I

(Rezoliucijos, rekomendacijos ir nuomonės)

NUOMONĖS

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl pasitikėjimo informacinėje visuomenėje skatinimo, stiprinant duomenų apsaugą ir privatumą

(2010/C 280/01)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

atsižvelgdamas į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 16 straipsnį,

atsižvelgdamas į Europos Sąjungos pagrindinių teisių chartiją, ypač į jos 7 ir 8 straipsnius,

atsižvelgdamas į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ([1]),

atsižvelgdamas į 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ([2]) su paskutiniais pakeitimais ,

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 ([3]),

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS

1. Informacinės ir ryšių technologijos (IRT) suteikia didžiulių galimybių beveik kiekvienoje mūsų gyvenimo srityje – naudodamiesi jomis mes dirbame, žaidžiame, bendraujame ir lavinamės. Jos turi esminės reikšmės šių dienų informacinei ekonomikai ir visuomenei apskritai.

2. Europos Sąjunga pasiekė pasaulinį lygį pažangiųjų IRT srityje ir yra pasiryžusi šį lygį išlaikyti. Siekdama susidoroti su šiuo iššūkiu, Europos Komisija netrukus turi priimti naują Europos skaitmeninę darbotvarkę, kuriai Komisijos narė N. Kroes patvirtino teikianti pirmenybę ([4]).

3. EDAPP pripažįsta IRT duodamą naudą ir sutinka, kad ES turi daryti viską, ką gali, kad skatintų jų plėtrą ir platų perėmimą. Jis taip pat visiškai pritaria Komisijos narių N. Kroes ir V. Reding nuomonėms, kad šioje naujoje aplinkoje svarbiausi turėtų būti asmenys ([5]). Asmenys turi turėti galimybę pasitikėti IRT gebėjimu saugoti jų informaciją ir kontroliuoti jos naudojimą, taip pat būti įsitikinę, kad jų privatumas ir duomenų apsaugos teisės skaitmeninėje erdvėje bus gerbiamos. Pagarba šioms teisėms turi esminės reikšmės, siekiant įgyti vartotojų pasitikėjimą. O toks pasitikėjimas turi esminės reikšmės, piliečiams norint naudotis naujomis paslaugomis ([6]).

([1]) OL L 281, 1995 11 23, p. 31.
([2]) OL L 201, 2002 7 31, p. 37.
([3]) OL L 8, 2001 1 12, p. 1.

([4]) Atsakymai į Europos Parlamento klausimyną Komisijos narei Neelie Kroes, vykstant EP klausymams, prieš paskiriant ją Komisijos nare.

([5]) Komisijos narės Neelie Kroes atsakymai į Europos Parlamento klausimyną, vykstant EP klausymams, prieš paskiriant ją Komisijos nare; Komisijos narės Viviane Reding kalba „Europos skaitmeninė darbotvarkė, skirta naujam skaitmeniniam vartotojui“, pasakyta BEUC įvairių suinteresuotųjų asmenų forume dėl vartotojų privatumo ir internetinės rinkodaros. Rinkos tendencijos ir politikos perspektyvos (*Multi-stakeholder Forum on Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives*), Briuselis, 2009 m. lapkričio 12 d.

([6]) Žr., pvz., RISEPTIS ataskaitą „Pasitikėjimas informacinėje visuomenėje“, Patariamosios tarybos ataskaita, RISEPTIS (Moksliniai tyrimai ir naujovės saugumo, privatumo ir pasitikėjimo informacinėje visuomenėje srityje). Ją galima rasti http://www.think-trust.eu/general/news-events/riseptis-report.html Taip pat žr. J. B Horrigan, „Broadband Adoption and Use in America“, FCC *Omnibus Broadband Initiative*, OBI darbo dokumentas, serija Nr. 1.

4. ES taikomi griežti duomenų apsaugos / privatumo srities teisės aktai, ir jų principai visiškai galioja skaitmeniniame amžiuje. Tačiau atsipalaiduoti negalima. Daugeliu atvejų IRT kelia naujų rūpesčių, į kuriuos esamuose teisės aktuose neatsižvelgta. Todėl reikalingi tam tikri veiksmai, siekiant užtikrinti, kad ES teisėje įtvirtintos asmenų teisės ir toliau užtikrintų veiksmingą apsaugą šioje naujoje aplinkoje.

5. Šioje nuomonėje aptariamos priemonės, kurias Europos Sąjunga galėtų remti arba kurių galėtų imtis, siekdama užtikrinti asmenų privatumą ir duomenų apsaugą globalizuotame pasaulyje, kuriam ir toliau įtakos turės naujos technologijos. Joje aptariamos su teisėkūra susijusios ir nesusijusios priemonės.

6. Apžvelgus IRT kaip naujovę, kuri ne tik suteikia galimybių, bet ir kelia grėsmių, šioje nuomonėje aptariamas poreikis praktiniu lygmeniu duomenų apsaugą ir privatumą integruoti nuo pat informacinių ir ryšių technologijų kūrimo pradžios (šis principas reiškia privatumo užtikrinimą projektuojant). Siekiant, kad šio principo būtų privalomai laikomasi, šioje nuomonėje aptariama būtinybė įtraukti privatumo užtikrinimo projektuojant principą į duomenų apsaugos teisės aktus bent dviem skirtingais būdais. Pirma, įtraukti jį kaip bendrąjį, privalomą principą, ir, antra, įtraukti jį į konkrečias IRT sritis, keliančias konkrečių grėsmių duomenų apsaugai ir (arba) privatumui, kurios gali būti sušvelnintos, kuriant tinkamą techninę struktūrą ir tinkamai projektuojant. Šios sritys yra radijo dažnių atpažinimas (RDA), socialinių tinklų programos ir naršyklių programos. Galiausiai šioje nuomonėje pateikiama siūlymų dėl kitų priemonių ir principų, kuriais siekiama apsaugoti asmens privatumą ir užtikrinti duomenų apsaugą IRT sektoriuje.

7. Nagrinėjant minėtus klausimus, nuomonėje plėtojami kai kurie 29 straipsnio darbo grupės nurodyti aspektai, kuriuos ji iškėlė dalyvaudama viešoje konsultacijoje dėl privatumo ateities ([1]). Joje taip pat papildomos ankstesnės EDAPP nuomonės, kaip antai 2007 m. liepos 25 d. nuomonė dėl Duomenų apsaugos direktyvos įgyvendinimo, 2007 m. gruodžio 20 d. nuomonė dėl RDA ir dvi jo nuomonės dėl E. privatumo direktyvos ([2]).

II. IRT SUTEIKIA NAUJŲ GALIMYBIŲ, TAČIAU KELIA IR NAUJŲ GRĖSMIŲ

8. IRT lyginamos su kitais svarbiais praeities išradimais, pvz., elektra. Nors gal vertinti jų tikrąjį istorinį poveikį dar per anksti, IRT ir ekonominio augimo ryšys išsivysčiusiose šalyse yra akivaizdus. IRT kuria darbo vietas, duoda ekonominę naudą ir prisideda prie bendros gerovės. IRT poveikis nėra vien ekonominis, nes jos turi esminės reikšmės skatinant naujoves ir kūrybiškumą.

9. Be to, IRT visiškai pakeitė žmonių darbo, bendravimo ir sąveikos būdus. Pavyzdžiui, žmonės vis dažniau pasikliauja IRT socialiniams ir ekonominiams ryšiams palaikyti. Asmenys gali naudotis įvairiausiomis naujomis IRT programomis, pvz., E. sveikatos, E. transporto, E. valdžios, taip pat naujoviškomis interaktyviosiomis pramogų ir mokymosi sistemomis.

10. Atsižvelgdamos į tokią naudą, visos Europos institucijos išreiškė įsipareigojimą remti IRT kaip būtiną priemonę Europos pramonės konkurencingumui gerinti ir Europos ekonomikos atsigavimui skatinti. Iš tikrųjų 2009 m. rugpjūčio mėn. Komisija priėmė Europos skaitmeninio konkurencingumo ataskaitą ([3]) ir pradėjo viešą konsultaciją dėl reikiamų būsimų IRT skatinimo strategijų. 2009 m. gruodžio 7 d. Taryba prisidėjo prie šios konsultacijos, priėmusi dokumentą „Informacinės visuomenės strategija po 2010 m. Siekiant atviros, ekologiškos ir konkurencingos žinių visuomenės“ ([4]). Europos Parlamentas visai neseniai

([1]) 29 straipsnio darbo grupės nuomonė Nr. 168 dėl privatumo ateities, bendras dalyvavimas Europos Komisijos konsultacijoje dėl pagrindinės teisės į asmens duomenų apsaugą teisės aktų, priimta 2009 m. gruodžio 1 d.

([2]) 2007 m. liepos 25 d. nuomonė dėl Komisijos komunikato Europos Parlamentui ir Tarybai dėl tolesnių veiksmų pagal Geresnio duomenų apsaugos direktyvos įgyvendinimo darbo programą, OL C 255, 2007 10 27, p. 1; 2007 m. gruodžio 20 d. nuomonė dėl Komisijos komunikato Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl radijo dažnių atpažinimo (RDA) Europoje: politikos sistemos formavimo veiksmai (COM(2007) 96), OL C 101, 2008 4 23, p. 1; 2008 m. balandžio 10 d. nuomonė dėl pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos, iš dalies keičiančios, be kita ko, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), OL C 181, 2008 7 18, p. 1; 2009 m. sausio 9 d. antroji nuomonė dėl Direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje peržiūros.

([3]) Europos skaitmeninio konkurencingumo ataskaita. Pagrindiniai 2010 m. strategijos pasiekimai 2005–2009 m. (SEC(2009) 1060).

([4]) Tarybos išvados „Informacinės visuomenės strategija po 2010 m. Siekiant atviros, ekologiškos ir konkurencingos žinių visuomenės“ (17107/09), priimta 2009 12 18.

priėmė pranešimą, kuriame siekiama pateikti gaires Komisijai, nustatant skaitmeninę darbotvarkę ([1]).

11. Kartu su IRT plėtra teikiamomis galimybėmis ir nauda atsiranda naujos grėsmės, visų pirma asmenų privatumui ir asmens duomenų apsaugai. Dėl IRT renkama, rūšiuojama, filtruojama, perduodama ar kitaip saugoma informacija neretai yra platinama (pakankamai dažnai asmenims nepastebimais būdais), todėl tokiems duomenims keleriopai padaugėja grėsmių.

12. Pvz., (kai kurių) vartojimo produktų brūkšniniai kodai keičiami RDA lustais. Gerinant informacijos srautą tiekimo grandinėje (ir taip mažinant „atsargų“ sandėlių poreikį, teikiant tikslesnes prognozes ir kt.), nauja sistema turėtų duoti naudos įmonėms ir vartotojams. Tačiau kartu atsiranda nerimą kelianti susekimo galimybė, kuria dėl pažymėto asmeninio turto įvairiais tikslais gali pasinaudoti įvairūs subjektai.

