I

(Rezolūcijas, ieteikumi un atzinumi)

ATZINUMI

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS

Eiropas Datu aizsardzības uzraudzītāja atzinums par uzticības veicināšanu informācijas sabiedrībā, veicinot datu aizsardzību un privātumu

(2010/C 280/01)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16. pantu,

ņemot vērā Eiropas Savienības Pamattiesību hartu un jo īpaši tās 7. un 8. pantu,

ņemot vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti [1],

ņemot vērā Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē [2], kurā jaunākie grozījumi izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti [3] un jo īpaši tās 41. pantu,

IR PIEŅĒMIS ŠĀDU ATZINUMU.

I. IEVADS

1. Informācijas un komunikāciju tehnoloģijas (IKT) paver ļoti plašas iespējas visos dzīves aspektos – darbā, izklaidēs, saskarsmē un izglītībā. Tās ir neaizvietojamas mūsdienu informācijas ekonomikā un sabiedrībā kopumā.

2. Eiropas Savienība ir viens no pasaules vadošajiem spēkiem progresīvu IKT jomā un ir apņēmības pilna šo statusu saglabāt. Lai šo mērķi sasniegtu, ir paredzams, ka Eiropas Komisija drīzumā pieņems jauno Eiropas Digitalizācijas programmu, kuru komisāre *Kroes* ir pasludinājusi par prioritāti [4].

3. EDAU apzinās IKT sniegtos ieguvumus un piekrīt, ka ES būtu jādara viss iespējamais, lai veicinātu to attīstību un plašu izmantošanu. Tāpat EDAU pilnībā atbalsta komisāres *Kroes* un komisāres *Reding* viedokli, ka personai ir jābūt šīs jaunās vides centrā [5]. Personām ir jābūt iespējai paļauties uz IKT spēju nodrošināt informācijas neaizskaramību un kontrolēt tās lietojumu, kā arī jābūt drošiem, ka viņu tiesības uz privātumu un datu aizsardzību digitālajā telpā tiek cienītas. Šo tiesību ievērošana ir ļoti būtisks nosacījums, lai radītu patērētāju uzticēšanos. Savukārt šāda uzticēšanās ir izšķirošs faktors, lai pilsoņi izmantotu jaunos pakalpojumus [6].

[1] OV L 281, 23.11.1995., 31. lpp.
[2] OV L 201, 31.7.2002., 37. lpp.
[3] OV L 8, 12.1.2001., 1. lpp.

[4] Atbildes uz Eiropas Parlamenta jautājumiem komisārei *Neelie Kroes*, kas uzdoti EP uzklausīšanas procedūras ietvaros pirms komisāra iecelšanas amatā.

[5] Atbildes uz Eiropas Parlamenta jautājumiem komisārei *Neelie Kroes*, kas uzdoti EP uzklausīšanas procedūras ietvaros pirms komisāra iecelšanas amatā; komisāres *Viviane Reding* 2009. gada 12. novembra runa "A European Digital Agenda for the New Digital Consumer" *BEUC* daudzpusējā forumā "Patērētāju privātums un mārketings tiešsaistē: tendences tirgū un politikas perspektīvas" *(BEUC Multi-stakeholder Forum on Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives)* Briselē.

[6] Skatīt, piemēram, *RISEPTIS* ziņojumu "Trust in the Information Society", *RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society)* konsultatīvās valdes ziņojums. Pieejams: http://www.think-trust.eu/general/news-events/riseptis-report.html Skatīt arī: *J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.*

4. ES ir stingrs tiesiskais regulējums attiecībā uz datu/privātuma aizsardzību, un tā principi ir pilnībā piemērojami arī digitālajā laikmetā. Tomēr nedrīkst ļauties bezrūpībai. Daudzos gadījumos IKT izraisa jaunas bažas, kas nav apzinātas esošajā regulējumā. Tādēļ ir nepieciešams veikt atsevišķas darbības, lai nodrošinātu, ka ES tiesību aktos paredzētās personu tiesības arī turpmāk garantē efektīvu aizsardzību šajā jaunajā vidē.

5. Šajā atzinumā tiek apspriesti pasākumi, kurus Eiropas Savienība varētu veicināt vai īstenot, lai garantētu personu privātuma un datu aizsardzību globalizētā pasaulē, kuras virzību arī turpmāk noteiks tehnoloģijas. Tiek apspriesti gan likumdošanas, gan citi instrumenti.

6. Pēc vispārēja pārskata par IKT kā jaunu parādību, kas rada gan iespējas, gan riskus, tiek apspriesta vajadzība praktiski integrēt datu un privātuma aizsardzību jau no pašiem jauno informācijas un komunikāciju tehnoloģiju pirmsākumiem (dēvēts par "integrētas privātās dzīves aizsardzības" *(Privacy by Design)* principu). Lai panāktu šā principa ievērošanu, tiek apspriesta vajadzība iekļaut "integrētas privātās dzīves aizsardzības" principu datu aizsardzības tiesiskajā regulējumā vismaz divos dažādos veidos. Pirmkārt, iestrādājot to kā vispārīgu, saistošu principu un, otrkārt, iestrādājot to noteiktās IKT jomās, kurās vērojami īpaši datu aizsardzības/privātuma neaizskaramības riski, kurus ir iespējams novērst ar pienācīgu tehnisko arhitektūru un uzbūvi. Šīs jomas ir radiofrekvenču identifikācija *(RFID)*, sociālo tīklu lietojumprogrammas un pārlūkprogrammas. Noslēgumā tiek sniegti priekšlikumi attiecībā uz citiem rīkiem un principiem, kuru mērķis ir personas privātuma un datu aizsardzība IKT jomā.

7. Attiecībā uz iepriekš minēto atzinumā tiek rūpīgi analizēti daži jautājumi, kurus sabiedriskajā apspriešanā par privātās dzīves nākotni [1] izvirzījusi 29. panta darba grupa. Turklāt šā atzinuma pamatā ir iepriekšējie EDAU atzinumi, piemēram, 2007. gada 25. jūlija atzinums par Datu aizsardzības direktīvas īstenošanu, 2007. gada 20. decembra atzinums par radiofrekvenču identifikāciju *(RFID)* un divi atzinumi par E-privātuma direktīvu. [2]

II. IKT PIEDĀVĀ JAUNAS IESPĒJAS, TAČU IZRAISA ARĪ JAUNUS RISKUS

8. IKT mēdz salīdzināt ar citiem būtiskiem pagātnes izgudrojumiem, piemēram, elektrību. Kaut arī varētu būt pāragri mēģināt novērtēt IKT patieso vēsturisko ietekmi, tomēr to saikne ar ekonomikas izaugsmi attīstītajās valstīs ir nepārprotama. IKT ir izveidojušas darba vietas, ieguvumus ekonomikā un sniegušas ieguldījumu vispārējā labklājībā. IKT ietekme neaprobežojas tikai ar ekonomiku, ņemot vērā tās būtisko lomu inovāciju un radošuma attīstībā.

9. Turklāt IKT ir mainījušas to, kā cilvēki strādā, sazinās un mijiedarbojas. Tā, piemēram, iedzīvotāji arvien vairāk paļaujas uz IKT attiecībā uz sociālo un ekonomisko mijiedarbību. Personas var izmantot daudzas IKT lietojumprogrammas, piemēram, e-veselības, e-transporta, e-valdības, kā arī inovatīvas interaktīvās sistēmas izklaidei un mācībām.

10. Apzinoties šos ieguvumus, visas Eiropas iestādes ir paudušas gatavību atbalstīt IKT kā rīku, kas nepieciešams Eiropas nozaru konkurētspējas paaugstināšanai un tās ekonomikas atlabšanas paātrināšanai. Tādēļ 2009. gada augustā Komisija pieņēma Ziņojumu par Eiropas konkurētspēju digitālajā jomā [3] un uzsāka sabiedrisko apspriedi par piemērotām nākotnes stratēģijām attiecībā uz IKT attīstības veicināšanu. Komisija 2009. gada 7. decembrī sniedza arī savu ieguldījumu šajā apspriedē, proti, "Post i2010 Strategy – Toward an open, green and competitive knowledge society" [4]. Eiropas Parlaments tikko ir arī

[1] 29. panta darba grupas 2009. gada 1. decembrī pieņemtais 168. atzinums "The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data".

[2] 2007. gada 25. jūlija atzinums attiecībā uz Komisijas paziņojumu Eiropas Parlamentam un Padomei par pasākumiem, kas veikti saskaņā ar Darba programmu labākai Datu aizsardzības direktīvas īstenošanai (OV C 255, 27.10.2007., 1. lpp); 2007. gada 20. decembra atzinums saistībā ar Komisijas paziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par radiofrekvenču identifikāciju *(Radio Frequency Identification – RFID)* Eiropā – ceļā uz politikas izstrādi (COM(2007) 96) (OV C 101, 23.4.2008., 1. lpp.); 2008. gada 10. aprīļa atzinums par priekšlikumu Eiropas Parlamenta un Padomes direktīvai, ar ko groza, citu starpā, Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektroniskajām komunikācijām) (OV C 181, 18.7.2008., 1. lpp.); Otrais atzinums (2009. gada 9. janvāris) par pārskatīto Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē.

[3] Ziņojums par Eiropas konkurētspēju digitālajā jomā – Galvenie sasniegumi, 2005.–2009. gadā īstenojot stratēģiju i-2010 (SEC(2009) 1060).

[4] Padomes secinājumi "Post i-2010 Strategy – Towards and Open, Green and Competitive Knowledge Society" (17107/09), pieņemti 18.12.2009.

pieņēmis ziņojumu, kura mērķis ir sniegt vadlīnijas Komisijai digitālās programmas formulēšanā [1].

11. Vienlaikus ar IKT attīstību saistītajām iespējām un ieguvumiem ir vērojami arī jauni riski, jo īpaši attiecībā uz privātumu un privātpersonu datu aizsardzību. IKT nereti izraisa savāktās, sašķirotās, atlasītās, pārsūtītās vai citādi saglabātās informācijas apjoma palielināšanos (nereti veidos, ko personas pat nepamana) un tādēļ pieaug arī risku skaits.

12. Piemēram, radiofrekvenču identifikācijas *(RFID)* mikroshēmas uz patēriņa precēm (atsevišķām) aizstāj svītru kodus. Uzlabojot informācijas plūsmu piegādes ķēdē (tādā veidā samazinot "drošības" rezervju nepieciešamību, nodrošinot precīzākas prognozes utt.), jaunajai sistēmai vajadzētu dot labumu gan uzņēmējiem, gan patērētājiem. Tomēr vienlaikus tas izraisa satraucošo iespējamību, ka dažādas personas dažādos nolūkos varētu veikt izsekošanu, izmantojot personu lietām pievienotos marķējumus.

