešti, bet nėra užsisakę jų paslaugų. EDAPP palankiai vertina šį požiūrį ir ragina EP bei Tarybą jam pritarti.

59. Tačiau EDAPP atkreipia dėmesį į keletą netikslumų, susijusių su rezoliucijoje, EP priimtoje per pirmąjį svarstymą, vartojamomis formuluotėmis, kurie turėtų būti ištaisyti. Pavyzdžiui, daugeliu, tačiau ne visais atvejais žodis „abonentai“ buvo pakeistas į žodį „paslaugų gavėjai“; kai kur jis pakeistas į žodį „vartotojai“. Tai turėtų būti suderinta.

III. **E. PRIVATUMO DIREKTYVOS TAIKYMO SRITIS. VIEŠIEJI IR PRIVATIEJI TINKLAI**

60. Šiuo metu galiojančios E. privatumo direktyvos 3 straipsnio 1 dalyje nustatyti subjektai, kuriems visų pirma aktuali ši direktyva, t. y. subjektai, kurie tvarko duomenis teikdami viešai prieinamas elektroninių ryšių paslaugas viešaisiais ryšių tinklais (pirmiau – PPECS) ([15]). PPECS veiklos pavyzdžiai – prieigos prie interneto suteikimas, informacijos perdavimas elektroniniais tinklais, judriojo ir telefono ryšio jungtys ir t. t.

61. EP priėmė 121 pakeitimą, iš dalies keičiantį pirminio Komisijos pasiūlymo 3 straipsnį, kuriuo išplečiama E. privatumo direktyvos taikymo sritis įtraukiant *„asmens duomenų tvarkymą, susijusį su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ir privačiaisiais ryšių tinklais ir viešai prieinamais privačiaisiais tinklais Bendrijoje, [...]“* (E. privatumo direktyvos 3 straipsnio 1 dalis). Deja, Tarybai ir Komisijai šis pakeitimas pasirodė nepriimtinas ir todėl jis nebuvo įtrauktas į bendrąją poziciją ir į iš dalies pakeistą pasiūlymą.

E. privatumo direktyvos taikymas viešai prieinamiems privatiesiems tinklams

62. Dėl toliau pateiktų priežasčių ir siekdamas susitarimo, EDAPP ragina išlaikyti 121 pakeitimo esmę. Be to, EDAPP siūlo įtraukti pakeitimą, kad būtų lengviau išaiškinti, kokių rūšių paslaugos patektų į išplėstą taikymo sritį.

63. Privačiaisiais tinklais dažnai naudojamasi teikiant elektroninių ryšių paslaugas, pavyzdžiui, prieigą prie interneto, neapibrėžtam žmonių skaičiui, kuris gali būti didelis. Taip yra, pavyzdžiui, interneto prieigos interneto kavinėse atveju, taip pat belaidžio interneto ryšio vietose viešbučiuose, restoranuose, oro uostuose, traukiniuose ir kitose viešosiose įstaigose, kur tokios paslaugos neretai suteikiamos papildant kitas paslaugas (pavyzdžiui, gėrimų pardavimą, apgyvendinimą ir t. t.).

64. Visais pirmiau nurodytais atvejais ryšių paslauga, pavyzdžiui, prieiga prie interneto, suteikiama visuomenei ne viešuoju tinklu, o veikiau tinklu, kuris gali būtų laikomas privačiuoju, t. y. privačiai tvarkomu tinklu. Be to, pirmiau nurodytais atvejais ryšių paslauga yra teikiama visuomenei, tačiau naudojamasi veikiau privačiuoju, o ne viešuoju tinklu, todėl šių paslaugų teikimui *tikriausiai* nėra taikoma visa E. privatumo direktyva arba kai kurie jos straipsniai ([16]). Todėl pagrindinės asmenų teisės, kurias užtikrina E. privatumo direktyva, šiais atvejais nėra apsaugotos, o paslaugos gavėjai, kuriems tos pačios interneto prieigos paslaugos suteikiamos viešosiomis telekomunikacijų priemonėmis, atsiduria nelygiavertėje teisinėje padėtyje palyginti su gavėjais, gaunančiais paslaugas privačiosiomis priemonėmis. Tokia padėtis susidaro nepaisant to, kad visais šiais atvejais asmenų privatumui ir asmens duomenims kyla toks pat pavojus, kaip ir naudojantis viešaisiais tinklais paslaugai suteikti. Trumpai tariant, neatrodo, kad būtų loginio pagrindo pateisinti diferencijuotą požiūrį, pagal Direktyvą taikomą ryšių paslaugoms, suteiktoms privačiuoju tinklu, palyginti su paslaugomis, suteiktomis viešuoju tinklu.

65. Todėl EDAPP pritartų pakeitimui, pavyzdžiui, EP 121 pakeitimui, pagal kurį E. privatumo direktyva taip pat būtų taikoma asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu *privačiaisiais* ryšių tinklais.

66. Tačiau EDAPP pripažįsta, kad tokia formuluotė galėtų turėti nenumatytų pasekmių, kurių galbūt nebuvo ketinta siekti. Iš tikrųjų vien tik nuorodą į privačiuosius tinklus galima interpretuoti taip, kad direktyva bus taikoma tokiais atvejais, kuriais ją taikyti akivaizdžiai nenumatyta. Pavyzdžiui, galėtų būti teigiama, kad pažodžiui ar

([15]) *„Ši direktyva taikoma asmens duomenims tvarkyti teikiant Bendrijoje viešai prieinamas elektroninių ryšių paslaugas viešaisiais ryšių tinklais“.*

([16]) Kita vertus, galima įrodinėti, kad dėl to, kad ryšių paslauga teikiama visuomenei, net ir privačiuoju tinklu, tokių paslaugų teikimui taikoma galiojanti teisinė sistema, nepaisant to, kad tinklas yra privatus. Pavyzdžiui, Prancūzijos darbdaviai, suteikiantys prieigą prie interneto savo darbuotojams, laikomi lygiaverčiais tiems subjektams, kurie suteikia prieigą prie interneto komerciniu pagrindu. Šiai interpretacijai nėra plačiai pritariama.

griežtai laikantis šios formuluotės namų su įrengtu belaidžiu interneto ryšiu ([17]), prie kurio gali prisijungti visi jo juostoje (dažniausiai tai namai) esantys asmenys, savininkams galėtų būti taikoma ši direktyva, nors 121 pakeitimu to nėra siekiama. Kad būtų išvengta tokio rezultato, EDAPP siūlo performuluoti 121 pakeitimą į E. privatumo direktyvos taikymo sritį įtraukiant *„asmens duomenų tvarkymą, susijusį su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ar viešai prieinamais privačiaisiais tinklais Bendrijoje...“*

67. Tai padėtų išaiškinti, kad E. privatumo direktyva būtų taikoma tik tiems privatiesiems tinklams, kurie yra viešai prienami. Taikant E. privatumo direktyvos nuostatas *tik viešai prieinamiems privatiesiems tinklams* (o ne visiems privatiesiems tinklams), nustatoma riba, kurios laikantis direktyva bus taikoma tik ryšių paslaugoms, teikiamoms privačiaisiais tinklais, kurie yra viešai prieinami to specialiai siekiant. Šia formuluote bus taip pat pabrėžta, kad sprendžiant, ar taikytina direktyva, svarbiausias veiksnys (be to, kad teikiamos viešųjų elektroninių ryšių paslaugos) yra privačiojo tinklo *prieinamumas plačiosios visuomenės nariams*. Kitaip tariant, nepriklausomai nuo to, ar tinklas viešas ar privatus, jeigu tinklas yra viešai prieinamas to specialiai siekiant ir juo naudojamasi viešosioms ryšių paslaugoms, pavyzdžiui, prieigai prie interneto, teikti, tokios rūšies paslaugai/tinklui būtų taikoma E. privatumo direktyva, net jeigu tokia paslauga papildo kitas paslaugas (*pvz.*, apgyvendinimą viešbutyje).