13. Kitas pavyzdys yra nuotoliniai ištekliai (angl. „cloud computing“), iš esmės – vartotojams ir ne vartotojams skirtų programų paslaugų pristatymas internetu. Tai yra ir foto bibliotekos, kalendoriai, internetinis paštas ir klientų duomenų bazės, taip pat sudėtingesnės su verslu susijusios paslaugos. Nauda verslui ir asmenims yra aiški; mažesnės sąnaudos (sąnaudos linkusios laipsniškai didėti), mažesnė priklausomybė nuo buvimo vietos (nesunkiai prieinama informacija bet kurioje pasaulio vietoje), automatizavimas (nebūtini specialūs IT ištekliai ir nuolatinis programinės įrangos atnaujinimas) ir kt. Kartu egzistuoja saugumo ir įsilaužimų grėsmė, kuri yra labai reali. Be to, rūpesčių kelia galimybė prarasti prieigą prie savo duomenų ir jų kontrolę.

14. Įrodyta, kad ir naudos, ir grėsmių yra ir kitose srityse, kuriose naudojamos IRT. Pavyzdžiui, E. sveikatos programa, kuri gali didinti veiksmingumą, mažinti sąnaudas, didinti prieinamumą ir bendrai gerinti sveikatos priežiūros paslaugų kokybę. Tačiau dėl E. sveikatos programos dažnai kyla šalutinio E. sveikatos informacijos naudojimo teisėtumo klausimas, todėl būtina atidžiai išanalizuoti bet kokio galimo šalutinio naudojimo tikslus ([2]). Be to, kadangi elektroniniai sveikatos įrašai naudojami vis plačiau, dėl pačių sistemų kyla nemažai skandalų, kurių metu atskleidžiama daug įsilaužimo į elektroninius sveikatos įrašus atvejų.

15. Apskritai tam tikras liekamosios grėsmės laipsnis gali būti, net ir atlikus tinkamus vertinimus ir taikant būtinas priemones. Tikėtis padėties, kur grėsmių visiškai nekyla, būtų naivu. Tačiau, kaip aptarta toliau, turi ir privalo būti įgyvendinamos tokios grėsmės sumažinimo iki atitinkamo lygio priemonės.

III. PRIVATUMO UŽTIKRINIMAS PROJEKTUOJANT KAIP PAGRINDINĖ PRIEMONĖ ASMENIMS PASITIKĖTI IRT

16. Galima IRT nauda galima mėgautis praktiškai tik tuomet, jei IRT gali kelti pasitikėjimą, kitaip tariant, jei jos gali užtikrinti naudotojo norą priklausyti nuo IRT dėl jų ypatybių ir teikiamos naudos. Toks pasitikėjimas gali būti įgytas, tik jei IRT yra patikimos, saugios, kontroliuojamos asmenų ir jei yra užtikrinama asmens duomenų ir privatumo apsauga.

17. Plačiai paplitusios pirmiau nurodytos grėsmės ir triktys, visų pirma, kai jos susijusios su neteisėtu asmens duomenų naudojimu ar pažeidimais ir asmenų privatumo atskleidimu, gali kelti pavojų naudotojų pasitikėjimui informacinėje visuomenėje. Tai galėtų rimtai pakenkti IRT plėtrai ir naudai, kurią jos gali teikti.

18. Tačiau šių grėsmių privatumui ir duomenų apsaugai negalima panaikinti, pašalinant galimybę naudotis IRT, neleidžiant jų naudoti ar atsisakant jas naudoti ar remti. Tai būtų ir praktiškai neįgyvendinama, ir nerealu; taip asmenys negalėtų gauti IRT teikiamos naudos ir būtų smarkiai apribota bendra gautina nauda.

19. EDAPP mano, kad būtų geriau kurti ir plėtoti IRT, paisant privatumo ir duomenų apsaugos. Todėl ypač svarbu, kad privatumas ir duomenų apsauga būtų diegiama per visą technologijos gyvavimo ciklą, nuo ankstyviausio projektavimo etapo iki galutinio įdiegimo, naudojimo ir galutinio utilizavimo. Paprastai tai vadinama privatumo užtikrinimu projektuojant ir aptariama toliau.

20. Privatumo užtikrinimas projektuojant gali būti susijęs su įvairiais veiksmais, priklausomai nuo konkretaus atvejo ar programos. Pavyzdžiui, kai kuriais atvejais gali reikėti pašalinti asmens duomenis ir (arba) sumažinti jų kiekį arba neleisti nebūtino ir (arba) nepageidaujamo tvarkymo. Kitais atvejais privatumo užtikrinimui projektuojant gali prireikti siūlyti priemones, skirtas didinti asmens atliekamą savo asmens duomenų kontrolę. Šias priemones reikėtų

([1]) Pranešimas dėl naujos Europos skaitmeninės darbotvarkės nustatymo. Nuo 2010 m. iki digital.eu (2009/2225 (INI)), priimtas 2010 3 18.

([2]) Pavyzdžiui, gydymo tikslais surinktos sveikatos informacijos pardavimas ar naudojimas negali būti priemonė pasirinkti satelitinių klinikų vietas, steigti ambulatorinės chirurgijos centrus ir kitaip planuoti būsimą veiklą, turinčią finansinio poveikio, ir tai reikėtų atidžiai ištirti.

apsvarstyti, nustatant standartus ir (arba) geriausią patirtį. Be to, jas galima įtraukti į informacijos ir ryšių sistemų struktūrą arba į asmens duomenis tvarkančių subjektų struktūrinį organizavimą.

III.1. **Privatumo užtikrinimo projektuojant principas, taikytinas įvairiose IRT aplinkose, ir jų poveikis**

21. Būtinybė taikyti privatumo užtikrinimo projektuojant principą iškyla daugelyje įvairių IRT aplinkų. Pavyzdžiui, sveikatos priežiūros sektorius vis dažniau naudoja IRT infrastruktūrą, o tai neretai reiškia centralizuotą su sveikata susijusios pacientų informacijos saugojimą. Norint taikyti minėtą principą sveikatos sektoriuje, reikėtų įvertinti įvairių priemonių, kaip antai galimybės iki minimumo sumažinti centriniu būdu saugomų duomenų kiekį arba jų apribojimo iki tam tikros rodyklės, naudojant šifravimo priemones, suteikiant prieigos teises griežtai pagal principą „būtina žinoti“, padarant duomenis anonimiškus, kai jie tampa nebereikalingi, ir kt., tinkamumą.

22. Transporto sistemose taip pat vis dažniau iš karto diegiamos pažangios IRT programos, įvairiais tikslais ir siekiant įvairių funkcijų sąveikaujančios su transporto priemone ir jos aplinka. Pavyzdžiui, automobiliuose vis dažniau įrengiama nauja IRT funkcija (GPS, GSM, jutiklių tinklai ir kt.), pagal kurią galima nustatyti ne tik automobilio buvimo vietą, bet ir jo techninę būklę realiuoju laiku. Ši informacija galėtų būti naudojama, pavyzdžiui, siekiant esamą kelių mokesčių sistemą pakeisti nuo naudojimo priklausoma kelių rinkliava. Taikant privatumo užtikrinimo projektuojant principą tuomet, kai kuriama tokių sistemų struktūra, turėtų būti siekiama, kad būtų tvarkoma ir toliau perduodama kuo mažiau asmens duomenų ([1]). Laikantis šio principo, vietoj centralizuotų struktūrų būtų geriau diegti decentralizuotas arba pusiau decentralizuotas struktūras, kurias naudojant, duomenys apie buvimo vietą būtų atskleidžiami tik centriniam punktui.

23. Minėti pavyzdžiai rodo, kad, jeigu informacinės ir ryšių technologijos kuriamos laikantis privatumo užtikrinimo projektuojant principo, grėsmes privatumui ir duomenų apsaugai galima gerokai sumažinti.

([1]) Žr. 2009 m. liepos 22 d. Europos duomenų apsaugos priežiūros pareigūno nuomonę dėl Komisijos komunikato „Pažangiųjų transporto sistemų diegimo Europoje veiksmų planas“ ir kartu pateikto pasiūlymo dėl Europos Parlamento ir Tarybos direktyvos, nustatančios kelių transporto ir jo sąsajų su kitų rūšių transportu srities intelektinių transporto sistemų diegimo sistemą, kurią galima rasti http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

III.2. **IRT, kurias projektuojant užtikrinamas privatumas, diegiama nepakankamai**

24. Svarbu tai, ar ūkio subjektai, IRT gamintojai ir (arba) tiekėjai ir duomenų valdytojai yra suinteresuoti pateikti rinkai ir IRT diegti privatumo užtikrinimo projektuojant principą. Šiomis aplinkybėmis taip pat svarbu įvertinti naudotojų paklausą privatumo užtikrinimui projektuojant.

25. 2007 m. Komisija išleido komunikatą, kuriame ragino įmones naudoti savo pajėgumus naujovių diegimo srityje ir kurti bei įgyvendinti PDT kaip būdą gerinti privatumo ir asmens duomenų apsaugą nuo pat vystymo ciklo pradžios ([2]).

26. Tačiau iki šiol gauti duomenys rodo, kad nei IRT gamintojai, nei duomenų valdytojai (privačiajame ar viešajame sektoriuje) nesugebėjo nuosekliai įgyvendinti privatumo užtikrinimo projektuojant principo ar įdiegti jo rinkoje. Motyvų nurodyta įvairių, įskaitant ekonominių paskatų ar institucijų paramos trūkumą, nepakankamą paklausą ir kt. ([3]).

27. Be to, privatumo užtikrinimas projektuojant nėra itin paklausus tarp naudotojų. IRT produktų ir paslaugų naudotojai gali pagrįstai manyti, kad jų privatumas ir asmens duomenys *de facto* yra apsaugoti, nors daugeliu atvejų taip nėra. Kai kada jie paprasčiausiai neturi galimybių imtis saugumo priemonių, būtinų savo ar kitų asmens duomenims apsaugoti. Daugeliu atvejų taip yra todėl, kad jiems visiškai arba iš dalies trūksta žinių apie grėsmes. Pavyzdžiui, apskritai jauni žmonės nepaiso grėsmių privatumui, susijusių su asmeninės informacijos rodymu socialiniuose tinkluose, ir dažnai ignoruoja privatumo nuostatas. Vis dėlto kiti naudojai apie šias grėsmes žino, tačiau gali neturėti reikiamos techninės patirties įdiegti apsaugos technologijas, pvz., apsaugančias jų interneto ryšį, arba gali nežinoti, kaip pakeisti naršyklės nuostatas, siekiant iki minimumo sumažinti skirstymą į profilius, stebint jų naršymo internete veiklą.

28. Vis dėlto grėsmės privatumo ir duomenų apsaugai yra labai tikros. Jei į privatumą ir duomenų apsaugą neatsižvelgiama nuo pat pradžių, ištaisyti sistemas paprastai būna pernelyg vėlu ir ekonomiškai sudėtinga, kaip ir per vėlu ištaisyti jau padarytą žalą. Vis daugiau duomenų saugumo pažeidimų pastaraisiais metais puikiai parodo šią

([2]) 2007 m. gegužės 2 d. Komisijos komunikatas Europos Parlamentui ir Tarybai dėl duomenų apsaugos stiprinimo naudojant privatumo didinimo technologijas (PDT), COM(2007) 228 galutinis.