13. Cits piemērs ir datu izkaisītā apstrāde *(cloud computing)*, kas pamatā ir viesotu lietojumprogrammu pakalpojumu piegāde internetā privātpersonām un juridiskām personām. Šeit ietilpst pakalpojumi, sākot no fotoattēlu datu bāzēm, kalendāriem, tīmekļa e-pasta un klientu datu bāzēm līdz sarežģītākiem ar uzņēmējdarbību saistītiem pakalpojumiem. Gan uzņēmēju, gan privātpersonu ieguvumi ir acīmredzami: izmaksu samazināšana (novēršamās izmaksas), neatkarība no vietas (viegla piekļuve informācijai jebkurā vietā pasaulē), automatizācija (nav nepieciešami īpaši IT resursi un programmatūras modernizācija) utt. Vienlaikus pastāv ļoti reāli drošības pārrāvumu un datorpirātisma riski. Ir arī draudi zaudēt piekļuvi un kontroli attiecībā uz personas pašas datiem.

14. Ieguvumu un risku līdzāspastāvēšana ir vērojama arī citās jomās, kurās lieto IKT. Piemēram, e-veselība, kas var paaugstināt efektivitāti, samazināt izmaksas, paplašināt pieejamību un kopumā uzlabot veselības aprūpes pakalpojumu kvalitāti. Tomēr saistībā ar e-veselību nereti aktualizēts jautājums par šādas informācijas sekundārās izmantošanas leģitimitāti, kas paredz jebkādas sekundārās izmantošanas mērķu rūpīgu analīzi [2]. Turklāt ar elektronisko veselības datu plašāku izmantojumu sistēmas saskaras ar nerimstošiem skandāliem, kas atklāj daudzus gadījumus, kad datorpirāti ielaužas elektronisko veselības datu sistēmās.

15. Kopumā zināmā mērā atlikušais risks visticamāk turpinās pastāvēt pat pēc atbilstīga novērtējuma veikšanas un nepieciešamo pasākumu piemērošanas. Nulles riska situācija būtu neiespējama. Tomēr, kā norādīts turpmāk, pasākumus var un vajag īstenot, lai šādus riskus samazinātu līdz piemērotam līmenim.

III. **INTEGRĒTA PRIVĀTĀS DZĪVES AIZSARDZĪBA KĀ GALVENAIS RĪKS, AR KO VEICINA PRIVĀTPERSONU UZTICĒŠANOS IKT**

16. Praksē IKT potenciālos ieguvumus var just tikai tad, ja tiek izveidota uzticība, citiem vārdiem, ja tiek nodrošināta lietotāju vēlme paļauties uz IKT to iezīmju un sniegto ieguvumu dēļ. Šāda uzticēšanās tiks izveidota tikai tad, ja IKT ir uzticamas, drošas, personiski kontrolējamas un garantē personas datu un privātuma aizsardzību.

17. Izplatīti riski un trūkumi, tādi kā iepriekš minētie, jo īpaši gadījumos, kad ir iesaistīta ļaunprātīga personas datu izmantošana vai pārkāpumi šajā jomā, tādējādi izpaužot personisku informāciju, visticamāk apdraudēs personu uzticēšanos informācijas sabiedrībai. Tas varētu nopietni apdraudēt IKT attīstību un to sniegtos potenciālos ieguvumus.

18. Vienlaikus draudus privātumam un datu aizsardzībai nevar risināt, likvidējot, nepieļaujot vai atsakoties no IKT lietošanas vai popularizēšanas. Tas nebūtu nedz iespējami, nedz reālistiski; tas neļautu personām izmantot IKT sniegtos ieguvumus un nopietni ierobežotu kopējās to sniegtās priekšrocības.

19. EDAU uzskata, ka daudz labāks risinājums ir IKT veidošana un attīstīšana tādā veidā, lai tiktu respektēts privātums un datu aizsardzība. Tādēļ ir ļoti būtiski iestrādāt privātumu un datu aizsardzību visā tehnoloģijas aprites ciklā, no sākotnējā projektēšanas posma līdz to galējai novietošanai, lietošanai un likvidēšanai. To parasti dēvē par "integrēto privātās dzīves aizsardzību" *(PbD)* un tā tiek analizēta turpmāk tekstā.

20. *PbD* var ietvert dažādas darbības atkarībā no konkrētā gadījuma vai lietojuma. Tā, piemēram, atsevišķos gadījumos var būt nepieciešams likvidēt/samazināt personas datus vai novērst nevajadzīgu un/vai nevēlamu datu apstrādi. Citos gadījumos *PbD* var ietvert rīkus, ar kuru palīdzību var uzlabot personu kontroli pār saviem datiem. Šādi pasākumi būtu jāapsver, formulējot standartus un/vai labo praksi. Tos var arī iestrādāt informācijas un

[1] Ziņojums par jaunu Eiropas digitālo programmu: no *i-2010* līdz *digital.eu* (2009/2225 (INI)), pieņemts 18.3.2010.

[2] Piemēram, iespējamība pārdot ārstēšanas nolūkos apkopotos veselības datus vai arī tos izmantot, izvēloties vietu slimnīcu filiālēm, izveidojot ambulatorās ķirurģijas centrus un citos veidos plānojot darbības ar finansiālām sekām, būtu rūpīgi jāizvērtē.

komunikāciju sistēmu arhitektūrā vai arī to vienību struktūrās, kas apstrādā personas datus.

III.1. **Dažādās IKT vidēs piemērojamais integrētas privātās dzīves aizsardzības princips un tā ietekme**

21. Nepieciešamība piemērot *PbD* principu ir vērojama daudzās dažādās IKT vidēs. Tā, piemēram, veselības aprūpes nozare arvien vairāk paļaujas uz IKT infrastruktūru, kas nereti ietver ar pacientu veselību saistītas informācijas centralizētu uzkrāšanu. *PbD* principa piemērošana veselības aprūpes nozarē nozīmētu dažādu pasākumu piemērotības izvērtēšanu, piemēram, iespēju makismāli samazināt centralizēti glabājamo datu apjomu vai ierobežot to līdz indeksam, izmantot šifrēšanas rīkus, piešķirt piekļuves tiesības, stingri balstoties uz principu "nepieciešams zināt", padarīt datus anonīmus, tiklīdz tie vairs nav nepieciešami utt.

22. Līdzīgi arī transporta sistēmas arvien biežāk tiek nodrošinātas ar modernām IKT lietojumprogrammām ar noklusējuma iestatījumiem, kas mijiedarbojas ar transportlīdzekli un tā vidi, īstenojot dažādus mērķus un funkcijas. Tā, piemēram, automobiļi arvien vairāk tiek aprīkoti ar jaunām IKT funkcijām (*GPS*, *GSM*, sensoru tīkls utt.), kas norāda ne tikai to atrašanās vietu, bet arī faktisko tehnisko stāvokli. Šo informāciju varētu izmantot, piemēram, lai aizstātu esošo ceļa nodokļa sistēmu ar ceļa nodevu, kas balstīta uz lietošanas biežumu. *PbD* piemērošanai šādu sistēmu arhitektūras izveidē vajadzētu atbalstīt pēc iespējas retāku personas datu apstrādi un tālāku pārsūtīšanu ([1]). Saskaņā ar šo principu centralizētas arhitektūras vietā priekšroka būtu dodama decentralizētai vai daļēji decentralizētai arhitektūrai, kas ierobežo datu izpaušanu un novietošanu līdz centrālajam punktam.

23. Minētie piemēri apliecina, ka gadījumos, kad informācijas un komunikāciju tehnoloģijas tiek veidotas saskaņā ar *PbD* principu, ir iespējams ievērojami samazināt riskus privātumam un datu aizsardzībai.

III.2. **Nepietiekama *PbD* principa piemērošana IKT ieviešanā**

24. Būtisks jautājums ir, vai uzņēmēji, IKT ražotāji/nodrošinātāji un datu apstrādātāji ir ieinteresēti *PbD* principa popularizēšanā un iestrādāšanā IKT. Šajā kontekstā svarīgi ir arī izvērtēt *PbD* pieprasījumu.

25. Komisija 2007. gadā publicēja paziņojumu, aicinot uzņēmējus izmantot inovāciju iespējas, lai radītu un ieviestu privātumu uzlabojošās tehnoloģijas *(PETs)*, šādi uzlabojot privātuma un personas datu aizsardzību no paša attīstības cikla sākuma ([2]).

26. Šobrīd pieejamie fakti liecina, ka ne IKT ražotāji, ne datu apstrādātāji (ne privātajā, ne sabiedriskajā sektorā) nav spējuši sistemātiski īstenot vai popularizēt *PbD*. Ir minēti dažādi pamatojumi, tostarp finansiālo stimulu vai institucionālā atbalsta trūkums, nepietiekams pieprasījums utt. ([3])

27. Vienlaikus lietotāju pieprasījums pēc *PbD* ir bijis diezgan zems. IKT produktu un pakalpojumu lietotāji varētu ar pilnām tiesībām uzskatīt, ka to privātums un personas dati ir aizsargāti *de facto*, kaut arī daudzos gadījumos tā nebūt nav. Dažos gadījumos viņi vienkārši nav spējīgi veikt nepieciešamos drošības pasākumus, lai aizsargātu savus personiskos vai citu datus. Nereti iemesls ir pilnīgu vai pat daļēju zināšanu trūkums attiecībā uz riskiem. Tā, piemēram, kopumā jaunieši ignorē privātuma riskus, kas saistīti ar personiskas informācijas norādīšanu sabiedriskajā tīmeklī un neņem vērā privātuma iestatījumus. Savukārt citi lietotāji apzinās riskus, bet, iespējams, viņiem nav nepieciešamās tehniskās zināšanas, lai piemērotu aizsardzības tehnoloģijas, piemēram, tādas, kas aizsargā interneta savienojumu, vai arī lai mainītu pārlūkprogrammu iestatījumus, tādējādi samazinot profilēšanu, kas balstīta uz viņu tīklklejošanas novērošanu.

28. Vienlaikus privātuma un datu aizsardzības apdraudējums ir ļoti reāls. Ja privātums un datu aizsardzība nav ņemta vērā jau no sākuma, tad nereti ir pārāk vēlu un ekonomiski pārāk neizdevīgi šādas sistēmas izlabot, kā arī pārāk

([1]) Skatīt Eiropas Datu aizsardzības uzraudzītāja 2009. gada 22. jūlija atzinumu saistībā ar Komisijas paziņojumu par rīcības plānu Eiropā ieviest inteliģentas transporta sistēmas un tam pievienoto ierosināto Eiropas Parlamenta un Padomes direktīvu, ar ko nosaka pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomā un saskarnēm ar citiem transporta veidiem, kas pieejams: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) 2007. gada 2. maija paziņojums. COM(2007) 228 galīgā redakcija, Komisijas paziņojums Eiropas Parlamentam un Padomei par datu aizsardzības veicināšanu, izmantojot privātuma uzlabojošas tehnoloģijas *(PETs)*.

([3]) *Study on the economic benefits of privacy enhancing technologies (PETS) jls/2008/D4/036*.

vēlu, lai novērstu jau nodarīto ļaunumu. Iepriekšējos gados vērojamais datu krātuvju uzlaušanas gadījumu skaita pieaugums pilnībā ilustrē šo problēmu un apstiprina integrētas privātās dzīves aizsardzības nepieciešamību.