68. EDAPP atkreipia dėmesį į tai, kad pirmesniais teiginiais grindžiamas požiūris, pagal kurį E. privatumo direktyvos nuostatos būtų taikomos *viešai prieinamiems privatiesiems tinklams*, atitinka požiūrį, kurio laikomasi keliose valstybėse narėse – jų valdžios institucijos jau dabar laiko, kad tokios rūšies paslaugoms, taip pat paslaugoms, kurios teikiamos išimtinai privačiais tinklais, taikytinos nacionalinės nuostatos, kuriomis įgyvendinama E. privatumo direktyva ([18]).

69. Kad teisinis tikrumas dėl subjektų, kurie patenka į naują taikymo sritį, būtų didesnis, gali būti naudinga į E. privatumo direktyvą įtraukti pakeitimą, kuriame būtų pateikta viešai prieinamų privačiųjų tinklų apibrėžtis ir kuris būtų suformuluotas taip: *„viešai prieinamas privatusis tinklas – privačiai tvarkomas tinklas, prie kurio prisijungti, už mokestį arba nemokamai ar teikiant kartu su kitomis paslaugomis ar pasiūlymais, plačiosios visuomenės nariai paprastai turi neribojamas galimybes su sąlyga, kad sutinka su taikomomis sąlygomis ir taisyklėmis“*.

([17]) Dažniausiai belaidžiai vietiniai tinklai (LAN).
([18]) Žr. 16 išnašą.

70. Praktiškai pirmiau pateiktas požiūris reikštų, kad direktyva taikoma privatiesiems tinklams viešbučiuose ir kitose įstaigose, kurios suteikia prieigą prie interneto plačiosios visuomenės nariams privačiuoju tinklu. Kita vertus, direktyva nebūtų taikoma ryšių paslaugų teikimui išimtinai privačiaisiais tinklais, kuriais teikiamos paslaugos ribotai asmenų, kuriuos galima nustatyti, grupei. Todėl, pavyzdžiui, direktyva nebūtų taikoma virtualiems privatiesiems tinklams ir vartotojų namams, kuriuose įrengtas belaidis interneto ryšys. Direktyva taip pat nebūtų taikoma paslaugoms, teikiamoms išimtinai bendrovių tinklams.

Privatieji tinklai, kuriems taikoma E. privatumo direktyva

71. Privačiųjų tinklų *per se* pašalinimas iš taikymo srities, kaip siūloma pirmiau, turėtų būti laikomas *laikina* priemone, kurią vėliau reikėtų aptarti. Iš tikrųjų, atsižvelgiant į tai, kokias pasekmes privatumui sukels išimtinai privačiųjų tinklų pašalinimas iš taikymo srities, ir kita vertus į tai, kad taip daromas poveikis daugeliui žmonų, kurie paprastai naudojasi internetu bendrovių tinklais, toks pasiūlymas ateityje galėtų būti persvarstytas. Todėl EDAPP, siekdamas paskatinti debatus šiuo klausimu, rekomenduoja į E. privatumo direktyvą įtraukti konstatuojamąją dalį, pagal kurią Komisija konsultuotųsi su visuomene dėl E. privatumo direktyvos taikymo visiems privatiesiems tinklams; be kita ko, turėtų būti konsultuojamasi su EDAPP, duomenų apsaugos institucijomis ir kitais susijusiais suinteresuotaisiais subjektais. Be to, konstatuojamojoje dalyje galėtų būti nurodyta, kad pasikonsultavusi su visuomene Komisija turėtų pateikti atitinkamą pasiūlymą, pagal kurį E. privatumo direktyva turėtų būti taikoma daugiau ar mažiau subjektų rūšių.

72. Be to, kas nurodyta pirmiau, atitinkamai turėtų būti pakeisti įvairūs E. privatumo direktyvos straipsniai, kad visos funkcinės nuostatos būtų aiškiai susijusios ne tik su viešaisiais, bet ir su viešai prieinamais privačiaisiais tinklais.

IV. SRAUTO DUOMENŲ TVARKYMAS SAUGUMO TIKSLAIS

73. Teisėkūros proceso, susijusio su E. privatumo direktyvos peržiūra, metu apsaugos paslaugas teikiančios bendrovės patikino, kad būtina į E. privatumo direktyvą įtraukti nuostatą, kuria būtų įteisintas srauto duomenų rinkimas siekiant užtikrinti veiksmingą internetinį saugumą.

74. Todėl EP įtraukė 181 pakeitimą, kuriuo buvo sukurta nauja 6 straipsnio 6a dalis, pagal kurią bus aiškiai leista tvarkyti srauto duomenis saugumo tikslais. „*Nepažeidžiant atitikimo nuostatoms, išskyrus Direktyvos 95/46/EB 7 straipsnio ir šios direktyvos 5 straipsnio nuostatas, srauto duomenys gali būti tvarkomi įgyvendinant teisėtus duomenų valdytojo interesus techninių priemonių įgyvendinimo tikslu, kad būtų užtikrintas tinklų ir informacijos saugumas, kaip nustatyta 2004 m. kovo 10 d. Europos Parlamento ir Tarybos Reglamento (EB) 460/2004, įsteigiančio Europos tinklų ir informacijos apsaugos agentūrą * , 4 straipsnio c dalyje, viešosios elektroninių ryšių paslaugos, viešojo arba privataus elektroninių ryšių tinklo, informacinės visuomenės paslaugos arba susijusio galinio ir elektroninių ryšių įrenginio saugumas, išskyrus tuos atvejus, kai svarbesni duomenų subjekto pagrindinių teisių ir laisvių užtikrinimo interesai. Toks tvarkymas apribojamas saugumo užtikrinimui būtinomis priemonėmis.*“

75. Iš principo šis pakeitimas buvo įtrauktas į iš dalies pakeistą Komisijos pasiūlymą, tačiau neįtraukiant sąlygos („*Nepažeidžiant [...] šios direktyvos...*“) buvo pašalinta labai svarbi sąlyga, kuri buvo skirta užtikrinti, kad būtų laikomasi kitų direktyvos nuostatų. Taryba priėmė performuluotą redakciją, kurioje buvo dar labiau sušvelnintos svarbios apsaugos priemonės ir siekiama didesnės interesų pusiausvyros nei 181 pakeitime: „*Srauto duomenys gali būti tvarkomi tik tada, kai reikia užtikrinti [...] tinklo ir informacijos saugumą, kaip apibrėžta 2004 m. kovo 10 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 460/2004, įsteigiančio Europos tinklų ir informacijos apsaugos agentūrą, 4 straipsnio c punkte.*“

76. Kaip bus paaiškinta toliau, 6 straipsnio 6a dalis nėra būtina; esama pavojaus, kad ja gali būti piktnaudžiaujama, ypač jeigu ji bus priimta neįtraukus svarbių apsaugos priemonių, sąlygų, užtikrinančių kitų direktyvos nuostatų laikymąsi, ir neužtikrinus interesų pusiausvyros. Todėl EDAPP rekomenduoja atmesti šį straipsnį arba bent jau užtikrinti, kad į bet kurį su šiuo klausimu susijusį straipsnį būtų įtrauktos tokios apsaugos priemonės, kokios buvo įtrauktos į EP priimtą 181 pakeitimą.

