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