([3]) Privatumo didinimo technologijų (PDT) ekonominės naudos tyrimas jls/2008/D4/036.

problemą ir didina poreikį taikyti privatumo užtikrinimo projektuojant principą.

29. Šie dalykai aiškiai rodo, kad asmens duomenų tvarkymui skirtų IRT gamintojai ir tiekėjai kartu su duomenų valdytojais turėtų būti įpareigoti jas kurti su įdiegtomis duomenų apsaugos ir privatumo garantijomis. Daugeliu atvejų tai reikštų, kad IRT turėtų būti kuriamos, diegiant privatumo garantijas numatytosiose nuostatose.

30. Tokiomis aplinkybėmis turime apsvarstyti, kokių veiksmų politikos kūrėjai turėtų imtis, kad kuriant IRT būtų skatinamas privatumo užtikrinimo projektuojant principo taikymas. Pirmas klausimas – ar esamuose duomenų apsaugos teisės aktuose yra pakankamai nuostatų, kurios užtikrintų, kad šį principą įgyvendintų ir duomenų valdytojai, ir gamintojai ir (arba) kūrėjai. Antrasis klausimas – ką reikėtų padaryti pagal Europos skaitmeninę darbotvarkę, siekiant užtikrinti, kad IRT sektorius įgytų vartotojų pasitikėjimą.

IV. **PRIVATUMO UŽTIKRINIMO PROJEKTUOJANT PRINCIPO ĮTVIRTINIMAS ES TEISĖS AKTUOSE IR POLITIKOJE**

IV.1. **Dabartiniai duomenų apsaugos ir privatumo srities teisės aktai**

31. ES, Direktyvoje 95/46/EB ([1]), Direktyvoje 2002/58/EB ([2]) ir Europos Žmogaus Teisių Teismo ([3]) bei Teisingumo Teismo jurisprudencijoje nustatyta griežta duomenų apsaugos ir privatumo sistema.

32. Duomenų apsaugos direktyva taikoma *bet kuriai operacijai ar operacijų rinkiniui, atliekamoms su asmens duomenimis* (rinkimui, saugojimui, atskleidimui ir kt.). Direktyvoje tvarkantiems asmens duomenis (duomenų valdytojams) nurodoma laikytis tam tikrų principų ir įpareigojimų. Joje nustatomos asmenų teisės, pvz., teisė susipažinti su asmenine informacija. E. privatumo direktyvoje konkrečiai reglamentuojamas privatumas elektroninių ryšių sektoriuje ([4])

33. Dabar galiojančioje Duomenų apsaugos direktyvoje nėra aiškaus reikalavimo dėl privatumo užtikrinimo projektuojant principo. Tačiau joje yra nuostatų, kuriose netiesiogiai, įvairiais atvejais, gali būti reikalaujama įgyvendinti šį principą. Visų pirma 17 straipsnyje reikalaujama, kad duomenų valdytojai įgyvendintų tinkamas technines ir organizacines priemones, skirtas apsaugoti nuo neteisėto duomenų tvarkymo ([5]). Todėl privatumo užtikrinimo projektuojant principas reglamentuojamas labai bendrai. Be to, direktyvos nuostatos iš esmės yra skirtos duomenų valdytojams ir jų atliekamam asmeninės informacijos tvarkymui. Jose nėra aiškaus reikalavimo, kad informacinės ir ryšių technologijos atitiktų privatumo ir duomenų apsaugos reikalavimus, nes tam reikia nurodyti IRT projektuotojus ir gamintojus, įskaitant standartizavimo etape atliekamą veiklą.

34. E. privatumo direktyvos nuostatos aiškesnės. Jos 14 straipsnio 3 dalyje numatyta: „Jeigu reikia, galima patvirtinti priemones, kurios užtikrintų, kad galinis įrenginys būtų suprojektuotas taip, kad jis būtų suderinamas su naudotojų teise apsaugoti ir kontroliuoti savo asmens duomenų naudojimą pagal Direktyvą 1999/5/EB ir 1986 m. gruodžio 22 d. Tarybos sprendimą 87/95/EEB dėl standartizacijos informacinių technologijų ir telekomunikacijų srityje“. Tačiau šia nuostata dar niekada nepasinaudota ([6]).

35. Nors minėtos abiejų direktyvų nuostatos padeda *skatinti* privatumo užtikrinimą projektuojant, praktiškai jų nepakanka *užtikrinti*, kad IRT būtų diegiamas privatumas.

36. Dėl tokios padėties teisės aktuose nepakankamai tiksliai reikalaujama, kad IRT būtų kuriamos pagal privatumo užtikrinimo projektuojant principą. Be to, duomenų

([1]) Europos Parlamento ir Tarybos direktyva 95/46/EB (toliau – Duomenų apsaugos direktyva).

([2]) Europos Parlamento ir Tarybos direktyva 2002/58/EB (toliau – E. privatumo direktyva).

([3]) 1950 m. lapkričio 4 d. Romoje priimtos Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (EŽTK) 8 straipsnyje nustatytų pagrindinių nuostatų ir sąlygų aiškinimas pagal tai, kaip jos taikomos įvairiose srityse.

([4]) Lisabonos sutartyje ši apsauga sustiprinta, ES pagrindinių teisių chartijos 7 ir 8 straipsniuose pagarbą privačiam gyvenimui ir asmens duomenų apsaugą pripažinus atskiromis pagrindinėmis teisėmis. ES pagrindinių teisių chartija tapo privaloma įsigaliojus Lisabonos sutarčiai.

([5]) 17 straipsnis: „Valstybės narės numato, kad duomenų valdytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami, ypač, kai tvarkomus duomenis tenka perduoti tinklu, taip pat apsaugoti nuo bet kokių kitų neteisėtų tvarkymo būdų“. 46 konstatuojamojoje dalyje šis straipsnis papildomas, nurodant: „kadangi dėl duomenų subjektų teisių ir laisvių apsaugos, tvarkant asmens duomenis reikia, kad būtų imamasi atitinkamų techninių ir organizacinių priemonių ir tuomet, kai kuriamos tvarkymo sistemos, ir tuomet, kai duomenys tvarkomi, ypač siekiant išlaikyti saugumą ir taip neleisti be leidimo tvarkyti duomenis“.

([6]) Komisija paskelbė apie planus iki 2010 m. pabaigos atnaujinti Direktyvą 1999/5/EB.

apsaugos institucijos neturi pakankamai įgaliojimų užtikrinti privatumo užtikrinimo projektuojant principo diegimą. Tai lemia neveiksmingumą. Pavyzdžiui, duomenų apsaugos institucijos gali taikyti sankcijas už nereagavimą į asmenų pateiktus prašymus leisti susipažinti su duomenimis ir jos turės įgaliojimų reikalauti įgyvendinti tam tikras priemones, skirtas neleisti neteisėto duomenų tvarkymo. Vis dėlto ne visada pakankamai aišku, ar jų įgaliojimai apima ir galimybę reikalauti, kad sistema būtų suprojektuota taip, kad būtų galima lengviau įgyvendinti asmenų duomenų apsaugos teises ([1]). Pavyzdžiui, pagal esamas teisės aktų nuostatas neaišku, ar galėtų būti reikalaujama informacinės sistemos struktūrą projektuoti taip, kad įmonėms būtų lengviau reaguoti į asmenų prašymus leisti susipažinti su duomenimis, idant šie prašymai būtų tvarkomi automatiškai ir greičiau. Be to, dėl tolesnių mėginimų pakeisti jau sukurtą ar įdiegtą technologiją susidarytų painiava, nes būtų daug sprendimų, kurie ne visiškai veikia ir, be to, yra ekonomiškai nenaudingi.

37. EDAPP nuomone, kuriai pritaria 29 straipsnio darbo grupė ([2]), pagal dabar galiojančius teisės aktus yra galimybė aiškiau įtvirtinti privatumo užtikrinimo projektuojant principą.

IV.2. **Privatumo užtikrinimo projektuojant principo diegimas įvairiais lygmenimis**

38. Atsižvelgdamas į tai, kas išdėstyta pirmiau, EDAPP rekomenduoja Komisijai laikytis keturių veiksmų krypčių:

a) siūlyti į duomenų apsaugos teisės aktus įtraukti bendrą nuostatą dėl privatumo užtikrinimo projektuojant;

b) pagal šią bendrą nuostatą parengti specialias nuostatas, siūlant skirtingiems sektoriams taikomus specialius teisės aktus. Šias specialias nuostatas jau dabar būtų galima įtraukti į teisės aktus; remiantis Duomenų apsaugos direktyvos 17 straipsniu (ir kitais galiojančiais teisės aktais);

c) įtraukti privatumo užtikrinimo projektuojant principą į Europos skaitmeninę darbotvarkę kaip pagrindinį principą;

d) įtraukti privatumo užtikrinimą projektuojant kaip principą į kitas ES iniciatyvas (daugiausia nesusijusias su teisėkūra).

Bendra nuostata dėl privatumo užtikrinimo projektuojant

39. EDAPP siūlo vienareikšmiai ir aiškiai įtraukti privatumo užtikrinimo projektuojant principą į esamus duomenų apsaugos teisės aktus. Taip privatumo užtikrinimo projektuojant principui būtų suteikta tvirtumo, aiškumo ir būtų priverčiama jį veiksmingai įgyvendinti, be to, vykdymo institucijos turėtų teisėtą pagrindą reikalauti *de facto* taikyti šį principą praktiškai. Visų pirma tai būtina, atsižvelgiant į pirmiau nurodytas aplinkybes, nes pats principas yra svarbus ne tik kaip priemonė pasitikėjimui skatinti, bet ir kaip paskata suinteresuotiesiems asmenims įgyvendinti privatumo užtikrinimo projektuojant principą ir didinti esamuose teisės aktuose numatytas garantijas.

40. Šiuo pasiūlymu papildoma 29 straipsnio darbo grupės rekomendacija nustatyti „privatumo užtikrinimo projektuojant principą“ kaip bendrąjį principą duomenų apsaugos teisės aktuose, visų pirma Duomenų apsaugos direktyvoje. Pasak 29 straipsnio darbo grupės, „šis principas turėtų būti privalomas technologijų projektuotojams ir gamintojams, o taip pat duomenų valdytojams, nusprendusiems įsigyti ir naudoti IRT. Jie turėtų būti įpareigoti atsižvelgti į technologinę duomenų apsaugą dar planuodami informacines-technologines procedūras ir sistemas. Tokių sistemų tiekėjai ar paslaugų teikėjai, taip pat duomenų valdytojai turėtų įrodyti, kad ėmėsi visų priemonių, būtinų šiems reikalavimams įvykdyti“.

41. EDAPP taip pat palankiai vertina tai, kad Komisijos narė Viviane Reding patvirtino privatumo užtikrinimo projektuojant principą, paskelbus Duomenų apsaugos direktyvos apžvalgą ([3]).