Srauto duomenų tvarkymo teisiniai pagrindai, taikomi elektroninių ryšių paslaugų teikėjams ir kitiems duomenų valdytojams pagal šiuo metu galiojančius duomenų apsaugos teisės aktus

77. E. privatumo direktyvos 6 straipsnyje reglamentuojama, kokiu mastu viešai prieinamų elektroninių ryšių paslaugų teikėjai gali teisėtai tvarkyti srauto duomenis; pagal šį straipsnį srauto duomenų tvarkymas gali būti vykdomas tik keliais tikslais, pavyzdžiui, sąskaitų pateikimo, atsiskaitymo už tinklų sujungimą ir rinkodaros tikslais. Toks tvarkymas gali būti vykdomas tik apibrėžtomis sąlygomis, pavyzdžiui, rinkodaros atveju asmenims sutikus. Be to, kiti duomenų valdytojai, pavyzdžiui, informacinės visuomenės paslaugų teikėjai, gali tvarkyti srauto duomenis laikydamiesi Duomenų apsaugos direktyvos 7 straipsnio, pagal kurį nustatyta, kad duomenų valdytojai gali tvarkyti duomenis tik laikydamiesi bent vieno iš išvardytų teisinių pagrindų.

78. Vienas tokio teisinio pagrindo pavyzdžių yra Duomenų apsaugos direktyvos 7 straipsnio a punktas, pagal kurį būtinas duomenų subjekto sutikimas. Pavyzdžiui, jeigu mažmeninis pardavėjas internetu nori tvarkyti srauto duomenis reklaminių skelbimų ar rinkodaros medžiagos siuntimo tikslu, jis turi gauti asmens sutikimą. Pagal kitą 7 straipsnyje pateiktą teisinį pagrindą tam tikrais atvejais leidžiama srauto duomenis tvarkyti saugumo tikslais, pavyzdžiui, tai gali daryti apsaugos bendrovės, siūlančios apsaugos paslaugas. Tai grindžiama 7 straipsnio f punktu, kuriame nustatyta, kad duomenų valdytojas gali tvarkyti asmens duomenis, jeigu tai būtina „*dėl teisėtų interesų, kurių siekia duomenų valdytojas arba trečioji šalis (šalys), kurioms atskleidžiami duomenys, išskyrus atvejus, kai duomenų subjekto [...] teisės ir laisvės yra viršesnės nei šie interesai*“. Duomenų apsaugos direktyvoje nenurodyti atvejai, kuriais asmenų duomenų tvarkymas atitiktų šį reikalavimą. Sprendimus priima duomenų valdytojai kiekvienu konkrečiu atveju, dažnai nacionalinėms duomenų apsaugos institucijoms ar kitoms institucijoms davus sutikimą.

79. Turėtų būti apsvarstyta Duomenų apsaugos direktyvos 7 straipsnio ir pasiūlytos E. privatumo direktyvos 6 straipsnio 6a dalies sąveika. Pasiūlytoje 6 straipsnio 6a dalyje nurodytos aplinkybės, kuriomis būtų įvykdyti pirmiau nurodyti 7 straipsnio f punkto reikalavimai. Iš tikrųjų, leidus tvarkyti srauto duomenis tam, kad būtų užtikrintas tinklo ir informacijos saugumas, 6 straipsnio 6a dalimi sudaromos galimybės tvarkyti tokius duomenis teisėto intereso tikslais, kurių siekia duomenų valdytojas.

80. Kaip paaiškinta toliau, EDAPP mano, kad pasiūlyta 6 straipsnio 6a dalis nėra būtina ar naudinga. Teisiniu požiūriu iš principo nėra būtina nustatyti, ar tam tikra duomenų tvarkymo veiklos rūšis, šiuo atveju srauto duomenų tvarkymas saugumo tikslais, atitinka Duomenų apsaugos direktyvos 7 straipsnio f punkto reikalavimus, pagal kuriuos reikalingas asmens sutikimas (*ex* 7 straipsnio a punktas). Kaip nurodyta pirmiau, paprastai tai įvertina duomenų valdytojai, *t. y.* bendrovės įgyvendinimo etape konsultuodamosi su duomenų apsaugos institucijomis ir prireikus su teismais. Bendrai tariant, EDAPP manymu, konkrečiais atvejais teisėtas srauto duomenų tvarkymas saugumo tikslais, atliekamas nekeliant pavojaus asmenų pagrindinėms teisėms ir laisvėms, veikiausiai atitiks Duomenų apsaugos direktyvos 7 straipsnio f punktą ir todėl gali būti atliekamas. Be to, Duomenų apsaugos

ar E. privatumo direktyvose nėra daugiau pavyzdžių, kad tam tikros duomenų tvarkymo veiklos rūšys, kurios atitiktų 7 straipsnio f punkto reikalavimus, būtų išskirtos arba ypatingai traktuojamos; nėra duomenų, kad toks išskirtinis traktavimas būtų reikalingas. Priešingai, kaip nurodyta pirmiau, atrodytų, kad daugeliu atvejų šios rūšies veikla visiškai atitiktų dabartinį tekstą. Todėl teisinė nuostata, patvirtinanti šį įvertinimą, iš principo nėra būtina.

EP, Tarybos ir Komisijos pateiktos 6 straipsnio 6a dalies redakcijos

81. Kaip paaiškinta pirmiau, nors ir nebūtina, tačiau svarbu pabrėžti, kad EP priimtas 181 pakeitimas vis tik buvo parengtas tam tikru mastu atsižvelgiant į privatumo ir duomenų apsaugos principus, įtvirtintus duomenų apsaugos teisės aktuose. EP 181 pakeitime galėtų būti dar labiau atsižvelgta į duomenų apsaugos ir privatumo interesus, pavyzdžiui, įterpus žodžius „konkrečiais atvejais“, kad būtų užtikrintas selektyvus šio straipsnio taikymas, arba įtraukiant konkretų saugojimo laikotarpį.

82. 181 pakeitime esama kelių pozityvių elementų. Jame patvirtinama, kad duomenų tvarkymas turėtų atitikti visus kitus duomenų apsaugos principus, taikomus asmens duomenų tvarkymui („*Nepažeidžiant atitikimo nuostatoms,... Direktyvos 95/46/EB [...] ir šios direktyvos [...]*“). Be to, nors 181 pakeitime leidžiama tvarkyti srauto duomenis saugumo tikslais, tačiau nustatoma subjekto, kuris tvarko srauto duomenis, ir asmenų, kurių duomenys tvarkomi, interesų pusiausvyra, kad toks duomenų tvarkymas galėtų būti atliekamas tik su sąlyga, kad subjekto, tvarkančio duomenis, interesai nebūtų laikomi svarbesniais nei asmens pagrindinių teisių ir laisvių užtikrinimo interesai („*...išskyrus tuos atvejus, kai svarbesni duomenų subjekto pagrindinių teisių ir laisvių užtikrinimo interesai*“). Šis reikalavimas yra esminis, kadangi jo laikantis gali būti leidžiama tvarkyti srauto duomenis konkrečiais atvejais, tačiau jo laikantis nebūtų sudarytos sąlygos subjektui tvarkyti srauto duomenų apskritai.

83. Tarybos performuluotoje pakeitimo redakcijoje esama sveikintinų elementų, pavyzdžiui, išlaikyta formuluotė „*tik tada, kai reikia užtikrinti*“, kuri pabrėžia ribotą šio straipsnio taikymą. Tačiau Tarybos redakcijoje nebeliko pirmiau minėtų duomenų apsaugos ir privatumo apsaugos priemonių. Nors iš principo bendros duomenų apsaugos nuostatos taikomos nepaisant kiekvienu atveju pateikiamos konkrečios nuorodos, vis dėlto Tarybos pateikta 6 straipsnio 6a dalies redakcija gali būti interpretuojama suprantant, kad duomenų valdytojui suteikiamos visos galios tvarkyti srauto duomenis savo nuožiūra jam netaikant jokių duomenų apsaugos ir privatumo apsaugos priemonių, kurios taikomos tvarkant srauto duomenis. Todėl gali būti teigiama, kad srauto duomenis galima rinkti, saugoti ir toliau naudoti nesilaikant duomenų apsaugos principų ir konkrečių įpareigojimų, kurie kitais atvejais taikomi atsakingiems subjektams, pavyzdžiui, kokybės principas ar sąžiningo ir teisėto duomenų tvarkymo įpareigojimas, ar įpareigojimas užtikrinti duomenų konfidencialumą ir saugumą. Be to, straipsnyje nėra nuorodų į taikomus duomenų apsaugos principus, pagal kuriuos nustatomi informacijos saugojimo terminai, ar į konkrečius terminus, todėl Tarybos redakcija gali būti interpretuojama suprantant, kad rinkti ir tvarkyti srauto duomenis saugumo tikslais galima neribotą laikotarpį.

