

## I

(Rezoliucijos, rekomendacijos ir nuomonės)

## NUOMONĖS

## EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

**Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos 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)**

(2008/C 181/01)

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 <sup>(1)</sup>,

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 <sup>(2)</sup>,

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 <sup>(3)</sup>,

atsižvelgdamas į 2007 m. lapkričio 16 d. gautą Europos Komisijos prašymą pateikti nuomonę laikantis Reglamento Nr. 45/2001 28 straipsnio 2 dalies,

PRIĖMĖ ŠIĄ NUOMONĘ:

### I. ĮVADAS

1. 2007 m. lapkričio 13 d. Komisija priėmė pasiūlymą dėl direktyvos, iš dalies keičiančios, be kita ko, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (toliau – pasiūlymas arba siūlomi pakeitimai). Dabartinė Direktyvos 2002/58/EB redakcija paprastai vadinama, be kita ko, ir šioje nuomonėje, E. privatumo direktyva.

<sup>(1)</sup> OLL 281, 1995 11 23, p. 31.

<sup>(2)</sup> OLL 201, 2002 7 31, p. 37.

<sup>(3)</sup> OLL 8, 2001 1 12, p. 1.

2. Pasiūlymo tikslas – pagerinti asmenų privatumo ir tvarkomų asmens duomenų apsaugą elektroninių ryšių sektoriuje. Tai daroma ne iš esmės reformuluojant galiojančią E. privatumo direktyvą, bet pasiūlant *ad hoc* pakeitimus, kuriais daugiausiai siekiama sugriežtinti su saugumu susijusias nuostatas ir pagerinti vykdymo užtikrinimo mechanizmus.
3. Pasiūlymas yra platesnės penkių ES telekomunikacijų srities direktyvų („telekomunikacijų reguliavimo paketo“) dalis. Be pasiūlymų dėl telekomunikacijų reguliavimo paketo peržiūros <sup>(1)</sup>, Komisija taip pat tuo pačiu metu priėmė pasiūlymą dėl reglamento dėl Europos elektroninių ryšių rinkos institucijos įsteigimo <sup>(2)</sup>.
4. Šioje nuomonėje pateiktos pastabos apsiriboja tik E. privatumo direktyvos siūlomais pakeitimais, išskyrus atvejus, kai siūlomi pakeitimai grindžiami sąvokomis ar nuostatomis, pateiktomis pasiūlymuose dėl telekomunikacijų reguliavimo paketo peržiūros. Be to, kai kurios šioje nuomonėje pateiktos pastabos grindžiamos E. privatumo direktyvos nuostatomis, kurios pasiūlyme nebuvo keistos.
5. Šioje nuomonėje nagrinėjami šie klausimai: i) E. privatumo direktyvos taikymo sritis, visų pirma susijusios paslaugos (siūlomas 3 straipsnio 1 dalies pakeitimas); ii) pranešimas apie saugumo pažeidimus (siūlomas pakeitimas, 4 straipsnį papildant naujomis 3 ir 4 dalimis); iii) nuostatos dėl „slapukų“, šnipinėjimo programų ir kitų panašių priemonių (siūlomas 5 straipsnio 3 dalies pakeitimas); iv) elektroninių ryšių paslaugų teikėjų ir kitų juridinių asmenų inicijuoti teisiniai veiksmai (siūlomas pakeitimas, 13 straipsnį papildant nauja 6 dalimi) ir v) vykdymo užtikrinimo nuostatų sugriežtinimas (siūlomas pakeitimas, direktyvą papildant nauju 15a straipsniu).

#### Konsultacijos su EDAPP ir platesnio masto viešosios konsultacijos

6. 2007 m. lapkričio 16 d. Komisija išsiuntė pasiūlymą EDAPP. EDAPP supranta šį komunikatą kaip prašymą patarti Bendrijos institucijoms ir įstaigoms, kaip numatyta 2000 m. gruodžio 18 d. Reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (toliau – Reglamentas (EB) Nr. 45/2001) 28 straipsnio 2 dalyje.
7. Prieš priimdama pasiūlymą Komisija dėl pasiūlymo projekto neoficialiai konsultavosi su EDAPP, kuris šias konsultacijas teigiamai įvertino, nes jos jam suteikė galimybę pateikti keletą siūlymų dėl projekto prieš pasiūlymą priimant Komisijai. EDAPP džiaugiasi matydamas, kad pasiūlyme atsispindi kelios iš jo pasiūlytų nuostatų.
8. Prieš priimant pasiūlymą buvo surengtos plataus masto viešosios konsultacijos, o šią praktiką EDAPP labai vertina. Iš tiesų 2006 m. birželio mėn. Komisija pradėjo viešąsias konsultacijas dėl jos parengto komunikato dėl telekomunikacijų reguliavimo paketo peržiūros, kuriame Komisija pateikė nuomonę dėl padėties ir pateikė keletą siūlomų pakeitimų <sup>(3)</sup>. 29 straipsnio duomenų apsaugos darbo grupė („29 straipsnio darbo grupė“), kurios sudėčiai priklauso EDAPP, pasinaudojo šia galimybe ir 2006 m. rugsėjo 26 d. priimtoje nuomonėje <sup>(4)</sup> pateikė savo nuomonę dėl siūlomų pakeitimų.

<sup>(1)</sup> Siūlomi telekomunikacijų srities direktyvų pakeitimai pateikti šiuose pasiūlymuose: i) pasiūlyme dėl Europos Parlamento ir Tarybos direktyvos, iš dalies keičiančios Direktyvą 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos, Direktyvą 2002/19/EB dėl elektroninių ryšių tinklų ir paslaugų sujungimo ir prieigos prie jų ir Direktyvą 2002/20/EB dėl elektroninių ryšių tinklų ir paslaugų leidimo, 2007 11 13, COM(2007) 697 galutinis; ii) pasiūlyme 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, 2007 11 13, COM(2007) 698 galutinis.

<sup>(2)</sup> Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl Europos elektroninių ryšių rinkos institucijos įsteigimo, 2007 11 13, COM(2007) 699 galutinis.

<sup>(3)</sup> 2006 m. birželio 29 d. priimtas komunikatas dėl ES elektroninių ryšių tinklų ir paslaugų reguliavimo sistemos (SEC (2006) 816). Prie komunikato pridamas Komisijos tarnybų darbinis dokumentas – (COM (2006) 334 galutinis).

<sup>(4)</sup> 2006 m. rugsėjo 26 d. Nuomonė 8/2006 dėl elektroninių ryšių ir paslaugų reguliavimo sistemos, kurioje daugiausiai dėmesio skiriama E. privatumo direktyvai.