29. Iepriekš minētais acīmredzami norāda, ka IKT ražotājiem un pakalpojumu sniedzējiem attiecībā uz tehnoloģijām, kas paredzētas personas datu apstrādei, būtu kopā ar datu apstrādātājiem jābūt atbildīgiem par to, lai tajās būtu iestrādāti datu un privātuma aizsardzības mehānismi. Daudzos gadījumos tas nozīmētu, ka privātums būtu jāiestrādā pēc noklusējuma.

30. Šajā kontekstā būtu jāapsver pasākumi, kas jāveic politikas veidotājiem, lai veicinātu *PbD* principa iestrādāšanu IKT attīstībā. Pirmkārt, ir jāsaprot, vai esošais datu aizsardzības tiesiskais regulējums ietver pietiekamus nosacījumus, lai nodrošinātu, ka *PbD* principu īsteno gan datu apstrādātāji, gan IKT ražotāji/attīstītāji. Otrkārt, ir jānoskaidro, kas būtu jādara saistībā ar Eiropas Digitalizācijas programmu, lai nodrošinātu, ka IKT nozare veido patērētāju uzticēšanos.

IV. INTEGRĒTAS PRIVĀTĀS DZĪVES AIZSARDZĪBAS PRINCIPA IESTRĀDE ES TIESĪBU AKTOS UN POLITIKĀ

IV.1. Esošais datu aizsardzības un privātuma tiesiskais regulējums

31. ES ir spēcīgs datu aizsardzības un privātuma regulējums, kas iestrādāts Direktīvā 95/46/EK ([1]), Direktīvā 2002/58/EK ([2]), kā arī Eiropas Cilvēktiesību tiesas ([3]) un Eiropas Kopienu Tiesas praksē.

32. Datu aizsardzības direktīva attiecas uz "jebkuru ar personas datiem veiktu darbību vai darbību kopumu" (vākšana, uzglabāšana, atklāšana utt.). Tajā ir noteikti principi un pienākumi, kas jāievēro tiem, kas apstrādā personas datus ("datu apstrādātāji"). Tajā ir paredzētas personas tiesības, piemēram, tiesības piekļūt personas datiem. E-privātuma direktīva īpaši attiecas uz privātuma aizsardzību elektronisko komunikāciju nozarē ([4]).

33. Spēkā esošā Datu aizsardzības direktīva neietver skaidru prasību attiecībā uz *PbD*. Tomēr tā ietver netiešus nosacījumus, atbilstoši kuriem dažādās situācijās ir iespējams pieprasīt *PbD* principa īstenošanu. Jo īpaši tās 17. pants paredz, ka datu apstrādātāji īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai novērstu nelikumīgu datu apstrādi ([5]). *PbD* tādējādi ir ietverts ļoti vispārīgā veidā. Turklāt direktīvas nosacījumi galvenokārt ir adresēti datu apstrādātājiem un personas datu apstrādei. Nosacījumi skaidri neparedz, ka informācijas un komunikāciju tehnoloģijās ir jāievēro privātums un datu aizsardzība, kā nodrošināšanai ir nepieciešams vērsties arī pie IKT izstrādātājiem un ražotājiem, tostarp ietverot standartizācijas posmā veiktās darbības.

34. E-privātuma direktīva ir konkrētāka. Tās 14. panta 3. punktā noteikts, ka "Ja nepieciešams, var pieņemt pasākumus, lai nodrošinātu, ka gala iekārta ir veidota tā, lai tā būtu savietojama ar lietotāju tiesībām aizsargāt un kontrolēt to personas datu izmantošanu, saskaņā ar Direktīvu 1999/5/EK un Padomes 1986. gada 22. decembra Lēmumu 87/95/EEK par standartizāciju informācijas tehnoloģijas un komunikāciju jomā". Tomēr šis nosacījums nekad nav bijis piemērots ([6]).

35. Lai gan abu direktīvu iepriekš minētie nosacījumi palīdz integrētas privātās dzīves aizsardzības principa *veicināšanā*, faktiski ar tiem nav bijis pietiekami, lai *nodrošinātu* privātuma iekļaušanu IKT.

36. Šīs situācijas rezultātā tiesību akti pietiekami precīzi nenosaka, ka IKT tiek veidotas saskaņā ar *PbD* principu. Tāpat arī datu aizsardzības iestādēm nav pietiekamu tiesību, lai nodrošinātu *PbD* principa iestrādi. Rezultāts ir neefektivitāte. Tā, piemēram, datu aizsardzības iestādes būtu tiesīgas sodīt par nespēju izpildīt personas piekļuves pieprasījumu un tām būs tiesības pieprasīt noteiktu pasākumu īstenošanu, lai novērstu datu prettiesisku apstrādi. Tomēr ne vienmēr ir pietiekami skaidrs, vai to tiesības ir gana plašas, lai pieprasītu tādas sistēmas izveidi, kas veicina personu datu aizsardzības tiesības ([7]). Piemēram, pamatojoties uz esošo tiesību aktu nosacījumiem, nav skaidrs, vai būtu iespējams pieprasīt, lai informācijas sistēmas arhitektūru veido tā, lai veicinātu situāciju, kurā uzņēmumi personu piekļuves pieprasījumus varētu apstrādāt ātrāk

([1]) Eiropas Parlamenta un Padomes Direktīva 95/46/EK (turpmāk – Datu aizsardzības direktīva).

([2]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (turpmāk tekstā – E-privātuma direktīva).

([3]) Interpretējot galvenos elementus un nosacījumus, kas norādīti 1950. gada 4. novembrī Romā pieņemtās Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas (ECK) 8. pantā, to atšķirīgam piemērojumam.

([4]) Ar Lisabonas līgumu šāda aizsardzība tiek pastiprināta, iekļaujot privātās dzīves neaizskaramību un personas datu aizsardzību kā atsevišķas pamattiesības ES Pamattiesību hartas 7. un 8. pantā. ES Pamattiesību harta kļuva saistoša no Lisabonas līguma spēkā stāšanās dienas.

([5]) 17. pants: "Dalībvalstis paredz to, ka personas datu apstrādātājam jāīsteno atbilstoši tehniski un organizatoriski pasākumi, lai aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai nejaušu pazaudēšanu, pārveidošanu, nesankcionētu atklāšanu vai piekļuvi, īpaši, ja apstrāde ietver datu pārraidi pa elektronisko sakaru tīklu, un pret visām citām nelikumīgām apstrādes formām." 46. paragrāfs to papildina: "Tā kā datu subjektu tiesību un brīvību aizsardzība, kas attiecas uz personas datu apstrādi, prasa atbilstošus tehniskus un organizatoriskus pasākumus gan apstrādes sistēmas izveides laikā, gan pašas apstrādes laikā, lai saglabātu šo datu drošību un tādējādi novērstu jebkādu nesankcionētu apstrādi."

([6]) Komisija ir norādījusi, ka tā plāno atjaunināt Direktīvu 1999/5/EK līdz 2010. gada beigām.

([7]) Skatīt AK informātikas komisāra biroja ziņojumu "Privacy by Design", kas publicēts 2008. gada novembrī.

un automātiski. Turklāt vēlāki mēģinājumi mainīt tehnoloģiju pēc tās izstrādes un novietošanas var kļūt par risinājumu savārstījumu, kas nedarbojas pilnīgi un ir finansiāli apgrūtinoši.

37. EDAU viedoklis, ko atbalsta arī 29. panta darba grupa ([1]), ir tāds, ka esošajā tiesiskajā regulējumā būtu vieta precīzāk noteiktam *PbD* principa apstiprinājumam.

IV.2. **Integrētas privātās dzīves aizsardzības principa iekļaušana dažādos līmeņos**

38. Šajā kontekstā EDAU iesaka Komisijai īstenot četrus darbības virzienus:

a) ierosināt datu aizsardzības tiesiskajā regulējumā iekļaut vispārīgu nosacījumu attiecībā uz *PbD*;

b) šo vispārīgo nosacījumu rūpīgi attīstīt īpašos nosacījumos, ierosinot īpašus tiesiskos instrumentus dažādās nozarēs. Šos īpašos nosacījumus jau šobrīd varētu iestrādāt tiesiskajos instrumentos, pamatojoties uz Datu aizsardzības direktīvas 17. pantu (un citiem spēkā esošiem tiesību aktiem);

c) iekļaut *PbD* kā galveno principu Eiropas Digitalizācijas programmā;

d) ieviest *PbD* kā principu citās ES iniciatīvās (galvenokārt ar likumdošanu nesaistītās).

([1]) 29. panta darba grupas 2009. gada 1. decembrī pieņemtais 168. atzinums "The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data".

Vispārīgs nosacījums attiecībā uz PbD

39. EDAU ierosina esošajā datu aizsardzības tiesiskajā regulējumā neatgriezeniskā un nepārprotamā veidā iekļaut integrētas privātās dzīves aizsardzības principu. Tas padarītu *PbD* principu stiprāku, skaidrāku un paredzēs tā efektīvu īstenošanu, papildus sniedzot vairāk leģitimitātes par tā ieviešanu atbildīgajām iestādēm pieprasīt tā *de facto* piemērošanu praksē. Tas ir jo īpaši nepieciešams, ņemot vērā iepriekš minētos faktus – ne tikai tādēļ, ka princips ir svarīgs uzticēšanās veicināšanas rīks, bet arī tādēļ, ka tas būtu stimuls ieinteresētajām personām ieviest *PbD* un uzlabot esošajā tiesiskajā regulējumā iekļautās garantijas.

40. Šis priekšlikums ir balstīts uz 29. panta darba grupas ieteikumu ieviest "integrētas privātās dzīves aizsardzību" kā vispārīgu principu datu aizsardzības tiesiskajā regulējumā, jo īpaši, Datu aizsardzības direktīvā. Atbilstīgi 29. panta darba grupai: "Šim principam vajadzētu būt saistošam tehnoloģiju izstrādātājiem un ražotājiem, kā arī datu apstrādātājiem, kas nolēmuši iegūt un izmantot IKT. Viņiem būtu jāuzliek par pienākumu ievērot tehnoloģisku datu aizsardzību jau informācijas-tehnoloģiju procedūru un sistēmu plānošanas posmā. Šādu sistēmu un pakalpojumu sniedzējiem, kā arī apstrādātājiem būtu jādemonstrē, ka viņi ir veikuši visus nepieciešamos pasākumus, lai ievērotu šos nosacījumus."

41. EDAU arī atzinīgi vērtē komisāres *Viviane Reding* atbalstu integrētas privātās dzīves aizsardzības principam kontekstā ar Datu aizsardzības direktīvas pārskata paziņošanu ([2]).

42. Iepriekš minētais nosaka šāda regulējuma saturu. Pirmais un svarīgākais – vispārīgajam integrētas privātās dzīves aizsardzības principam vajadzētu būt tehnoloģiski neitrālam. Ar šo principu nebūtu jāmēģina regulēt tehnoloģiju, tas ir, tam nevajadzētu ietvert konkrētus specifiskus risinājumus. Tā vietā tam būtu jānosaka, ka esošie privātuma un datu aizsardzības principi būtu jāintegrē informācijas un komunikāciju sistēmās un risinājumos. Tas ļautu ieinteresētajām personām, ražotājiem, datu

([2]) "Integrētas privātās dzīves aizsardzība ir princips, kas ir gan pilsoņu, gan uzņēmumu interesēs. Integrēta privātās dzīves aizsardzība labāk pasargās indivīdus, kā arī vairos ticību un paļāvību jaunajiem pakalpojumiem un izstrādājumiem, kam savukārt būs laba ietekme uz ekonomiku. Ir novēroti jau daži labi piemēri, bet priekšā vēl ir daudz darāmā." (Atklāšanas runa Datu aizsardzības dienā 2010. gada 28. janvārī Eiropas Parlamentā, Briselē).

apstrādātājiem un datu aizsardzības iestādēm interpretēt principa nozīmi atbilstīgi katram konkrētajam gadījumam. Otrkārt, principa ievērošanai būtu jābūt saistošai dažādos posmos, sākot no standartu noteikšanas un arhitektūras izveides līdz brīdim, kad datu apstrādātāji tos ieviež.