42. Tai nulemia tokio reguliavimo turinį. Visų pirma ir svarbiausia, bendrasis privatumo užtikrinimo projektuojant principas turėtų būti technologiškai neutralus. Šiuo principu neturėtų būti siekiama reguliuoti technologijų, t. y. jis neturėtų nustatyti konkrečių techninių sprendimų. Vietoj to pagal jį turėtų būti įpareigota esamus privatumo ir duomenų apsaugos principus integruoti į informacines ir ryšių sistemas bei sprendimus. Taip suinteresuotieji asmenys, gamintojai, duomenų valdytojai ir duomenų apsaugos institucijos galėtų kiekvienu konkrečiu atveju

([1]) Žr. JK *Information Commissioner's Office* ataskaitą „Privacy by Design“, paskelbtą 2008 m. lapkričio mėn.

([2]) Žr. 29 straipsnio darbo grupės nuomonę Nr. 168 dėl privatumo ateities, bendras dalyvavimas Europos Komisijos konsultacijoje dėl pagrindinės teisės į asmens duomenų apsaugą teisės aktų, priimtą 2009 m. gruodžio 1 d.

([3]) Privatumo užtikrinimo projektuojant principas – tai principas, kuriuo yra suinteresuoti ir piliečiai, ir įmonės. Dėl privatumo užtikrinimo projektuojant bus geriau apsaugoti asmenys, taip pat bus labiau pasitikima naujomis paslaugomis ir produktais, o tai savo ruožtu turės teigiamą poveikį ekonomikai. Jau yra įkvepiančių pavyzdžių, tačiau dar reikia daug padaryti. 2010 m. sausio 28 d., Duomenų apsaugos dieną pasakyta kalba, Europos Parlamentas, Briuselis.

aiškinti principo reikšmę. Antra, laikytis principo turėtų būti privaloma įvairiais etapais, nuo standartų kūrimo ir struktūros suprojektavimo, iki kol juos įgyvendina duomenų valdytojas.

Specialių teisės aktų nuostatos

43. Į dabartinius ir būsimus teisės aktus privatumo užtikrinimo projektuojant principas turi būti integruotas remiantis galiojančiais teisės aktais, o priėmus pirmiau pasiūlytą bendrąją nuostatą, remiantis šia nuostata. Pavyzdžiui, vadovaujantis dabartinėmis iniciatyvomis, susijusiomis su pažangiomis transporto sistemomis, Komisijai teks speciali pirminė atsakomybė apibrėžti priemones, standartizavimo iniciatyvas, procedūras ir geriausią patirtį. Įgyvendinant šiuos uždavinius, privatumo užtikrinimo projektuojant principas turėtų būti pagrindinis.

44. Be to, EDAPP pažymi, kad privatumo užtikrinimo projektuojant principas turi specialios reikšmės laisvės, saugumo ir teisingumo srityje, visų pirma Informacijos valdymo strategijos tikslų atžvilgiu, kaip numatyta Stokholmo programoje ([1]). Nuomonėje dėl Stokholmo programos EDAPP pabrėžė, kad keitimosi informacija architektūra turėtų būti grindžiama privatumo užtikrinimo projektuojant principu ([2]): „Tiksliau, tai reiškia, kad informacinės sistemos, kurios sukurtos siekiant užtikrinti visuomenės saugumą, visada turėtų būti kuriamos laikantis privatumo projektuojant principo“.

45. 29 straipsnio darbo grupės nuomonėje dėl privatumo ateities ([3]) dar tiksliau nurodoma, kad laisvės, saugumo ir teisingumo srityje, kur valdžios institucijos atlieka pagrindinį vaidmenį ir kur priežiūros didinimo priemonės turi tiesioginio poveikio pagrindinėms teisėms į privatumą ir duomenų apsaugą, privatumo užtikrinimo projektuojant reikalavimai turėtų būti privalomi. Nustačius šiuos reikalavimus informacinėse sistemose, valdžios institucijos taip pat paskatintų privatumo užtikrinimą projektuojant kaip pradedančiosios vartotojos.

Privatumo užtikrinimo projektuojant principas – pagrindinis Europos skaitmeninės darbotvarkės principas

46. Informacijos ir ryšių technologijos vis sudėtingėja ir kelia vis daugiau grėsmių privatumui ir duomenų apsaugai. Apskritai skaitmeninio formato informacijai, kurią lengviau gauti, kopijuoti ir perduoti, gresia daug daugiau pavojų, nei popieriuje esančiai informacijai. Pereinant prie tarpusavyje susietų objektų tinklų, šių grėsmių tik daugės. Kuo didesnė grėsmė privatumui ir (arba) duomenų apsaugai, tuo didesnis bus didesnių duomenų apsaugos ir (arba) privatumo garantijų poreikis. Todėl motyvai diegti privatumo užtikrinimo projektuojant principą yra svaresni IRT sektoriuje. Be to, kaip jau aptarta pirmiau, asmenų pasitikėjimas IRT yra esminis dalykas, norint, kad piliečiai naudotų šias naujas paslaugas, o privatumas ir duomenų apsauga yra pagrindiniai tokio pasitikėjimo elementai.

47. Tai rodo, kad IRT plėtros strategijoje turi būti patvirtintas poreikis kurti šias technologijas su neatsiejamu privatumo ir duomenų apsaugos elementu, t. y. atsižvelgiant į privatumo užtikrinimo projektuojant principą.

48. Todėl Europos skaitmeninėje darbotvarkėje privatumo užtikrinimo projektuojant principas turėtų būti aiškiai įtvirtintas kaip būtinas elementas, skirtas užtikrinti piliečių pasitikėjimą IRT ir internetu teikiamomis paslaugomis. Joje turėtų būti pripažinta, kad privatumas ir pasitikėjimas yra neatsiejami dalykai ir kad privatumo užtikrinimas projektuojant turėtų būti orientyras plėtojant pasitikėjimą keliantį IRT sektorių.

Privatumo užtikrinimas projektuojant kaip principas kitose ES iniciatyvose

49. Komisija turėtų laikyti privatumo užtikrinimą projektuojant pagrindiniu principu įgyvendindama politiką, veiklą ir iniciatyvas konkrečiuose IRT sektoriuose, įskaitant e. sveikatą, e. pirkimus, e. socialinį saugumą, e. mokymąsi ir kt. Dauguma šių iniciatyvų bus Europos skaitmeninės darbotvarkės veiksmų punktai.

50. Tai reiškia, pavyzdžiui, jog į iniciatyvas, skirtas užtikrinti didesnį valdžios programų veiksmingumą ir šiuolaikiškumą, kad asmenys galėtų bendrauti su administracija, turėtų būti įtrauktas reikalavimas jas projektuoti ir eksploatuoti pagal privatumo užtikrinimo projektuojant principą. Tas pats taikytina Komisijos politikai ir veiklai, kuria siekiama greitesnio interneto, skaitmeninio turinio arba bendrai skatinti fiksuotus ir belaidžius ryšius bei duomenų perdavimą.

([1]) Stokholmo programa. Atvira ir saugi Europa piliečių labui ir saugumui. Patvirtinta Europos Vadovų Tarybos 2009 m. gruodžio mėn.

([2]) 2009 m. liepos 10 d. nuomonė dėl Komisijos komunikato Europos Parlamentui ir Tarybai „Laisvės, saugumo ir teisingumo erdvė piliečių labui“ OL C 276, 2009 11 17, p. 8, 60 punktas.

([3]) 29 straipsnio darbo grupės nuomonė Nr. 168 dėl privatumo ateities, bendras dalyvavimas Europos Komisijos konsultacijoje dėl pagrindinės teisės į asmens duomenų apsaugą teisės aktų, priimta 2009 m. gruodžio 1 d.

51. Tai taip pat apima sritis, kuriose Komisija yra atsakinga už didelės apimties IT sistemas, kaip antai SIS ir VIS, taip pat tuos atvejus, kai Komisija yra atsakinga tik už tokios sistemos, pvz., Europos nuosprendžių registrų informacinės sistemos (ECRIS), bendros infrastruktūros plėtojimą ir priežiūrą.

52. Tai, kaip tiksliai bus plėtojamas privatumo užtikrinimo projektuojant principas, priklausys nuo kiekvieno konkretaus sektoriaus ir aplinkybių. Pavyzdžiui, kai kartu su Komisijos iniciatyvomis pateikiami teisės aktų pasiūlymai dėl konkretaus IRT sektoriaus, daugeliu atveju būtų gerai įtraukti aiškią nuorodą į privatumo užtikrinimo projektuojant sąvoką, taikomą konkrečios IRT programos arba sistemos projektavimui. Rengiant konkrečios srities veiksmų planus, juose turėtų būti sistemingai užtikrintas teisės aktų taikymas, o konkrečiau – nustatytos garantijos, kad atitinkama IRT technologija bus kuriama, atsižvelgiant į privatumo užtikrinimą projektuojant.

53. Kalbant apie mokslinius tyrimus, Septintoji bendroji programa ir vėlesnės programos turėtų būti naudojamos kaip priemonė remti projektams, kuriais siekiama analizuoti standartus, IRT technologijas ir struktūrą, kuri geriau užtikrina privatumą ir ypač privatumo užtikrinimo projektuojant principą. Be to, privatumo užtikrinimas projektuojant turėtų būti būtinas dalykas, į kurį reikėtų atsižvelgti platesniuose IRT projektuose, kuriais siekiama tvarkyti asmens duomenis.

Ypatingą susirūpinimą keliančios sritys

54. Kai kuriais atvejais dėl konkrečių grėsmių asmenų privatumui ir duomenų apsaugai arba dėl kitų veiksnių (pramonės nenoro tiekti privatumo užtikrinimo projektuojant produktus, vartotojų paklausos ir kt.) gali reikėti teisės aktuose arba kitais būdais nustatyti aiškesnes ir konkretesnes privatumo užtikrinimo projektuojant priemones, kurios privalo būti įtrauktos į konkrečios rūšies informacinį ir ryšių produktą arba technologiją.

55. EDAPP nustatė įvairias sritis (RDA, socialinių tinklų kūrimas ir naršyklės programos), kurias, jo nuomone, šiame etape Komisija turėtų atidžiai apsvarstyti ir kurių atveju reikėtų daugiau realaus įsikišimo, kuris minėtas pirmiau. Šios trys sritys aptariamos toliau.

V. **RADIJO DAŽNIŲ ATPAŽINIMAS (RDA)**

56. RDA žymenys gali būti integruoti į objektus, gyvūnus ir žmones. Jie gali būti naudojami asmens duomenims, kaip antai medicininiams įrašams, rinkti ir saugoti, atsekti žmogaus judėjimą arba įvairiais tikslais apibūdinti jų elgesį. Tą galima daryti, asmeniui apie tai nežinant ([1]).

57. Veiksmingos duomenų apsaugos, privatumo ir visų susijusių etinių dalykų garantijos yra ypač svarbios, kad visuomenė pasitikėtų RDA ir daiktų interneto ateitimi. Tik tuomet technologija gali teikti didelę ekonominę ir visuomeninę naudą.

V.1. **Galiojančių duomenų apsaugos teisės aktų spragos**

58. Duomenų apsaugos direktyva ir E. privatumo direktyva taikomos duomenų rinkimui, atliekamam naudojant RDA programas ([2]). Pagal jas, be kita ko, eksploatuojant RDA programas reikalaujama atitinkamų privatumo garantijų ([3]).