84. Be to, Tarybos redakcijoje susilpnintos privatumo apsaugos priemonės tam tikrose teksto dalyse naudojant pernelyg neapibrėžtas formuluotes. Pavyzdžiui, buvo panaikinta nuoroda į „*teisėtus duomenų valdytojo interesus*“ taip sukeliant abejonių dėl to, kurių rūšių subjektai galėtų pasinaudoti šia išimtimi. Nepaprastai svarbu nesudaryti sąlygų bet kuriam paslaugų gavėjui ar juridiniam asmeniui pasinaudoti šiuo pakeitimu.

85. Pastarieji svarstymai EP ir Taryboje rodo, kad yra sunku teisiškai nustatyti, kokiu mastu ir kokiomis sąlygomis duomenų tvarkymas saugumo tikslais gali būti vykdomas teisėtai. Joks šiuo metu galiojantis ar būsimas straipsnis veikiausiai nepanaikins akivaizdaus pavojaus, kad išimtis bus pernelyg plačiai taikoma kitokiu nei išimtinai apsaugos užtikrinimo pagrindu ar kad išimtį taikys subjektai, kurie neturėtų turėti galimybės ja naudotis. Tai nereiškia, kad toks tvarkymas apskritai neturėtų būti vykdomas. Tačiau įvertinti, ar ir kokiu mastu jis galėtų būtų vykdomas, geriausia būtų įgyvendinimo etape. Subjektai, pageidaujantys vykdyti tokį tvarkymą, turėtų aptarti mastą ir sąlygas su duomenų apsaugos institucijomis ir galbūt su 29 straipsnio darbo grupe. Kita vertus, E. privatumo direktyvoje galėtų būti straipsnis, pagal kurį būtų leidžiama saugumo tikslais tvarkyti srauto duomenis gavus tikslų duomenų apsaugos institucijų leidimą.

86. Atsižvelgdamas į pavojų, kurį 6 straipsnio 6a dalis kelia pagrindinei teisei į asmens duomenų ir privatumo apsaugą, ir į tai, kad teisiniu požiūriu, kaip parodyta pirmiau šioje nuomonėje, šis straipsnis nėra būtinas, EDAPP priėjo išvadą, kad geriausia būtų pasiūlytą 6 straipsnio 6a dalį apskritai išbraukti.

87. Jeigu nepaisant EDAPP rekomendacijos bus priimtas tekstas, panašus į dabartinę 6 straipsnio 6a dalies redakciją, į jį būtinai turėtų būti įtrauktos duomenų apsaugos priemonės, aptartos pirmiau. Tekstas taip pat turėtų būti tinkamai integruotas į dabartinę 6 straipsnio struktūrą, pageidautina kaip nauja 2a dalis.

V. **GALIMYBĖ JURIDINIAMS ASMENIMS IMTIS VEIKSMŲ E. PRIVATUMO DIREKTYVOS PAŽEIDIMŲ ATVEJU**

88. EP priėmė 133 pakeitimą, kuriuo prieigos prie interneto teikėjams ir kitiems juridiniams asmenims, pavyzdžiui, vartotojų asociacijoms, suteikiama galimybė pateikti ieškinį teismui dėl E. privatumo direktyvos nuostatų pažeidimų ([19]). Deja, nei Komisija, nei Taryba pakeitimui nepritarė. EDAPP manymu, šis pakeitimas ypač teiktinas, ir rekomenduoja jį išlaikyti.

89. Siekiant geriau suprasti, koks svarbus šis pakeitimas, būtina suvokti, kad privatumo ir duomenų apsaugos srityje žala, padaryta atskiram asmeniui, paprastai yra nepakankama, kad jis galėtų pateikti ieškinį teismui. Asmenys paprastai nesikreipia į teismą dėl to, kad gavo nepageidaujamų elektroninių laiškų ar jų pavardės neteisėtai buvo įtrauktos į abonentų knygą. Šiuo pakeitimu būtų sudarytos sąlygos vartotojų asociacijoms ir profesinėms sąjungoms, atstovaujančioms kolektyviniams vartotojų interesams, jų vardu pateikti ieškinį teismui. Platesnė vykdymo užtikrinimo mechanizmų įvairovė taip pat paskatintų geriau laikytis reikalavimų ir todėl yra reikalinga siekiant veiksmingai taikyti E. privatumo direktyvos nuostatas.

90. Kai kurių valstybių narių teisinėse sistemose jau esama teisinių precedentų, kuriais numatyta galimybė atlyginti kolektyvinę žalą ir kuriais sudaromos sąlygos vartotojams ar interesų grupėms reikalauti kompensacijos iš žalą padariusios šalies.

91. Be to, kai kuriose valstybėse narėse konkurencijos įstatymais ([20]) suteikiama teisė vartotojams, interesų grupėms (kaip ir *konkurentui, kuriam buvo pakenkta*) apskųsti teismui pažeidimą padariusį subjektą. Toks požiūris grindžiamas samprotavimu, kad konkurencijos įstatymus pažeidžiančios bendrovės veikiausiai naudojasi tuo, kad vartotojai, kuriems padaroma nedidelė žala, paprastai vengia kreiptis į teismą. Šį loginį paaiškinimą galima *mutantis mutandi* pritaikyti duomenų apsaugos ir privatumo srityje.

92. Dar svarbiau, kaip minėta pirmiau, tai, kad suteikiant juridiniams asmenims, pavyzdžiui, vartotojų asociacijoms ir PPECS, teisę pateikti teismui ieškinius sustiprinama vartotojų padėtis, o tai apskritai skatina laikytis duomenų apsaugos teisės aktų. Jeigu pažeidimus darančioms bendrovėms grės didesnis pavojus būti apskųstoms teismui, jos veikiausiai daugiau investuos į tai, kad būtų laikomasi asmens duomenų apsaugos teisės aktų; dėl to galiausiai pakils privatumo ir vartotojų apsaugos lygis. Dėl visų šių priežasčių EDAPP ragina EP ir Tarybą priimti nuostatą, pagal kurią sudaromos galimybės juridiniams asmenims pateikti ieškinį teismui dėl E. privatumo direktyvos nuostatų pažeidimų.

([19]) Per pirmąjį svarstymą priimtos EP rezoliucijos 13 straipsnio 6 dalis.
([20]) Žr., pavyzdžiui, 8 paragrafą UWG – Vokietijos nesąžiningos konkurencijos įstatymą.

VI. **IŠVADA**

93. Tarybos bendrojoje pozicijoje, per pirmąjį svarstymą priimtoje EP rezoliucijoje ir iš dalies pakeistame Komisijos pasiūlyme yra įvairaus lygio pozityvių elementų, kurie būtų naudingi gerinant asmenų privatumo ir asmens duomenų apsaugą.

94. Tačiau EDAPP mano, kad dar yra ką tobulinti, ypač Tarybos bendrojoje pozicijoje, kurioje, deja, neišlaikyti kai kurie EP pakeitimai, skirti užtikrinti adekvačią asmens privatumo ir asmens duomenų apsaugą. EDAPP ragina EP ir Tarybą atkurti tekstą, susijusį su privatumo apsaugos priemonėmis, kuris buvo pateiktas per pirmąjį svarstymą priimtoje EP rezoliucijoje.