Īpašo tiesisko instrumentu nosacījumi

43. Balstoties uz esošo tiesisko regulējumu, kā arī iepriekš ierosināto vispārīgo nosacījumu pēc tā pieņemšanas, *PbD* princips ir jāintegrē esošajos un topošajos likumdošanas instrumentos. Tā, piemēram, atbilstīgi pašreizējām ar inteliģentajām transporta sistēmām saistītajām iniciatīvām Komisijai būs īpaša sākotnēja atbildība par pasākumu, standartizācijas iniciatīvu, procedūru un labās prakses definēšanu. Šo uzdevumu izpildē *PbD* principam būtu piešķirama svarīgākā nozīme.

44. Tāpat EDAU norāda, ka integrētas privātās dzīves aizsardzības principam ir īpaša nozīme arī attiecībā uz brīvību, drošību un tiesiskumu, jo īpaši saistībā ar informācijas pārvaldības stratēģijas mērķiem, kas paredzēti Stokholmas programmā ([1]). Atzinumā saistībā ar Stokholmas programmu EDAU uzsvēra, ka informācijas apmaiņas arhitektūra būtu jābalsta uz "integrētu privātās dzīves aizsardzību" ([2]). "Proti, tas nozīmē, ka informācijas sistēmas, kuras tiek plānotas sabiedrības drošības mērķiem, vienmēr ir jāizstrādā saskaņā ar principu "konstrukcijā iekļauta privātās dzīves neaizskaramība"."

45. 29. panta darba grupa savā atzinumā par privātuma nākotni ([3]) vēl konkrētāk uzstāj uz to, ka attiecībā uz brīvību, drošību un tiesiskumu – tas ir, jomās, kurās valsts sektora iestādes ir galvenās dalībnieces un kurās uzraudzību palielinoši pasākumi tieši skar pamattiesības uz privātumu un datu aizsardzību – integrētas privātās dzīves aizsardzības nosacījumi būtu jāpadara obligāti ievērojami. Valdības ar šo nosacījumu ieviešanu informācijas sistēmās veicinātu integrētu privātās dzīves aizsardzību kā attīstību veicinoši pasūtītāji.

PbD kā pamatprincips Eiropas Digitalizācijas programmā

46. Informācijas un komunikāciju tehnoloģijas kļūst arvien sarežģītākas un ietver lielākus privātuma un datu aizsardzības riskus. Kopumā digitālā informācija, kurai ir vieglāk piekļūt, kuru ir vieglāk kopēt un pārsūtīt, ir pakļauta lielākam riskam nekā informācija, kas tiek glabāta uz papīra. Virzoties uz savstarpēji savienotu objektu tīmekļiem, riski pieaugs. Jo lielāki ir privātuma/datu aizsardzības riski, jo lielāks būs pieprasījums pēc uzlabotiem datu/privātuma aizsardzības mehānismiem. Tādēļ *PbD* īstenošanas nepieciešamības pamatojums ir neatspēkojamāks IKT nozarē. Papildus, kā aprakstīts iepriekš, personu uzticēšanās IKT ir pamats tam, lai pilsoņi pieņemtu šos jaunos pakalpojumus, savukārt privātums un datu aizsardzība ir šīs uzticības stūrakmeņi.

47. Iepriekš minētais norāda uz to, ka IKT attīstības stratēģijai ir jāietver nepieciešamība iestrādāt privātumu un datu aizsardzību kā neatņemamu IKT elementu, tas ir, jāņem vērā integrētas privātās dzīves aizsardzības princips.

48. Tādējādi Eiropas Digitalizācijas programmā būtu nepārprotami jāapstiprina integrētas privātās dzīves aizsardzības princips kā nepieciešams elements, lai nodrošinātu pilsoņu uzticēšanos IKT un tiešsaistes pakalpojumiem. Tajā būtu jāapliecina, ka privātuma neaizskaramība un uzticība ir savstarpēji saistītas un ka integrētas privātās dzīves aizsardzībai ir jābūt par pamatfaktoru uzticamas IKT nozares attīstībā.

PbD kā princips citās ES iniciatīvās

49. Komisijai būtu jānosaka integrēta privātās dzīves aizsardzība kā pamatprincips politikas, darbību un iniciatīvu īstenošanā konkrētās IKT nozarēs, tostarp tādās kā e-veselība, e-iepirkums, e-sociālā drošība, e-mācības utt. Daudzas no šīm iniciatīvām būs veicamās darbības atbilstīgi Eiropas Digitalizācijas programmai.

50. Tas nozīmē, ka, piemēram, iniciatīvas, kas paredzētas, lai nodrošinātu valdības lietojumu lielāku efektivitāti un atbilstību jaunākajiem sasniegumiem, tādējādi ļaujot personām sazināties ar pārvaldes iestādēm, būtu jāveido un jāīsteno saskaņā ar integrētas privātās dzīves aizsardzības principu. Tas pats attiecas uz Komisijas politiku un darbībām, kas vērstas uz ātrāku internetu un digitālā satura pārraidi vai vispārēju fiksēto un bezvadu sakaru un datu pārraides veicināšanu.

([1]) Eiropas Padomes 2009. gada decembrī apstiprinātā Stokholmas programma – *An open and secure Europe serving and protecting the citizen*.

([2]) 2009. gada 10. jūlija atzinums par Komisijas paziņojumu Eiropas Parlamentam un Padomei "Brīvības, drošības un tiesiskuma telpa pilsoņu interesēs" (OV C 276, 17.11.2009., 8. lpp., 60. punkts).

([3]) 29. panta darba grupas 2009. gada 1. decembrī pieņemtais 168. atzinums par *The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*.

51. Iepriekš minētais attiecas arī uz jomām, kurās Komisija ir atbildīga par liela mēroga IT sistēmām, tādām kā *SIS* un *VIS*, kā arī uz tiem gadījumiem, kuros Komisijas atbildība attiecas vien uz šādas sistēmas kopējās infrastruktūras izstrādi un uzturēšanu, piemēram, Eiropas Sodāmības reģistru informācijas sistēmas *(ECRIS)* gadījumā.

52. *PbD* principa attīstība būs atkarīga no katras konkrētās nozares un situācijas. Tā, piemēram, gadījumos, kad tiesību aktu priekšlikumi papildinās Komisijas iniciatīvas konkrētās IKT nozarēs, daudzos gadījumos būs pieņemami iekļaut skaidru atsauci uz *PbD* jēdziena piemērošanu konkrētā IKT lietojuma/sistēmas izstrādē. Izstrādājot konkrētas nozares rīcības plānus, būtu jānodrošina, ka tie paredz sistemātisku tiesiskā regulējuma piemērošanu un jo īpaši garantē, ka attiecīgā IKT tiek veidota saskaņā ar integrētās privātās dzīves aizsardzības principu.

53. Attiecībā uz pētniecību – Septītā un turpmākās pamatprogrammas būtu jāizmanto kā rīks, lai atbalstītu projektus, kuru mērķis ir analizēt standartus, IKT tehnoloģijas un arhitektūru, kas labāk nodrošina privātumu un jo īpaši integrētas privātās dzīves aizsardzības principu. Papildus *PbD* principam būtu jākļūst par nepieciešamu elementu, kas jāņem vērā plašākos IKT projektos, kuru mērķis ir personas datu apstrāde.

Jomas, kas izraisa īpašas bažas

54. Ņemot vērā īpašus riskus personu privātumam un datu aizsardzībai vai citus faktorus (rūpniecības nozares nevēlēšanās nodrošināt *PbD* produktus, patērētāju pieprasījums utt.), dažos gadījumos varētu būt nepieciešams likumdošanas un citos instrumentos definēt skaidrākus un specifiskākus pasākumus integrētai privātās dzīves aizsardzībai, kas būtu iestrādājami noteikta veida informācijas un komunikāciju produktā/tehnoloģijā.

55. EDAU ir identificējis vairākas nozares (*RFID*, sociālo tīklu veidošana un pārlūkprogrammu lietojumi), kuras, viņaprāt, šajā posmā Komisijai būtu rūpīgi jāizvērtē un kurām būtu nepieciešams stingrāks regulējums, ņemot vērā iepriekš pausto viedokli. Šīs trīs jomas tiek apspriestas turpmāk.

V. **RADIOFREKVENČU IDENTIFIKĀCIJA – *RFID***

56. *RFID* marķējumu var iestrādāt priekšmetos, dzīvniekos un cilvēkos. Tos var lietot, lai savāktu un uzglabātu personas datus, piemēram, slimības vēsturi, kā arī izsekotu cilvēku pārvietošanos vai dažādiem mērķiem noteiktu uzvedības profilu. Tas ir izdarāms, personām par to nezinot ([1]).

57. Lai sabiedrība uzticētos *RFID* un nākotnes "lietiskajam internetam", ir nepieciešamas efektīvas garantijas attiecībā uz datu aizsardzību, privātumu un visiem saistītajiem ētiskajiem apsvērumiem. Tikai tad tehnoloģijas varēs sniegt to neskaitāmos ekonomiskos un sociālos ieguvumus.

V.1. **Piemērojamā datu aizsardzības tiesiskā regulējuma trūkumi**

58. Datu aizsardzības direktīvu un E-privātuma direktīvu piemēro ar *RFID* lietojumu palīdzību veikto datu apkopošanai ([2]). Cita starpā tās paredz, ka ir nepieciešams ieviest atbilstošu privātuma aizsardzību pirms *RFID* lietojumu darbības uzsākšanas ([3]).

59. Vienlaikus šis tiesiskais regulējums pilnībā neatrisina visas šīs tehnoloģijas izraisītās bažas saistībā ar datu un privātuma aizsardzību. Tas ir tādēļ, ka direktīvas nav pietiekami detalizētas attiecībā uz *RFID* lietojumos ieviešamo aizsardzības mehānismu veidu. Esošos nosacījumus ir nepieciešams papildināt ar tādiem, kas nosaka specifiskus aizsardzības mehānismus, jo īpaši paredzot, ka tehnisku

([1]) *RFID* – radiofrekvenču identifikācija. Radiofrekvenču identifikācijas tehnoloģijas vai infrastruktūras pamatsastāvdaļas ir marķējums (t. i., mikroshēma), lasītājs un lietojumprogramma, kas savienota ar marķējumiem un lasītājiem, izmantojot starpprogrammatūru, un tiek lietota izveidoto datu apstrādei. Marķējumu veido elektroniskā ķēde, kurā tiek glabāti dati, un antenas, kas pārraida datus, izmantojot radioviļņus. Lasītājs ir aprīkots ar antenu un demodulatoru, kas pārvērš ienākošo analogo informāciju no radiolīnijas digitālajos datos. Pēc tam, izmantojot tīklus, informāciju var sūtīt uz datu bāzēm un serveriem tās turpmākai apstrādei datorā.