59. Tačiau šiuose teisės aktuose ne visiškai išspręsti visi šios technologijos keliami duomenų apsaugos ir privatumo srities rūpesčiai. Taip yra todėl, kad direktyvos nėra pakankamai išsamios garantijų, kurios turėtų būti diegiamos, kuriant RDA programas, požiūriu. Esamas taisykles reikėtų papildyti, nustatant konkrečias garantijas, visų pirma – privalomą reikalavimą RDA technologijose diegti

([1]) RDA – radijo dažnių atpažinimas. Svarbiausios radijo dažnių atpažinimo technologijos *arba* infrastruktūros sudedamosios dalys yra *žymuo* (t. y. mikrolustas), skaitytuvas ir programa, susieta su žymenimis ir skaitytuvais, naudojant tarpinę programinę įrangą ir tvarkant pateiktus duomenis. Žymenį sudaro elektroninė grandinė, kurioje saugomi duomenys ir kurioje yra antena, perduodanti duomenis radijo bangomis. Skaitytuvas turi anteną ir demoduliatorių, kuris paverčia radijo ryšiu perduodamą analoginę informaciją skaitmeniniais duomenimis. Tuomet informacija gali būti siunčiama tinklais į duomenų bazes ir serverius, kad ją apdorotų kompiuteris.

([2]) E. privatumo direktyvoje RDA paminėtas 3 straipsnyje: „Ši direktyva taikoma asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais Bendrijoje, įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius“. Šią nuostatą papildo 56 konstatuojamoji dalis: „Technologijų pažanga suteikia galimybę kurti naujas programas, grindžiamas duomenų rinkimo ir identifikavimo įrenginiais, kurie galėtų būti radijo dažnius naudojantys bekontakčiai įrenginiai. Pavyzdžiui, radijo dažnių atpažinimo įrenginiai (RFID) naudoja radijo dažnius duomenims nuskaityti iš vienareikšmiškai identifikuojamų žymenų, , o duomenys po to gali būti perduodami esamais ryšių tinklais. Plačiai naudojant tokias technologijas, jei piliečiai tam pritartų, gali būti sukurta didelė ekonominė ir socialinė nauda ir tokiu būdu svariai prisidėta prie vidaus rinkos plėtojimo. To siekiant būtina užtikrinti, kad būtų apsaugotos visos pagrindinės asmens teisės, pirmiausia teisės į privatumą ir duomenų apsaugą. Kai tokie įrenginiai prijungiami prie viešųjų elektroninių ryšių tinklų arba naudojasi elektroninių ryšių paslaugomis kaip pagrindine infrastruktūra, turėtų būti taikomos atitinkamos Direktyvos 2002/58/EB (Direktyvos dėl privatumo ir elektroninių ryšių) nuostatos, įskaitant nuostatas dėl saugumo, srauto ir vietos nustatymo duomenų bei konfidencialumo“.

([3]) Pavyzdžiui, Duomenų apsaugos direktyvos 17 straipsnyje nustatytas įpareigojimas įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar neteisėtai atskleisti.

techninius sprendimus (privatumo užtikrinimą projektuojant). Tai taikytina žymenims, kuriuose saugoma asmeninė informacija, nes juose turėtų būti pašalinimo komandos, o žymenyse, kuriuose saugoma tam tikrų rūšių asmeninė informacija, turėtų būti naudojama kriptografija.

V.2. **Savireguliavimas kaip pirmas žingsnis**

60. 2007 m. kovo mėn. Komisija priėmė komunikatą ([1]), kuriuo, be kita ko, pripažino poreikį nustatyti išsamias gaires dėl praktinio RDA įgyvendinimo ir norą patvirtinti projektavimo kriterijus, siekiant išvengti grėsmių privatumui ir saugumui.

61. Norėdama pasiekti šiuos tikslus, 2009 m. gegužės mėn. Komisija priėmė rekomendaciją dėl privatumo ir duomenų apsaugos principų įgyvendinimo RDA programose ([2]). Mažmeninėje prekyboje naudojamose RDA programose reikalaujama padaryti žymenį neveiksmingą pardavimo vietoje, nebent asmuo sutinka, kad žymuo išliktų veiksmingas. Tokia tvarka taikoma, nebent, atlikus poveikio privatumui ir duomenų apsaugai vertinimą, įrodoma, kad žymenys nekelia galimos grėsmės privatumui arba asmens duomenų apsaugai, nes tokiu atveju jie gali toliau veikti ir produktą pardavus, tačiau asmenys gali nuspręsti nemokamai šiuos žymenis pašalinti.

62. EDAPP pritaria Komisijos nuomonei naudoti savireguliavimo priemones. Tačiau, kaip aprašyta toliau, suprantama, kad savireguliavimas neduos numatomų rezultatų; todėl jis ragina Komisiją būti pasirengus imtis alternatyvių priemonių.

V.3. **Rūpestį keliančios sritys ir galimos papildomos priemonės, jei savireguliavimas nepasiteisintų**

63. EDAPP kelia rūpestį tai, kad RDA programas mažmeniniame sektoriuje eksploatuojančios organizacijos gali nepastebėti, jog RDA žymenis gali stebėti nepageidaujami tretieji asmenys. Atliekant tokį stebėjimą, gali būti atskleisti žymenyje saugomi (jei saugomi) asmens duomenys, tačiau trečiasis asmuo taip pat gali sekti ar atpažinti asmenį, tiesiog naudodamas unikaliuosius atpažinimo kodus, esančius viename ar daugiau asmens nešiojamų žymenų, tokioje aplinkoje, kurios netgi neapima RDA programos veiklos perimetras. Be to, rūpestį jam kelia ir tai, kad RDA programas eksploatuojantiems asmenims gali kilti pagunda nepagrįstai pasinaudoti išimtimi ir palikti žymenį veiksmingą pardavus produktą.

64. Jei taip nutiktų, sušvelninti grėsmes asmenų duomenų apsaugai ir privatumui, kuriems jau gali būti padarytas neigiamas poveikis, gali būti per vėlu. Be to, atsižvelgiant į savireguliavimo pobūdį, nacionalinės vykdymo institucijos gali turėti mažiau galimybių reikalauti RDA programas eksploatuojančių organizacijų taikyti konkrečias privatumo užtikrinimo projektuojant priemones.

65. Atsižvelgdamas į tai, kas nurodyta, EDAPP ragina Komisiją būti pasirengusią siūlyti teisės aktus, kuriais būtų reglamentuojami svarbiausi RDA naudojimo klausimai, jei esamų teisės aktų nebūtų įmanoma veiksmingai įgyvendinti. Komisijos vertinimo nereikėtų nepagrįstai atidėlioti; jei būtų atidėliojama, kiltų grėsmė asmenims ir būtų pakenkta pramonės produktyvumui, nes teisinis netikrumas yra pernelyg didelis, o problemų gali tik padaugėti ir jų ištaisymas kainuotų pernelyg brangiai.

66. Tarp priemonių, kurias gali reikėti siūlyti, EDAPP rekomenduoja nustatyti pasirinkimo pardavimo vietoje principą, pagal kurį visi prie vartojimo produktų pritvirtinti RDA žymenys pagal bendrą taisyklę būtų padaromi neveiksmingais pardavimo vietoje. Komisijai nebūtina ir nereikia nurodyti konkrečios technologijos, kurią reikia naudoti. Europos Sąjungos teisėje turi būti teisiškai įtvirtinta pareiga gauti sutikimą, paliekant subjektams laisvę nuspręsti, kokiais būdais įvykdyti šį reikalavimą.

V.4. **Kiti svarstytini klausimai. Daiktų interneto valdymas**

67. RDA žymenų teikiama informacija, pvz., informacija apie produktą, gali būti prijungta prie pasaulinio ryšių infrastruktūros tinklo. Tai paprastai vadinama „daiktų internetu“. Duomenų apsaugos arba privatumo klausimai kyla todėl, kad RDA žymenys gali atpažinti realius pasaulio objektus, kuriuose, be produkto informacijos, gali būti asmens duomenų.

68. Kyla daug neatsakytų klausimų dėl to, kas valdys informacijos, susijusios su pažymėtais daiktais, saugojimą. Kaip jis bus organizuojamas? Kas galės su šia informacija susipažinti? 2009 m. birželio mėn. Komisija priėmė komunikatą dėl daiktų interneto ([3]), kuriame aiškiai įvardytos galimos duomenų apsaugos ir privatumo problemos, kurių gali kelti šis reiškinys.

([1]) 2007 m. kovo 15 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Radijo dažnių atpažinimas (RDA) Europoje: politikos sistemos formavimo veiksmai, COM(2007) 96 galutinis.

([2]) 2009 m. gegužės 12 d. Komisijos rekomendacija dėl privatumo ir duomenų apsaugos principų įgyvendinimo taikomosiose priemonėse, kurių naudojimas pagrįstas radijo dažniniu atpažinimu (C(2009) 3200 galutinis).

([3]) Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Daiktų internetas. Europos veiksmų planas, 2009 6 18, COM(2009) 278 galutinis.

69. EDAPP norėtų pabrėžti kai kuriuos komunikate iškeltus klausimus, kuriems, jo nuomone, reikėtų skirti daug dėmesio, plėtojant daiktų internetą. Pirma, dėl poreikio diegti decentralizuotas struktūras gali būti lengviau užtikrinti atsakomybę ir ES teisės aktų įgyvendinamumą. Antra, turi būti kuo labiau saugoma asmenų teisė nebūti sekamiems. Kitaip tariant, turi būti labai nedaug atvejų, kai asmenys būtų sekami naudojant RDA žymenis be jų sutikimo. Toks sutikimas turėtų būti aiškus. Paprastai tai vadinama „lustų tylėjimu“ ir teise būti netrukdomam. Galiausiai, projektuojant daiktų internetą, privatumo užtikrinimo projektuojant principas turėtų būti pagrindinis. Pavyzdžiui, šiuo tikslu reikės, kad konkrečios RDA programos, kuriose įmontuoti kontrolę naudotojams suteikiantys mechanizmai, būtų kuriamos, padarant privatumo nuostatas numatytosiomis.

70. EDAPP tikisi, kad, Komisijai įgyvendinant komunikate numatytus veiksmus, visų pirma rengiant komunikatą dėl privatumo ir pasitikėjimo universalioje informacinėje visuomenėje, su juo bus pasikonsultuota.

VI. **SOCIALINIAI TINKLAI IR NUMATYTŲJŲ PRIVATUMO NUOSTATŲ POREIKIS**

71. Socialiniai tinklai yra „mėnesio tendencija“. Jie pasirodė esą populiaresni už elektroninį paštą. Jie tarpusavyje sujungia panašių interesų turinčius ir (arba) panašia veikla užsiimančius asmenis. Žmonės gali susikurti savo profilius internete ir dalytis rinkmenomis, pvz., vaizdo medžiaga, nuotraukomis, muzika, o taip pat savo karjeros profiliais.

72. Jaunimas greitai priėmė socialinius tinklus ir ši tendencija tęsiasi. Vidutinis interneto naudotojų amžius Europoje per pastaruosius kelis metus sumažėjo: dabar devynmečiai ir dešimtmečiai prisijungia prie interneto keletą kartų per savaitę, dvylikamečiai – keturiolikmečiai prisijungia kasdien, paprastai – nuo vienos iki trijų valandų.