95. Be to, EDAPP mano, kad būtų tinkama supaprastinti kai kurias direktyvos nuostatas. Tai ypač pasakytina apie nuostatas dėl saugumo pažeidimų, nes, EDAPP manymu, iš pat pradžių nustačius teisinę sistemą bus geriausiai pasinaudota visais pranešimų apie pažeidimus sistemos privalumais. Galiausiai, EDAPP nuomone, būtų tinkama pagerinti ir patikslinti kai kurių direktyvos nuostatų formuluotes.

96. Atsižvelgdamas į tai, EDAPP ragina EP ir Tarybą padidinti pastangas gerinant ir tikslinant kai kurias E. privatumo direktyvos nuostatas, taip pat atkurti EP pirmuoju svarstymu priimtų pakeitimų, kuriais siekiama užtikrinti tinkamą privatumo ir duomenų apsaugos lygį, tekstą. Šiuo tikslu 97, 98, 99 ir 100 punktuose pateikiama keblių klausimų santrauka, taip pat rekomendacijos ir redakcinių pasiūlymų. EDAPP ragina visas susijusias šalis į tai atsižvelgti prieš galutinai priimant E. privatumo direktyvą.

Saugumo pažeidimas

97. Europos Parlamentas, Komisija ir Taryba laikosi skirtingų požiūrių į pranešimo apie saugumo pažeidimus sistemą. Trys modeliai skiriasi; skirtumai yra susiję, *inter alia*, su subjektais, kuriems taikoma ši pareiga, standartu ar priežastimi, kuriais remiantis atsiranda pareiga pranešti, duomenų subjektais, kuriems turi būti pranešta, ir t. t. EP ir Tarybai būtina dėti visas pastangas, kad būtų sukurta vientisa teisinė sistema, skirta saugumo pažeidimams. Šiuo tikslu EP ir Taryba turėtų:

— *išlaikyti* saugumo pažeidimo apibrėžtį EP, Tarybos ir Komisijos tekstuose, kadangi ji pakankamai plati ir apima daugumą svarbių situacijų, kai reikėtų pranešti apie saugumo pažeidimus.

— *įtraukti* informacinės visuomenės paslaugų teikėjus į subjektų, kuriems taikomas pasiūlytas reikalavimas pranešti, sąrašą. Internetiniai mažmeniniai prekybininkai, internetiniai bankai ir internetinės vaistinės, taip pat kaip ir telekomunikacijų bendrovės, net ir labiau, gali nukentėti dėl saugumo pažeidimų. Piliečiams tikėsis, kad jiems bus pranešta ne tik tais atvejais, kai prieigos prie interneto paslaugų teikėjai nukenčia dėl saugumo pažeidimų, bet ir ypač tada, kai tai atsitinka jų internetiniams bankams ir internetinėms vaistinėms.

— Priežasties, dėl kurios atsiranda pareiga pranešti, klausimu EDAPP mano, kad iš dalies pakeistame pasiūlyme nurodytas standartas *„yra pagrindo manyti, kad bus padaryta žala“* yra tinkamas standartas, užtikrinantis sistemos funkcionalumą. Tačiau svarbu užtikrinti, kad „žalos“ sąvoka būtų pakankamai plati ir apimtų visus atitinkamus neigiamo poveikio privatumui ar kitiems teisėtiems asmenų interesams atvejus. Priešingu atveju, būtų pageidautina sukurti naują standartą, pagal kurį pranešti būtų privaloma tais atvejais, *„jeigu yra pagrindo manyti, kad pažeidimas turės neigiamą poveikį asmenims*“. Tarybos požiūris, pagal kurį reikalaujama, kad pažeidimas turėtų *rimtos* įtakos asmens privatumui, suteiktų netinkamą asmenų apsaugą, nes tokiu standartu reikalaujama, kad poveikis privatumui būtų „rimtas“. Be to, taip sudaromos sąlygos subjektyviam vertinimui.

— Žinoma, institucijos dalyvavimas sprendžiant, ar atitinkamas subjektas privalo pranešti asmenims, yra teigiamas dalykas, tačiau tai gali būti sunku praktiškai pritaikyti, be to, tam gali prireikti skirti išteklių, kurie galėtų būti paskirti kitiems svarbiems prioritetams. EDAPP nuogąstauja, kad tuo atveju, kai institucijos nesugebėtų veikti ypač sparčiai, taikant tokią sistemą asmenų apsauga netgi sumažėtų, o institucijos patirtų perdėtą spaudimą. Todėl EDAPP rekomenduoja *nustatyti* tokią sistemą, kurią taikant patys atitinkami subjektai vertintų, ar jie privalo pranešti.

— Siekiant sudaryti sąlygas institucijoms vykdyti įvertinimų, kuriuos atlieka atitinkami subjektai dėl to, ar reikia pranešti, priežiūrą, reikėtų *įgyvendinti* šias apsaugos priemones:

  — *Užtikrinti*, kad tokie subjektai būtų įpareigojami pranešti institucijoms apie visus pažeidimus, kurie atitinka privalomą standartą.

  — *Suteikti* institucijoms priežiūros funkciją, pagal kurią jos galėtų ją vykdyti selektyviai ir taip veikti efektyviai. To, kas nurodyta pirmiau, tikslu papildyti tokia formuluote: *„jeigu abonentui ar atitinkamam asmeniui dar nepranešta, kompetentinga nacionalinė institucija, išnagrinėjusi pažeidimo pobūdį, gali pareikalauti, kad PPECS arba ISSP tai padarytų.*“

  — *Priimti* naują nuostatą, pagal kurią subjektai turėtų tiksliai ir išsamiai registruoti vidaus audito istoriją. Tai būtų galima pasiekti įrašant tokią formuluotę: *„PPECS ir ISSP renka bei saugo išsamius duomenis apie visus padarytus saugumo pažeidimus, su jais susijusią atitinkamą techninę informaciją ir veiksmus, kurių imtasi padėčiai ištaisyti. Šiuose įrašuose taip pat daroma nuoroda į visus abonentams ar atitinkamiems asmenims ir kompetentingoms nacionalinėms institucijoms pateiktus pranešimus, įskaitant jų datą ir turinį. Šie įrašai pateikiami kompetentingai nacionalinei institucijai, jai pateikus prašymą.*“

— Siekiant užtikrinti pranešimų apie saugumo pažeidimus sistemos įgyvendinimo nuoseklumą, *suteikti* Komisijai galimybes priimti technines įgyvendinamąsias priemones, prieš tai pasikonsultavus su EDAPP, 29 straipsnio darbo grupe ir kitais susijusiais suinteresuotaisiais subjektais.

— Kalbant apie asmenis, kuriems turi būti pranešta, *vartoti* Komisijos ar EP terminus „atitinkami asmenys“ ar „paslaugų gavėjai, kuriuos... paveikė“, kadangi jie apima visus asmenis, kurių asmens duomenims iškilo pavojus.

Viešai prieinami privatieji tinklai

98. Ryšių paslaugos dažnai suteikiamos visuomenei ne viešaisiais, bet privačiai tvarkomais tinklais (pavyzdžiui, belaidžio interneto ryšio vietose viešbučiuose, oro uostuose), kuriems direktyva netaikoma. EP priėmė 121 pakeitimą (3 straipsnis), kuriuo išplečiama direktyvos taikymo sritis įtraukiant viešuosius ir privačiuosius ryšių tinklus, taip pat viešai prieinamus privačiuosius tinklus. Šiuo klausimu EP ir Taryba turėtų:

— *Išlaikyti* 121 pakeitimo esmę, tačiau jį *performuluoti*, į E. privatumo direktyvos taikymo sritį įtraukiant tik *„asmens duomenų tvarkymą, susijusį su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ar viešai prieinamais privačiaisiais tinklais Bendrijoje...*“ Išimtinai privačiai tvarkomi tinklai (kaip priešprieša viešai prieinamiems privatiesiems tinklams) nebūtų aiškiai įtraukti į taikymo sritį.