**EDAPP bendra nuomonė**

9. EDAPP nuomonė dėl pasiūlymo iš esmės yra teigiama. EDAPP visiškai pritaria Komisijos siekiui priimti pasiūlymą, kuriuo pagerinama asmenų privatumo ir asmens duomenų apsauga elektroninių ryšių sektoriuje. EDAPP pirmiausiai palankiai vertina tai, kad buvo nustatyta privalomo pranešimo apie saugumo pažeidimus sistema (E. privatumo direktyvos 4 straipsnio pakeitimas, kuriuo straipsnis papildytas naujomis 3 ir 4 dalimis). Kai susiduriama su duomenų tvarkymo pažeidimais, pranešimo privatumui yra aiškūs; reikalavimas pranešti sustiprintų organizacijų atsakomybę, paskatintų įmones įgyvendinti griežtas saugumo priemones ir sudarytų galimybę nustatyti patikimiausias technologijas informacijos apsaugos srityje. Be to, susiję asmenys turėtų galimybę imtis apsaugos nuo tapatybės vagystės ar asmens duomenų netinkamo panaudojimo kitu būdu priemonių.
10. EDAPP palankiai vertina kitus pasiūlymo pakeitimus, pavyzdžiui, nuostatą, pagal kurią teisėtą interesą turintys juridiniai asmenys turėtų pagrindą pareikšti kai kurias E. privatumo direktyvos nuostatas pažeidusiems subjektams ieškinį teisme (13 straipsnio pakeitimas, kuriuo straipsnis papildytas nauja 6 dalimi). Be to, teigiamai vertintina tai, kad buvo sustiprintos nacionalinių reguliavimo institucijų teisės atlikti tyrimą, nes tai joms padės įvertinti, ar duomenys tvarkomi laikantis įstatymo, ir nustatyti pažeidėjus (nauja 15a straipsnio 3 dalis). Siekiant apsaugoti asmenų teises ir laisves, būtina kuo greičiau nustatyti priemonę, įgalinančią sustabdyti neteisėto asmens duomenų tvarkymo veiksmus ir privatumo pažeidimus. Tuo tikslu labai teigiamai vertinamos siūlomos 15a straipsnio 2 dalies nuostatos, kuriomis pripažįstama nacionalinių reguliavimo institucijų teisė nurodyti nutraukti pažeidimus; tokia teisė suteiks joms galimybę užtikrinti, kad didelio masto neteisėto tvarkymo veiksmai būtų nedelsiant sustabdyti.
11. Pasiūlymu ir daugeliu siūlomų pakeitimų laikomasi požiūrio, kuris atitinka ankstesnėse EDAPP nuomonėse, pavyzdžiui, nuomonėje dėl duomenų apsaugos direktyvos įgyvendinimo <sup>(1)</sup>, pateiktą nuomonę dėl duomenų apsaugos politikos ateityje. Šis požiūris, be kita ko, grindžiamas įsitikinimu, kad neatsižvelgiant į tai, jog nauji duomenų apsaugos principai nebūtini, reikia nustatyti konkretesnes taisykles, kurių laikantis būtų sprendžiami duomenų apsaugos klausimai, kurie kyla dėl naujų technologijų, pavyzdžiui, interneto, radijo dažninio atpažinimo (RFID) ir t. t., ir priemonės, kurios padėtų užtikrinti duomenų apsaugos srities teisės aktų laikymąsi ir veiksmingumą, pavyzdžiui, suteikiant teisę juridiniams asmenims inicijuoti veiksmus duomenų apsaugos pažeidimo atveju ir įpareigojant duomenų valdytojus pranešti apie saugumo pažeidimus.
12. Nors nuomonė dėl pasiūlymo iš esmės teigiama, EDAPP apgailestauja, kad pasiūlymo tikslai nėra tokie ambicingi, kokie galėtų būti. Iš tiesų nuo 2003 m. stebint E. privatumo direktyvos nuostatų taikymą ir atidžiai nagrinėjant jos objektą paaiškėjo, kad kai kurios direktyvos nuostatos toli gražu nėra aiškios ir sukelia teisinį neaiškumą ir problemų dėl atitikties. Pavyzdžiui, yra neaišku, koku mastu E. privatumo direktyva taikoma pusiau viešųjų subjektų teikiamoms elektroninių ryšių paslaugoms. Galima buvo tikėtis, kad Komisija, norėdama išspręsti kai kurias dar neišspręstas problemas, pasinaudos telekomunikacijų reguliavimo paketo, visų pirma E. privatumo direktyvos peržiūros galimybe. Be to, sprendžiant naujus klausimus, pavyzdžiui, klausimą dėl privalomo pranešimo apie pažeidimus sistemos, pasiūlyme numatytas tik dalinis sprendimo būdas, tarp organizacijų, kurios yra įpareigosios pranešti apie saugumo pažeidimus, nenurodant slaptus ar neskelbtinus duomenis tvarkančių subjektų, pavyzdžiui, elektroninių bankų ar elektroninių sveikatos paslaugų teikėjų. EDAPP dėl to apgailestauja.
13. EDAPP tikisi, kad pasiūlymui skirtose teisėkūros proceso metu teisės aktų leidėjas atsižvelgs į šioje nuomonėje pateiktas pastabas ir pasiūlymus, kad būtų išspręsti klausimai, kurie Komisijos pasiūlyme nenagrinėjami.

<sup>(1)</sup> 2007 m. liepos 25 d. Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Komisijos komunikato Europos Parlamentui ir Tarybai dėl tolesnių veiksmų pagal Geresnio duomenų apsaugos direktyvos įgyvendinimo darbo programą, OL C 255, 2007 10 27, p. 1.

## II. PASIŪLYMO ANALIZĖ

## II.1. E. privatumo direktyvos taikymo sritis, visų pirma susijusios paslaugos

14. Vienas svarbiausių šios E. privatumo direktyvos klausimų – jos taikymo sritis. Pasiūlymas teigiamai vertintinas dėl to, kad jo nuostatomis stengiamasi apibrėžti ir patikslinti pasiūlymo taikymo sritį, visų pirma su direktyva siejamas paslaugas, kurios apibūdinamos toliau pateiktame i) punkte. Deja, siūlomais pakeitimais išsprendžiamos ne visos problemos. Kaip nurodyta toliau pateiktame ii) punkte, apgailestaujama, kad siūlomais pakeitimais nesistengiama išplėsti direktyvos taikymo srities, kad ji būtų taikoma privačiais tinklais teikiamoms elektroninių ryšių paslaugoms.
15. E. privatumo direktyvos 3 straipsnyje apibūdinamos su direktyva susijusios paslaugos, t. y. paslaugos, kurių atžvilgiu taikomos direktyvoje nustatytos prievolės: „Ši direktyva taikoma asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais“.
16. Tai reiškia, kad su E. privatumo direktyva susijusias paslaugas teikia viešųjų elektroninių ryšių paslaugų teikėjai (PPECS) viešaisiais ryšių tinklais. PPECS sąvoka apibrėžta pagrindų direktyvos <sup>(1)</sup> 2 straipsnio c punkte. Viešojo ryšio tinklo sąvoka apibrėžtis pateikiama pagrindų direktyvos 2 straipsnio d punkte <sup>(2)</sup>. PPECS veiklos pavyzdžiai – prieigos prie interneto suteikimas, informacijos perdavimas elektroniniais tinklais, judriojo ir telefono ryšio jungtys ir t. t.
- i) Siūlomi E. privatumo direktyvos 3 straipsnio pakeitimai: susijusios paslaugos, apimant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo prietaisus
17. Pasiūlymu iš dalies keičiamas E. privatumo direktyvos 3 straipsnis, konkrečiai nurodant, kad viešiesiems elektroninių ryšių tinklams priklauso „viešieji ryšių tinklai, palaikantys duomenų rinkimo ir atpažinimo prietaisus“. 28 konstatuojamojoje dalyje paaiškinama, kad kuriant taikomąsias programas, pagrįstas informacijos, įskaitant asmens duomenis, rinkimu naudojant radijo dažnius, pavyzdžiui radijo dažnių atpažinimą, E. privatumo direktyvą būtina taikyti tuo atveju, kai jie sujungti su viešaisiais ryšių tinklais ar paslaugomis ar jais naudojami.
18. EDAPP teigiamai vertina šią nuostatą, nes ji patikslina, kad E. privatumo direktyva bus taikoma keletui RFID pritaikymo būdų; taip šiek tiek išsklaidomi neaiškumai šiuo klausimu ir išvengiama nesusipratimų aiškinant teisės aktus.
19. Iš tiesų, pagal dabartinę E. privatumo direktyvos 3 straipsnį direktyva jau taikoma tam tikriems RFID pritaikymo būdams. Tam yra kelios bendros priežastys. Pirma, elektroninių ryšių paslaugų sąvoka apima RFID taikymą. Antra, todėl, kad toks taikymas užtikrinamas naudojant elektroninių ryšių tinklą, grindžiamą perdavimo sistema, kuri perduoda signalus bevielėmis ryšio priemonėmis. Ir galiausiai,

<sup>(1)</sup> 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyva 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos, OL L 108, 2002 4 24, p. 33. Pagrindų direktyvoje apribojama elektroninių ryšių sistemos sąvoka, t.y.: i) „elektroninių ryšių paslauga“ – paslauga, paprastai teikiama už atlygį, kuri susideda iš signalų perdavimo tinklais, įskaitant telekomunikacijų ir perdavimo paslaugas tinklais. ii) Į elektroninių ryšių paslaugų sąvokos apibrėžtį neįtraukiamos elektroniniais ryšių tinklais ir paslaugomis perduodamo turinio teikimo paslaugos. iii) Paslaugų teikimas – tinklo sukūrimas, eksploatavimas, kontrolė ar galimybės juo naudotis suteikimas. iv) Elektroninių ryšių paslaugos neapima informacinės visuomenės paslaugų, kurios E. komercijos direktyvoje apibrėžiamos kaip paslauga (-os), paprastai teikiama už atlyginimą per atstumą, elektroninėmis priemonėmis ir asmeniškai paslaugų gavėjo prašymu.