VI.1. **Socialiniai tinklai bei duomenų apsaugos ir privatumo srityje galiojantys teisės aktai**

73. Dėl socialinių tinklų plėtros naudotojai įgijo galimybę į internetą įkelti informaciją apie save ir trečiuosius asmenis. Tai darydami, pasak 29 straipsnio darbo grupės ([1]), interneto naudotojai veikia kaip duomenų valdytojai pagal Duomenų apsaugos direktyvos ex 2 straipsnio d punktą jų įkeliamų duomenų atžvilgiu ([2]). Tačiau daugeliu atvejų tokiam tvarkymui taikoma direktyvos ex 3 straipsnio 2 dalies išimtis. Kartu socialinių tinklų kūrimo paslaugos prilygsta duomenų valdytojams, nes jomis suteikiama galimybė tvarkyti naudotojų duomenis ir teikiamos visos su naudotojo valdymu susijusios pagrindinės paslaugos (pvz., paskyrų registravimas ir ištrynimas).

74. Teisiškai tai reiškia, kad interneto naudotojams ir socialinių tinklų operatoriams kaip „duomenų valdytojams“, kaip apibrėžta direktyvos 2 straipsnio d punkte, tenka bendra atsakomybė už asmens duomenų tvarkymą, tačiau šios atsakomybės laipsnis ir įsipareigojimai yra skirtingi.

75. Todėl naudotojai turėtų žinoti ir suvokti, kad, jiems tvarkant asmeninę savo ir kitų asmenų informaciją, jiems taikomos ES duomenų apsaugos teisės aktų nuostatos, pagal kurias reikalaujama, be kita ko, gauti tų asmenų, kurių informacija yra įkeliama, laisvą sutikimą ir suteikti suinteresuotiesiems asmenims teisę ištaisyti jų duomenis, prieštarauti ir kt. Be to, teikiant socialinių tinklų paslaugas, turi būti diegiamos atitinkamos techninės ir organizacinės priemonės, skirtos neleisti neteisėto tvarkymo, atsižvelgiant į grėsmes, kurias kelia tvarkymas ir duomenų pobūdis. Tai savo ruožtu reiškia, kad teikiant socialinių tinklų paslaugas turi būti užtikrintos privatumą garantuojančios numatytosios nuostatos, įskaitant nuostatas, kuriomis ribojama prieiga per profilį prie paties naudotojo pasirinktų kontaktų. Nuostatose taip pat turėtų būti reikalaujama naudotojo patvirtinamojo sutikimo dėl to, ar profilis būtų prieinamas tretiesiems asmenims, o ribotos prieigos profilių neturi būti galima surasti naudojant vidaus paieškos priemones.

76. Deja, tarp teisinių reikalavimų ir faktinio jų vykdymo yra atotrūkis. Nors teisiškai interneto naudotojai laikomi duomenų valdytojais ir jiems taikomi ES duomenų apsaugos ir privatumo teisės aktai, iš tikrųjų jie neretai apie šią savo funkciją nežino. Apskritai jie menkai išmano apie tai, kad tvarko asmens duomenis ir kad skelbiant tokią informaciją kyla privatumo ir duomenų apsaugos grėsmių. Visų pirma medžiagą internete skelbia jaunuoliai, nepakankamai įvertinę padarinius sau ir kitiems. Šiuo padarinius jie pajunta vėliau, pavyzdžiui, studijuodami švietimo įstaigose arba ieškodami darbo.

([1]) Žr. 29 straipsnio darbo grupės nuomonę Nr. 163, 5/2009 dėl internetinių socialinių tinklų, priimtą 2009 m. birželio 12 d.

([2]) „Duomenų valdytojas“ – juridinis asmuo, valstybės valdžios institucija, agentūra ar kitas organas, kuris vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir būdus; jei tvarkymo tikslai ir būdai yra nustatyti nacionalinėje ar Bendrijos teisėje, duomenų valdytojas ar konkretūs jo skyrimo kriterijai gali būti nustatyti nacionalinėje arba Bendrijos teisėje.

77. Kartu socialinių tinklų operatoriai neretai iš anksto parenka numatytąsias nuostatas, remdamiesi nesutikimais, ir taip palengvindami asmeninės informacijos atskleidimą. Tai kelia klausimų, ar asmenys iš tikrųjų sutiko su atskleidimu, ir ar socialiniai tinklai laikosi direktyvos 17 straipsnio (aprašyto pirmiau), kuriame reikalaujama, kad jie diegtų tinkamas technines ir organizacines priemones, skirtas apsaugoti nuo neteisėto tvarkymo.

VI.2. **Socialinių tinklų keliamos grėsmės ir pasiūlymai, kaip šias grėsmes šalinti**

78. Dėl pirmiau nurodytų dalykų daugėja grėsmių asmens privatumui ir duomenų apsaugai. Dėl to interneto naudotojai ir asmenys, kurių duomenys įkeliami, gali susidurti su šiurkščiais jų privatumo ir duomenų apsaugos pažeidimais.

79. Tokiomis aplinkybėmis Komisija turėtų nuspręsti, ką reikėtų ir ką galima būtų padaryti šiai padėčiai pakeisti. Šioje nuomonėje išsamaus atsakymo į šį klausimą nepateikiama, tačiau pateikiami tam tikri svarstytini siūlymai.

Investavimas į interneto naudotojų švietimą

80. Pirmasis siūlymas – investuoti į naudotojų švietimą. Šiuo atžvilgiu ES ir nacionalinės institucijos turėtų investuoti į švietimą ir informuotumo apie socialinių tinklų interneto svetainių keliamas grėsmes didinimą. Pavyzdžiui, Informacinės visuomenės generalinis direktoratas sukūrė Saugesnio interneto programą, kuria vaikams ir jauniems žmonėms siekiama suteikti teisių ir juos apsaugoti, pavyzdžiui, vykdant informuotumo didinimo veiklą ([1]). Neseniai ES institucijos pradėjo kampaniją „Pagalvok prieš skelbdamas“, kad didintų informuotumą apie dalijimąsi asmenine informacija su nepažįstamaisiais.

81. EDAPP ragina Komisiją toliau remti šio pobūdžio veiklą. Tačiau socialinių tinklų operatoriai ir patys turėtų būti aktyvūs, nes jiems tenka teisinė ir socialinė atsakomybė šviesti naudotojus dėl to, kaip saugiai ir nepažeidžiant privatumo naudotis jų paslaugomis.

82. Kaip aprašyta pirmiau, skelbiant informaciją socialiniuose tinkluose, ją galima padaryti prieinamą pagal numatytąsias nuostatas įvairiais būdais. Pavyzdžiui, informacija gali būti prieinama visuomenei apskritai, įskaitant paieškos priemones, kurios gali šią informaciją registruoti ir taip pateikti į ją tiesiogines nuorodas. Kita vertus, informacija gali būti apribota „pasirinktais draugais“ arba saugoma visiškai privačiai. Akivaizdu, kad profilio leidimai ir vartojama terminologija skiriasi, priklausomai nuo interneto svetainės.

83. Tačiau, kaip nurodyta pirmiau, labai nedaug socialinių tinklų paslaugų naudotojų žino, kaip kontroliuoti prieigą prie jų skelbiamos informacijos, nepaisant to, kaip pakeisti numatytąsias privatumo nuostatas. Privatumo nuostatos paprastai lieka nepakeistos, nes naudotojai nežino apie jų nepakeitimo padarinius arba nežino, kaip jas pakeisti. Todėl dažniau privatumo nuostatų nepakeitimas nereiškia, kad asmenys laisvai priėmė sprendimą sutikti dalytis informacija. Tokiomis aplinkybėmis ypač svarbu, kad tretieji asmenys, kaip antai paieškos priemonės, nesusietų su atskirais profiliais pagal prielaidą, kad naudotojai išreiškė sutikimą pagal numatytąsias nuostatas (nepakeitę savo privatumo nuostatų) padaryti informaciją neribotai prieinamą.

84. Nors naudotojų švietimas gali padėti pakeisti šią padėtį, tai neįvyks savaime. Kaip 29 straipsnio darbo grupė rekomendavo savo nuomonėje dėl socialinių tinklų, socialinių tinklų operatoriai turėtų siūlyti privatumo nepažeidžiančias, nemokamas numatytąsias privatumo nuostatas. Taip naudotojai daugiau žinotų apie savo veiksmus ir galėtų geriau pasirinkti, ar jie nori dalytis informacija, ir su kuo jie nori tai daryti.

Savireguliavimo vaidmuo

85. Komisija sudarė susitarimą su dvidešimčia socialinių tinklų operatorių, vadinamą „Saugesnių socialinių tinklų principai ES“ ([2]). Susitarimo tikslas – gerinti nepilnamečių saugumą, naudojant socialinių tinklų interneto svetaines Europoje. Tarp šių principų yra daug reikalavimų, kylančių taikant pirmiau aprašytus duomenų apsaugos teisės aktus. Tai, pavyzdžiui, yra reikalavimas suteikti naudotojams teises per priemones ir technologijas, užtikrinti, kad jie galėtų kontroliuoti jų asmeninės informacijos naudojimą ir sklaidą. Tai taip pat apima poreikį nustatyti numatytąsias privatumo nuostatas.

86. 2010 m. sausio mėn. pradžioje Komisija paskelbė ataskaitos, kurioje įvertintas šių principų įgyvendinimas, išvadas ([3]). EDAPP kelia rūpestį tai, kad ši ataskaita rodo, jog tam tikrų veiksmų imtasi, tačiau nepakankamai. Pavyzdžiui, ataskaitoje nustatytos problemos, susijusios

([1]) Informaciją apie šią programą galima rasti http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Šiuos principus galima rasti http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Saugesnių socialinių tinklų principų ES įgyvendinimo vertinimo ataskaita, kurią galima rasti http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

su pranešimu apie interneto svetainėse prieinamas saugumo priemones ir įrankius. Joje taip pat nustatyta, kad mažiau kaip pusė susitarimą pasirašiusių šalių suteikia prieigą prie nepilnamečių profilių tik jų draugams.

Būtinybė numatytosiose nuostatose padaryti privatumą privalomu

87. Šiomis aplinkybėmis svarbiausias klausimas yra tas, ar papildomos politikos priemonės yra būtinos užtikrinti, kad socialiniai tinklai teiktų paslaugas kartu su numatytosiomis privatumo nuostatomis. Šį klausimą iškėlė buvusi už informacinės visuomenės klausimus atsakinga Komisijos narė Viviane Reding, pažymėjusi, kad tam gali reikėti teisės aktų ([1]). Kartu Europos ekonomikos ir socialinių reikalų komitetas nurodė, kad, nepaisant savireguliavimo, teisės aktuose turi būti nustatyti būtinieji apsaugos standartai ([2]).

88. Kaip jau nurodyta, socialinių tinklų operatorių pareiga įdiegti numatytąsias privatumo nuostatas gali būti netiesiogiai kildinama iš Duomenų apsaugos direktyvos 17 straipsnio ([3]), kuriame duomenų valdytojams nustatoma pareiga imtis tinkamų techninių ir organizacinių priemonių („ir tuomet, kai kuriamos tvarkymo sistemos, ir tuomet, kai duomenys tvarkomi“), siekiant išlaikyti saugumą ir taip neleisti be leidimo tvarkyti duomenis, atsižvelgiant į tvarkymo keliamas grėsmes ir duomenų pobūdį.