— Atitinkamai *iš dalies pakeisti* visas funkcines nuostatas, kad jos būtų aiškiai susijusios ne tik su viešaisiais, bet ir su viešai prieinamais privačiaisiais tinklais.

— *Įterpti* pakeitimą, kuriame būtų apibrėžta: *„viešai prieinamas privatusis tinklas – privačiai tvarkomas tinklas, prie kurio prisijungti, už mokestį ar nemokamai teikiant kartu su kitomis paslaugomis ar pasiūlymais, plačiosios visuomenės nariai paprastai turi neribojamas galimybes su sąlyga, kad sutinka su taikomomis sąlygomis ir taisyklėmis“*. Taip bus padidintas teisinis tikrumas dėl subjektų, kurie patenka į naują taikymo sritį.

— *Priimti* naują konstatuojamąją dalį, pagal kurią Komisija konsultuotųsi su visuomene dėl E. privatumo direktyvos taikymo visiems privatiesiems tinklams; be kita ko, turėtų būti konsultuojamasi su EDAPP, 29 straipsnio darbo grupe ir kitais susijusiais suinteresuotaisiais subjektais. Nurodyti, kad pasikonsultavusi su visuomene Komisija turėtų pateikti atitinkamą pasiūlymą, pagal kurį E. privatumo direktyva turėtų būti taikoma daugiau ar mažiau subjektų rūšių.

Srauto duomenų tvarkymas saugumo tikslais

99. EP pirmuoju svarstymu priėmė 181 pakeitimą (6 straipsnio 6 a dalį), pagal kurią leidžiama tvarkyti srauto duomenis saugumo tikslais. Tarybos bendrąja pozicija buvo priimta nauja redakcija, kurioje susilpnintos kai kurios privatumo apsaugos priemonės. Šiuo klausimu EDAPP rekomenduoja EP ir Tarybai:

— *Atmesti* visą šį straipsnį, kadangi jis nėra būtinas, o juo netinkamai naudojantis galima sukelti didelį pavojų duomenų apsaugai ir asmenų privatumui.

— Kita vertus, jeigu būtų priimtas koks nors dabartinės 6 straipsnio 6a dalies redakcijos variantas, *įtraukti* duomenų apsaugos priemones, aptartas šioje nuomonėje (tokias pat kaip EP pakeitime).

Veiksmai E. privatumo direktyvos pažeidimų atveju

100. Parlamentas priėmė 133 pakeitimą (13 straipsnio 6 dalis), kuriuo juridiniams asmenims suteikiama galimybė pateikti ieškinį teismui dėl direktyvos nuostatų pažeidimų. Deja, Taryba jo neišlaikė. Taryba ir EP turėtų:

— *Patvirtinti* nuostatą, kuria juridiniams asmenims, pavyzdžiui, vartotojų ar prekybos asociacijoms, suteikiama teisė pateikti ieškinį teismui dėl bet kurių šios direktyvos nuostatų pažeidimų (ne tik dėl nuostatos, susijusios su negeidaujamų elektroninių laiškų siuntimu, pažeidimo, kaip numatyta bendrojoje pozicijoje ir iš dalies pakeistame pasiūlyme). Platesnė vykdymo užtikrinimo mechanizmų įvairovė paskatintų geriau laikytis reikalavimų ir veiksmingai taikyti visas E. privatumo direktyvos nuostatas.

Išsūkis

101. Visais pirmiau aptartais klausimais EP ir Taryba turi nustatyti tinkamas taisykles ir nuostatas, kurios būtų ne tik praktiškai įvykdomos ir veiktų, bet kuriomis būtų gerbiamos asmenų teisės į privatumą ir duomenų apsaugą. EDAPP tikisi, kad susijusios šalys padarys viską, kad įvykdytų šią užduotį, ir tikisi, kad šia nuomone bus prisidėta prie šių pastangų.

Briuselis, 2009 m. sausio 9 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas

Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl pasiūlymo dėl Tarybos direktyvos, įpareigojančios valstybes nares išlaikyti privalomąsias žalios naftos ir (arba) naftos produktų atsargas

(2009/C 128/05)

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 [1],

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 [2],

atsižvelgdamas į 2008 m. lapkričio 14 d. Europos duomenų apsaugos priežiūros pareigūno (EDAPP) gautą prašymą pateikti nuomonę pagal Reglamento (EB) Nr. 45/2001 28 straipsnio 2 dalį,

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS

1. 2008 m. lapkričio 13 d. Komisija priėmė pasiūlymą dėl Tarybos direktyvos, įpareigojančios valstybes nares išlaikyti privalomąsias žalios naftos ir (arba) naftos produktų atsargas (toliau – pasiūlymas) [3].

2. Šiuo pasiūlymu siekiama užtikrinti aukštą Bendrijos aprūpinimo nafta patikimumo lygį, pasitelkiant patikimus ir skaidrius mechanizmus, pagrįstus valstybių narių savitarpio solidarumu, išlaikant privalomąsias žalios naftos ir (arba) naftos produktų atsargas bei įdiegiant reikiamas procedūrines priemones rimtoms tiekimo problemoms spręsti.

3. 2008 m. lapkričio 14 d. pagal Reglamento (EB) Nr. 45/2001 28 straipsnio 2 dalį Komisija, norėdama pasikonsultuoti, nusiuntė pasiūlymą EDAPP. EDAPP palankiai vertina tai, kad su juo konsultuojamasi šiuo klausimu, ir pažymi, kad nuoroda į šią konsultaciją pagal Reglamento (EB) Nr. 45/2001 28 straipsnį pateikta pasiūlymo preambulėje.

4. Prieš priimdama pasiūlymą, Komisija neoficialiai konsultavosi su EDAPP dėl pasiūlymo projekto konkretaus straipsnio (dabartinis 19 straipsnis). EDAPP palankiai vertina neoficialias konsultacijas, nes tokiu būdu jam buvo suteikta galimybė prieš Komisijai priimant pasiūlymą pateikti keletą pasiūlymų.

II. PASIŪLYMO ANALIZĖ

Bendroji analizė

5. Šis klausimas yra puikus pavyzdys, kad reikėtų nuolatos paisyti duomenų apsaugos taisyklių. Situacijoje, susijusioje su valstybėmis narėmis ir jų pareiga išlaikyti privalomąsias naftos atsargas, kurių savininkai daugiausia yra juridiniai asmenys, asmens duomenų tvarkymo klausimas nėra labai akivaizdus, bet, net jei toks tvarkymas ir nėra numatytas, jis gali būti vykdomas. Todėl bet kokiu atveju reikėtų atsižvelgti į tikimybę, kad asmens duomenys bus tvarkomi, ir elgtis atitinkamai.

6. Dabartinėje situacijoje direktyvoje iš esmės yra nustatytos dvi veiklos rūšys, kurios galėtų apimti asmens duomenų tvarkymą. Pirmoji yra valstybių narių renkama informacija apie naftos atsargas ir tolesnis šios informacijos perdavimas Komisijai. Antroji veiklos rūšis yra susijusi su Komisijos įgaliojimais vykdyti kontrolę valstybėse narėse. Apie naftos atsargų savininkus surinkta informacija gali apimti asmens duomenis, tokius kaip vardai ir pavardės bei įmonių direktorių kontaktiniai duomenys. Tokiu būdu šis informacijos surinkimas ir tolesnis jos perdavimas Komisijai reikštų asmens duomenų tvarkymą ir nulemtų, jog priklausomai nuo to, kas tvarko duomenis, turi būti taikomi arba nacionaliniai teisės aktai, kuriais įgyvendinamos Direktyvos 95/46/EB nuostatos, arba Reglamentas (EB) Nr. 45/2001. Be to, Komisijai suteikti įgaliojimai tikrinti privalomąsias atsargas valstybėse narėse, kurie apima įgaliojimus apskritai rinkti informaciją, galėtų apimti asmens duomenų rinkimą, taigi – ir tvarkymą.