([2]) E-privātuma direktīvas 3. pants atsaucas uz *RFID*: "Šī direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Kopienā, tostarp publiskos komunikāciju tīklos, kuros var izmantot datu vākšanas un identifikācijas ierīces." To papildina 56. apsvērums: "Tehnoloģiju attīstība dod iespēju izstrādāt jaunas lietotnes, kuru pamatā ir datu vākšanas un identifikācijas ierīces, kas varētu būt bezkontakta ierīces, kuras izmanto radiofrekvences. Piemēram, radiofrekvenču identifikācijas ierīces (RFID) izmanto radiofrekvences, lai no tagiem ar unikālu identifikatoru tvertu datus, ko pēc tam var pārraidīt pa izveidotajiem komunikāciju tīkliem. Šādu tehnoloģiju plaša izmantošana, ja tā iedzīvotājiem ir pieņemama, var dot ievērojamu ekonomisku un sociālu ieguvumu un tādējādi būtiski veicināt iekšējā tirgus darbību. Lai to panāktu, ir jānodrošina, ka tiek aizsargātas visas personu pamattiesības, tostarp tiesības uz privātās dzīves un personas datu aizsardzību. Ja šādas ierīces pieslēdz publiski pieejamiem elektronisko komunikāciju tīkliem vai tās izmanto elektronisko komunikāciju pakalpojumus kā pamata infrastruktūru, būtu jāpiemēro Direktīvas 2002/58/EK (Direktīva par privāto dzīvi un elektronisko komunikāciju) attiecīgie noteikumi, tostarp noteikumi par drošību, informāciju par datu plūsmu un atrašanās vietu un konfidencialitāti."

([3]) Piemēram, Datu aizsardzības direktīvas 17. pantā noteikts, ka ir jāīsteno atbilstoši tehniski un organizatoriski pasākumi, lai aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai nesankcionētu atklāšanu.

risinājumu (integrētas privātās dzīves aizsardzības) iestrāde *RFID* tehnoloģijā ir obligāta. Tas attiecas uz marķējumiem, kuros uzglabā personas datus, kam būtu jāietver deaktivācijas komandas, kā arī uz kriptogrāfijas metožu lietošanu marķējumos, kuros uzglabā noteikta veida personu datus.

V.2. **Pašregulējums kā pirmais solis**

60. Komisija 2007. gada martā pieņēma paziņojumu ([1]), kurā cita starpā atzīta vajadzība izstrādāt detalizētas vadlīnijas praktiskai *RFID* ieviešanai, kā arī nepieciešamība pieņemt projektēšanas kritērijus, lai izvairītos no privātuma un drošības apdraudējuma.

61. Šo mērķu sasniegšanai Komisija 2009. gada maijā pieņēma ieteikumu par privātuma un datu aizsardzības principu īstenošanu *RFID* lietojumos ([2]). Attiecībā uz *RFID* lietojumiem mazumtirdzniecībā tajā ir paredzēta marķējuma deaktivēšana tirdzniecības vietā, ja vien personas neiebilst pret tā saglabāšanu. Tas pieļaujams tikai tad, ja privātuma un datu aizsardzības ietekmes novērtējumā ir atzīts, ka marķējums, ja tas saglabā darbspēju ārpus tirdzniecības vietas, nerada iespējamu privātuma vai personas datu aizsardzības apdraudējumu, un ar nosacījumu, ka personas var pieprasīt marķējuma bezmaksas deaktivēšanu.

62. EDAU atbalsta Komisijas pieeju lietot pašregulācijas instrumentus. Tomēr, kā turpmāk norādīts, ir paredzams, ka pašregulācija nenodrošinās gaidīto rezultātu, līdz ar to EDAU aicina Komisiju būt gatavai pieņemt alternatīvus pasākumus.

V.3. **Jomas, kas izraisa bažas, un iespējamie papildu pasākumi, ja pašregulācija nenodrošina gaidīto**

63. EDAU bažījas, ka *RFID* lietojumus apkalpojošās organizācijas mazumtirdzniecības sektorā varētu neievērot iespēju, ka *RFID* marķējumu varētu novērot nevēlamas trešās personas. Šāda novērošana varētu atklāt marķējumā saglabātos personas datus (ja tādi ir), kā arī ļaut trešai personai vēlāk izsekot vai atpazīt personu, vienkārši izmantojot unikālos identifikatorus, kas ietverti vienā vai vairākos personu pārnēsātājos marķējumos, vidē, kas var būt pat ārpus *RFID* lietojumu darbības zonas. Turklāt EDAU uztrauc, ka *RFID* lietojumu operatoriem varētu būt vēlme pārlieku paļauties uz izņēmuma gadījumu, tādējādi saglabājot marķējuma darbspēju ārpus tirdzniecības vietas.

64. Ja iepriekš minētais piepildās, tad varētu būt pārāk vēlu, lai mazinātu riskus, iespējams, jau skarto personu datu un privātuma aizsardzībai. Vēl jo vairāk, ņemot vērā pašregulējuma iezīmes, valstu ieviešanas iestādes varētu atrasties vājākā pozīcijā, pieprasot *RFID* lietojumu operatoriem piemērot īpašus integrētas privātās dzīves aizsardzības pasākumus.

65. Šajā kontekstā EDAU aicina Komisiju būt gatavai ierosināt tiesību aktu instrumentus, kas regulētu *RFID* lietošanas pamatelementus gadījumā, ja esošā tiesiskā regulējuma efektīva īstenošana neizdodas. Komisijas novērtējuma pieņemšanu nevajadzētu pārlieku atlikt, jo atlikšana pakļautu personas apdraudējumam, turklāt tas varētu negatīvi iespaidot nozari, ņemot vērā pārāk augsto tiesisko nenoteiktību un potenciāli lielākas grūtības un izmaksas, kas nepieciešamas iesakņojušos problēmu risināšanai.

66. Attiecībā uz potenciāli ierosināmajiem pasākumiem EDAU iesaka nodrošināt izvēles principu, atbilstoši kuram visi patēriņa produktiem pievienotie *RFID* marķējumi pēc noklusējuma tiktu deaktivēti tirdzniecības vietā. Varētu būt, ka Komisijai noteikt konkrētu izmantojamo tehnoloģiju nav nepieciešama vai atbilstoša rīcība. Tā vietā Savienības tiesību aktiem būtu jāievieš juridiski saistošs pienākums saņemt piekrišanu, atstājot uzņēmumu ziņā šīs prasības īstenošanas veidu.

V.4. **Citi apspriežamie jautājumi: lietiskā interneta pārvaldība**

67. *RFID* marķējuma radītā informācija, piemēram, informācija par produktu, nākotnē varētu tik iesaistīta globālajā sakaru infrastruktūras tīklā. To parasti sauc par "lietisko internetu". Bažas saistībā ar datu/privātuma aizsardzību rodas, jo, izmantojot *RFID* marķējumu, kas papildu informācijai par produktu var ietvert arī personas datus, ir iespējams identificēt faktiskos priekšmetus/objektus.

68. Joprojām ir neskaidrības attiecībā uz to, kas nodrošinās ar *RFID* marķējumu saistītās informācijas uzglabāšanu. Kā tā tiks organizēta? Kam būs piekļuves tiesības? Komisija 2009. gada jūnijā pieņēma paziņojumu par lietisko internetu ([3]), kurā skaidri norādītas potenciālās datu un privātuma aizsardzības problēmas šajā jomā.

([1]) Komisijas 2007. gada 15. marta paziņojums Eiropas Parlamentam, Padomei, Eiropas ekonomikas un sociālo lietu komitejai un Reģionu komitejai: "Radiofrekvenču identifikācija *(RFID)* Eiropā ceļā uz politikas īstenošanas pasākumiem" (COM(2007) 96 galīgā redakcija).

([2]) Komisijas 2009. gada 12. maija ieteikums: "Par privātuma un datu aizsardzības principu īstenošanu saistībā ar radiofrekvenciālās identificēšanas lietojumiem" (C(2009) 3200 galīgā redakcija).

([3]) Komisijas 2009. gada 18. jūnija paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Lietiskais internets – rīcības plāns Eiropai" (COM(2009) 278 galīgā redakcija).

69. EDAU vēlas uzsvērt dažus no paziņojumā skartajiem jautājumiem, kam, viņaprāt, būtu jāpievērš pienācīga uzmanība, lietiskajam internetam attīstoties. Pirmkārt, decentralizētas arhitektūras nepieciešamība varētu veicināt ES tiesiskā regulējuma pārskatāmību un izpildāmību. Otrkārt, cik vien iespējams, būtu jāsaglabā personas tiesības uz to, ka tā netiek izsekota. Citiem vārdiem, personas bez to piekrišanas ar *RFID* marķējuma palīdzību varētu izsekot tikai ļoti nedaudzos gadījumos. Šādai piekrišanai vajadzētu būt nepārprotamai. To parasti sauc par "mikroshēmu apklusināšanu" *(silence of chips)* un tiesībām uz vienatni. Visbeidzot – integrētai privātās dzīves aizsardzībai vajadzētu būt lietiskā interneta veidošanas pamatprincipam. Tas, piemēram, varētu nozīmēt, ka konkrēti *RFID* lietojumi ar iegultiem mehānismiem, kas sniedz lietotājiem kontroles iespējas, tiek izstrādāti, izmantojot privātuma noklusējuma iestatījumus.

70. EDAU cer, ka Komisija ar to konsultēsies, īstenojot paziņojumā paredzētās darbības, jo īpaši izstrādājot paziņojumu par privātumu un uzticēšanos globālajā informācijas sabiedrībā.

VI. **SOCIĀLIE TĪKLI UN PRIVĀTUMA NOKLUSĒJUMA IESTATĪJUMU NEPIECIEŠAMĪBA**

71. Sociālie tīkli šobrīd ir ļoti populāri. Šķiet, ka tie pārspēj pat e-pastus. Tie vieno cilvēkus ar līdzīgām interesēm un/vai darbībām. Ir iespējams veidot savus profilus tiešsaistē un koplietot tādus multivides failus kā videoklipus, fotoattēlus, mūzikas ierakstus, kā arī karjeras profilus.

72. Sociālo tīklu izmantošana ir strauji kļuvusi populāra jauniešu vidū, un šo tīklu popularitāte arvien pieaug. Pēdējo gadu laikā interneta lietotāju vidējais vecums Eiropā ir samazinājies: bērni deviņu līdz desmit gadu vecumā to lieto vairākas reizes nedēļā, savukārt jaunieši 12 līdz 14 gadu vecumā – katru dienu, nereti no vienas līdz trīs stundām.