89. Tačiau šis straipsnis yra pernelyg bendras ir nekonkretus ir šiame kontekste. Jame aiškiai nenurodyta, ką reiškia tinkamos techninės ir organizacinės priemonės socialinių tinklų atveju. Todėl dabartinė situacija susijusi su teisiniu neapibrėžtumu, dėl to kyla problemų ir reguliuotojams, ir asmenims, kurių privatumas ir asmens duomenys nėra visiškai apsaugoti.

90. Atsižvelgdamas į tai, kas nurodyta, EDAPP ragina Komisiją parengti teisės aktus, kuriuose būtų bent jau bendra pareiga, pagal kurią reikalaujama privalomųjų privatumo nuostatų, nustatant ir tikslesnius reikalavimus:

a) numatyti nuostatas, pagal kurias prieiga prie naudotojo profilio suteikiama tik paties naudotojo pasirinktiems kontaktiniams asmenims. Pagal šias nuostatas prieš padarant profilį prieinamą tretiesiems asmenims, taip pat turi būti reikalaujama naudotojo sutikimo;

b) užtikrinti, kad ribotos prieigos profilių nebūtų galima rasti naudojant vidaus ar išorės paieškos priemones.

91. Reikia numatyti ne tik privalomas numatytąsias privatumo nuostatas, bet ir atsakyti į klausimą, ar nereikėtų papildomų, konkrečių duomenų apsaugos ir kitų priemonių (pavyzdžiui, susijusių su nepilnamečių apsauga). Tai kelia platesnį klausimą, ar šioms konkrečioms paslaugoms nereikėtų sukurti specialios sistemos, kuria, be privalomų privatumo nuostatų, būtų reguliuojami ir kiti aspektai. EDAPP prašo Komisijos atsižvelgti į šį aspektą.

VII. **NUMATYTOSIOS NARŠYKLĖS PRIVATUMO NUOSTATOS, SIEKIANT UŽTIKRINTI LAISVĄ SUTIKIMĄ GAUTI REKLAMAS**

92. Reklamos skelbimų tinklų operatoriai naudoja slapukus ir kitus įtaisus stebėti atskirų naudotojų elgesį, jiems mėginant naršyti internete, kad galėtų registruoti jų interesus ir kurti profilius. Tuomet ši informacija naudojama jiems siunčiant tikslinę reklamą ([4]).

VII.1. **Tebesančios problemos ir grėsmės pagal šiuo metu galiojančius duomenų apsaugos ir (arba) privatumo teisės aktus**

93. Šiam tvarkymui taikoma Duomenų apsaugos direktyva (asmens duomenų atveju), taip pat E. direktyvos 5 straipsnio 3 dalis. Šiame straipsnyje konkrečiai reikalaujama, kad naudotojui būtų pranešta ir suteikta galimybė reaguoti, duodant sutikimą arba nesutinkant jo kompiuteryje ar kitame įrenginyje saugoti įtaisus, kaip antai slapukus ir kt. ([5]).

94. Iki šiol reklamos skelbimų tinklų operatoriai naudojo naršyklės nuostatas ir privatumo politiką, kad informuotų naudotojus ir leistų jiems priimti slapukus arba juos atmesti. Leidėjo privatumo politikoje jie paaiškina, kaip

([1]) Europos Komisijos narė Viviane Reding, atsakinga už informacinę visuomenę ir žiniasklaidą, „Galvok prieš skelbdamas! Kaip padaryti socialinių tinklų svetaines saugesnes vaikams ir nepilnamečiams?“. Saugesnio interneto diena, 2010 m. vasario 9 d., Strasbūras.

([2]) Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl socialinių tinklų svetainių poveikio piliečiams ir vartotojams, 2009 m. lapkričio 4 d.

([3]) Išsamiau aprašytos šios nuomonės 33 punkte.

([4]) Sekimo slapukai yra nedidelės tekstinės rinkmenos, kuriose yra unikalusis atpažinimo kodas. Paprastai reklamos skelbimų tinklų operatoriai (taip pat interneto svetainių operatoriai ar leidėjai) patalpina slapukus lankytojo standžiajame diske, visų pirma interneto naudotojų interneto naršyklėje, naudotojams pirmą kartą apsilankius interneto svetainėse, kuriose yra aptarnaujami reklamos skelbimai, esantys jų tinklo dalimi. Naudodamas slapuką, reklamos skelbimų tinklo operatorius gali atpažinti ankstesnį lankytoją, grįžtantį į tą interneto svetainę arba apsilankantį kitoje interneto svetainėje, kuri yra reklamos tinklo partnerė. Pagal tokius pakartotinius apsilankymus reklamos skelbimų tinklo operatorius gali kurti lankytojo profilį.

([5]) E. privatumo direktyvos 5 straipsnio 3 dalis neseniai buvo iš dalies pakeista, siekiant sustiprinti apsaugą nuo naudotojų ryšių perėmimo, naudojant, pavyzdžiui, šnipinėjimo programas ir slapukus, saugomus naudotojo kompiuteryje ar kitame įrenginyje. Pagal naująją direktyvą naudotojams turėtų būti siūloma geresnė informacija ir lengvesni būdai kontroliuoti, ar jie nori, kad slapukai būtų išsaugoti jų galinėje įrangoje.

galima atsisakyti priimti visus slapukus arba juos priimti kiekvienu konkrečiu atveju. Taip jie ketino įvykdyti pareigą siūlyti naudotojams teisę atsisakyti slapukų.

95. Nors teoriškai šis metodas (naudojant naršyklę) iš tikrųjų galėtų užtikrinti reikšmingą laisvą sutikimą, tikrovėje yra visai kitaip. Apskritai naudotojams trūksta bendro suvokimo apie bet kokių duomenų rinkimą, juo labiau iš trečiųjų asmenų, apie tokių duomenų vertę, jų naudojimą, tai, kaip veikia technologija ir ypač – kaip ir kur galima atsisakyti. Veiksmai, kuriuos turi atlikti naudotojas, kad atsisakytų, atrodo ne tik sudėtingi, bet ir perdėti (pirmiausia jis turi nusistatyti savo naršyklės nuostatas, kad galėtų priimti slapukus, tuomet pasinaudoti atsisakymo galimybe).

96. Dėl to iš tikrųjų labai nedaug žmonių pasinaudoja atsisakymo galimybe ne todėl, kad jie priėmė laisvą sprendimą priimti reklamą, bet veikiau todėl, kad jie nesuvokia, jog, nepasinaudoję atsisakymo galimybe, jie iš tikrųjų išreiškia sutikimą.

97. Todėl, nors teisiškai E. privatumo direktyvos 5 straipsnio 3 dalyje praktiškai numatyta veiksminga teisinė apsauga, interneto naudotojai laikomi davę sutikimą būti stebimi, kad jiems būtų siunčiami elgsena grindžiami reklamos skelbimai, tačiau iš tikrųjų paprastai (ir dažniausiai) jie visiškai nežino, kad yra stebimi.

98. 29 straipsnio darbo grupė rengia nuomonę, kuria siekiama patikslinti teisinius reikalavimus vykdyti elgsena grindžiamą reklamos veiklą, ir tai yra sveikintina. Tačiau išaiškinimo gali savaime nepakakti išspręsti šią padėtį ir todėl Europos Sąjungai gali tekti imtis papildomų veiksmų.

VII.2. **Būtinybė toliau imtis veiksmų, visų pirma užtikrinti privalomas numatytąsias privatumo nuostatas**

99. Kaip aprašyta pirmiau, naršantieji internete leidžia tam tikrų rūšių slapukams vykdyti tam tikrą kontrolę. Šiuo metu daugelio interneto naršyklių numatytosios nuostatos priima daugumą slapukų. Kitaip tariant, pagal numatytąsias nuostatas naršyklės užprogramuotos priimti visus slapukus, nepaisant slapuko tikslo. Ir tik jei naudotojas pakeičia savo naršyklės programos nuostatas ir nurodo neleisti slapukų, o tai, kaip jau minėta, padaro labai mažai naudotojų, jis slapukų negaus. Be to, pirmą kartą diegiant ar naujinant naršyklės programas, nėra privatumo vediklio.

100. Minėtą problemą galima sumažinti įdiegus naršyklėse numatytąsias privatumo nuostatas. Kitaip tariant, jei naršyklėse būtų įdiegta nuostata „nepriimti trečiųjų asmenų slapukų“. Papildomai ir siekiant didesnio veiksmingumo, naršyklės turėtų reikalauti naudotojų pirmą kartą ją diegiant arba atnaujinant perskaityti privatumo vediklį. Būtinas didesnis išsamumas ir aiški informacija apie slapukų rūšis ir kai kurių iš jų naudingumą. Naudotojai, norintys būti stebimi, kad gautų reklamos skelbimus, bus tinkamai informuojami ir jiems reikės pakeisti naršyklės nuostatas. Taip jie galės labiau kontroliuoti savo asmens duomenis ir privatumą. EDAPP nuomone, tai būtų veiksmingas būdas paisyti naudotojo sutikimo ir jį išsaugoti ([1]).

101. Atsižvelgiant, viena vertus, į paplitusį problemos pobūdį, t. y. interneto naudotojų, kurie šiuo metu yra stebimi pagal tariamą sutikimą, skaičių, ir, kita vertus, į susijusius interesus, papildomų garantijų reikia dar labiau. Įdiegus privatumo užtikrinimo projektuojant principą interneto naršyklių programose asmenims būtų suteikta visiškai kitokia galimybė kontroliuoti duomenų rinkimo veiksmus, kurie naudojami reklamos tikslais.

102. Dėl šių priežasčių EDAPP ragina Komisiją apsvarstyti teisės aktus, pagal kuriuos būtų reikalaujama privalomų numatytųjų naršyklės nuostatų ir reikiamos informacijos teikimo.

VIII. **KITI PRINCIPAI, KURIAIS SIEKIAMA APSAUGOTI ASMENŲ PRIVATUMĄ IR UŽTIKRINTI DUOMENŲ APSAUGĄ**

103. Nors privatumo užtikrinimo projektuojant principas suteikia daug galimybių pagerinti asmens duomenų ir privatumo apsaugą, būtina teisiškai parengti ir įtvirtinti papildomus principus, kuriais būtų užtikrintas vartotojų pasitikėjimas IRT. Dėl to EDAPP atkreipia dėmesį į atsakomybės principą ir privalomos saugumo pažeidimo sistemos, taikomos visiems sektoriams, kūrimo užbaigimą.

VIII.1. **Atsakomybės principas, siekiant garantuoti, kad būtų laikomasi privatumo užtikrinimo projektuojant principo**

104. 29 straipsnio darbo grupės dokumente „Privatumo ateitis“ ([2]) rekomenduota atsakomybės principą įtraukti į Duomenų apsaugos direktyvą. Pagal šį principą, kuris

([1]) Kartu EDAPP žino, kad tai iki galo neišspręstų problemos, nes yra slapukų, kurių neįmanoma kontroliuoti naršykle, pvz., taip yra vadinamųjų mirgančių slapukų atveju. Tam naršyklių kūrėjai naujose naršyklių versijose turėtų į savo numatytąsias slapukų kontrolės nuostatas integruoti mirgančių slapukų kontrolės priemones.