[1] OL L 281, 1995 11 23, p. 31.
[2] OL L 8, 2001 1 12, p. 1.
[3] COM(2008) 775 galutinis.

7. Neoficialių konsultacijų, kuriose buvo svarstoma tik nuostata dėl Komisijos įgaliojimų atlikti tyrimą, metu EDAPP patarė Komisijai nustatyti, ar asmens duomenų tvarkymas Komisijai atliekant tyrimą būtų tik atsitiktinis ar vykdomas reguliariai ir pasitarnautų tyrimo tikslui. Atsižvelgiant į šio įvertinimo rezultatus, buvo pasiūlyti du požiūriai.

8. Jei asmens duomenų tvarkymas nėra numatytas ir todėl būtų tik atsitiktinis, EDAPP rekomendavo, pirma, aiškiai atsisakyti, kad asmens duomenys būtų tvarkomi Komisijos tyrimo tikslais, ir, antra, nurodyti, kad asmens duomenys, su kuriais Komisija susidurtų vykdydama tyrimą, nebūtų renkami arba į juos nebūtų atsižvelgiama, o jei jie būtų atsitiktinai surinkti, būtų nedelsiant sunaikinti. Be to, kaip bendrą atsarginę sąlygą EDAPP pasiūlė įtraukti nuostatą, kurioje būtų teigiama, kad direktyva nepažeidžia duomenų apsaugos taisyklių, išdėstytų Direktyvoje 95/46/EB ir Reglamente (EB) Nr. 45/2001.

9. Kita vertus, jei būtų numatyta, kad Komisijai atliekant tyrimą duomenų tvarkymas yra vykdomas reguliariai, EDAPP rekomendavo Komisijai įtraukti tekstą, kuris atspindėtų tinkamo duomenų apsaugos įvertinimo rezultatus. Jis turėtų apimti šiuos elementus: I) tikrąjį duomenų tvarkymo tikslą, II) būtinybę tvarkyti duomenis siekiant šio tikslo ir III) duomenų tvarkymo proporcingumą.

10. Nors EDAPP neoficialus patarimas buvo susijęs tik su Komisijos įgaliojimais atlikti tyrimą, jo pastabos taip pat buvo taikomos kitai pagrindinei siūlomoje direktyvoje įvardytai veiklai, tai yra valstybių narių atliekamam informacijos rinkimui ir jos perdavimui Komisijai.

11. Galutinis pasiūlymas dėl direktyvos aiškiai parodo, kad Komisija padarė išvadą, jog šioje direktyvoje asmens duomenų tvarkymas nenumatomas. EDAPP malonu matyti, kad šis pirmasis pasiūlytasis požiūris visapusiškai atspindėtas pasiūlyme.

12. Todėl EDAPP pritaria būdui, kuriuo Komisija siūlomoje direktyvoje užtikrino asmens duomenų apsaugos taisyklių laikymąsi. Likusioje šio pasiūlymo dalyje bus pateiktos tik kelios išsamios rekomendacijos.

Pastabos dėl kai kurių aspektų

13. Siūlomos direktyvos 15 straipsnyje nustatyta valstybių narių pareiga kiekvieną savaitę siųsti Komisijai valstybės narės teritorijoje laikomų komercinių atsargų dydžių statistinę suvestinę. Tarp tokios informacijos paprastai bus mažai asmens duomenų. Tačiau ji galėtų apimti informaciją apie fizinius asmenis, kurie yra naftos atsargų savininkai arba kurie dirba juridiniam asmeniui, kuris yra atsargų savininkas. Siekiant išvengti, kad valstybės narės teiktų Komisijai tokią informaciją, 15 straipsnio 1 dalyje teigiama, kad jei valstybės narės tai daro, jos „nenurodo tų atsargų savininkų pavadinimų“. Nors galima būtų manyti, kad pavadinimo nenurodymas ne visada leis išvengti, kad duomenys negalėtų būti susieti su fiziniu asmeniu, dabartinėje situacijoje (naftos atsargų dydžių statistinės suvestinės) šio papildomo sakinio, atrodo, pakaks užtikrinti, kad Komisijai nebūtų perduodami asmens duomenys.

14. Komisijos įgaliojimai atlikti tyrimą nustatyti siūlomos direktyvos 19 straipsnyje. Iš šio straipsnio aiškiai matyti, kad Komisija laikėsi pirmojo požiūrio, išdėstyto 8 punkte. Jame nurodyta, kad asmens duomenų rinkimas negali būti Komisijos atliekamų patikrinimų dalimi. Ir net jei Komisija susiduria su tokiais duomenimis, į juos negalima atsižvelgti, o juos atsitiktinai surinkus jie turi būti sunaikinti. Siekiant suvienodinti šią formuluotę su duomenų apsaugą reglamentuojančiuose teisės aktuose vartojama formuluote ir užkirsti kelią neteisingam supratimui, EDAPP rekomenduoja 2 dalies pirmame sakinyje žodį „rinkimas“ pakeisti žodžiu „tvarkymas“.

15. EDAPP džiaugiasi matydamas, kad į pasiūlymą įtraukta ir bendra atsarginė sąlyga dėl atitinkamų asmens duomenų apsaugą reglamentuojančių teisės aktų. 20 straipsnyje valstybėms narėms ir Komisijai bei kitoms Bendrijos institucijoms aiškiai primenama apie jų prievoles pagal atitinkamai Direktyvą 95/46/EB ir Reglamentą (EB) Nr. 45/2001. Be to, šia sąlyga pabrėžiamos teisės, kurias duomenų subjektai turi pagal šias taisykles, pavyzdžiui, teisė nesutikti, kad jų duomenys būtų tvarkomi, teisė gauti informaciją apie savo duomenis ir teisė į tai, kad jų duomenys būtų patikslinti, jei jie netikslūs. Galbūt galima būtų padaryti vieną pastabą dėl šios nuostatos išdėstymo pasiūlyme. Dėl jos bendro pobūdžio ji taikoma ne tik Komisijos įgaliojimams atlikti tyrimą. Todėl EDAPP rekomenduoja perkelti šį straipsnį į pirmą direktyvos dalį, pavyzdžiui, po 2 straipsnio.

16. 25 konstatuojamoje dalyje taip pat nurodoma Direktyva 95/46/EB ir Reglamentas (EB) Nr. 45/2001. Tačiau šios konstatuojamosios dalies tikslas yra gana neaiškus, kadangi joje paminėti tik duomenų apsaugą reglamentuojantys teisės aktai ir nenustatoma nieko daugiau. Konstatuojamoje dalyje turėtų būti aiškiai nurodyta, kad direktyvos nuostatos nepažeidžia tų teisės aktų. Be to, atrodo, kad paskutiniu konstatuojamosios dalies sakiniu norima pasakyti, jog duomenų apsaugą reglamentuojančiuose teisės aktuose aiškiai reikalaujama, kad tikrintojai atsitiktinai surinktus duomenis sunaikintų nedelsiant. Nors tai gali būti nustatytų taisyklių pasekmė, tokios prievolės tuose teisės aktuose nerasime. Tai, kad asmens duomenys nesaugomi ilgiau negu būtina norint pasiekti tikslus, dėl kurių jie

buvo surinkti ar yra toliau tvarkomi, yra bendras duomenų apsaugos principas. Jei pirmoji konstatuojamosios dalies dalis bus patikslinta taip, kaip ką tik buvo pasiūlyta, paskutinis sakinys taps nereikalingas. Todėl EDAPP siūlo išbraukti paskutinį 25 konstatuojamosios dalies sakinį.