<sup>(2)</sup> „viešasis ryšių tinklas“ – elektroninių ryšių tinklas, naudojamas vien tik ar didžiąja dalimi viešai prieinamoms elektroninių ryšių paslaugoms teikti.

tinklas gali būti viešasis ir privatusis. Jei tai viešasis tinklas, laikoma, kad RFID taikymas yra „susijusios paslaugos“, todėl jam taikoma E. privatumo direktyva. Siūlomu pakeitimu būtų išsklaidytos likusios abejonės šiuo klausimu ir todėl užtikrintų daugiau teisinio aiškumo.

20. Žinoma, kaip nurodyta ankstesnėje EDAPP nuomonėje dėl RFID <sup>(1)</sup>, ši nuostata neužkerta kelio galimybei priimti papildomas teisinius dokumentus dėl RFID. Tačiau šios priemonės turėtų būti patvirtintos ne šiame pasiūlyme, bet kitame kontekste.

ii) *Poreikis įtraukti elektroninių ryšių paslaugas į privačiuosius ar pusiau privačiuosius tinklus*

21. Nors EDAPP palankiai vertina pirmiau pateiktą patikslinimą, jis apgailestauja, kad pasiūlymas neužtikrino, kad bus paaiškintas labai miglotas skirtumas tarp privačiųjų ir viešųjų tinklų. Be to, EDAPP apgailestauja, kad į paslaugų, kurioms taikoma E. privatumo direktyva, sąvokos apibrėžtį nebuvo įtraukti privatieji tinklai. Pagal dabartinę formuluotę E. privatumo direktyvos 3 straipsnio 1 dalis taikoma tik *elektroninių ryšių paslaugoms, kurios teikiamos viešaisiais tinklais*.
22. EDAPP atkreipia dėmesį į vis labiau privačiųjų-viešųjų paslaugų augimo tendenciją. Pavyzdžiui, universitetai, kurie suteikia galimybę tūkstančiams studentų naudotis internetu ir elektroninio pašto paslaugomis. Pusiau viešųjų (arba pusiau privačiųjų) tinklų gebėjimai kėsintis į privatumą yra akivaizdūs, todėl reikia, kad šios rūšies paslaugoms būtų taikomos tokios pačios taisyklės, kurios taikomos vien tik viešiesiems tinklams. Be to, privatieji tinklai, pavyzdžiui, darbdavių, suteikiančių darbuotojams galimybę naudotis internetu, viešbučių ar apartamentų savininkų, leidžiančių svečiams naudotis telefonu ir elektroniniu paštu, taip pat interneto kavinių tinklai, daro poveikį šioms paslaugomis besinaudojančių asmenų asmens duomenų tvarkymui ir privatumui, todėl galima daryti prielaidą, kad E. privatumo direktyva turėtų būti taikoma ir tokiems tinklams.
23. Faktiškai pagal kai kurių valstybių narių teisminę praktiką elektroninių ryšių paslaugoms, kurios teikiamos privačiais tinklais, taikomos tokios pačios prievolės, kurios numatytos viešaisiais tinklais teikiamoms paslaugoms <sup>(2)</sup>. Taip pat pagal Vokietijos teisę duomenų apsaugos institucijos yra nustačiusios, kad bendrovė, kuri leidžia naudotis elektroniniu paštu asmeniniais tikslais, galima laikyti viešųjų telekomunikacijų paslaugų operatoriumi; tokiu atveju jai būtų taikomos E. privatumo direktyvos nuostatos.
24. Apibendrinant galima teigti, kad didėjanti mišrių (privačiųjų/viešųjų) ir privačiųjų tinklų reikšmė kasdiniame gyvenime ir dėl to atitinkamai didėjanti rizika asmens duomenims ir privatumui pateisina poreikį tokioms paslaugoms taikyti tas pačias taisykles, kurios taikomos viešųjų elektroninių ryšių paslaugoms. Todėl EDAPP nuomone, direktyva turėtų būti iš dalies pakeista, į jos taikymo sritį įtraukiant šios rūšies privačiąsias paslaugas; 29 straipsnio darbo grupė laikosi tokios pat nuomonės <sup>(3)</sup>.

## II.2. Pranešimas apie saugumo pažeidimus. 4 straipsnio pakeitimas

25. E. privatumo direktyvos 4 straipsnis iš dalies keičiamas, straipsnį papildant dviem naujomis dalimis (3 ir 4), kuriose nustatyta prievolė pranešti apie saugumo pažeidimus. Iš tiesų, pagal 4 straipsnio 3 dalį viešųjų elektroninių ryšių paslaugų teikėjai (PPECS) privalo, viena vertus, nedelsdami pranešti nacionalinėms reguliavimo institucijoms apie visus saugumo pažeidimus, dėl kurių atsitiktinai arba neteisėtai sunaikinami, prarandami, pakeičiami, neteisėtai atskleidžiami asmens duomenys, kurie perduodami, saugomi ar kitu būdu tvarkomi teikiant elektroninių ryšių paslaugas, arba su tokiais duomenimis susiję (t. y. „kyla pavojus duomenims“); kita vertus, PPECS yra taip pat įpareigoti apie tai informuoti savo klientus.

<sup>(1)</sup> 2007 m. gruodžio 20 d. Nuomonė dėl Komisijos komunikato Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui: „Radijo dažnių atpažinimas (RDA) Europoje: politikos sistemos formavimo veiksmai“ COM (2007) 96

<sup>(2)</sup> Pavyzdžiui, Paryžiaus apeliacinio teismo 2005 m. vasario 4 d. priimtu sprendimu byloje *BNP Paribas prieš World Press Online* nustatyta, kad nėra skirtumo tarp interneto paslaugų teikėjų, suteikusių prieigą prie interneto komerciniui pagrindu, ir darbdavių, suteikusių prieigą prie interneto savo darbuotojams.

<sup>(3)</sup> 2006 m. rugsėjo 26 d. Nuomonė 8/2006 dėl elektroninių ryšių ir paslaugų reguliavimo sistemos, kurioje daugiausiai dėmesio skiriama E. privatumo direktyvai.

*Šios prievolės privalumai*

26. EDAPP palankiai vertina šias nuostatas (4 straipsnio 3 ir 4 dalys), nustatančias privalomo pranešimo apie saugumo pažeidimus sistemą. Pranešimas apie saugumo pažeidimus turi teigiamo poveikio asmens duomenų ir privatumo apsaugai; ši sistema jau buvo išbandyta Jungtinėse Valstijose, kuriose jau keletą metų valstijų lygiu įgyvendinami pranešimų apie pažeidimus reglamentuojantys teisės aktai.
27. Pirmą pranešimą apie pažeidimus reglamentuojantys teisės aktai didina PPECS atsakomybę dėl informacijos, kuriai kilo pavojus. Pagal duomenų apsaugos ar privatumo politikos teisės aktus atsakomybė reiškia, kad kiekviena organizacija yra atsakinga už jos tvarkomą ar kontroliuojamą informaciją. Prievolė pranešti prilygsta pakartotiniam pareiškimui, kad, viena vertus, duomenis, kuriems kilo pavojus, kontroliavo PPECS ir, kita vertus, ši organizacija turi imtis būtinų priemonių šių duomenų atžvilgiu.
28. Antra, tai, kad pranešimo apie saugumo pažeidimus sistema egzistuoja, pasitvirtino vienu iš veiksnių, skatinančiu asmens duomenis tvarkančias organizacijas investuoti į saugumo priemones. Iš tiesų vien tai, kad organizacijos privalo viešai pranešti apie saugumo pažeidimus, verčia jas įgyvendinti aukštesnius saugumo standartus, kurie apsaugo asmens duomenis ir užkerta kelią pažeidimams. Be to, pranešimo apie saugumo pažeidimus sistema padės nustatyti ir atlikti patikimą statistinę analizę dėl veiksmingiausių saugumo priemonių ir mechanizmų. Ilgą laiką trūko patikimų duomenų apie saugumo sistemos gedimus ir tinkamiausias informacijos apsaugos technologijas. Tikėtina, kad ši problema, kaip pasitvirtino JAV įstatymais dėl pranešimo apie saugumo pažeidimus, bus išspręsta nustatytomis priemonėmis pranešti apie saugumo pažeidimus, nes pranešimai suteiks informacijos apie pažeidimams neatspariausias technologijas <sup>(1)</sup>.
29. Galiausiai, pranešus apie saugumo pažeidimus, asmenys sužino apie tai, su kokia rizika jie susiduria, jei jų asmens duomenims kyla pavojus, ir todėl gali imtis būtinų priemonių tokiai rizikai sumažinti. Pavyzdžiui, jeigu kilo pavojus banko duomenims, informuotas asmuo gali pakeisti jam/jai suteiktos prieigos prie jo/jos banko sąskaitos duomenis ir taip užkirsti kelią kitiems asmenims pasinaudoti šia informacija neteisėtais tikslais (paprastai tai vadinama „tapatybės vagyste“). Apibendrinant galima pasakyti, kad ši prievolė sumažina galimybę, kad asmenys galėtų tapti tapatybės vagystės aukomis, o nukentėjusiems asmenims gali padėti imtis būtinų veiksmų problemoms išspręsti.