VI.1. **Sociālie tīkli un datu/privātuma aizsardzībai piemērojamais tiesiskais regulējums**

73. Sociālo tīklu attīstība ir sniegusi lietotājiem iespēju internetā augšupielādēt informāciju par sevi un trešām personām. To darot, saskaņā ar 29. panta darba grupu [1] interneta lietotāji attiecībā uz to augšupielādētajiem datiem ir uzskatāmi par datu apstrādātajiem atbilstīgi Datu aizsardzības direktīvas bijušajam 2.d pantam [2]. Tomēr lielākajā daļā gadījumu šāda apstrāde ir uzskatāma par mājsaimniecības atbrīvojumam atbilstošu saskaņā ar bijušo direktīvas 3. panta 2. punktu. Vienlaikus sociālo tīklu pakalpojumu sniedzēji ir uzskatāmi par datu apstrādātājiem, ciktāl tie nodrošina līdzekļus lietotāju datu apstrādei un sniedz visus ar lietošanas pārvaldību saistītos pamatpakalpojumus (piemēram, kontu reģistrāciju un dzēšanu).

74. Juridiski tas nozīmē, ka atbilstīgi bijušajam direktīvas 2.d pantam interneta lietotāji un sociālo tīklu pakalpojumu sniedzēji kā "datu apstrādātāji" ir līdzatbildīgi personas datu apstrādē, lai gan atbildības pakāpe un pienākumu kopums atšķiras.

75. Tātad lietotājiem būtu jāzina un jāsaprot, ka, apstrādājot savu un citu personisko informāciju, uz tiem attiecas ES tiesību aktu nosacījumi par datu aizsardzību, kas cita starpā paredz pienākumu iegūt apzinātu piekrišanu no tiem, kuru informācija tiek augšupielādēta, kā arī iesaistītajām personām nodrošināt labošanas, noraidīšanas utt. tiesības. Līdzīgi arī sociālo tīklu pakalpojumu sniedzējiem ir cita starpā jāīsteno pienācīgi tehniskie un organizatoriskie pasākumi, kas, ievērojot apstrādes potenciālos riskus un datu veidu, novērstu nesankcionētu apstrādi. Tas savukārt nozīmē, ka sociālo tīklu pakalpojumu sniedzējiem būtu jānodrošina privātumu veicinoši noklusējuma iestatījumi, tostarp iestatījumi, kas piekļuvi profilam ierobežo līdz lietotāja paša izvēlētām personām. Iestatījumiem būtu jāietver arī prasība saņemt lietotāja piekrišanu pirms tā profils kļūst pieejams trešām personām, un ierobežotas piekļuves profili nedrīkstētu parādīties meklēšanas rezultātos, izmantojot iekšējās meklētājprogrammas.

76. Diemžēl starp likumdošanas prasībām un faktisko izpildi ir starpība. No juridiskā viedokļa raugoties, interneta lietotāji ir uzskatāmi par datu apstrādātājiem un ir pakļauti ES datu un privātuma aizsardzības tiesiskajam regulējumam, tomēr faktiski lietotāji nereti neapzinās šo lomu. Kopumā lietotāji nepietiekami apzinās, ka viņi apstrādā personas datus un ka, publicējot šādu informāciju, ir iespējami privātuma un datu aizsardzības apdraudējumi. Jo īpaši jaunieši publicē informāciju tiešsaistē, neizvērtējot šādas rīcības sekas sev un citiem, piemēram, attiecībā uz turpmāko pieteikšanos izglītības iestādēs vai darbā.

[1] Skatīt 29. panta darba grupas 2009. gada 12. jūnijā pieņemto 163. atzinumu (5/2009) par tiešsaistes sociālo tīklu veidošanu.

[2] " "Personas datu apstrādātājs" ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita iestāde, kura viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus; ja apstrādes nolūkus un līdzekļus nosaka valsts vai Kopienas tiesību akti vai noteikumi, personas datu apstrādātāju vai viņa iecelšanas konkrētos kritērijus var noteikt valsts vai Kopienas tiesību akti."

77. Vienlaikus sociālo tīklu pakalpojumu sniedzēji nereti atteikšanos *(opt-outs)* izvēlas kā noklusējuma iestatījumu, tādējādi sekmējot personiskās informācijas atklāšanu. Citi kā noklusējuma iestatījumu uzliek profilu pieejamību vispārējām meklētājprogrammām. Tas liek apšaubīt faktisko personu piekrišanu informācijas atklāšanai, kā arī sociālo tīklu atbilstību direktīvas 17. panta nosacījumiem (aprakstīts iepriekš), kas paredz pienācīgu tehnisku un organizatorisku pasākumu īstenošanu, lai novērstu nesankcionētu apstrādi.

VI.2. **Sociālo tīklu izraisītie riski un ieteicamās darbības to novēršanai**

78. Iepriekš minētais palielina personu privātuma un datu aizsardzības apdraudējumu. Tas pakļauj interneta lietotājus, kā arī personas, kuru dati tiek augšupielādēti, acīmredzamiem viņu privātuma un datu aizsardzības tiesību pārkāpumiem.

79. Šādā kontekstā jautājums, uz kuru Komisijai jāatbild, ir šāds – kas būtu jādara un ko būtu iespējams darīt, lai šo problēmu risinātu. Šajā atzinumā netiek sniegta visaptveroša atbilde uz jautājumu, tā vietā tiek piedāvāti vairāki priekšlikumi turpmākai izvērtēšanai.

Ieguldījumi interneta lietotāju izglītībā

80. Pirmais priekšlikums ir ieguldīt lietotāju izglītībā. Tātad ES iestādēm un dalībvalstīm būtu jāiegulda līdzekļi, lai izglītotu un uzlabotu izpratni par sociālo tīklu tīmekļa vietņu izraisītajiem draudiem. Tā, piemēram, Informācijas sabiedrības un saziņas līdzekļu ĢD īsteno programmu "Drošāks internets", kuras mērķis ir dot iespējas un aizsargāt bērnus un jauniešus, līdzfinansējot, piemēram, izpratnes veicināšanas pasākumus ([1]). Nesen ES iestādes uzsāka kampaņu "Padomā, pirms ievieto internetā" ar nolūku veicināt izpratni par apdraudējumu, ko rada personiskas informācijas koplietošana ar svešiniekiem.

81. EDAU aicina Komisiju turpināt atbalstīt šāda veida darbības. Vienlaikus arī pašiem sociālo tīklu pakalpojumu nodrošinātājiem vajadzētu būt aktīviem, jo viņi ir juridiski un sociāli atbildīgi par lietotāju izglītošanu attiecībā uz viņu pakalpojumu izmantošanu drošā un privātumu neapdraudošā veidā.

82. Kā minēts iepriekš, sociālajā tīklā publicēto informāciju dažādos veidos ir iespējams padarīt pieejamu visiem, izmantojot noklusējuma iestatījumus. Tā, piemēram, informācija var būt pieejama sabiedrībai kopumā, tostarp caur meklētājprogrammām, kas tai var piešķirt indeksu un tādā veidā arī tieši novirzīt. Tomēr informācijas pieejamību var ierobežot, piešķirot piekļuves tiesības "izvēlētiem draugiem", vai arī saglabāt tās pilnīgu privātumu. Protams, tīmekļa vietnēs profila pieejamība un lietotā terminoloģija atšķiras.

83. Vienlaikus, kā uzsvērts iepriekš, tikai retais sociālās tīklošanas pakalpojumu lietotājs zina, kā regulēt piekļuvi viņu publicētajai informācijai, un tikai retais domā par to, kā mainīt privātuma noklusējuma iestatījumus. Privātuma iestatījumi parasti netiek mainīti, jo lietotāji neapzinās šādas bezdarbības sekas, vai arī nezina, kā tas izdarāms. Līdz ar to vairākumā gadījumu privātuma iestatījumu nenomainīšana nenozīmē, ka personas ir pieņēmušas apzinātu lēmumu koplietot informāciju. Tādēļ ir jo īpaši svarīgi, ka trešās personas, piemēram, meklētājprogrammas neuzrāda individuālos profilus, balstoties uz pieņēmumu, ka, nenomainot noklusējuma iestatījumus (attiecībā uz privātumu), lietotāji ir piekrituši informācijas vispārējai pieejamībai.

84. Kaut arī lietotāju izglītošana varētu līdzēt problēmas risināšanā, tomēr ir nepieciešamas arī papildu darbības. Kā savā atzinumā par sociālajiem tīkliem ierosina 29. panta darba grupa, sociālo tīklu pakalpojumu nodrošinātājiem būtu jāpiedāvā privātumu neapdraudoši bezmaksas privātuma noklusējuma iestatījumi. Tas ļautu lietotājiem labāk apzināties savas darbības, kā arī ļautu pamatotāk izlemt, vai viņi vēlas apmainīties ar informāciju, un ja vēlas, tad ar ko.

Pašregulējuma loma

85. Komisija ir noslēgusi nolīgumu ar 20 sociālo tīklu pakalpojumu sniedzējiem, kas zināms kā "Drošāki sociālo kontaktu veidošanas principi Eiropas Savienībai" ([2]). Nolīguma mērķis ir uzlabot nepilngadīgo drošību, kad viņi izmanto sociālo kontaktu vietnes Eiropā. Šādi principi ietver daudzus nosacījumus, kas izriet no iepriekš aprakstītā datu aizsardzības tiesiskā regulējuma. Tie ietver, piemēram, nosacījumu, ka ar rīku un tehnoloģiju palīdzību ir jāsniedz lietotājiem iespējas pašiem kontrolēt savas personiskās informācijas lietojumu un izplatīšanu. Tajā ir ietverta arī nepieciešamība nodrošināt privātuma noklusējuma iestatījumus.

86. Komisija 2010. gada janvāra sākumā nāca klajā ar ziņojumu, kurā ietverti principu īstenošanas novērtējuma rezultāti ([3]). EDAU bažījas par ziņojumā norādīto – proti, vairāki pasākumi ir veikti, tomēr daudzi citi nav. Tā, piemēram, ziņojumā minētas problēmas attiecībā uz informācijas pieejamību par tīmekļa vietnēs pieejamajiem drošības pasākumiem un rīkiem. Tāpat tajā norādīts,

([1]) Informācija par šādu programmu ir pieejama: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Principi ir pieejami: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) *Report on the assessment of the implementation of the Safer Social Network Principles for the EU*, pieejams: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

ka mazāk kā puse nolīguma parakstītāju ir ierobežojuši piekļuvi nepilngadīgo profiliem, padarot to pieejamu tikai viņu draugiem.

Nepieciešamība iekļaut privātuma aizsardzību kā obligātu noklusējuma iestatījumu

87. Saistībā ar šo galvenais jautājums ir par to, vai ir nepieciešami papildu politikas pasākumi, lai nodrošinātu, ka sociālajos tīklos ir iestrādāti privātuma noklusējuma iestatījumi. Šo jautājumu aktualizēja iepriekšējā informācijas sabiedrības komisāre *Viviane Reding*, kas norādīja uz iespējamu tiesību aktu nepieciešamību ([1]). Līdzīgi arī Eiropas Ekonomikas un sociālo lietu komiteja norādīja, ka paralēli pašregulējumam minimālos aizsardzības standartus būtu nepieciešams noteikt arī tiesību aktos ([2]).

88. Kā iepriekš norādīts, sociālo tīklu pakalpojumu sniedzēju pienākums iestrādāt privātuma noklusējuma iestatījumus ir netieši noteikts Datu aizsardzības direktīvas 17. pantā ([3]), kas paredz datu apstrādātājiem veikt pienācīgus tehniskos un organizatoriskos pasākumus ("gan apstrādes sistēmas izveides laikā, gan pašas apstrādes laikā"), lai, ievērojot datu apstrādes riskus un šo datu veidu, saglabātu to drošību un novērstu jebkādu nesankcionētu apstrādi.

89. Tomēr šis pants ir pārlieku vispārīgs un tam trūkst konkrētības arī šajā saistībā. Tas skaidri neraksturo pienācīgus tehniskos un organizatoriskos pasākumus sociālo tīklu kontekstā. Tādēļ šobrīd pastāv tiesiska nenoteiktība, kas rada problēmas gan regulētājiem, gan personām, kuru privātums un personas dati netiek pilnībā aizsargāti.

90. Ņemot vērā iepriekš minēto, EDAU aicina Komisiju sagatavot tiesību aktus, kas iekļautu vismaz vispārēju nosacījumu attiecībā uz obligātiem privātuma aizsardzības iestatījumiem, kuru papildinātu konkrētākas prasības:

a) nodrošināt iestatījumus, kuru rezultātā piekļūt lietotāju profiliem var tikai viņu pašu izvēlētas personas. Iestatījumos būtu jānosaka arī, ka pirms profila pieejamības trešām personām ir nepieciešams lietotāja apstiprinājums;

b) nodrošināt, ka ierobežotas piekļuves profili neuzrādītos iekšējo/ārējo meklētājprogrammu meklējumos.

91. Līdztekus obligātai privātuma noklusējuma iestatījumu nodrošināšanai joprojām ir aktuāls jautājums par to, vai papildu konkrēti datu aizsardzības un citi pasākumi (piemēram, attiecībā uz nepilngadīgo aizsardzību) arī būtu atbilstoši. Plašākā kontekstā tas ir jautājums par to, vai līdztekus obligātai privātuma iestatījumu nodrošināšanai būtu adekvāti radīt konkrētu satvaru arī šādiem pakalpojumiem, kas attiecīgi regulētu citus aspektus. EDAU lūdz Komisiju ņemt vērā šo jautājumu.

VII. **PRIVĀTUMA NOKLUSĒJUMA IESTATĪJUMI PĀRLŪKPROGRAMMĀS, LAI GARANTĒTU APZINĀTU PIEKRIŠANU SAŅEMT REKLĀMAS**

92. Reklāmu tīklu pakalpojumu sniedzēji izmanto sīkfailus un citas ierīces, lai novērotu lietotāju uzvedību, viņiem klejojot internetā, ar nolūku apkopot informāciju par viņu interesēm un izveidot profilus. Vēlāk šī informācija tiek izmantota, lai izsūtītu attiecīgās reklāmas ([4]).

VII.1. **Atlikušās problēmas un riski pašreizējā datu/privātuma aizsardzības tiesiskajā regulējumā**

93. Datu apstrādi regulē Datu aizsardzības direktīva (attiecībā uz personas datiem) un arī E-privātuma direktīvas 5. panta 3. punkts. Šis pants precīzi nosaka, ka lietotājs ir jāinformē un viņam ir jāsniedz iespēja piekrist vai noraidīt ierīču, tādu kā sīkfaili utt., uzglabāšanu viņu datorā vai citā ierīcē ([5]).

94. Līdz šim reklāmu tīklu pakalpojumu sniedzēji ir paļāvušies, ka pārlūkprogrammu iestatījumi un privātuma aizsardzības stratēģijas nodrošinās lietotāju informētību un ļaus viņiem atļaut vai noraidīt sīkfailu saņemšanu. Viņi ir skaidrojuši izdevēju privātuma stratēģijās, kā atteikties

([1]) Par informācijas sabiedrību un plašsaziņas līdzekļiem atbildīgā Eiropas Komisijas locekle *Viviane Reding*: Padomā, pirms ievieto internetā! Kā padarīt sociālo kontaktu veidošanas vietnes drošākas bērniem un pusaudžiem? Drošāka interneta diena Strasbūrā 2010. gada 9. februārī.

([2]) Eiropas Ekonomikas un sociālo lietu komitejas atzinums par sociālo tīklu vietņu ietekmi uz pilsoņiem/patērētājiem (2009. gada 4. novembris).

([3]) Plašāk analizēts arī šā dokumenta 33. punktā.

([4]) Izsekojošie sīkfaili ir mazi teksta faili ar unikālu identifikatoru. Parasti reklāmu tīklu pakalpojumu sniedzēji (tāpat kā tīmekļa vietņu operatori vai izdevēji) novieto sīkfailus uz apmeklētāju datora cietā diska, īpaši interneta lietotāju pārlūkprogrammās, viņiem pirmoreiz apmeklējot tīmekļa vietnes, kas sniedz reklāmas pakalpojumus kā daļu no sava tīkla. Sīkfails ļauj reklāmu tīkla pakalpojumu sniedzējam atpazīt apmeklētāju, kas atkārtoti atgriežas tīmekļa vietnē vai arī apmeklē jebkuru citu tīmekļa vietni, kas ir reklāmas tīkla partneris. Šādi atkārtoti apmeklējumi ļaus reklāmas tīklu pakalpojumu sniedzējiem izveidot apmeklētāju profilu.

([5]) E-privātuma direktīvas 5. panta 3. pants nesen tika grozīts, lai uzlabotu aizsardzību pret lietotāju sakaru pārtveršanu, izmantojot, piemēram, lietotāja datorā vai citā ierīcē uzglabāto spiegprogrammatūru vai sīkfailus. Atbilstīgi jaunajai direktīvai lietotājus būtu labāk jāinformē, kā arī jāpiedāvā vieglākas kontroles iespējas attiecībā uz viņu vēlmi uzglabāt sīkfailus savā gala iekārtā.

no sīkfailu saņemšanas pilnībā vai arī atļaut to atkarībā no attiecīgā gadījuma. To darot, viņi ir centušies izpildīt savu pienākumu sniegt lietotājiem iespēju atteikties no sīkfailu saņemšanas.

95. Kaut arī teorētiski šī metode (ar pārlūkprogrammu) varētu nodrošināt jēgpilnu, apzinātu piekrišanu, faktiskā situācija ir pavisam citāda. Kopumā lietotājiem nav pat pamata sapratnes par jebkādu datu savākšanu, vēl jo vairāk, ka to dara trešās personas, šādu datu vērtību, to izmantošanu, tehnoloģijas darbību un jo īpaši, kā un kur var atteikties. Darbības, kas veicamas lietotājam, lai atteiktos, šķiet ne tikai sarežģītas, bet arī pārmērīgas (vispirms ir jāiestata pārlūkprogramma, lai saņemtu sīkfailus, un tad jāveic atteikšanās funkcija).

96. Rezultātā tikai nedaudzi veic atteikšanās funkciju, un ne tādēļ, ka viņi ir pieņēmuši apzinātu lēmumu saņemt uz viņu uzvedību balstītu reklāmu, bet drīzāk tādēļ, ka viņi neapzinās, ka, neizmantojot atteikšanās iespēju, viņi patiesībā piekrīt to saņemt.

97. Tādējādi, lai gan no juridiskā viedokļa E-privātuma direktīvas 5. panta 3. punkts nodrošina efektīvu tiesisku aizsardzību, faktiski, interneta lietotāji ir pakļauti novērošanai ar nolūku nosūtīt uz viņu uzvedības balstītu reklāmu, kaut arī faktiski daudzos, ja ne lielākajā daļā gadījumu, viņi vispār neapzinās, ka tiek novēroti.

98. 29. panta darba grupa gatavo atzinumu, kura mērķis ir skaidrot juridiskos nosacījumus uz uzvedību balstītas reklāmas veikšanai, kas ir apsveicami. Tomēr situācijas risināšanai ar interpretāciju varētu nepietikt un varētu būt, ka Eiropas Savienībai būs jāveic papildu darbības.

VII.2. **Turpmākas rīcības, tas ir, obligātas privātuma noklusējuma iestatījumu nodrošināšanas, nepieciešamība**

99. Kā minēts iepriekš, tīmekļa pārlūkprogrammas parasti pieļauj zināmas kontroles iespējas attiecībā uz konkrētiem sīkfailu veidiem. Šobrīd vairākuma tīmekļa pārlūkprogrammu noklusējuma iestatījumi pieļauj visu sīkfailu saņemšanu. Citiem vārdiem, pārlūkprogrammas ir iestatītas tā, lai saņemtu visus sīkfailus neatkarīgi no to mērķiem. Tikai gadījumos, kad lietotāji maina iestatījumus savos pārlūkprogrammu lietojumos, lai noraidītu sīkfailu saņemšanu, viņi tos nesaņems, bet kā minēts iepriekš, tikai retais lietotājs šādu darbību veic. Turklāt, pirmoreiz instalējot vai atjauninot pārlūkprogrammu lietojumus, privātuma vednis nedarbojas.

100. Šo problēmu varētu risināt, pārlūkprogrammās iestrādājot privātuma noklusējuma iestatījumus. Citiem vārdiem sakot, ja tajās būtu nodrošināts iestatījums "nepieņemt trešo personu sīkfailus". Lai šo risinājumu papildinātu un padarītu to efektīvāku, pārlūkprogrammām būtu jāpieprasa, lai lietotāji izskatītu privātuma vedni, pirmoreiz instalējot vai atjauninot pārlūkprogrammu. Ir nepieciešams vairāk granularitātes un skaidrākas informācijas par sīkfailu veidiem un dažu noderīgumu. Lietotāji, kas vēlas tikt novēroti ar nolūku saņemt reklāmu, tiks pienācīgi informēti un viņiem vajadzēs mainīt iestatījumus. Tas sniegtu labākas kontroles iespējas pār viņu personas datiem un privātumu. EDAU uzskata, ka tas būt efektīvs veids, kā cienīt un saglabāt lietotāju piekrišanu ([1]).

101. No vienas puses, ņemot vērā problēmas plašumu, citiem vārdiem, pašreiz uz iluzoras piekrišanas balstītu novēroto interneta lietotāju skaitu, no otras puses, problēmas svarīgumu, papildu aizsardzības mehānismu nepieciešamība kļūst aktuālāka. *PbD* principa iestatīšana tīmekļa pārlūkprogrammās varētu sniegt būtisku ieguldījumu, lai sniegtu personām iespēju kontrolēt datu savākšanu, kas tiek veikta reklāmas mērķiem.

102. Lai sekmētu šos mērķus, EDAU aicina Komisiju apsvērt likumdošanas pasākumus, pieprasot obligātu privātuma noklusējuma iestatījumu iestrādi pārlūkprogrammās un attiecīgās informācijas nodrošināšanu.

VIII. **CITI UZ PERSONU PRIVĀTUMA/DATU AIZSARDZĪBU VĒRSTI PRINCIPI**

103. Lai gan ar *PbD* principa ieviešanu ir lielas iespējas uzlabot personu datu un privātuma aizsardzību, papildu principu ieviešana tiesību aktu izstrādē un īstenošanā ir nepieciešama, lai nodrošinātu patērētāju uzticēšanos IKT. Šajā saistībā EDAU norāda uz pārskatāmības principu un obligātā drošības pārkāpumu regulējuma pieņemšanu, kas būt piemērojams visās nozarēs.