III. **IŠVADA**

17. EDAPP norėtų pareikšti pritariantis būdui, kuriuo Komisija siūlomoje direktyvoje užtikrino asmens duomenų apsaugos taisyklių laikymąsi.

18. EDAPP rekomenduoja šiuos konkrečius pakeitimus:

— 19 straipsnio 2 dalies pirmame sakinyje žodį „rinkimas“ pakeisti žodžiu „tvarkymas“;

— 20 straipsnį, kuris yra bendro pobūdžio nuostata dėl duomenų apsaugos, perkelti į pirmą direktyvos dalį, tai yra iš karto po 2 straipsnio;

— 25 konstatuojamoje dalyje įtraukti teiginį, kad direktyvos nuostatos nepažeidžia Direktyvos 95/46/EB ir Reglamento (EB) Nr. 45/2001 nuostatų;

— išbraukti paskutinį 25 konstatuojamosios dalies sakinį.

Priimta Briuselyje, 2009 m. vasario 3 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas

IV

(Pranešimai)

EUROPOS SĄJUNGOS INSTITUCIJŲ IR ORGANŲ PRANEŠIMAI

KOMISIJA

Euro kursas [1]

2009 m. birželio 5 d.

(2009/C 128/06)

1 euro =

	Valiuta	Valiutos kursas		Valiuta	Valiutos kursas
USD	JAV doleris	1,4177	AUD	Australijos doleris	1,7606
JPY	Japonijos jena	137,48	CAD	Kanados doleris	1,5657
DKK	Danijos krona	7,4472	HKD	Honkongo doleris	10,9887
GBP	Svaras sterlingas	0,87920	NZD	Naujosios Zelandijos doleris	2,2263
SEK	Švedijos krona	10,9250	SGD	Singapūro doleris	2,0530
CHF	Šveicarijos frankas	1,5191	KRW	Pietų Korėjos vonas	1 768,65
ISK	Islandijos krona		ZAR	Pietų Afrikos randas	11,4189
NOK	Norvegijos krona	8,9700	CNY	Kinijos ženminbi juanis	9,6871
BGN	Bulgarijos levas	1,9558	HRK	Kroatijos kuna	7,3550
CZK	Čekijos krona	27,003	IDR	Indonezijos rupija	14 078,75
EEK	Estijos kronos	15,6466	MYR	Malaizijos ringitas	4,9556
HUF	Vengrijos forintas	289,10	PHP	Filipinų pesas	67,016
LTL	Lietuvos litas	3,4528	RUB	Rusijos rublis	43,5789
LVL	Latvijos latas	0,7094	THB	Tailando batas	48,464
PLN	Lenkijos zlotas	4,5420	BRL	Brazilijos realas	2,7345
RON	Rumunijos lėja	4,2185	MXN	Meksikos pesas	18,7066
TRY	Turkijos lira	2,1834	INR	Indijos rupija	66,7910

[1] *Šaltinis*: valiutų perskaičiavimo kursai paskelbti ECB.

KLAIDŲ IŠTAISYMAS

Palūkanų normos taikomos Europos centrinio banko pagrindinėms pakartotinio finansavimo operacijoms, klaidų ištaisymas

(Europos Sąjungos oficialusis leidinys C 124, 2009 m. birželio 4 d.)

(2009/C 128/07)

1 puslapyje ir viršelyje:

yra: „1,00 % 2009 m. birželio 4 d.“,

turi būti: „1,00 % 2009 m. birželio 1 d.“.

2009 m. prenumeratos kainos (be PVM, įskaitant paprastosios siuntos išlaidas)

ES oficialusis leidinys, L ir C serijos, tik spausdintinė versija	22 oficialiosiomis ES kalbomis	1 000 EUR per metus (*)
ES oficialusis leidinys, L ir C serijos, tik spausdintinė versija	22 oficialiosiomis ES kalbomis	100 EUR per mėnesį (*)
ES oficialusis leidinys, L ir C serijos, spausdintinė versija ir metinis kompaktinis diskas	22 oficialiosiomis ES kalbomis	1 200 EUR per metus
ES oficialusis leidinys, L serija, tik spausdintinė versija	22 oficialiosiomis ES kalbomis	700 EUR per metus
ES oficialusis leidinys, L serija, tik spausdintinė versija	22 oficialiosiomis ES kalbomis	70 EUR per mėnesį
ES oficialusis leidinys, C serija, tik spausdintinė versija	22 oficialiosiomis ES kalbomis	400 EUR per metus
ES oficialusis leidinys, C serija, tik spausdintinė versija	22 oficialiosiomis ES kalbomis	40 EUR per mėnesį
ES oficialusis leidinys, L ir C serijos, mėnesinis kaupiamasis kompaktinis diskas	22 oficialiosiomis ES kalbomis	500 EUR per metus
Oficialiojo leidinio priedas, S serija (Konkursai ir viešieji pirkimai), kompaktinis diskas, leidžiamas du kartus per savaitę	daugiakalbis: 23 oficialiosiomis ES kalbomis	360 EUR per metus (30 EUR per mėnesį)
ES oficialusis leidinys, C serija. Konkursai	konkursų kalbomis	50 EUR per metus

(*) Egzempliorių kainos: iki 32 puslapių: 6 EUR,
33–64 puslapiai: 12 EUR,
daugiau nei 64 puslapiai: kaina nustatoma kiekvienu atveju.

Europos Sąjungos oficialųjį leidinį, leidžiamą oficialiosiomis Europos Sąjungos kalbomis, galima prenumeruoti bet kuria iš 22 kalbų. Jį sudaro L (teisės aktai) ir C (informacija ir pranešimai) serijos.

Kiekviena kalba leidžiamas leidinys prenumeruojamas atskirai.

Oficialieji leidiniai airių kalba parduodami atskirai, remiantis 2005 m. birželio 18 d. Oficialiajame leidinyje L 156 paskelbtu Tarybos reglamentu (EB) Nr. 920/2005, nurodančiu, kad Europos Sąjungos institucijos laikinai neįpareigojamos rengti ir skelbti visų aktų airių kalba.

Oficialiojo leidinio priedas (S serija. Konkursai ir viešieji pirkimai) skelbiamas viename daugiakalbiame kompaktiniame diske visomis 23 oficialiosiomis kalbomis.

Pateikę paprastą prašymą *Europos Sąjungos oficialiojo leidinio* prenumeratoriai gali gauti įvairius Oficialiojo leidinio priedus. Apie priedų išleidimą prenumeratoriai informuojami pranešime skaitytojui, kuris skelbiamas *Europos Sąjungos oficialiajame leidinyje*.

Pardavimas ir prenumerata

Oficialiųjų leidinių biuro leidžiamų mokamų leidinių galima įsigyti mūsų pardavimo biuruose. Pardavimo biurų sąrašą galima rasti internete adresu

http://publications.europa.eu/others/agents/index_lt.htm

EUR-Lex (http://eur-lex.europa.eu) – tai tiesioginė ir nemokama prieiga prie Europos Sąjungos teisės aktų. Šiame tinklalapyje galima skaityti *Europos Sąjungos oficialųjį leidinį*, susipažinti su sutartimis, teisės aktais, precedentine teise bei parengiamaisiais teisės aktais.

Išsamesnės informacijos apie Europos Sąjungą rasite http://europa.eu

Leidinių biuras
Publications.europa.eu

EUROPOS BENDRIJŲ OFICIALIŲJŲ LEIDINIŲ BIURAS
L-2985 LIUKSEMBURGAS

LT