([2]) 29 straipsnio darbo grupės nuomonė Nr. 168 dėl privatumo ateities, bendras dalyvavimas Europos Komisijos konsultacijoje dėl pagrindinės teisės į asmens duomenų apsaugą teisės aktų, priimta 2009 m. gruodžio 1 d.

yra pripažįstamas kai kuriose tarptautinėse duomenų apsaugos priemonėse ([1]), organizacijų reikalaujama įgyvendinti procesus, kurie atitiktų esamus teisės aktus, ir nustatyti metodus, pagal kuriuos būtų įvertinama, ar laikomasi teisės aktų ir kitų privalomų dokumentų, ir tai įrodyta.

105. EDAPP visiškai pritaria 29 straipsnio darbo grupės rekomendacijai. Jis mano, kad šis principas bus ypač svarbus, skatinant veiksmingą duomenų apsaugos principų ir įsipareigojimų taikymą. Pagal atsakomybės principą duomenų valdytojai turės įrodyti įdiegę mechanizmą, būtiną siekiant laikytis galiojančių duomenų apsaugos teisės aktų. Tai galėtų padėti veiksmingai įgyvendinti privatumo užtikrinimo projektuojant IRT technologijas principą, nes tai yra itin tinkama priemonė atsakomybei įrodyti.

106. Kad įvertintų ir įrodytų atsakomybę, duomenų valdytojai galėtų naudoti vidaus procedūras, o tretieji asmenys galėtų atlikti auditą ar kitų rūšių patikras ir vėliau skirti patvirtinimus ar apdovanojimus. Šiomis aplinkybėmis EDAPP ragina Komisiją apsvarstyti, ar, be bendrojo atsakomybės principo, teisės aktuose gali būti naudinga reikalauti konkrečių atsakomybės priemonių, pvz., būtinybės teikti poveikio privatumui ir duomenų apsaugai vertinimus, ir kokiomis sąlygomis tai daryti.

VIII.2. **Saugumo pažeidimai. Teisės aktų kūrimas**

107. Praėjusiais metais iš dalies pakeitus E. direktyvą buvo nustatytas reikalavimas pranešti susijusiems asmenims ir reikiamoms institucijoms apie duomenų pažeidimus. Duomenų pažeidimas plačiai apibrėžiamas kaip bet koks pažeidimas, dėl kurio atsitiktinai arba neteisėtai sunaikinami, prarandami, atskleidžiami ir kt. asmens duomenys arba atsiranda galimybė jais naudotis, kai jie buvo perduodami, saugomi ar kitaip tvarkomi teikiant paslaugą. Pranešimo asmenims reikės, jei duomenų pažeidimas gali turėti neigiamos įtakos jų asmens duomenims ar privatumui. Taip gali nutikti, jei dėl pažeidimo gali būti įvykdyta tapatybės vagystė arba asmuo labai pažeminamas ar sugadinama jo reputacija. Reikiamoms institucijoms privaloma pranešti apie visus duomenų pažeidimo atvejus, nepaisant to, ar kyla grėsmė asmenims.

Saugumo pažeidimo srities įpareigojimų taikymas visuose sektoriuose

108. Deja, šis įpareigojimas taikomas tik viešai prieinamų elektroninių ryšių paslaugų teikėjams, pvz., telefono ryšio įmonėms, interneto prieigos teikėjams, internetinio pašto operatoriams ir kt. EDAPP ragina Komisiją teikti pasiūlymus dėl saugumo pažeidimo taikymo visuose sektoriuose. Kalbant apie šios sistemos turinį, EDAPP mano, kad saugumo pažeidimo srities teisinėmis nuostatomis, įtrauktomis į E. privatumo direktyvą, užtikrinama tinkama asmenų teisių, įskaitant jų teisę į asmens duomenis ir privatumą, apsaugos ir atitinkamiems subjektams nustatytų įpareigojimų pusiausvyra. Kartu ši sistema suteikia tikrą apsaugą, nes ji paremta reikšmingomis įgyvendinimo užtikrinimo nuostatomis, pagal kurias institucijoms suteikiama pakankamai tyrimo įgaliojimų ir galimybė taikyti sankcijas reikalavimų nevykdymo atveju.

109. Todėl EDAPP ragina Komisiją priimti teisės akto pasiūlymą, taikant šią sistemą visuose sektoriuose, prireikus jas atitinkamai pakoregavus. Be to, taip būtų užtikrinta, kad visuose sektoriuose būtų taikomi tie patys standartai ir procedūros.

E. privatumo direktyvoje įtvirtintos teisinės tvarkos kūrimas taikant komitologijos procedūrą

110. Pagal persvarstytą E. privatumo direktyvą Komisijai suteikiami įgaliojimai imtis techninių įgyvendinimo priemonių, t. y. išsamių priemonių dėl pranešimo apie saugumo pažeidimą, taikant komitologijos procedūrą ([2]). Šie įgaliojimai pateisinami siekiant užtikrinti nuoseklų saugumo pažeidimo teisės aktų įgyvendinimą ir taikymą. Nuoseklus įgyvendinimas padeda užtikrinti, kad asmenys Bendrijoje turėtų vienodai aukštą apsaugos lygį, o atitinkamiems subjektams netektų skirtingų pranešimo reikalavimų našta.

111. E. privatumo direktyva priimta 2009 m. lapkričio mėn. Atrodo, kad nėra jokių priežasčių, dėl kurių reikėtų atidėti pradedamuosius darbus, susijusius su techninių įgyvendinimo priemonių patvirtinimu. EDAPP surengė du seminarus, kuriais siekta pasidalyti patirtimi ir jos įgyti pranešimo apie duomenų pažeidimus srityje. Jis džiaugtųsi, galėdamas pasidalyti šių seminarų rezultatais, ir nekantrauja dirbti su Komisija bei kitais suinteresuotaisiais asmenimis, kad būtų patobulinta bendra duomenų pažeidimo prevencijos teisės aktų sistema.

112. EDAPP ragina Komisiją kuo greičiau imtis būtinų veiksmų. Prieš patvirtindama technines įgyvendinimo priemones, Komisija turi plačiai konsultuotis su ENISA, EDAPP ir 29 straipsnio darbo grupe. Be to, į konsultacijas turi būti įtraukti ir kiti „suinteresuotieji asmenys“, visų pirma siekiant informuoti apie geriausias prieinamas technines ir ekonomines įgyvendinimo priemones.

([1]) 1980 m. EBPO gairės dėl privatumo apsaugos ir tarptautinio asmens duomenų judėjimo; 2009 m. lapkričio 3 d. Madrido privatumo deklaracija dėl pasaulinių privatumo standartų globaliame pasaulyje.

([2]) Komitologijos procedūra susijusi su techninių įgyvendinimo priemonių patvirtinimu valstybės narės atstovų, kuriam pirmininkauja Komisija, komitete. E. privatumo direktyvos atveju taikoma vadinamoji reguliavimo su tikrinimu procedūra, o tai reiškia, kad Europos Parlamentas ir Taryba gali prieštarauti Komisijos siūlomoms priemonėms. Išsamiau žr. http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **IŠVADOS**

113. Pasitikėjimas, arba veikiau jo stoka, buvo įvardytas kaip pagrindinis rūpestį keliantis dalykas, kuriant ir sėkmingai diegiant informacines ir ryšių technologijas. Jei žmonės nepasitikės IRT, šios technologijos gali būti pasmerktos nesėkmei. Pasitikėjimas IRT priklauso nuo įvairių veiksnių; svarbiausia yra užtikrinti, kad šios technologijos neiškreiptų asmenų pagrindinių teisių į privatumą ir asmens duomenų apsaugą.

114. Siekiant toliau stiprinti duomenų apsaugos/privatumo teisės aktus, kurių principai visiškai galioja informacinėje visuomenėje, EDAPP siūlo Komisijai privatumo užtikrinimo projektuojant principą diegti įvairiais teisėkūros ir politikos kūrimo lygmenimis.

115. Jis rekomenduoja Komisijai laikytis keturių veiksmų krypčių:

a) siūlyti į duomenų apsaugos teisės aktus įtraukti bendrą nuostatą dėl privatumo užtikrinimo projektuojant. Ši nuostata turėtų būti technologiškai neutrali, o jos laikytis turi būti privaloma įvairiais etapais;

b) pagal šią bendrą nuostatą parengti specialias nuostatas, siūlant skirtingiems sektoriams taikomus specialius teisės aktus. Šias specialias nuostatas jau dabar būtų galima įtraukti į teisės aktus; remiantis Duomenų apsaugos direktyvos 17 straipsniu (ir kitais galiojančiais teisės aktais);

c) įtraukti privatumo užtikrinimo projektuojant principą į Europos skaitmeninę darbotvarkę kaip pagrindinį principą;

d) įtraukti privatumo užtikrinimą projektuojant kaip principą į kitas ES iniciatyvas (daugiausia nesusijusias su teisėkūra).

116. Numatytose trijose IRT srityse EDAPP rekomenduoja Komisijai įvertinti būtinybę teikti pasiūlymus, kuriais įgyvendinamas privatumo užtikrinimo projektuojant principas, šiais konkrečiais būdais:

a) RDA atveju siūlyti teisės aktus, kuriais būtų reglamentuojami svarbiausi RDA naudojimo klausimai, jei veiksmingas esamų teisės aktų įgyvendinimas, taikant savireguliavimą, nepasiteisintų. Visų pirma numatyti sutikimo pardavimo vietoje principą, pagal kurį visi RDA žymenys, pritvirtinti prie vartojimo produktų, pagal bendrą taisyklę būtų padaromi neveiksmingais pardavimo vietoje;

b) socialinių tinklų srityje parengti teisės aktus, į kuriuos būtų įtrauktas bent jau visuotinis įpareigojimas įdiegti privalomas privatumo nuostatas, ir nustatyti tikslesnius reikalavimus dėl to, kad prieiga prie naudotojo profilių būtų suteikiama tik paties naudotojo pasirinktiems kontaktiniams asmenims, taip pat numatyti, kad ribotos prieigos profilių nebūtų galima rasti naudojant vidaus ar išorės paieškos priemones;

c) tikslinės reklamos srityje apsvarstyti teisės aktus, pagal kuriuos būtų privaloma įdiegti tokias numatytąsias naršyklės nuostatas, kurios atmestų trečiųjų asmenų slapukus, o naudotojai, pirmą kartą diegdami ar atnaujindami naršyklę, privalėtų perskaityti privatumo vediklį.

117. Galiausiai EDAPP Komisijai siūlo:

a) apsvarstyti atsakomybės principo įtraukimo į esamą Duomenų apsaugos direktyvą galimybę, ir

b) parengti taisykles ir procedūras, skirtas įgyvendinti E. direktyvos nuostatas dėl pranešimo apie saugumo pažeidimą, ir jas išplėsti, kad jos būtų taikomos visiems duomenų valdytojams apskritai.

Priimta Briuselyje 2010 m. kovo 18 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas