I

(Rezoliucijos, rekomendacijos ir nuomonės)

NUOMONĖS

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

Europos duomenų apsaugos priežiūros pareigūno nuomonė apie Komisijos komunikatą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Radijo dažnių atpažinimas (RDA) Europoje: politikos sistemos formavimo veiksmai“ COM(2007) 96

(2008/C 101/01)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

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

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

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

atsižvelgdamas 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

1. 2007 m. kovo 15 d. Komisija priėmė komunikatą „Radijo dažnių atpažinimas (RDA) Europoje: politikos sistemos formavimo veiksmai“ ([1]) (toliau – komunikatas). Pagal Reglamento 45/2001 41 straipsnį EDAPP yra atsakingas už Bendrijos institucijų ir įstaigų konsultavimą visais su asmens duomenų tvarkymu susijusiais klausimais. Laikydamasis šio straipsnio EDAPP pateikia savo nuomonę.

2. Ši nuomonė turėtų būti laikoma EDAPP atsaku į komunikatą bei kitus veiksmus RDA srityje, kurių buvo imtasi priėmus komunikatą. Šioje nuomonėje buvo atsižvelgta į tokius kitus atitinkamus veiksmus:

— 2007 m. birželio 28 d. Komisijos sprendimas dėl radijo dažnių atpažinimo technologijos ekspertų grupės sudarymo ([2]), kuris yra tiesiogiai susijęs su komunikato priėmimu. Ši grupė taip pat vadinama RDA srities suinteresuotųjų subjektų grupe. Pagal sprendimo 4 straipsnio 4 dalies b punktą EDAPP dalyvauja grupės veikloje stebėtojo teisėmis.

— 2007 m. kovo 22 d. Tarybos rezoliucija dėl saugios informacinės visuomenės strategijos Europoje ([3]).

— Europos Parlamento inicijuotas projektas „RDA ir tapatybės valdymas“ ([4]).

([1]) COM (2007) 96 galutinis.
([2]) Sprendimas 467/2007/EB, OL L 176, 2007 7 6, p. 25.
([3]) OL C 68, 2007 3 24, p. 1.
([4]) Projektas „RDA ir tapatybės valdymas. Tyrimai, skirti raidai išmaniosios aplinkos link“, kurį Europos Parlamento Mokslinių technologijų galimybių įvertinimo tarnybos užsakymu vykdė ETAG (Europos technologijų įvertinimo grupė), http://europarl.europa.eu/stoa/default_en.htm

— Duomenų apsaugos darbo grupės 2007 m. birželio mėn. priimta Nuomonė 4/2007 dėl duomenų apsaugos sąvokos ([1]).

— Komisijos komunikatas Europos Parlamentui ir Tarybai dėl tolesnių veiksmų pagal Geresnio Duomenų apsaugos direktyvos įgyvendinimo darbo programos ([2]) ir EDAPP 2007 m. liepos 25 d. nuomonė apie šį komunikatą ([3]).

— Komisijos pasiūlymas dėl direktyvos, iš dalies keičiančios (*inter alia*) Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ([4]).

3. EDAPP palankiai vertina Komisijos komunikatą dėl RDA, kadangi jame sprendžiami pagrindiniai klausimai, susiję su RDA technologijos įdiegimu, ir nepamirštama atsižvelgti į lemiamus su privatumu ir duomenų apsauga susijusius veiksnius. Komunikatas parengtas nuosekliai ir kruopščiai. Jį rengiant įvyko penki šiai temai skirti seminarai, taip pat Komisijos užsakymu buvo atlikta visuomenės nuomonės apklausa internetu ([5]).

4. EDAPP pritaria nuomonei, kad RDA sistemos galėtų atlikti vieną iš pagrindinių vaidmenų informacinės visuomenės raidos pakopoje, kuri paprastai vadinama „daiktų internetu“, ir visiškai pritaria susirūpinimui, kuris buvo pareikštas komunikato 3.2 dalyje, kad RDA sistemos gali kelti grėsmę asmens privatumui ir duomenų apsaugos teisėms. EDAPP savo 2005 m. metinėje ataskaitoje nurodė, kad RDA, biometriniai duomenys, „išmaniosios“ terpės ir tapatybės valdymo sistemos yra technologijos, kurių vystymasis gali daryti didelį poveikį duomenų apsaugai.

5. EDAPP nuomone, RDA technologijos bus pritaikytos kasdienėje aplinkoje ir visuotinai taikomos ne tik dėl to, kad jomis yra patogu naudotis ar kad jomis pasiūlomos naujos paslaugos, bet taip pat dėl to, kad bus naudojamos specialiai parengtos ir darnios duomenų apsaugos priemonės.

6. Trumpai tariant, EDAPP mano, kad RDA yra iš esmės nauja technologijos pakopa, kuri Komisijos komunikate pamatuotai vadinama vartais į naują informacinės visuomenės vystymosi etapą.

7. Taip vystantis technologijoms, įvairiose srityse kyla svarbių klausimų, vienas iš kurių yra susijęs su duomenų apsaugos ir privatumo sritimi. Šioje EDAPP nuomonėje apsiribojama šios srities klausimais.

II. **NUOMONĖS PAGRINDINIAI ASPEKTAI**

8. Šioje nuomonėje dėmesys visų pirma skiriamas galimiems šios raidos padariniams duomenų apsaugos ir privatumo srityje. Šiuo metu sunku apibūdinti padarinius, nes RDA sistemos labai sparčiai vystosi, jos vis labiau pritaikomos kasdienėje aplinkoje ir visiškai neaišku, kokią raidos pakopą jos pasieks.

9. Todėl EDAPP laikosi tokio požiūrio:

— visų pirma reikia išaiškinti, kokie bus RDA sistemų įdiegimo praktiniai padariniai duomenų apsaugos ir privatumo srityje;

— antra, reikia konkrečiai nurodyti šiuos padarinius atsižvelgiant į galiojančią teisinę sistemą duomenų apsaugos ir privatumo srityje;

— trečia, EDAPP nagrinėja klausimą, ar atsižvelgiant į šiuos padarinius reikalingos konkretesnės taisyklės, kuriomis reglamentuojami duomenų apsaugos klausimai, kylantys naudojant RDA technologijas. Šį klausimą EDAPP jau kėlė savo nuomonėje apie komunikatą dėl Duomenų apsaugos direktyvos, o šioje nuomonėje jis bus nagrinėjamas toliau.

10. EDAPP šiuo požiūriu siekia skatinti, kad plėtojant RDA sistemas ir vis plačiau jas pritaikant kasdienėje aplinkoje būtų atsižvelgiama į duomenų apsaugos ir privatumo klausimus.

III. **PADARINIŲ NUSTATYMAS**

RDA sistemos ir žymenys

11. Nepaisant to, kad, kaip buvo minėta, RDA sistemos labai sparčiai vystosi ir nėra aišku, kokią raidos pakopą jos pasieks, tikrai yra įmanoma apibūdinti pagrindinius šios raidos bruožus atsižvelgiant į jų padarinius duomenų apsaugos srityje.

([1]) Dokumentas WP 136, paskelbtas darbo grupės tinklavietėje.
([2]) 2007 m. kovo 7 d. Komisijos komunikatas Europos Parlamentui ir Tarybai dėl tolesnių veiksmų pagal Geresnio duomenų apsaugos direktyvos įgyvendinimo darbo programą, COM (2007) 87 galutinis.
([3]) OL C 255, 2007 10 27, p. 1. Toliau – Nuomonė apie komunikatą dėl duomenų apsaugos direktyvos.
([4]) 2007 m. lapkričio 13 d. 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, ir 2002 m. liepos 12 d. Europos Parlamento ir Tarybos 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 galutinis. Į Direktyvą 2002/58/EC bus nurodoma kaip į E. privatumo direktyvą.
([5]) http://www.rfidconsultation.eu/

12. Vertinant RDA technologijos aspektus, kurie gali būti susiję su duomenų apsauga ir privatumu, labai reikėtų aptarti ne tik RDA žymenis, bet ir visą RDA infrastruktūrą, kurią sudaro žymuo, skaitytuvas, tinklas, nuorodų duomenų bazė ir duomenų bazė, kurioje saugomi sąveikaujant žymeniui ir skaitytuvui gauti duomenys. Komunikato įvade yra glaustai pabrėžta, kad RDA – tai ne tik „elektroniniai žymenys“, todėl sprendžiant duomenų apsaugos klausimus nebus apsiribota tik žymenimis, o bus aptariama visa RDA infrastruktūra. Juk kiekviena infrastruktūros dalis prireikus atlieka tam tikrą vaidmenį įgyvendinant Europos duomenų apsaugos teisinę sistemą. Joms įtakos turės informacinės visuomenės raidos pagrindinės tendencijos (pavyzdžiui, beveik neribojamas dažnių juostos plotis, universalūs tinklų ryšiai ir neriboti duomenų saugojimo pajėgumai).

RDA sistemų ir žymenų poveikis

13. Nepaisant to, kad reikalingas, kaip pabrėžta ankstesnėje pastraipoje, platesnis požiūris, dėl įvairių priežasčių reikia visų pirma sutelkti dėmesį į RDA žymenų tvirtinimą ant plataus vartojimo prekių mažmeninės prekybos sektoriuje. Akivaizdu, kad jie vis labiau naudojami, kaip ir buvo prognozuota, ir kad ateityje jie gali būti taikomi visuotinai. Kitų RDA įrenginių naudojimo sritis yra siaura arba ribota, tuo tarpu ant prekių tvirtinami žymenys gali tapti masiniu rinkos produktu. Jau dabar prie daugelio plataus vartojimo prekių yra pritvirtinti RDA žymenys. Toks RDA technologijų naudojimas turės įtakos daugeliui asmenų, kurių asmens duomenys gali būti tvarkomi kiekvieną kartą, kai jie įsigyja produktą su RDA žymeniu.

14. Atskirai reikėtų aptarti, kokie bus RDA žymenų tvirtinimo padariniai prekių savininkams. RDA sistemos gali išplėsti prekės ir jos savininko santykių sąvoką. Išplėtus šiuos santykius, savininkas skenuojant gali būti priskirtas „nedideles pajamas turinčiųjų“ klasei arba būsimų sandorių požiūriu „patraukliai tikslinei grupei“; pernelyg konkrečiai priskiriant ([1]) prekę vienam ar kitam asmeniui, gali būti pradėta automatiškai „bausti“ už tam tikrą veiklą (perdirbimo įpareigojimas, atliekos ir t. t.). Asmenų atžvilgiu neturėtų būti automatiškai priimami jiems nepalankūs sprendimai. Dėl RDA technologijų teikiamų vis didesnių galimybių kyla grėsmė, kad informacinė visuomenė priartės prie situacijos, kai sprendimai bus priimami automatiškai, o technologija bus piktnaudžiaujama siekiant reguliuoti žmonių elgesį.

15. RDA žymens saugomi arba juo gauti duomenys gali būti asmens duomenys, kaip apibrėžta Duomenų apsaugos direktyvos 2 straipsnyje. Pavyzdžiui, kelionėje naudojamose išmaniosiose kortelėse gali būti užfiksuota informacija apie asmens tapatybę ir apie jos turėtojo pastarąsias keliones. Jeigu nesąžiningas asmuo panorėtų sekti asmenis, jam pakaktų strategiškai svarbiose vietose išdėstyti skaitytuvus, kuriais būtų gauta informacija apie kortelių turėtojų judėjimą, tokiu būdu pažeidžiant jų teisę į privatumą ir asmeninės informacijos apsaugą.

16. Panašios grėsmės privatumui gali kilti net jeigu RDA žymuo neišsaugotų informacijos, susijusios su asmens vardais. RDA žymenyse saugomi unikalūs identifikavimo vardai, priskirti plataus vartojimo prekėms: jeigu kiekvienas žymuo turi unikalų identifikavimo vardą, toks identifikavimas gali būti naudojamas priežiūros tikslais. Pavyzdžiui, jeigu kas nors nešiotų rankinį laikrodį, prie kurio pritvirtintas RDA žymuo su identifikavimo numeriu, juo naudojantis galima būtų identifikuoti ir tą, kuris nešioja rankinį laikrodį, net jeigu jo asmens tapatybė nebūtų žinoma. Ar direktyva galėtų būti taikoma, ar ne, priklausytų nuo to, kaip informacija būtų naudojama ir su kuo ji būtų siejama — su pačiu laikrodžiu ar su asmeniu. Ji būtų taikoma, jeigu, pavyzdžiui, būtų pateikiama informacija apie asmens buvimo vietą, kuri gali būti naudojama vykdant jų elgesio stebėseną, arba, pavyzdžiui, pasinaudojant informacija būtų diferencijuojamos kainos, atsisakoma suteikti prieigą arba prieš asmens norą viešai paskelbiami duomenys apie jį.

17. Todėl būtina užtikrinti, kad RDA įrenginiuose būtų įdiegtos būtinos technologinės priemonės, skirtos iki minimumo sumažinti nepageidaujamo informacijos atskleidimo pavojų. Galėtų būti reikalaujama projektuoti RDA infrastruktūrą, visų pirma RDA žymenis, tokiu būdu, kad būtų užkirstas kelias tokiems padariniams. Pavyzdžiui, būtų galima RDA žymenyse įdiegti deaktyvavimo komandą. Ši galimybė bus aptarta toliau šios nuomonės IV skyriuje.

18. RDA sistemos teikia galimybę sekti produktą jau jį pardavus, todėl diskusijose dėl privatumo iškyla naujų klausimų. Analizuojant šių sistemų poveikį, reikės atsižvelgti į du aspektus: į tai, kokiu mastu prekė laikoma asmeniniu daiktu, ir į tos prekės judumą ([2]).

19. Atliekant reikiamą rizikos analizę gali būti atsižvelgta ir į objekto gyvavimo ciklą, tokiu būdu prisidedant prie galimų grėsmių privatumui kiekybinio įvertinimo. Atsižvelgiant į tai, kad žymuo gali nebūti deaktyvuotas, galutinio vartotojo vartojamas produktas, turintis ilgą gyvavimo ciklą, galės užfiksuoti daugiau su produkto savininku susijusių duomenų ir sudaryti tikslesnę jo asmens bylą. Kita vertus, prekė, kurios gyvavimo ciklas – nuo pagaminimo iki perdirbimo stadijos – yra trumpas, pavyzdžiui, sodos vandens skardinė, gali būti mažiau pavojinga ir jai reikėtų taikyti švelnesnes priemones negu produktui, kurio gyvavimo ciklas yra daug ilgesnis.

([1]) Dr. Sarah Spiekermann, Berlyno internetinis ekonomikos tyrimų centras, RDA ir universaliems kompiuterių tinklams skirtas seminaras, kurį surengė Transatlantinio vartotojų dialogo organizacija (2007 m. kovo 13 d.)

([2]) Dara J. Glasser, Kenneth W. Goodman ir Norman G. Einspruch, „Chips, tags and scanners:Ethical challenges for radio frequency identification“, *Ethics and Information Technology*, t. 9, Nr. 2, 2007.

Privatumo ir duomenų apsaugos klausimai diegiant RDA sistemas

20. Siekiant geriau numatyti RDA sistemų padarinius privatumo ir duomenų apsaugos srityje, galima išskirti penkis pagrindinius su privatumu ir saugumu susijusius klausimus.

21. Pirmas klausimas yra duomenų subjekto nustatymas. Daug prieš šešiasdešimt metų RDA žymeniu buvo siekiama nustatyti, ar artėja „draugas ar priešas“. Šiandien naudojant RDA sistemas galima ne tik nustatyti pagrindines objekto sudedamąsias dalis, bet ir galų gale nustatyti asmens tapatybę, todėl kyla poreikis, kad šio proceso metu nenukentėtų duomenų apsauga.

22. Antras klausimas yra duomenų valdytojo (-ų) nustatymas. RDA sistemų atveju gali būti sunku nustatyti, kas yra duomenų valdytojas, kaip apibrėžta Duomenų apsaugos direktyvos 2 straipsnio d punkte, todėl šį klausimą reikia išnagrinėti išsamiau. Tačiau tebėra svarbu nustatyti, kas yra duomenų valdytojas, nustatant kiekvieno iš atitinkamų subjektų, kurie turės laikytis duomenų apsaugos teisinės sistemos reikalavimų, atsakomybę. Žymens gyvavimo ciklo laikotarpiu galėtų, atsižvelgiant į papildomas paslaugas, kurių teikimas gali būti susijęs su žymeniu pažymėtu objektu, keletą kartų pasikeisti duomenis tvarkantis duomenų valdytojas.

23. Trečias klausimas yra tradicinio asmeninės ir viešosios srities atskyrimo reikšmės sumažėjimas. Nors ir praeityje asmeninė ir viešoji erdvės nevisada buvo aiškiai atskirtos, dauguma žmonių žino, kur yra jas skirianti riba (bei pilkosios zonos), ir pagrįstai arba intuityviai priima sprendimus, kaip elgtis vienu ar kitu atveju. E.T. Hall nuomone ([1]), asmeninė erdvė paprastai yra siejama su asmenį nuo kitų asmenų skiriančiu fiziniu atstumu. Privatumo valdymas gali taip pat būti laikomas dinaminiu ribų reguliavimo procesu ([2]). Todėl nenuostabu, kad dėl žymenimis palaikomų ryšių bevielio pobūdžio, taip pat jų gebėjimo nuskenuoti informaciją už regėjimo lauko ribų, kyla susirūpinimas dėl privatumo apsaugos, nes šios tradicinės ribos ir jų valdymas tampa labai neaiškūs. Kyla baimė, kad asmuo gali iš dalies arba visiškai prarasti iki šiol turėtą kontrolę, kai per atstumą valdomi jo duomenys. Todėl pirmųjų įdiegiamų RDA sistemų skenavimo per atstumą galimybėms dėmesį skyrė ir šalininkai, ir priešininkai.

24. Ketvirtas klausimas yra RDA žymenų dydis ir fizinės savybės. Žymuo iš esmės turi būti mažas ir pigus, todėl savaime suprantama, kad šioje RDA sistemos dalyje taikomos saugumo priemonės yra ribotos. Be to, bevieliai ryšiai sukuria papildomą grėsmių spektrą palyginti su laidiniu ryšiu, todėl reikalingi papildomi saugumo reikalavimai.

25. Penktas klausimas yra nepakankamas tvarkymo skaidrumas. Naudojant RDA sistemas gali būti nepastebimai renkama ir tvarkoma informacija, kuri gali būti naudojama asmens byloms sudaryti. Tai gali būti labai akivaizdžiai pademonstruota, jeigu RDA sistemas palygintume su mobiliuoju telefonu, – dažniausiai daromas būtent toks palyginimas. Viena vertus, mobiliųjų telefonų technologijos buvo priimtos labai palankiai, nepaisant galimo brovimosi į privatumo sritį pavojaus. Galima būtų daryti išvadą, kad RDA bus priimtos lygiai taip pat. Kita vertus, reikia pabrėžti, kad mobilusis telefonas yra matomas objektas, kurį vis dar kontroliuoja galutinis vartotojas, nes jį galima išjungti. RDA atveju tai neįmanoma.

26. Nors pirmiau minėtas nepastebimas informacijos rinkimas ir tvarkymas gali būti teisėtas, gali būti ir tam tikromis aplinkybėmis net labai tikėtina, kad tokie duomenys bus renkami ir tvarkomi neteisėtai.

27. Šiame skyriuje pateikti paaiškinimai pagrindžia tokią išvadą. Platus RDA technologijos naudojimas yra iš esmės naujas reiškinys, galintis turėti lemiamos įtakos mūsų visuomenei ir pagrindinių teisių, pavyzdžiui, teisių į privatumą ir duomenų apsaugą, apsaugai mūsų visuomenėje. RDA gali lemti kokybinius pokyčius.

IV. **PASEKMIŲ APIBŪDINIMAS**

Įvadas

28. Šiame skyriuje daugiausia dėmesio bus skirta poveikiui, kurį RDA daro visuomenės pagrindinių teisių apsaugai, pavyzdžiui, privatumo ir duomenų apsaugai. Bus išdėstyti du šio klausimo aspektai: visų pirma bus trumpai apibūdinta, kaip šios pagrindinės teisės yra saugomos pagal dabartinę teisinę sistemą. Antra, EDAPP paaiškins, kaip būtų galima visapusiškai pasinaudoti dabartine teisine sistema. Nuomonėje dėl komunikato dėl Duomenų apsaugos direktyvos šis siekis buvo įvardytas kaip „visapusiškas dabartinių direktyvos nuostatų įgyvendinimas“.

29. Remiamasi šiuo atskaitos tašku: naujų technologijų, pavyzdžiui, RDA sistemų, raida turi akivaizdžios įtakos duomenų apsaugą reglamentuojančiai veiksmingai teisinei sistemai keliamiems reikalavimams. Be to, dėl poreikio veiksmingai apsaugoti individo asmens duomenis, gali būti ribojamas naudojimasis šiomis naujomis technologijomis. Todėl sąveika yra abipusė: technologijos daro įtaką teisės aktams, o teisės aktai daro įtaką technologijoms ([3]).

([1]) Hall, E.T, *The Hidden Dimension*, 1-as leidimas, Garden City, N.Y: Doubleday, 1966.

([2]) Altman, I., *The Environment and Social Behaviour*, Brooks/Cole Monterrey, 1975

([3]) Žr. 2006 m. kovo mėn. EDAPP pastabas dėl Komisijos komunikato dėl Europos duomenų bazių sąveikos, paskelbtas EDAPP tinklavietėje.

Pagrindinių teisių apsauga

30. Pagrindinių teisių apsaugą, įskaitant privatumo ir duomenų apsaugą, Europos Sąjungoje visų pirma garantuoja teisės sistema, kuri yra reikalinga, kadangi tai yra teisės, pripažintos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnyje bei Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose. Duomenų apsaugą ir RDA reglamentuojančią atitinkamą teisės sistemą iš esmės sudaro Duomenų apsaugos direktyva 95/46/EB ir E. privatumo direktyva 2002/58/EB ([1]).

31. Direktyvoje 95/46/EB nustatyta duomenų apsaugą reglamentuojanti bendroji teisės sistema taikoma RDA, jei RDA sistemose tvarkomiems duomenims taikoma asmens duomenų sąvokos apibrėžtis. Nors tam tikrais atvejais naudojant RDA įrenginius akivaizdžiai tvarkomi asmens duomenys ir šie įrenginiai neabejotinai patenka į Duomenų apsaugos direktyvos taikymo sritį, taip pat yra įrenginių, kurių naudojimo atveju Duomenų apsaugos direktyvos taikomumas gali būti ne toks akivaizdus. Pagal 29 straipsnio nuostatas įsteigtos Duomenų apsaugos darbo grupės nuomonėje Nr. 4/2007 dėl asmens duomenų sąvokos siekiama padėti aiškiau suformuluoti asmens duomenų sąvoką, kuri būtų bendrai pripažinta, ir tokiu būdu sumažinti šį neaiškumą ([2]).

32. Su E. privatumo direktyva susijusi padėtis paaiškinta toliau. Iki šiol nėra aišku, ar ši direktyva taikoma RDA įrenginiams. Dėl šios priežasties į 2007 m. lapkričio 13 d. Komisijos pasiūlymą dėl direktyvos pakeitimo įtraukta nuostata, kuria siekiama patikslinti, kad direktyva iš tikrųjų yra taikoma tam tikriems RDA įrenginiams. Tačiau kitiems RDA įrenginiams ji gali būti netaikoma, kadangi ši direktyva taikoma tik asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešuosiuose ryšių tinkluose.

33. Asmens duomenų apsaugą gali papildyti įvairios savireguliavimo priemonės (nesusijusios su teisės sistema). Naudotis tokiomis priemonėmis aktyviai skatinama abiejose direktyvose, pirmiausia Duomenų apsaugos direktyvos 27 straipsnyje, kuriame nustatyta, kad valstybės narės ir Komisija skatina rengti elgesio kodeksus, kurie padėtų tinkamai įgyvendinti direktyvą. Be to, savireguliavimo priemonės galėtų veiksmingai padėti įgyvendinti saugumo priemones, nustatytas Duomenų apsaugos direktyvos 17 straipsnyje ir E. privatumo direktyvos 14 straipsnyje.

Visapusiškas galiojančios sistemos įgyvendinimas

34. Nuomonėje dėl komunikato dėl Duomenų apsaugos direktyvos nurodomos kelios geresniam direktyvos įgyvendinimui skirtos priemonės. Daugelis toje nuomonėje nurodytų neprivalomųjų priemonių yra susijusios su RDA, pavyzdžiui, aiškinamieji ar kito pobūdžio pranešimai, geriausios praktikos propagavimas, privatumo apsaugos ženklų naudojimas ir trečiosios šalies atliekamas privatumo auditas. Galimybė priimti konkrečias RDA taikomas taisykles bus išnagrinėta V skyriuje. Vis dėlto yra galimybių tobulinti ir galiojančią sistemą.

Savireguliavimo priemonės

35. EDAPP pritaria Komisijos nuomonei, kad pirmajame etape tikslinga sudaryti savireguliavimo galimybę, kad suinteresuotieji subjektai galėtų greitai sukurti teisės normas atitinkančią aplinką ir tokiu būdu padėtų sukurti saugesnę teisinę aplinką.

36. Komisija, konsultuodamasi su RDA suinteresuotųjų subjektų grupe, turėtų skatinti savireguliavimo procesą ir jam vadovauti. Todėl EDAPP palankiai vertina komunikate minimą rekomendaciją, kurioje turėtų būti pateikti konkretūs nurodymai, kuriais remiantis bus nustatyti *„principai, kuriuos valdžios institucijos ir kiti suinteresuotieji subjektai turėtų taikyti, kai naudojamas RDA“*.

37. Komunikate numatoma, kad savireguliavimą reglamentuoja elgesio kodeksas arba geros praktikos kodeksas. EDAPP nuomone, neatsižvelgiant į savireguliavimo reglamentavimo būdą:

— turėtų būti nustatyti konkretūs praktiniai nurodymai, susiję su konkrečiais RDA įrenginių tipais ir tokiu būdu padedama laikytis duomenų apsaugą reglamentuojančios teisinės sistemos reikalavimų;

— turėtų būti sprendžiami konkretūs duomenų apsaugos klausimai ir problemos, su kuriais susiduriama naudojant bendruosius RDA įrenginius;

— turėtų būti prisidedama prie vienodo ir suderinto Duomenų apsaugos direktyvos taikymo visoje ES, pirmiausia tame ES sektoriuje, kuriame gali būti naudojami to paties tipo RDA įrenginiai;

— savireguliavimo priemones turėtų taikyti visi suinteresuotieji subjektai. Šių priemonių nesilaikymas turėtų turėti neigiamų pasekmių (galbūt finansinių).

([1]) Šios nuomonės 59 punkte bus aptartas trečiosios direktyvos – 1999 m. kovo 9 d. Europos Parlamento ir Tarybos direktyvos 1999/5/EB dėl radijo ryšio įrenginių ir telekomunikacijų galinių įrenginių bei abipusio jų atitikties pripažinimo (OL L 91, 1999 4 7, p. 10) – aktualumas.

([2]) Žr., *inter alia*, 5 išnašoje nurodytos nuomonės p. 10.

38. EDAPP nurodo vieną sritį, kurioje savireguliavimo priemonės bus ypač naudingos. Tų RDA įrenginių, kuriuos naudojant tvarkomi asmens duomenys, atveju Duomenų apsaugos direktyvoje, visų pirma jos 17 straipsnyje (tvarkymo saugumas) ir 7 straipsnyje (poreikis tvarkyti duomenis tik remiantis tinkamu teisiniu pagrindu), duomenų valdytojams nustatomos įvairios prievolės. Pagal šias nuostatas duomenų valdytojai, viena vertus, privalo nustatyti priemones, kurios padėtų užkirsti kelią neteisėtam duomenų atskleidimu. Kita vertus, duomenų valdytojai privalo užtikrinti, kad atitinkamais atvejais duomenys būtų tvarkomi, pavyzdžiui, informacija atskleidžiama naudojant skaitytuvus, tik gavus asmens, su kuriuo šie duomenys yra susiję ir kuriam prieš tai buvo suteikta informacija, apgalvotą sutikimą.

39. Gali būti suprantama, kad šiomis Duomenų apsaugos direktyvos nuostatomis nustatoma, jog RDA įrenginiuose būtų įdiegti reikiami techniniai sprendimai, kad būtų užkirstas kelias nepageidaujamam informacijos atskleidimui ar sumažinta tokio atskleidimo rizika, ir atitinkamais atvejais būtų užtikrinta, kad duomenys būtų tvarkomi ar perduodami tik gavus asmens, kuriam prieš tai buvo suteikta informacija, sutikimą. EDAPP nuomone, tokia prievolė (pavyzdžiui, įdiegti reikiamus techninius sprendimus, kad būtų užkirstas kelias nepageidaujamam informacijos atskleidimui ar sumažinta tokio atskleidimo rizika) ir reikalavimas, kad RDA įrenginių naudotojai ją vykdytų, bus dar griežtesni ir aiškesni, jei šis reikalavimas bus įtrauktas į pirmiau paminėtą būsimą elgesio kodeksą ar geros praktikos kodeksą. Dėl šių priežasčių EDAPP primygtinai rekomenduoja į Komisijos rekomendaciją įtraukti tokį Duomenų apsaugos direktyvos aiškinimą, pabrėžiant prievolę RDA įrenginiuose įdiegti reikiamas technologines priemones, kad būtų užkirstas kelias nepageidaujamam informacijos rinkimui ar jos atskleidimui.

Poreikis parengti nurodymus

40. EDAPP rekomenduoja Komisijai, glaudžiai bendradarbiaujant su RDA ekspertų grupe, parengti vieną ar kelis dokumentus, kuriuose būtų išdėstyti aiškūs nurodymai, kaip dabartinę teisinę sistemą taikyti RDA aplinkai. Nurodymuose turėtų būti numatyti praktiniai būdai, kaip laikytis Duomenų apsaugos direktyvoje ir E. privatumo direktyvoje nustatytų principų. EDAPP toliau pateikia pasiūlymus dėl bendro požiūrio, kuriuo bus grindžiami nurodymai, ir jų konkretaus turinio.

41. Nurodymai, kuriuose būtų išdėstyti RDA naudojimui taikomi principai, turėtų būti pakankamai sukoncentruoti ir pagrįsti sektoriui pritaikytu metodu. „Visiems atvejams tinkantis“ požiūris nepadės užtikrinti aiškios ir nuoseklios sistemos. Vietoj to, nurodymai turi būti taikomi tik tinkamai apibrėžtiems konkrečių sektorių RDA įrenginiams.

42. Be to, nurodymuose turėtų būti pasiūlyti praktiški ir veiksmingi *metodų ir standartų* kūrimo metodai, kurie galėtų būti naudingi užtikrinant RDA sistemų suderinimą su duomenų apsaugos teisine sistema ir kuriuos taikant būtų naudojamos technologijos, kuriose į privatumą atsižvelgiama projektuojant.

43. Taikant dabartinę teisinę sistemą RDA aplinkai, ypatingas dėmesys turi būti skiriamas duomenų apsaugos principų taikymui ir RDA įrenginių duomenų valdytojams nustatytas prievoles. Ypač svarbios yra šios prievolės ir principai:

— teisės gauti informaciją principas, įskaitant teisę žinoti, kada duomenys renkami skaitytuvais, ir kad atitinkamais atvejais prie produktų tvirtinami žymenys;

— sutikimo, kaip vieno iš teisinių pagrindų tvarkyti duomenis, sąvoka. Tai apima prievolę deaktyvuoti RDA žymenis parduodant, nebent duomenų subjektas būtų davęs sutikimą ([1]). Teisė deaktyvuoti RDA žymenis taip pat padeda užtikrinti informacijos saugumą, t. y. užtikrinti, kad RDA žymenyse tvarkomi duomenys nebūtų atskleisti nepageidaujamoms trečiosioms šalims;

— asmenų teisė, kad jų atžvilgiu nebūtų priimami nepalankūs sprendimai, grindžiami tik tam tikros asmens bylos automatiniu tvarkymu.

44. Teisės gauti informaciją atžvilgiu nurodymuose turėtų būti nustatyta, kad asmenims turi būti suteikta *informacija* apie jų asmens duomenų tvarkymą. Visų pirma jie, *inter alia*, turėtų būti įspėti apie *i)* skaitytuvus ir ant produktų ar jų pakuotės esančius aktyvius RDA žymenis; *ii)* tokių skaitytuvų ir žymenų naudojimo pasekmes, susijusias su informacijos rinkimu ir *iii)* tikslus, kuriems ketinama naudoti surinktą informaciją.

45. Logotipų naudojimas gali būti tinkama informavimo priemonė. Logotipai gali būti naudojami norint įspėti apie skaitytuvus ir RDA žymenis, kurie turėtų būti aktyvūs. Tačiau norint užtikrinti teisingą informacijos tvarkymą ir įvykdyti įpareigojimą aiškiai ir suprantamai informuoti duomenų subjektus, tik logotipų nepakaks. Logotipų naudojimas turėtų būti laikomas papildoma priemone, naudojama suteikiant išsamesnę informaciją.

([1]) Išsamesnė informacija pateikiama šios nuomonės 46–50 punktuose.

Svarbiausias principas – savanoriško sutikimo (*opt-in*) principas

46. Būtina, kad visuose atitinkamuose RDA įrenginiuose diegiant techninius sprendimus būtų atsižvelgta į savanoriško sutikimo (*opt-in*) principą ir šis principas būtų įgyvendinamas pardavimo metu. Būtų neteisėta, jei po pardavimo RDA žymenys ir toliau galėtų skleisti informaciją, nebent duomenų valdytojas turėtų tam tinkamą teisinį pagrindą. Tinkamas teisinis pagrindas paprastai būtų tik: a) duomenų subjekto sutikimas arba b) jei atskleisti duomenis buvo būtina norint suteikti paslaugą — specialus ir nevaržomas atitinkamo asmens prašymas ([1]). Abu teisiniai pagrindai būtų laikomi savanoriško sutikimo (*opt-in*) principu.

47. Remiantis savanoriško sutikimo (*opt-in*) principu, žymenys turėtų būti deaktyvuojami pardavimo metu, nebent asmuo, kuris įsigijo produktą, prie kurio yra pritvirtintas žymuo, norėtų, kad jis liktų aktyvus. Pasinaudodamas teise palikti žymenį aktyvų, asmuo sutiktų, kad jo duomenys būtų toliau tvarkomi, pavyzdžiui, sutiktų kad kito jo apsilankymo pas duomenų valdytoją metu duomenys būtų perkelti į skaitytuvą.

48. EDAPP pabrėžia, kad atsižvelgiant į tai, kad RDA įrenginių asortimentas plečiasi, ir siekiant sudaryti palankesnes sąlygas naujų naujoviškų verslo modelių kūrimui, svarbu laikytis lankstaus požiūrio. Turi būti numatyta galimybė lanksčiai įgyvendinti savanoriško sutikimo (*opt-in*) principą.

49. Esama įvairių galimybių įgyvendinti savanoriško sutikimo (*opt-in*) principą. Pavyzdžiui, vietoj galimybės nuimti žymenį, gali būti numatyta galimybė užblokuoti žymenį, laikinai apriboti jo veikimą arba remiantis saugumo politikos modeliu – vadinamuoju „išsiritusio ančiuko modeliu“ ([2]) – leisti žymeniu naudotis tik konkrečiam naudotojui. Jei žymens veikimo ciklas yra trumpas, iš nuorodų duomenų bazės taip pat galėtų būti ištrintas žymens adresas, kuriame fiksuojama duomenų bazėje saugoma informacija, kad būtų išvengta naudojant žymenį surinktų papildomų duomenų tolesnio tvarkymo.

50. Daroma išvada, kad nors EDAPP teigia, jog savanoriško sutikimo (*opt-in*) principo laikymasis pardavimo metu yra teisinė prievolė, kuri daugeliu atvejų jau yra numatyta Duomenų apsaugos direktyvoje, esama tinkamų priežasčių reikalauti, kad ši prievolė būtų apibrėžta savireguliavimo priemonėse, taip pat siekiant užtikrinti, kad šis principas būtų kuo tinkamiau įgyvendintas. Bet kuriuo atveju būtina numatyti konkrečias įgyvendinimo nuostatas, kurios būtų taikomos tiems RDA įrenginiams, kuriems netaikoma Duomenų apsaugos direktyva.

Poreikis užtikrinti, kad „į privatumą atsižvelgiama projektuojant“

51. Siekiant sumažinti privatumui ir duomenų apsaugai kylančią grėsmę, Komisijos komunikato 3.2 dalyje (p. 6) patvirtinamas poreikis apibrėžti ir patvirtinti išankstinius projektavimo kriterijus. EDAPP palankiai vertina šį požiūrį. Iš tiesų patvirtinus specifikacijas ir projektavimo kriterijus, vadinamus „geriausiais turimais metodais“, bus veiksmingai prisidėta prie duomenų apsaugos reglamentavimo ir saugumo reikalavimų įgyvendinimo. Nustačius tokius technologinius ir struktūrinius kriterijus, kurie būtų dažnai peržiūrimi, bus stiprinama privatumo modelio ir saugumo reikalavimų, kuriuos Europos Sąjunga plėtoja, simbiozė.

52. Tinkamas RDA sistemų privatumo ir saugumo užtikrinimo geriausių turimų metodų apibrėžimas taip pat turės lemiamos reikšmės kuriant patikimą aplinką, kurioje bus stiprinamas šių metodų platus pripažinimas tarp galutinių naudotojų ir jų reikšmė Europos pramonės konkurencingumui.

53. Atlikti RDA sistemoms taikomų geriausių turimų metodų atrankos procesą turėtų padėti poveikio privatumui ir saugumui įvertinimai, kurių atlikimui dar reikia skirti pastangų. EDAPP nuomone, Europos tinklų ir informacijos apsaugos agentūra (ENISA) ir Europos Komisijos jungtiniai tyrimų centrai, bendradarbiaudami su atitinkamais pramonės suinteresuotaisiais subjektais, gali padėti nustatyti šios geriausios praktikos pavyzdžius ir sukurti tokius metodus. Vokietijos informacijos apsaugos federalinio biuro neseniai pradėtas RDA techninių gairių projektas ([3]) yra tinkamas geriausių turimų metodų orientacinis pavyzdys, kuris šiuo metu turėtų būti pradėtas plėtoti Europos lygiu.

54. Standartai taip pat gali būti ypač svarbūs siekiant kuo anksčiau pradėti taikyti principą, kad į privatumą atsižvelgiama projektuojant. Todėl Komisija turėtų padėti patvirtinti privatumo ir duomenų apsaugos priemones plėtojant tarptautinius RDA standartus. 29 straipsnio darbo grupės parengtame darbo dokumente ([4]) dėl RDA aiškiai išdėstyta, kaip nustačius standartus būtų galima padėti kurti pagarbą privatumui užtikrinančias RDA sistemas.

([1]) Kai kurių RDA įrenginių atveju gali būti įmanoma remtis kitu pagrindu, pavyzdžiui, 7f straipsniu (duomenų valdytojo teisėti interesai, atsižvelgiant į atitinkamas apsaugos priemones).

([2]) Šio modelio pavadinimą sugalvojo Frank Stajano and Ross Anderson iš Kembridžo universiteto; juos įkvėpė tai, „kaip ančiukas suvokia, kad pirmasis judantis objektas, kurį jis pamato turi būti jo motina“.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) 2005 m. sausio 19 d. darbo dokumentas (WP 105) dėl duomenų apsaugos klausimų, susijusių su RDA technologijomis.

55. Be to, EDAPP palankiai vertina Komisijos poziciją dėl RDA technologijų mokslinių tyrimų ir plėtojimo bei dėl poreikio švelninti privatumui gresiančią riziką. Iš tikrųjų principas, kad į privatumą atsižvelgiama projektuojant, turi būti įgyvendintas kuo ankstesniame technologijų kūrimo etape, kadangi tai padės užtikrinti, kad šios technologijos geriau atitiktų duomenų apsaugos teisinės sistemos reikalavimus. 2006 m. EDAPP metinėje ataskaitoje užsiminta, kad EDAPP prisidės prie šių pastangų konkrečiais atvejais pateikdamas nuomones ir rekomendacijas dėl projektų, susijusių su 7-aja bendrąja programa (2007–2013 m.).

V. **AR REIKALINGOS KONKREČIOS TEISĖS PRIEMONĖS?**

56. Visapusiškam galiojančios duomenų apsaugos ir privatumo sistemos reikalavimams įgyvendinti tik savireguliavimo priemonių gali nepakakti. Net jei savireguliavimo priemonės atitinka pirmiau išdėstytus reikalavimus, jos taikomos savanoriškai, o už jų netaikymą ne visada gali būti taikomos veiksmingos sankcijos. Be to, vis dar gali reikėti privalomų teisės priemonių, kad būtų užtikrinta asmenų teisių į privatumą apsauga ir duomenų apsauga. Tokios priemonės pirmiausia būtinos tuo atveju, kai nepavyksta įgyvendinti savireguliavimo priemonių.

57. Pagrindinis klausimas yra susijęs su teisinių priemonių, kurios yra būtinos siekiant užtikrinti, kad RDA įrenginiuose būtų veiksmingai įdiegti reikiami techniniai sprendimai, kurie padėtų užkirsti kelią duomenų apsaugai ir privatumui gresiančiai rizikai ar padėtų kuo labiau sumažinti tokią riziką, o atsakingi duomenų valdytojai imtųsi tinkamų priemonių, kad įvykdytų galiojančiose teisinėse sistemose nustatytas prievoles, nustatymu. Dėl šios priežasties kyla papildomų klausimų:

— ar reikalingos konkrečios taisyklės?

— jei jos reikalingos, ar šias taisykles galima priimti pagal galiojančią teisės sistemą, pavyzdžiui, taikant galiojančias komitologijos procedūras?

— ar reikia naujos teisės priemonės, kad būtų užtikrintas veiksmingas griežtesnę privatumo apsaugą užtikrinančių technologijų naudojimas RDA įrenginiuose?

58. Šiame skyriuje bus nagrinėjamos galimybės priimti privalomas teisės priemones pagal galiojančią teisinę sistemą, o VI skyriuje bus išnagrinėtas poreikis priimti naują teisinę priemonę, kadangi tai yra atskiras klausimas.

59. Pirmiausia ypatingas dėmesys turėtų būti skirtas Direktyvos 95/46/EB 17 straipsnio, Direktyvos 2002/58/EB 14 straipsnio 3 dalies ir Direktyvos 1999/5/EB 3 straipsnio 3 dalies c punkto nuostatoms. 14 straipsnio 3 dalimi valstybėms narėms leidžiama patvirtinti priemones siekiant užtikrinti, kad galiniai įrenginiai būtų sukonstruoti taip, kad nebūtų pažeista naudotojų teisė apsaugoti ir valdyti savo asmens duomenų naudojimą pagal Direktyvą 1999/5/EB ([1]). Direktyvos 1999/5/EB 3 straipsnio 3 dalies c punkte numatyta, kad laikydamasi komitologijos procedūros Komisija gali priimti sprendimą, kad tam tikrai įrenginio klasei priklausančio aparato arba konkretaus tipo aparato konstrukcija turi būti tokia, kad jame būtų apsaugos priemonės, užtikrinančios naudotojo bei abonento asmeninių duomenų bei privatumo apsaugą. Direktyvos 1999/5/EB 3 straipsnio 3 dalies c punkto nuostatomis iki šiol dar nebuvo pasinaudota.

60. Šiomis nuostatomis teisės aktų leidėjui nacionaliniu ir Bendrijos lygiu suteikiami įgaliojimai nustatyti, kad privatumo ir duomenų apsaugos priemonės privalo būti įdiegtos gaminant RDA sistemas; tai yra koncepcija, žinoma kaip „į privatumą atsižvelgiama projektuojant“ ([2]). Be to, pagal šią koncepciją raginama naudoti geriausius turimus metodus.

61. Tai, kad taikyti koncepciją „į privatumą atsižvelgiama projektuojant“ būtų privaloma, EDAPP rekomenduoja Komisijai naudoti Direktyvos 99/5/EB 3 straipsnio 3 dalies c punkte nustatytą mechanizmą konsultuojantis su RDA ekspertų grupe.

62. Antra, galima patikslinti galiojančios teisės sistemos taikymą RDA iš dalies keičiant pačias direktyvas. Kaip minėta, Komisija neseniai pateikė pasiūlymą iš dalies keisti E. privatumo direktyvą, kuriame numatyta nauja nuostata šiuo aspektu. EDAPP palankiai vertina šį pirmąjį patvirtinimą, kad direktyva gali būti taikoma RDA įrenginiams. EDAPP konkrečius klausimus, iškilusius dėl E. privatumo direktyvos ir RDA santykio, aptars savo nuomonėje dėl pasiūlymo dėl pakeitimo, kuri bus pateikta 2008 m. pradžioje.

63. Atsižvelgiant į tai, kad Komisija nenumato artimiausioje ateityje iš dalies keisti Duomenų apsaugos direktyvos ([3]), galimybės patikslinti galiojančios teisės sistemos taikymą RDA yra ribotos.

VI. **AR REIKALINGA SPECIALI RDA REGLAMENTUOJANTI TEISINĖ SISTEMA?**

Komisijos ketinimai

64. Komunikate ([4]) pabrėžiama projektuojant užtikrinto saugumo ir privatumo svarba. Be to, reikalaujama visų suinteresuotųjų subjektų dalyvavimo. Komisijos veiklos pagrindinis rezultatas bus „*Rekomendacija nustatyti pricipus, kuriuos*

([1]) Ir pagal 1986 m. gruodžio 22 d. Tarybos sprendimą 87/95/EEB dėl standartizacijos informacinių technologijų ir telekomunikacijų srityje (OL L 36, 1987 2 7, p. 31).
([2]) Žr. IV skyrių.
([3]) Europos duomenų apsaugos priežiūros pareigūnas pritaria šiam požiūriui, žr. 64 punktą.
([4]) Žr. Komunikato 4.1 punktą.

valdžios institucijos ir kiti suinteresuotieji subjektai turėtų taikyti, kai naudojamas RDA“. Rekomendacija tikriausiai bus priimta 2008 m. pavasarį. Komunikate minimas teisėkūros užmojis susideda iš dviejų dalių. Komisija:

— svarstys atitinkamas nuostatas dėl RDA būsimame pasiūlyme dėl E. privatumo direktyvos pakeitimo. Kaip minėta pirmiau, Komisija tokį E. privatumo direktyvos pakeitimą pasiūlė 2007 m. lapkričio mėn., patvirtindama, kad direktyva gali būti taikoma RDA įrenginiams ([1]), tačiau nepasiūlydama E. privatumo direktyvą pradėti taikyti ir privatiems tinklams;

— įvertins kitų teisėkūros veiksmų, skirtų užtikrinti duomenų apsaugą ir privatumą, poreikį.

65. Atsižvelgiant į šią politiką, tikėtina, kad Komisija nenumato, bet jau artimiausioje ateityje, siūlyti naujų konkrečių teisės aktų duomenų apsaugai ir privatumui RDA srityje užtikrinti.

Gairės teisės aktų leidėjui

66. Nuomonėje dėl komunikato dėl Duomenų apsaugos direktyvos EDAPP pateikė kai kurias teisėkūros veiklos gaires, susijusias su asmens duomenų tvarkymu, kurias galima apibendrinti taip:

— pirma, reikėtų laikytis pagrindinių duomenų apsaugos principų: „*Nauji principai nėra būtini, tačiau akivaizdu, kad būtinos kitos administracinės priemonės, kurios, viena vertus, būtų veiksmingos ir tinkamos tinklais susietoje visuomenėje, ir, kita vertus, sumažintų administracines išlaidas*“ ([2]);

— antra, pasiūlymus dėl teisės aktų reikėtų teikti tik tuo atveju, jei yra pakankamų įrodymų, kad jie yra būtini ir kad laikomasi proporcingumo principo. Dėl šios priežasties artimiausioje ateityje nereikėtų keisti bendros duomenų apsaugos teisės sistemos;

— trečia, permaininga visuomenės raida gali lemti specifinių teisinių sistemų atsiradimą siekiant Duomenų apsaugos direktyvos principus pritaikyti prie konkrečių technologijų, pavyzdžiui, RDA, taikymo padarinių. Akivaizdu, kad ir šiuo atveju turi būti įvykdytos būtinumo ir proporcingumo sąlygos.

67. Toliau yra naudinga įvardyti lūkesčius, į kuriuos teisės aktų leidėjas turi atsižvelgti RDA srityje:

— teisės aktai turi pasižymėti lankstumu ir užtikrinti inovacijų bei technologinio vystymosi galimybes. Todėl teisės aktai turėtų būti pakankamai neutralūs technologijų atžvilgiu;

— antra, teisės aktuose reikia užtikrinti teisinį tikrumą. Todėl teisės aktai turėtų būti pakankamai konkretūs. Suinteresuotieji subjektai privalo tiksliai žinoti, kaip reglamentuojami jų veiksmai;

— trečia, teisės aktais turi būti veiksmingai užtikrinta visų atsiradusių pateisinamų interesų apsauga. Bet kuriuo atveju tam reikia vykdyti teisės aktus ir aiškiai apibrėžti atsakomybę: kuri šalis atsako už kokius veiksmus? ([3]) Šie reikalavimai yra ypač svarbūs tais atvejais, kai yra aktualūs privatumo ir duomenų apsaugos klausimai, asmens pagrindinės teisės pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją bei Europos Sąjungos pagrindinių teisių chartiją.

Europos duomenų apsaugos priežiūros pareigūno požiūris

68. Duomenų apsaugos priežiūros pareigūnui yra aišku, kad Europos teisės aktų leidėjas neturėtų reaguoti į visus technologijų pokyčius. Technologijos gali keistis sparčiai, o teisės aktams priimti ir įsigalioti reikia laiko, ir į tai turėtų būti atsižvelgiama. Teisės aktais turėtų būti užtikrinama visų interesų pusiausvyra. Kai pasirinkta priemonė yra direktyva, laiko reikia dar daugiau, kadangi direktyvas būtina visapusiškai įgyvendinti valstybių narių teisinėse sistemose.

69. Tačiau RDA – tai ne tik dar vienas technologinio vystymosi pavyzdys, kaip pabrėžiama keliose šios nuomonės vietose. Komisijos teigimu, RDA atveria vartus į naują informacinės visuomenės vystymosi etapą, dažnai vadinamą „daiktų internetu“, o RDA žymenys bus pagrindiniai „išmaniųjų“ terpių elementai. Tokios terpės taip pat yra svarbus žingsnis tam, kad vystytųsi dažnai vadinama „sekimo visuomenė“ ([4]). Todėl teisėkūros veiksmus RDA srityje galima pateisinti. RDA gali lemti kokybinius pokyčius.

([1]) Žr. siūlomą Direktyvos 2002/58 naują 3 straipsnį.
([2]) Nuomonės dėl komunikato dėl Duomenų apsaugos direktyvos 24 punktas.
([3]) Vartojant duomenų apsaugos terminus tai reiškia „duomenų valdytojo“ nustatymą.
([4]) Šis mintis buvo pakartota Londone 2006 m. lapkričio 2 d. priimtame Europos duomenų apsaugos institucijų pareiškime, kuris pateikiamas Europos duomenų apsaugos priežiūros pareigūno tinklavietėje adresu: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Šiuo požiūriu EDAPP rekomenduoja svarstyti, ar priimti Bendrijos teisės aktus, reglamentuojančius pagrindinius RDA naudojimo atitinkamuose sektoriuose klausimus (pasiūlymą dėl jų), jei nepavyktų tinkamai įgyvendinti galiojančios teisinės sistemos. Įsigaliojusi tokia teisės priemonė privalo būti laikoma *lex specialis* palyginti su bendrąja duomenų apsaugos sistema.

71. Tokios teisės priemonės priėmimas pasižymėtų šiais privalumais:

— šia priemone būtų galima nustatyti savireguliacijos mechanizmų esminius parametrus;

— teisės priemonės priėmimo perspektyva gali tapti veiksminga paskata suinteresuotiesiems subjektams sukurti savireguliacijos mechanizmus, užtikrinančius kruopščiai vykdomą apsaugą.

72. Praktiniais sumetimais Komisijos galėtų būti paprašyta parengti rekomendacijų dokumentą, apimantį argumentus už ir prieš konkrečius teisės aktus bei tokių teisės aktų pagrindines sudedamąsias dalis. Suinteresuotųjų subjektų neabejotinai gali būti paprašyta pateikti nuomonę dėl šios rekomendacijos. Šioje veikloje taip pat galėtų dalyvauti 29 straipsnio darbo grupė.

Galimos sąlygos

73. Teisės aktų leidėjui ėmusis veiksmų, gali būti sukurta speciali teisinė sistema, kurią sudarytų įvairios reguliavimo priemonės, patikslinančios ir papildančios galiojančią teisinę sistemą. Ši speciali teisinė sistema turėtų būti grindžiama žinomais duomenų apsaugos principais, o dėmesys joje turėtų būti sutelktas į atsakomybės pasidalijimą ir į kontrolės mechanizmų veiksmingumą.

74. Konkreti priežastis, kodėl gali būti reikalingi tokie specialūs teisės aktai, yra susijusi su tuo, kad ne visi RDA įrenginiai turi asmens duomenų tvarkymo funkciją. Kitaip tariant, jei naudojant RDA įrenginius asmens duomenys netvarkomi, RDA žymenis turinčių produktų gamyboje ir pardavime dalyvaujančios šalys nėra teisiškai įpareigotos įgyvendinti technologines priemones, kuriomis būtų užkirtas kelias slaptam pasiklausymui arba skaitytuvų įmontavimui asmenų tinkamai neinformavus. Vis dėlto, kaip įrodyta, tokių RDA įrenginių atveju taip pat kyla pavojus privatumui, nes galimas asmenų sekimas, todėl reikalingos panašios rūšies privatumo apsaugos priemonės. Konkretus pavyzdys galėtų būti žymenų tvirtinimas ant plataus vartojimo prekių *prieš* jas parduodant. Galima teigti, RDA įrenginiai, kuriuos naudojant asmens duomenys netvarkomi, vis dėlto gali kelti grėsmę asmenų privatumui, nes gali būti slapta sekama, o informacija naudojama nepriimtinais tikslais.

75. EDAPP nuomone, tokių netinkamų pasekmių reikėtų vengti. Kadangi galiojančiuose teisės aktuose, bent jau RDA įrenginių, kuriuos naudojant asmens duomenys netvarkomi, atveju, iš dalies nepavyko pasipriešinti privatumui kylančiai grėsmei ir atsižvelgiant į tai, kad neprivalomos teisės nuostatos nėra tinkamas sprendimas, atrodo, kad siekiant gero rezultato būtina naudoti privalomas teisės priemones.

76. Tokiomis priemonėmis bet kuriuo atveju reikėtų:

— nustatyti savanoriško sutikimo (*opt-in*) principą, taikomą pardavimo metu, kurio taikymas būtų laikomas aiškia ir neginčijama teisine pareiga, taip pat ir tais atvejais, kai RDA įrenginiams netaikoma Duomenų apsaugos direktyva ([1]).

— nustatyti, kad RDA įrenginiuose privaloma įdiegti tinkamas technines charakteristikas arba taikyti principą, kad į privatumą atsižvelgiama projektuojant.

VII. **VALDYMO KLAUSIMAS**

77. Nors komunikate RDA sistemų „savaime tarpvalstybinis“ aspektas aiškinamas tik vidaus rinkos požiūriu, EDAPP mano, kad šis aspektas turi būti nagrinėjamas labiau tarptautiniu lygiu. Parduotuvėje RDA sistemos jau yra „tarpvalstybinės“, kadangi žymuo gali veikti ir po pardavimo. Visos RDA sistemos lygiu šios technologijos taip pat įgauna „tarpvalstybinį pobūdį“, kai asmens duomenys gali būti perduoti į trečiąją šalį, kadangi prekės su RDA sistemos žymenimi gamintojo veiklos vieta yra už Europos Sąjungos ribų ([2]).

78. Žiūrint į ateitį, RDA tapatybės duomenų bazių valdymas taip pat yra itin svarbus aspektas tinkamai įgyvendinant Europos duomenų apsaugos teisinę sistemą. EDAPP ragina ieškoti sprendimo, kadangi tolesnis šios sistemos silpnėjimas būtų nepriimtinas.

79. EDAPP RDA valdymo klausimą laiko pagrindiniu uždaviniu, kuriam įvykdyti reikės nemažų investicijų. Siekiant tokioje tarptautinėje aplinkoje užtikrinti deramą pagarbą duomenų apsaugos teisėms, reikės sukurti tinkamą derybų forumą ir tinkamiausią valdymo infrastruktūrą.

([1]) IV skyriuje teigiama, kad „savanoriško sutikimo“ (*opt-in*) principo taikymas pardavimo metu yra teisinė pareiga, kuri jau yra numatyta Duomenų apsaugos direktyvoje.

([2]) Pareigos, susijusios su asmens duomenų perdavimu, numatytos Duomenų apsaugos direktyvos 25–26 straipsniuose.

80. Šiuo požiūriu EDAPP prašo Komisijos pateikti nuomonę valdymo klausimu, jei įmanoma, pasikonsultavus su RDA suinteresuotųjų subjektų grupe.

VIII. **IŠVADA**

81. EDAPP palankiai vertina Komisijos komunikatą dėl RDA, kadangi jame sprendžiami pagrindiniai klausimai, susiję su RDA technologijos įdiegimu, ir nepamirštama atsižvelgti į lemiamus su privatumu ir duomenų apsauga susijusius veiksnius. Jis pritaria nuomonei, kad RDA sistemos galėtų atlikti vieną iš pagrindinių vaidmenų informacinės visuomenės raidos etape, kuris dažnai vadinamas „daiktų internetu“.

Padarinių išaiškinimas

82. Platus RDA technologijos naudojimas yra iš esmės naujas reiškinys, galintis turėti lemiamos įtakos mūsų visuomenei ir pagrindinių teisių, pavyzdžiui, teisių į privatumą ir duomenų apsaugą, apsaugai mūsų visuomenėje. RDA gali lemti kokybinius pokyčius.

83. Galima išskirti penkis pagrindinius privatumo ir saugumo klausimus:

— duomenų subjekto nustatymas;

— duomenų valdytojo nustatymas;

— tradicinio asmeninės ir viešosios srities atskyrimo reikšmės sumažėjimas;

— RDA žymenų dydžio ir fizinių savybių lemiamos pasekmės;

— nepakankamas duomenų tvarkymo skaidrumas.

Padarinių įvardijimas

84. Direktyvoje 95/46/EB nustatyta duomenų apsaugą reglamentuojanti bendroji teisės sistema taikoma RDA, jei RDA sistemose tvarkomi duomenys atitinka asmens duomenų sąvokos apibrėžtį.

85. E. privatumo direktyvos klausimu 2007 m. lapkričio 13 d. Komisijos pasiūlyme dėl direktyvos pakeitimo įtraukta nuostata, kuria siekiama patikslinti, kad direktyva iš tikrųjų yra taikoma tam tikriems RDA įrenginiams. Tačiau tam tikriems kitiems RDA įrenginiams ši direktyva gali būti netaikoma, kadangi ji taikoma tik asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešuosiuose ryšių tinkluose.

86. Asmens duomenų apsaugą gali papildyti įvairios savireguliavimo priemonės. Tikslinga suteikti tokio savireguliavimo galimybes, jei:

— numatomi konkretūs ir įgyvendinami nurodymai, susiję su konkrečiais RDA įrenginių tipais;

— sprendžiami konkretūs duomenų apsaugos klausimai ir problemos, su kuriais susiduriama naudojant bendruosius RDA įrenginius;

— prisidedama prie vienodo ir suderinto Duomenų apsaugos direktyvos taikymo visoje ES;

— šias priemones taiko visi atitinkami suinteresuotieji subjektai.

87. EDAPP rekomenduoja Komisijai, glaudžiai bendradarbiaujant su RDA ekspertų grupe, parengti vieną ar kelis dokumentus, kuriuose būtų išdėstyti aiškūs nurodymai, kaip dabartinę teisinę sistemą taikyti RDA aplinkai.

88. Nurodymai, kuriuose būtų išdėstyti RDA naudojimui taikomi principai, turėtų būti pakankamai sukoncentruoti ir pagrįsti sektoriui pritaikytu metodu. Juose turėtų būti pasiūlyti praktiški ir veiksmingi *metodų ir standartų* kūrimo metodai, kurie galėtų būti naudingi užtikrinant RDA sistemų suderinimą su duomenų apsaugos teisine sistema ir kuriuos taikant būtų naudojamos projektuojant užtikrinančios privatumą technologijos.

89. EDAPP palankiai vertina Komisijos komunikate pateiktą siūlymą pritarti idėjai, kad reikia apibrėžti ir priimti išankstinius projektavimo kriterijus.

90. Nors, EDAPP nuomone, „savanoriško sutikimo“ (*opt-in*) principo taikymas pardavimo metu yra teisinė pareiga, jau numatyta Duomenų apsaugos direktyvoje daugeliu atvejų, šią pareigą reikėtų apibrėžti savireguliavimo priemonėmis.

Ar reikalingos konkrečios priemonės?

91. Tam, kad naudoti koncepciją „į privatumą atsižvelgiama projektuojant“ būtų privaloma, EDAPP rekomenduoja Komisijai, konsultuojantis su RDA ekspertų grupe, naudoti Direktyvos 99/5/EB 3 straipsnio 3 dalies c punkte nustatytą mechanizmą.

92. EDAPP rekomenduoja svarstyti, ar priimti Bendrijos teisės aktus, reglamentuojančius pagrindinius RDA naudojimo atitinkamuose sektoriuose klausimus (pasiūlymą dėl jų), jei nepavyktų tinkamai įgyvendinti galiojančios teisinės sistemos. Įsigaliojusi tokia teisės priemonė privalo būti laikoma *lex specialis* palyginti su bendrąja duomenų apsaugos sistema. Šiomis teisės priemonėmis turėtų būti sprendžiami ir susirūpinimą keliantys privatumo ir duomenų apsaugos klausimai, kylantys tam tikrų RDA įrenginių atvejais, pavyzdžiui, prekių žymėjimo žymenimis prieš pardavimą atveju, kai nebūtinai vykdomas asmens duomenų tvarkymas.

93. Komisija turėtų parengti rekomendacijų dokumentą, apimantį argumentus už ir prieš konkrečius teisės aktus bei tokių teisės aktų pagrindines sudedamąsias dalis.

94. Teisės aktų leidėjui ėmusis veiksmų, galėtų būti sukurta speciali teisinė sistema, kurią sudarytų įvairios reguliavimo priemonės, patikslinančios ir papildančios galiojančią teisinę sistemą. Priemonėmis bet kuriuo atveju reikėtų:

— nustatyti savanoriško sutikimo (*opt-in*) principą, taikomą pardavimo metu, kurio taikymas būtų laikomas aiškia ir neginčijama teisine pareiga, taip pat ir RDA įrenginių, kurie nepatenka į Duomenų apsaugos direktyvos taikymo sritį ([1]), atveju.

— nustatyti, kad RDA įrenginiuose privaloma įdiegti tinkamas technines charakteristikas arba taikyti principą, kad „į privatumą atsižvelgiama projektuojant“.

Valdymo klausimas

95. EDAPP prašo Komisijos pateikti nuomonę valdymo klausimu, jei įmanoma, pasikonsultavus su RDA suinteresuotųjų subjektų grupe.

Priimta 2007 m. gruodžio 20 d. Briuselyje.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas

([1]) IV skyriuje teigiama, kad „savanoriško sutikimo“ (*opt-in*) principo taikymas pardavimo metu yra teisinė pareiga, kuri jau yra numatyta Duomenų apsaugos direktyvoje.