*Siūlomo pakeitimo trūkumas*

30. Nors EDAPP palankiai vertina 4 straipsnio 3 ir 4 dalyse nustatytą pranešimo apie saugumo pažeidimus sistemą, jam būtų buvusi priimtinesnė platesnio masto sistema, kuri apimtų informacinės visuomenės paslaugų teikėjus. Tai reikštų, kad toks teisės aktas būtų taikomas elektroniniams bankams, elektroninėms įmonėms, elektroninių sveikatos paslaugų teikėjams ir t. t. <sup>(2)</sup>
31. Priežastys, pagrindžiančios viešųjų elektroninių ryšių paslaugų teikėjams, t. y. PPECS, keltiną reikavimą įgyvendinti pranešimo apie saugumo pažeidimus sistemą galioja ir kitoms organizacijoms, kurios taip pat tvarko didelius asmens duomenų, kurių atskleidimas galėtų turėti daug žalos duomenų subjektams, kiekius. Tokios organizacijos, be kita ko, yra elektroniniai bankai, duomenų makleriai ir kiti elektroninių paslaugų teikėjai, pavyzdžiui, tie, kurie tvarko neskelbtinus duomenis (be kita ko, duomenis apie sveikatą, politines pažiūras ir t. t.). Jeigu kyla pavojus elektroninių bankų ir elektroninių įmonių turimai informacijai, kuri gali apimti ne tik banko sąskaitos numerius, bet ir kredito kortelių duomenis, tikėtina tapatybės vagystė, o tokiu atveju svarbu, kad susijusiems asmenims apie tai būtų pranešta, kad jie galėtų imtis būtinų priemonių. Pastaruoju atveju (elektroninių sveikatos paslaugų atveju), jeigu atskleidžiami neskelbtini duomenys, tikėtina, kad asmenims bus padaryta moralinė žala, nors finansinių nuostolių jie ir nepatirs.

<sup>(1)</sup> Žr. Prof. Ross Anderson, Rainer Böhme, Richard Clayton ir Tyler Moore pranešimą „Security Economics and the Internal Market“, kurį užsakė ENISA. Pranešimas pateikiamas tinklavietėje adresu: [http://www.enisa.europa.eu/doc/pdf/report\\_sec\\_econ\\_&\\_int\\_mark\\_20080131.pdf](http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf)

<sup>(2)</sup> E. komercijos direktyvoje pateikiama tokia informacinės visuomenės paslaugų apibrėžtis: paslauga (-os), paprastai teikiama (-os) už atlyginimą per atstumą, elektroninėmis priemonėmis ir asmeniškų paslaugų gavėjo prašymu.

32. Be to, išplėtus prievolės taikymo sritį, su prievolės nustatymu susiję tikėtini pirmiau aprašyti privatumai bus juntami ne tik viename veiklos sektoriuje, t. y. viešųjų elektroninių ryšių paslaugų teikėjų sektoriuje, bet išsiplės į visą informacinės visuomenės paslaugų sritį. Iš tiesų prievolė informacinės visuomenės paslaugų teikėjams, pavyzdžiui, elektroniniams bankams, pranešti apie saugumo pažeidimus ne tik padidins jų atsakomybę, bet ir paskatins sugriežtinti saugumo priemones ir taip išvengti galimų saugumo pažeidimų ateityje.
33. Yra dar keli E. privatumo direktyvos taikymo ne tik PPECS precedentai, pavyzdžiui, 15 straipsnis dėl pranešimų konfidencialumo ir 13 straipsnis dėl nepageidaujamų elektroninių laiškų. Tai patvirtina, kad praelyje teisės aktų leidėjas labai sumaniai nusprendė išplėsti E. privatumo direktyvos tam tikrų nuostatų taikymo sritį, nes jautė, kad tai tikslinga ir būtina. EDAPP tikisi, kad šiuo metu teisės aktų leidėjas nedvejos ir, laikydamasis panašaus lankstaus požiūrio, išplės 4 straipsnio taikymo sritį įtraukiant informacinės visuomenės paslaugų teikėjus. Tam tikslui 4 straipsnio 3 dalyje pakaktų tokios nuorodos į informacinės visuomenės paslaugų teikėjus: „Saugumo pažeidimo atveju, dėl kurio atsitiktinai arba ..., viešųjų elektroninių ryšių paslaugų teikėjas ir informacinės visuomenės paslaugų teikėjas ... apie tokį pažeidimą praneša atitinkamam abonentui ir nacionalinei reguliavimo institucijai“.
34. EDAPP nuomone, ši prievolė ir jos nustatymas PPECS ir informacinės visuomenės paslaugų teikėjams būtų pirmas pokytis, kuris galiausiai būtų pritaikytas apskritai visiems duomenų valdytojams.

*Saugumo pažeidimams taikomi konkretūs teisės aktai, kuriuos reikia priimti taikant komitologijos procedūrą*

35. Pasiūlyme nenagrinėjama keletas klausimų, susijusių su prievole pranešti apie saugumo pažeidimus. Klausimai, kuriuos reikia nagrinėti, be kita ko, yra dėl pranešimo aplinkybių, formos ir taikytinų procedūrų. Vietoj to, pasiūlymo 4 straipsnio 4 dalyje numatyta, kad šie sprendimai pagal 1999 m. birželio 28 d. sprendimą turi būti priimti „komitologijos“ komitete<sup>(1)</sup>, t. y. juos turi priimti Ryšių komitetas, įsteigtas pagal pagrindų direktyvos 22 straipsnį. Tokios priemonės pirmiausiai būtų patvirtintos laikantis 1999 m. birželio 28 d. Tarybos sprendimo 5 straipsnyje nurodytos reguliavimo procedūros, kuri taikoma „bendro pobūdžio priemonėms, skirtoms taikyti neesmines pagrindinio dokumento nuostatas“.
36. EDAPP neprieštarauja pasirinkimui visuos šiuos klausimus reglamentuoti įgyvendinimo teisės aktuose. Tikėtina, kad teisės aktų priėmimui taikant komitologijos procedūrą, teisėkūros procedūra bus trumpesnė. Be to, komitologija padės užtikrinti suderinamumo tikslą, kurio galiausiai turėtų būti siekiama.
37. Atsižvelgiant į tai, kad klausimų, kuriuos reikės nagrinėti įgyvendinimo priemonėse, yra daug ir į šių klausimų svarbą, kaip pabrėžiama pirmiau pateiktame tekste, atrodytų tikslinga juos visus nagrinėti ne padrikai, o viename bendrame teisės aktų rinkinyje, vienus klausimus reglamentuojant E. privatumo direktyvoje, o kitus paliekant įgyvendinimo teisės aktams. Todėl Komisijos požiūriu, šių klausimų sprendimą paliekant įgyvendinimo teisės aktuose, kurie turi būti priimami pasikonsultavus su EDAPP ir, tikėtina, kitais suinteresuotaisiais subjektais (žr. žemiau pateiktą punktą) reikia vertinti teigiamai.

*Klausimai, kuriuos reikės spręsti įgyvendinimo priemonėmis*

38. Tik pakankamai išsamiai išmanant klausimus, kurie turės būti sprendžiami įgyvendinimo priemonėmis, galima suprasti šių įgyvendinimo priemonių svarbą. Iš tiesų įgyvendinimo priemonėmis gali būti nustatyti pranešimo teikimo standartai. Pavyzdžiui, jose bus apibrėžta saugumo pažeidimo sąvoka, pranešimo teikimo asmenims ir valdžios institucijoms sąlygos, pranešimo teikimo terminas ir pranešimo teikimas.

<sup>(1)</sup> EB teisėkūros procedūros, kuriose dalyvauja komitetai, sudaryti iš valstybių narių vyriausybės atstovų valstybės tarnautojų lygiu.

39. EDAPP nuomone, E. privatumo direktyvoje ir visų pirma jos 4 straipsnyje neturėtų būti nustatyta jokių prievolės pranešti išimčių. Todėl EDAPP palankiai vertina požiūrį, kurio laikosi Komisija 4 straipsnyje, kuriame nustatoma prievolė pranešti, nenumatant jokių išimčių, bet sudaromos sąlygos šį ir kitus klausimus spręsti įgyvendinimo teisės aktuose. EDAPP yra susipažinęs su argumentais, galinčiais pateisinti kai kurių šios prievolės išimčių nustatymą, tačiau jis teikia pirmenybę tam, kad šis ir kiti klausimai būtų atidžiai nagrinėjami įgyvendinimo teisės aktuose, surengus išsamius ir visuotinius debatus dėl visų keblių klausimų. Kaip nurodyta pirmiau, dėl klausimų, susijusių su prievole pranešti apie saugumo pažeidimus, be kita ko, susijusių su tai, ar tikslinga nustatyti išimtis ar apribojimus, sudėtingo pobūdžio juos būtina spręsti vieningai, t. y. viename teisės akte, kuriame būtų nagrinėjamas tik šis klausimas.

*Konsultavimasis su EDAPP ir poreikis išplėsti konsultacijas*

40. Atsižvelgiant į įgyvendinimo priemonių poveikio asmens duomenų apsaugai mastą, svarbu, kad prieš patvirtinama šias priemones Komisija surengtų tinkamas konsultacijas. Todėl EDAPP palankiai vertina pasiūlyme pateikiamą 4 straipsnio 4 dalį, kurioje aiškiai nustatyta, kad prieš priimdama įgyvendinimo priemones Komisija konsultuosis su Europos duomenų apsaugos priežiūros pareigūnu. Tokios priemonės ne tik bus susijusios su asmens duomenų ir asmenų privatumo apsauga, bet ir turės svarbios įtakos jai. Todėl svarbu konsultuotis su EDAPP, kaip reikalaujama pagal Reglamento 45/2001 41 straipsnį.
41. Be konsultavimosi su EDAPP, gali būti tikslinga įtraukti nuostatą, kuria nustatoma, kad dėl įgyvendinimo priemonių projekto turi būti surengtos viešos konsultacijos, siekiant gauti patarimų ir skatinti dalijimąsi patirtimi ir geriausios praktikos pavyzdžiais šiais klausimais. Tokiu tinkamu būdu savo nuomones pateiks ne tik pramonės subjektai, bet ir kiti suinteresuotieji subjektai, įskaitant duomenų apsaugos institucijas ir 29 straipsnio darbo grupę. Viešų konsultacijų poreikį sustiprina tai, kad teisės akto priėmimui yra taikoma komitologijos procedūra, pagal kurią Europos Parlamento indėlis yra ribotas.
42. EDAPP pažymi, kad pasiūlyme dėl 4 straipsnio 4 dalies numatyta, kad prieš priimdama įgyvendinimo taisyklės Komisija taip pat konsultuosis su Europos elektroninių ryšių rinkos institucija. EDAPP palankiai vertina tai, kad bus konsultuojamasi su Elektroninių ryšių rinkos institucija, kuri kaupia ENISA sukauptą patirtį ir turimas žinias tinklų ir informacijos saugumo klausimais. Kol Elektroninių ryšių rinkos institucija neįkurta, gali būti tikslinga siūlomame pakeitime (4 straipsnio 4 dalis) numatyti, kad laikinai būtų konsultuojamasi su ENISA.

**II.3. Nuostata dėl slapukų, šnipinėjimo programų ir kitų panašių priemonių: 5 straipsnio 3 dalies pakeitimas**

43. E. privatumo direktyvos 5 straipsnio 3 dalyje nagrinėjamas technologijų, kurios sudaro sąlygas prieigai prie informacijos ir informacijos saugojimui naudotojų galiniame įrenginyje naudojant elektroninių ryšių tinklus, klausimas. Pavyzdžiui, taikant 5 straipsnio 3 dalį naudojami slapukai<sup>(1)</sup>. Taip pat, pavyzdžiui, gali būti naudojamos tokios technologijos, kaip šnipinėjimo programos (slaptos stebėjimo programos) ir Trojos arkliai (pranešimuose ar kitose akivaizdžiai nekenksmingose programose paslėptos programos). Tokiomis technologijomis gali būti siekiama įvairiausių tikslų: kai kuriomis jų visiškai nesiekiami pakenkti ar net siekiama padėti naudotojui, tuo tarpu kitomis – akivaizdžiai siekiama labai pakenkti ir kelti pavojų.

<sup>(1)</sup> Slapukus informacinės visuomenės paslaugų teikėjai (tinklavietės) naudotojų galiniame įrenginyje įrašo įvairiais tikslais, įskaitant tikslą atpažinti lankytoją, kai jis dar kartą apsilanko tinklavietėje. Praktikoje, kai tinklavietėje interneto naudotojui siunčiamas slapukas, naudotojo kompiuteriui suteikiamas unikalus numeris (t. y. iš A tinklavietės slapukus gavęs kompiuteris tampa „slapuko 111 kompiuterinis savininkas“). Tinklavietėje šis numeris išsaugomas kaip nuoroda. Jei slapuką 111 gavusio kompiuterio naudotojas (-ai) slapuko rinkmenos neištrina, kitą kartą jam apsilankius toje pačioje tinklavietėje, ji galės kompiuterį identifikuoti kaip slapuko 111 savininką. Tinklavietė, žinoma, nustato, kad naudojant šį kompiuterį jau buvo apsilankyta šioje tinklavietėje. Mechanizmas, kuris sudaro sąlygas tinklavietei atpažinti kompiuterį kaip daugiakartį lankytoją, veikia paprastai. Kai kompiuteris turi slapukus, pavyzdžiui, slapuką 111, ir lankosi tinklavietėje, kuri ankstesnio apsilankymo metu sukūrė tą slapuką, jis naudotojo standžiajame diske atliks slapuko rinkmenos numerio paiešką. Jei naudotojo naršyklė suranda slapuko rinkmeną, kuri atitinka tinklavietėje saugomą nuorodą, tinklavietei nurodoma, kad kompiuteris turi slapuką 111.



44. E. privatumo 5 straipsnio 3 dalyje nustatomos sąlygos, kurios taikomos siekiant gauti prieigą prie informacijos ar ją saugoti naudotojų, naudojančių, be kita ko, pirmiau nurodytas technologijas, galiniame įrenginyje. Visų pirma pagal 5 straipsnio 3 dalį i) interneto naudotojams turi būti pateikta aiški ir išsami informacija pagal Direktyvą 95/45/EB, *inter alia*, apie duomenų tvarkymo tikslus ir ii) interneto naudotojams turi būti suteikta teisė atsisakyti tokio vykdomo duomenų tvarkymo, t. y. pasirinkti, jog iš jo galinio įrenginio gauta informacija nebūtų tvarkoma.

#### *Siūlomo pakeitimo privalumai*

45. E. privatumo direktyvos galiojanti 5 straipsnio 3 dalis taikoma tik tais atvejais, kai prieigai prie informacijos ir informacijos saugojimui naudotojų galiniame įrenginyje naudojami *elektroninių ryšių tinklai*. Tai apima pirmiau apibūdintą atvejį dėl slapukų bei kitų technologijų, pavyzdžiui, šnipinėjimo programų, naudojimo elektroninių ryšių tinklais. Tačiau neaišku, ar 5 straipsnio 3 dalis taikoma tais atvejais, kai panašios technologijos (slapukai/šnipinėjimo programos ir pan.) platinamos per išorinėje laikmenoje esančią programinę įrangą, kurią reikia atsisiųsti į naudotojų galinius įrenginius. Atsižvelgiant į tai, kad grėsmė privatumui egzistuoja neatsižvelgiant į ryšių kanalą, 5 straipsnio 3 dalies taikymas tik vienam ryšių kanalui yra netinkamas sprendimas.
46. Todėl EDAPP palankiai vertina 5 straipsnio 3 dalies pakeitimą, kuriuo, panaikinant nuorodą į elektroninių ryšių tinklus, iš tiesų išplečiama 5 straipsnio 3 dalies taikymo sritis. Iš tikrųjų iš dalies pakeista 5 straipsnio 3 dalis taikoma, kai prieigai prie informacijos ir informacijos saugojimui naudotojų galiniame įrenginyje naudojami ne tik elektroninių ryšių tinklai, bet ir kitos išorinės laikmenos, pavyzdžiui, kompaktiniai diskai, pastoviosios atminties kompaktiniai diskai (CD-ROM), USB raktai ir t. t.

#### *Techninis saugojimas siekiant palengvinti informacijos perdavimą*

47. Paskutinis E. privatumo 5 straipsnio 3 dalies sakinyss iš dalies pakeistoje redakcijoje lieka nepakitęs. Pagal paskutinį sakinį 5 straipsnio 3 dalies pirmo sakinio reikalavimai „*nedraudžia techninio saugojimo ar priėjimo prie informacijos, kurio vienintelis tikslas yra vykdyti informacijos perdavimą elektroninių ryšių tinklu ar jį palengvinti, taip pat būtinais atvejais teikti informacinės visuomenės paslaugas...*“. Taigi, 5 straipsnio 3 dalies pirmame sakinyje nustatytos privalomos taisyklės (būtinybė teikti informaciją ir pasiūlyti galimybę atsakyti duomenų tvarkymo) netaikomos, kai prieigos prie naudotojo galinio įrenginio ar informacijos saugojimo vienintelis tikslas – *palengvinti* perdavimą, taip pat būtinais atvejais teikti informacinės visuomenės paslaugas, kurių paprašo naudotojas.
48. Direktyvoje nenurodomi atvejai, kuomet prieigos prie informacijos ir informacijos saugojimo vienintelis tikslas – sudaryti palankesnes sąlygas perduoti informaciją ir teikti informaciją. Ši išimtis neabejotinai būtų taikoma internetinio ryšio nustatymo atveju. Taip yra dėl to, kad internetiniam ryšiui nustatyti būtina gauti IP adresą<sup>(1)</sup>. Galutinio naudotojo kompiuterio bus prašoma prieigos prie interneto teikėjui suteikti tam tikros informacijos apie save, o prieigos prie interneto teikėjas jam suteiks IP adresą. Šiuo atveju galutinio naudotojo galiniame įrenginyje saugoma informacija bus persiunčiama prieigos prie interneto teikėjui, kad naudotojui būtų suteikta prieiga prie interneto. Šiuo atveju prieigos prie interneto teikėjas neprivalo pranešti apie šį informacijos rinkimą ir suteikti naudotojui atsisakymo teisę, jeigu tai yra būtina, norint teikti paslaugą.
49. Prisijungęs prie interneto ir norėdamas apsilankyti tam tikroje tinklavietėje naudotojas turi siųsti prašymą serveriui, kuriame yra tinklavietės priegloba. Pastarasis atsakys, jei jam yra žinomas informacijos siuntimo adresas, t. y. naudotojo IP adresas. Atsižvelgiant į tai, kaip šis adresas saugomas, tinklavietei, kurią naudotojas nori aplankyti, vėl būtina gauti interneto naudotojo galiniame įrenginyje esančią informaciją. Akivaizdu, kad ši operacija taip pat priklausytų išimties taikymo sričiai. Iš tiesų šiais atvejais atrodo tikslinga netaikyti 5 straipsnio 3 dalies reikalavimų.

<sup>(1)</sup> IP adresas (internetų protokolo adresas) yra unikalus adresas, kurį naudoja tam tikri elektroniniai įtaisai, kad galėtų atpažinti vienas kitą ir palaikyti ryšį kompiuteriniame tinkle, naudojančiame interneto protokolo standartą (IP); paprasčiau sakant, tai – kompiuterio adresas. Bet kuris prijungtas tinklo įtaisas, įskaitant maršrutizatorius, perjungiklius, kompiuterius, infrastruktūros serverius (pvz., NTP, DNS, DHCP, SNMP ir t. t.), spausdintuvus, internetinio ryšio fakso aparatus ir kai kuriuos telefonus, gali turėti savo adresą, kuris yra unikalus konkrečiame tinkle. Kai kurie IP adresai gali būti unikalus visuotiniame internete, tuo tarpu kiti yra unikalus tik įmonėje.

50. EDAPP nuomone, tikslinga pirmiau aprašytais atvejais atleisti nuo prievolės informuoti ir suteikti galimybę atsisakyti duomenų tvarkymo, kai techninis saugojimas ar prieiga prie naudotojo galinio įrenginio *būtinai* tik siekiant perduoti informaciją elektroninių ryšių tinklu. Tas pats taikoma, kai techninis saugojimas ar prieiga būtinai tik siekiant suteikti informacinės visuomenės paslaugą. Tačiau EDAPP nemano, kad reikia atleisti nuo prievolės informuoti ir suteikti teisę atsisakyti duomenų tvarkymo tais atvejais, kai techninio saugojimo ir prieigos tikslas – tik *palengvinti* informacijos perdavimą. Pavyzdžiui, pagal šio straipsnio paskutinį sakinį duomenų subjektui galima nepateikti informacijos ar nenurodyti jo teisės prieštarauti duomenų apie jį tvarkymui, jei slapukas surenka informaciją apie jo pasirinktą kalbą ar gyvenamąją vietovę (pvz., Belgija, Kinija), kadangi galėtų būti teigiama, kad tokių slapukų tikslas yra palengvinti informacijos perdavimą. EDAPP žinoma, kad programinės įrangos požiūriu praktikoje duomenų subjektams suteikiama galimybė atsisakyti saugoti slapukus ar juos moduluoti. Tačiau to pakankamai aiškiai nenumato jokia teisinė nuostata, kuria vadovaudamasis duomenų subjektas galėtų oficialiai ginti savo teises pirmiau nurodytu atveju.
51. Siekiant to išvengti EDAPP siūlo šiek tiek pakeisti 5 straipsnio 3 dalies paskutinę dalį, t. y. sakinyje išbraukti žodį „palengvinti“: „*nedraudžia techninio saugojimo ar priėjimo prie informacijos, kurio vienintelis tikslas yra vykdyti informacijos perdavimą elektroninių ryšių tinklu ar jį palengvinti, taip pat būtiniais atvejais teikti informacinės visuomenės paslaugas...*“.

#### II.4. PPECS ir juridinių asmenų inicijuoti teisiniai veiksmai: 13 straipsnio papildymas 6 dalimi

52. Siūloma 13 straipsnio 6 dalimi nustatomos teisėtą interesą turinčio fizinio ar juridinio asmens, visų pirma elektroninių ryšių paslaugų teikėjo, turinčio verslo interesų kovoti su E. privatumo direktyvos 13 straipsnio pažeidėjais, teisių gynimo priemonės pagal civilinę teisę. Šiame straipsnyje nagrinėjamas nepageidaujama komercinių pranešimų siuntimo klausimas.
53. Siūlomu pakeitimu bus sudarytos sąlygos, pavyzdžiui, prieigos prie interneto teikėjams kovoti su nepageidaujama elektroninių laiškų siuntėjais dėl piktnaudžiavimo jų tinklais, paduoti į teismą subjektus, klastojančius siuntėjo adresus ar neteisėtai naudojančius serverius siekiant per juos siųsti nepageidaujama elektroninius laiškus ir pan.
54. E. privatumo direktyva aiškiai nereglementavo, ar PPECS turėjo teisę imtis veiksmų nepageidaujama elektroninių laiškų siuntėjų atžvilgiu; tik labai retais atvejais PPECS pateikė ieškinius teisme dėl 13 straipsnio, kaip jis yra įgyvendinamas valstybės narės teisės aktuose, pažeidimo <sup>(1)</sup>. Pripažįstant teisinių veiksmų, skirtų elektroninių ryšių paslaugų teikėjams apsaugoti savo verslo interesus, pagrindą, pasiūlymu patvirtinama, kad E. privatumo direktyva siekiama ne tik apsaugoti atskirus abonentus, bet ir elektroninių ryšių paslaugų teikėjus.
55. EDAPP palankiai vertina tai, kad pasiūlyme nustatoma galimybė verslo interesą turintiems elektroninių ryšių paslaugų teikėjams pateikti ieškinius nepageidaujama elektroninių laiškų siuntėjams. Išskyrus išskirtines aplinkybes, atskiri abonentai neturi nei pinigų, nei motyvacijos inicijuoti tokius veiksmus teisme. Tuo tarpu prieigos prie interneto teikėjai ir kiti PPECS yra finansiškai pajėgūs ir turi technologinių galimybių tirti nepageidaujama elektroninių laiškų siuntimo kampanijas, nustatyti pažeidėjus, todėl atrodo tikslinga jiems suteikti teisę imtis teisinių veiksmų nepageidaujama elektroninių laiškų siuntėjų atžvilgiu.
56. EDAPP ypač vertina siūlomą pakeitimą, jei juo taip pat būtų sudarytos sąlygos vartotojų asociacijoms ir profesinėms sąjungoms, atstovaujančioms nepageidaujama elektroninių laiškų gavusių vartotojų interesams, jų vardu imtis teisinių veiksmų teisme. Kaip nurodyta pirmiau, nepageidaujama elektroninių laiškų gaviamam duomenų subjektui padaryta žala atskirai vertinant paprastai nėra pakankamai didelė, kad jis inicijuotų teisinius veiksmus teismuose. Iš tiesų EDAPP jau yra bendrais bruožais pasiūlęs šią priemonę dėl privatumo ir duomenų apsaugos pažeidimų nuomonėje dėl tolesnių veiksmų pagal

<sup>(1)</sup> Pavyzdžiui, Microsoft korporacija prieš Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

Geresnio duomenų apsaugos direktyvos įgyvendinimo darbo programą <sup>(1)</sup>. EDAPP nuomone, pasiūlymo nuostatos galėjo būti išsamesnės ir pasiūlyti imtis bendrų veiksmų, piliečių grupėms suteikiančių teisę kartu bylinėtis bylose, susijusiose su asmens duomenų apsauga. Nepageidaujamų elektroninių laišku atveju, kai jas gauna daug asmenų, šios asmenų grupės gali susiburti ir imtis bendrų veiksmų nepageidaujamų elektroninių laišku siuntėjų atžvilgiu.

57. EDAPP ypač apgailestauja, kad pasiūlymu apribojama galimybė juridiniams asmenims imtis teisių veiksmų direktyvos 13 straipsnio pažeidimo atvejais, t. y. tais atvejais, kai pažeidžiama nuostata dėl nepageidaujamų e. pašto pranešimų. Iš tiesų pagal siūlomą pakeitimą juridiniai asmenys neturėtų galimybės imtis teisių veiksmų dėl kitų E. privatumo direktyvos nuostatų pažeidimų. Pavyzdžiui, pagal dabartinę nuostatą toks juridinis asmuo kaip vartotojų asociacija negali imtis teisių veiksmų prieš priegios prie interneto teikėją, kuris atskleidė milijonų vartotojų asmens duomenis. Ne tik šio straipsnio, bet ir visos E. privatumo direktyvos įgyvendinimas būtų daug geriau užtikrintas, jei 13 straipsnio 6 dalies nuostatos taptų bendro pobūdžio ir tuomet juridiniai asmenys galėtų imtis teisių veiksmų bet kurios E. privatumo direktyvos nuostatų pažeidimo atveju.
58. Šiai problemai išspręsti EDAPP siūlo 13 straipsnio 6 dalį pateikti atskiru straipsniu (14 straipsniu). Be to, 13 straipsnio 6 dalies formuluotė turėtų būti šiek tiek pakeista: „pagal šį straipsnį“ turėtų būti pakeista į „pagal šią direktyvą“.

## II.5. Vykdymo užtikrinimo nuostatų griežtinimas: papildymas 15a straipsniu

59. E. privatumo direktyva nenustato aiškių vykdymo užtikrinimo nuostatų. Tačiau joje daroma nuoroda į Duomenų apsaugos direktyvos <sup>(2)</sup> dalį dėl vykdymo užtikrinimo. EDAPP palankiai vertina pasiūlyme pateikiamą naują 15a straipsnį, kuriame aiškiai sprendžiami vykdymo užtikrinimo klausimai pagal šią direktyvą.
60. Pirma, EDAPP pažymi, kad pagal veiksmingą vykdymo užtikrinimo politiką šioje srityje, kaip reikalaujama pagal siūlomą 15a straipsnio 3 dalį, nacionalinės valdžios institucijos turi įgaliojimus atlikti tyrimą siekiant gauti reikiamos informacijos. Labai dažnai E. privatumo direktyvos nuostatų pažeidimo įrodymai būna elektroninio pobūdžio ir gali būti saugomi skirtinguose kompiuteriuose ir įtaisuose ar tinkluose. Atsižvelgiant į tai, svarbu suteikti vykdymo agentūroms galimybę gauti kratos orderį, suteikiantį teisę įeiti į patalpą ir atlikti kratą bei poėmį.
61. Antra, EDAPP ypač palankiai vertina siūlomą pakeitimą, t. y. 15a straipsnio 2 dalį, pagal kurią nacionalinės reguliavimo institucijos turi turėti teisę uždrausti tam tikrus veiksmus, t. y. nurodyti nutraukti pažeidimus, ir reikiamus įgaliojimus bei išteklius tyrimui atlikti. Nacionalinės reguliavimo institucijos, įskaitant nacionalines duomenų apsaugos institucijas, turėtų turėti teisę nustatyti draudimą, pagal kurį pažeidėjai turėtų nutraukti veiklą, kuria pažeidžiama E. privatumo direktyva. Draudimas ar įgaliojimai nurodyti nutraukti pažeidimą yra naudinga priemonė nuolatinio asmenų teises pažeidžiančio elgesio atveju. Draudimas bus naudinga priemonė siekiant nutraukti E. privatumo direktyvos pažeidimus, pavyzdžiui, 13 straipsnio dėl nepageidaujamų komercinių pranešimų siuntimo, kuris dėl jo pobūdžio laikomas nuolatinio elgesiu, pažeidimo.
62. Trečia, pasiūlymu Komisijai sudaroma galimybė nustatyti technines įgyvendinimo priemones, siekiant užtikrinti veiksmingą tarpvalstybinį bendradarbiavimą nacionalinių įstatymų vykdymo užtikrinimo srityje (siūlomas pakeitimas dėl 15a straipsnio 4 dalies). Vykdamas bendradarbiavimą šioje srityje Komisijos iniciatyva buvo sudarytas susitarimas, nustatantis tarpvalstybinių skundų dėl nepageidaujamų elektroninių laišku tvarkymo bendrą procedūrą.

<sup>(1)</sup> Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl Komisijos komunikato Europos Parlamentui ir Tarybai dėl tolesnių veiksmų pagal Geresnio duomenų apsaugos direktyvos įgyvendinimo darbo programą (OL C 255, 2007 10 27, p. 1).

<sup>(2)</sup> 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo

63. EDAPP manymu, jei remdamosi teisės aktais įvairių šalių reguliavimo institucijos padeda vienos kitoms, tai šie teisės aktai neabejotinai padės užtikrinti vykdymą tarpvalstybiniu lygiu. Todėl reikia pasiūlymu užtikrinti, kad Komisija galėtų sudaryti tarpvalstybiniam bendradarbiavimui užtikrinti reikiamas sąlygas, be kita ko, nustatytų keitimosi informacija procedūras.

### III. IŠVADOS IR REKOMENDACIJOS

64. EDAPP palankiai vertina pasiūlymą. Siūlomais pakeitimais sustiprinama asmenų privatumo ir asmens duomenų apsauga elektroninių ryšių sektoriuje; tai pasiekama nesunkiai ir nesudarant nepagrįstos ir bereikalingos naštos organizacijoms. Konkrečiau, EDAPP mano, kad daugumos siūlomų pakeitimų nereikėtų keisti, jei jais tinkamai pasiekiami tikslai. 69 punkte išvardyti pakeitimai, kurie, EDAPP tiki, nebus pakeisti.
65. Nepaisant to, kad EDAPP pasiūlymą iš esmės vertina teigiamai, kai kuriuos jo pakeitimus reikėtų patobulinti siekiant užtikrinti, jog jais būtų veiksmingai garantuota asmens duomenų ir asmenų privatumo apsauga. Ypač reikėtų tobulinti nuostatas dėl pranešimo apie saugumo pažeidimus ir nuostatas dėl teisinių veiksmų, kuriuos inicijuoja elektroninių ryšių paslaugų teikėjai dėl nuostatų, susijusių su nepageidaujamais elektroniniais laiškais, pažeidimo. Be to, EDAPP apgailestauja, kad pasiūlyme nenagrinėjami kai kurie klausimai, kurie nėra tinkamai nagrinėjami galiojančioje E. privatumo direktyvoje, tokiu būdu prarandant galimybę šios peržiūros metu išspręsti likusias neišspręstas problemas.
66. Siekiant išspręsti abi problemas, t. y. pasiūlyme netinkamai nagrinėjamus ar visai nenagrinėjamus klausimus, šioje nuomonėje pateikiama keletas redakcinių pasiūlymų. 67 ir 68 punktuose apibendrinamos problemos ir pateikiamos konkrečios formuluotės. EDAPP ragina teisės akto leidėją į jas atsižvelgti pasiūlymui skirtu teisėkūros proceso metu.
67. Pasiūlyme pateikti pakeitimai, kuriuos, tvirtu EDAPP įsitikinimu, reikėtų keisti, yra šie:

- i) **pranešimai apie saugumo pažeidimus.** Siūlomos formuluotės pakeitimas, kuriuo 4 straipsnis papildomas 4 dalimi, taikoma viešųjų elektroninių ryšių paslaugų teikėjams viešaisiais tinklais (internetu paslaugų teikėjams, tinklo operatoriams), kurie yra įpareigoti pranešti nacionalinėms reguliavimo institucijoms ir jų vartotojams apie saugumo pažeidimus. EDAPP visapusiškai pritaria šiai prievolei. Tačiau EDAPP mano, kad ši prievolė taip pat turėtų būti taikoma informacinės visuomenės paslaugų teikėjams, kurie dažnai turi neskelbtinų asmens duomenų. Taigi, elektroniniai bankai ir elektroniniai draudikai, elektroniniai sveikatos paslaugų teikėjai ir kitokios elektroninės įmonės turės laikytis šios prievolės.

Tam tikslui 4 straipsnio 3 dalyje EDAPP siūlo įtraukti tokią nuorodą į informacinės visuomenės paslaugų teikėjus: „Saugumo pažeidimo atveju ..., viešųjų elektroninių ryšių paslaugų teikėjas ir informacinės visuomenės paslaugų teikėjas ... apie tokį pažeidimą praneša atitinkamam abonentui ir nacionalinei reguliavimo institucijai“.

- ii) **Viešųjų elektroninių ryšių paslaugų teikėjų viešaisiais tinklais inicijuoti teisiniai veiksmai.** Siūlomos formuluotės pakeitimu, kuriuo 13 straipsnis papildomas 6 dalimi, nustatomos teisėtą interesą turinčio fizinio ar juridinio asmens, visų pirma elektroninių ryšių paslaugų teikėjo, teisių gynimo priemonės pagal civilinę teisę, siekiant kovoti su E. privatumo direktyvos 13 straipsnio dėl nepageidaujamų elektroninių laiškų pažeidimais. EDAPP palankiai vertina šią nuostatą. Tačiau EDAPP nesuvokia, kodėl ši nauja galimybė taikoma tik 13 straipsnio pažeidimo atveju. EDAPP siūlo sudaryti sąlygas juridiniams asmenims imtis teisinių veiksmų bet kurios E. privatumo direktyvos nuostatos pažeidimo atveju.

Šiam tikslui pasiekti EDAPP siūlo 13 straipsnio 6 dalį pateikti atskiru straipsniu (14 straipsniu). Be to, 13 straipsnio 6 dalies formuluotė turėtų būti šiek tiek pakeista: „pagal šį straipsnį“ turėtų būti pakeista į „pagal šią direktyvą“.

68. E. privatumo direktyvos taikymo sritis, kuri šiuo metu apima tik viešųjų elektroninių ryšių tinklų teikėjus, yra vienas iš didžiausių susirūpinimą keliančių klausimų, kuris nėra nagrinėjamas pasiūlyme. EDAPP mano, kad direktyvą reikėtų iš dalies pakeisti, siekiant išplėsti jos taikymo sritį, ją taikant taip pat elektroninių ryšių paslaugų teikėjams mišriais (privaciaisiais/viešaisiais) ir privačiais tinklais.
69. Pakeitimai, kurių, tvirtu EDAPP įsitikinimu, nereikėtų keisti:
- i **RFID**. Siūlomas 3 straipsnio pakeitimas, pagal kurį viešiesiems elektroninių ryšių tinklams priklauso „viešieji ryšių tinklai, palaikantys duomenų rinkimo ir atpažinimo prietaisus“ yra visiškai priimtinas. Ši nuostata yra itin teigiama, kadangi tampa aišku, kad keleto RFID programų naudojimo atveju turi būti laikomasi E. privatumo direktyvos reikalavimų; taip išskaidomas šio toks teisinis netikrumas šiuo klausimu.
  - ii **Slapukai/šnipinėjimo programa**. Siūlomą pakeitimą dėl 5 straipsnio 3 dalies reikėtų vertinti palankiai, kadangi prievolė informuoti ir suteikti teisę atsisakyti, jog būtų saugomi slapukai/šnipinėjimo įranga galiniame įrenginyje, taip pat bus taikoma šias priemones įdiegiant per išorines duomenų laikmenas, pavyzdžiui, pastoviosios atminties kompaktinius diskus (CD-ROM), USB raktus. Tačiau EDAPP siūlo šiek tiek pakeisti 5 straipsnio 3 dalies paskutinę dalį, t. y. sakinyje išbraukti žodį „palengvinti“.
  - iii **Komitologijos procedūros su konsultavimusi su EDAPP pasirinkimas bei prievolės pranešti sąlygos/apribojimai**. Siūlomu pakeitimu, kuriuo 4 straipsnis papildomas 4 dalimi dėl pranešimo apie saugumo pažeidimus, nustatoma, kad sudėtingų klausimų, susijusių su pranešimo apie saugumo pažeidimus sistemos aplinkybėmis, forma ir procedūromis, sprendimui taikoma komitologijos procedūra, pasikonsultavus su EDAPP. EDAPP tvirtai remia šį vieningą požiūrį. Teisės aktai dėl pranešimo apie saugumo pažeidimą yra atskira tema, kurią reikia nagrinėti surengus išsamius debatus ir atlikus išsamią analizę.  
  
Su šiuo klausimu yra susijęs kai kurių suinteresuotųjų subjektų raginimas 4 straipsnio 4 dalyje nustatyti prievolės pranešti apie saugumo pažeidimus išimtis. EDAPP griežtai prieštarauja tokiam požiūriui. Jis veikiau laikosi nuomonės, kad bendrą pranešimo dalyką, pranešimo būdą, pranešimo galimo sutrumpinimo ar kitokio apribojimo aplinkybes reikėtų analizuoti laikantis holistinio požiūrio, surengus tinkamus debatus.
  - iv **Vykdyto užtikrinimas**. Siūlomame pakeitime, kuriuo įterpiamas 15a straipsnis, nagrinėjama daug naudingų elementų, kuriuos būtina išsaugoti ir kurie padės užtikrinti veiksmingą reikalavimų laikymąsi, įskaitant nacionalinių reguliavimo institucijų įgaliojimų atlikti tyrimą stiprinimą (15a straipsnio 3 dalis) ir įgaliojimų nurodyti nutraukti pažeidimus suteikimą nacionalinėms reguliavimo institucijoms.

Priimta 2008 m. balandžio 10 d. Briuselyje

Peter HUSTINX  
Europos duomenų apsaugos priežiūros  
pareigūnas