VIII.1. **Pārskatāmības princips, lai nodrošinātu atbilstību integrētas privātās dzīves aizsardzības principam**

104. 29. panta darba grupa dokumentā "Future of Privacy" ([2]) ir ieteikusi iekļaut pārskatāmības principu Datu aizsardzības direktīvā. Šis vairākos starptautiskos datu aizsardzības

([1]) Vienlaikus EDAU apzinās, ka šis problēmu neatrisinātu pilnībā, jo ir sīkfaili, kurus nevar kontrolēt caur pārlūkprogrammu, piemēram, tā dēvētos programmas *Flash* sīkfailus. Lai risinātu šo situāciju, varētu būt nepieciešams, ka pārlūkprogrammu izstrādātāji integrē zibatmiņas kontroles savās sīkfailu kontrolēs kā noklusējuma iestatījumus attiecībā uz jaunajām pārlūkprogrammām.

([2]) 29. panta darba grupas 2009. gada 1. decembrī pieņemtais 168. atzinums par *The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.*

instrumentos ([1]) atzītais princips paredz, ka iestādēm ir jāievieš procesi, lai nodrošinātu atbilstību esošajiem tiesību aktiem, kā arī jāizstrādā metodes, lai novērtētu un parādītu atbilstību tiesību aktiem un citiem saistošiem instrumentiem.

105. EDAU pilnībā atbalsta 29. panta darba grupas ieteikumu. Tas uzskata, ka šis princips būs ļoti svarīgs, lai veicinātu efektīvu datu aizsardzības principu un pienākumu piemērošanu. Atbilstīgi pārskatāmības principam datu apstrādātājiem būs jāpierāda, ka viņi ir ieviesuši nepieciešamos mehānismus, lai ievērotu attiecīgos datu aizsardzības tiesību aktus. Tas visticamāk sniegs ieguldījumu efektīvā integrētas privātās dzīves aizsardzības kā īpaši piemērota pārskatāmību apliecinoša elementa ieviešanā IKT tehnoloģijās.

106. Lai izvērtētu un parādītu pārskatāmību, datu apstrādātāji varētu izmantot iekšējās procedūras, savukārt trešās personas, kas veic auditu vai cita veida pārbaudes un verifikāciju, noslēgumā varētu piešķirt apstiprinājumu vai balvas. Šajā kontekstā EDAU aicina Komisiju apsvērt, vai papildus vispārējam pārskatāmības principam būtu noderīgi tiesību aktos noteikt konkrētus pasākumus pārskatāmības nodrošināšanai, piemēram, izstrādāt privātuma un datu aizsardzības ietekmes novērtējumu un nosacījums, ar kādiem tas izstrādājams.

VIII.2. **Drošības pārkāpumi: tiesiskā regulējuma pabeigšana**

107. Pagājušā gada grozījumi E-privātuma direktīvā ieviesa prasību paziņot par datu aizsardzības pārkāpumiem cietušajām personām un arī attiecīgajām iestādēm. Datu aizsardzības pārkāpums ir vispārēji definēts kā jebkurš ar pakalpojumu saistīts pārkāpums, kura rezultātā notiek nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, izpaušana utt. Personu informēšana tiks pieprasīta, ja ir ticams, ka drošības pārkāpums varētu nelabvēlīgi ietekmēt viņu personas datus vai privātumu. Tas varētu attiekties uz gadījumiem, kad pārkāpums varētu izraisīt identitātes piesavināšanos, nopietnu pazemojumu vai kaitējumu reputācijai. Attiecīgo iestāžu informēšana par jebkuru datu aizsardzības pārkāpumu būs obligāta neatkarīgi no tā, vai tie rada personu apdraudējumu.

Nosacījumu piemērošana attiecībā uz drošības pārkāpumiem visās nozarēs

108. Diemžēl šis nosacījums attiecas tikai uz publiski pieejamiem elektronisko sakaru pakalpojumiem, piemēram, tālruņu sakaru uzņēmumiem, interneta piekļuves pakalpojumu sniedzējiem, tīmekļa e-pasta pakalpojumu sniedzējiem utt. EDAU aicina Komisiju iesniegt priekšlikumus par drošības pārkāpumu nosacījumu piemērošanu visās nozarēs. Attiecībā uz šāda regulējuma saturu EDAU uzskata, ka drošības pārkāpumu tiesiskais regulējums, kas iekļauts E-privātuma direktīvā, norāda uz pieņemamu līdzsvaru starp personu tiesību aizsardzību, tostarp tiesību uz personas datu un privātuma neaizskaramību, un nosacījumiem, kas vērsti uz attiecīgām iestādēm. Vienlaikus tas ir regulējums ar "īstiem zobiem", jo tas ietver jēgpilnus īstenošanas nosacījumus, kas iestādēm sniedz pietiekamas pilnvaras izmeklēt un sodīt nepakļaušanās gadījumā.

109. Tādējādi EDAU aicina Komisiju pieņemt tiesību akta priekšlikumu, lai šo regulējumu piemērotu visām nozarēm, to pienācīgi pielāgojot, ja nepieciešams. Papildus tiktu nodrošināta standartu un procedūru vienotība visās nozarēs.

E-privātuma direktīvā iestrādāto tiesiska regulējuma pabeigšana, izmantojot komitoloģijas procedūru

110. Pārskatītā E-privātuma direktīva ļauj Komisijai pieņemt tehniskus īstenošanas pasākumus, t. i., detalizētus pasākumus attiecībā uz datu drošības pārkāpumu paziņošanu, piemērojot komitoloģijas procedūru ([2]). Šādas pilnvaras ir pamatotas ar nepieciešamību nodrošināt konsekventu drošības pārkāpumu tiesiskā regulējuma īstenošanu un piemērošanu. Konsekventa īstenošana sekmē to, ka personas visā Kopienā saņem vienādi augsta līmeņa aizsardzību un ka attiecīgās iestādes nav apgrūtinātas ar atšķirīgiem paziņošanas nosacījumiem.

111. E-privātuma direktīvu pieņēma 2009.gada novembrī. Nav redzamu attaisnojošu iemeslu, kādēļ būtu atliekams darbs pie tehnisko īstenošanas pasākumu pieņemšanas. EDAU rīkoja divus semināru, kuru mērķis bija dalīties ar un apkopot informāciju attiecībā uz paziņošanu par datu aizsardzības pārkāpumiem. EDAU labprāt dalītos ar šādā veidā iegūtajiem rezultātiem un cer sadarboties ar Komisiju un citām ieinteresētajām personām, lai uzlabotu vispārējo datu aizsardzības pārkāpumu tiesisko regulējumu.

112. EDAU aicina Komisiju veikt nepieciešamās darbības īsā laikā. Pirms tehnisko īstenošanas pasākumu pieņemšanas Komisijai ir jāiesaistās plašā diskusijā, kurā jākonsultējas ar Eiropas Tīklu un informācijas drošības aģentūru, EDAU un 29. panta darba grupu. Turklāt diskusijā ir jāiesaista arī citas "attiecīgās ieinteresētās personas", jo īpaši, lai informētu par labākajiem iespējamajiem tehniskajiem un ekonomiskajiem īstenošanas līdzekļiem.

([1]) EDSO vadlīnijas, kas regulē privātās dzīves aizsardzību un personas datu pārrobežu plūsmu (1980); *Madrid Privacy Declaration on Global Privacy Standards for a Global World* (2009. gada 3. novembris).

([2]) Atbilstīgi komitoloģijas procedūrai tehniskās īstenošanas pasākumus pieņem dalībvalstu pārstāvju komiteja, ko vada Komisija. E-privātuma direktīvas gadījumā tiek piemērota tā saucamā regulatīvās kontroles procedūra, proti, gan Eiropas Parlaments, gan Padome var iebilst pret Komisijas ierosinātajiem pasākumiem. Plašāka informācija: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **SECINĀJUMI**

113. Uzticēšanās vai drīzāk tās trūkums ir atzīta par galveno problēmu informācijas un komunikāciju tehnoloģiju radīšanā un veiksmīgā ieviešanā. Ja cilvēki neuzticēsies tehnoloģijām, tās visticamāk netiks attīstītas. Uzticēšanās IKT ir atkarīga no dažādiem faktoriem; galvenais faktors ir nodrošināt, ka šīs tehnoloģijas nesagrauj personu pamattiesības uz privātuma un personas datu neaizskaramību.

114. Lai turpinātu stiprināt datu/privātuma aizsardzības tiesisko regulējumu, kura principi ir pilnībā attiecināmi arī uz informācijas sabiedrību, EDAU ierosina Komisijai iestrādāt integrētas privātās dzīves aizsardzības principu dažādos tiesību aktu un politikas veidošanas līmeņos.

115. EDAU iesaka Komisijai īstenot četrus darbības virzienus:

a) ierosināt datu aizsardzības tiesiskajā regulējumā iekļaut vispārīgu nosacījumu attiecībā uz integrētu privātās dzīves aizsardzību. Šim nosacījumam vajadzētu būt tehnoloģiski neitrālam un tā ievērošanai – obligātai dažādos posmos;

b) šo vispārīgo nosacījumu rūpīgi iestrādāt īpašos nosacījumos, ierosinot īpašus tiesiskos instrumentus dažādās nozarēs. Šos īpašos nosacījumus jau šobrīd varētu iestrādāt tiesiskajos instrumentos, pamatojoties uz Datu aizsardzības direktīvas 17. pantu (un citiem spēkā esošiem tiesību aktiem);

c) iekļaut *PbD* kā galveno principu Eiropas Digitalizācijas programmā;

d) ieviest *PbD* kā principu citās ES iniciatīvās (galvenokārt ar likumdošanu nesaistītās).

116. Trijās minētajās IKT nozarēs EDAU iesaka Komisijai izvērtēt nepieciešamību izstrādāt priekšlikumus, lai ieviestu integrētas privātās dzīves aizsardzības principu īpašos/konkrētos veidos:

a) attiecībā uz *RFID* ierosināt tiesību aktu pasākumus, lai regulētu *RFID* lietošanas pamata jautājumus gadījumā, ja neizdodas efektīva esošā tiesiskā regulējuma (caur pašregulējumu) īstenošana. Jo īpaši nodrošināt piekrišanas izvēles principu, atbilstoši kuram visi patēriņa produktiem pievienotie *RFID* marķējumi noklusējuma režīmā tiktu deaktivēti tirdzniecības vietā;

b) attiecībā uz sociālajiem tīkliem sagatavot tiesību aktus, kas iekļautu vismaz vispārēju pienākumu attiecībā uz obligātiem privātuma aizsardzības iestatījumiem, kuru papildinātu konkrētākas prasības, un kas piekļuvi lietotāju profiliem ierobežotu līdz lietotāja paša izvēlētām personām, kā arī nodrošinātu, ka ierobežotas piekļuves profili neuzrādītos iekšējo/ārējo meklētājprogrammu meklējumos;

c) attiecībā uz uzvedībā balstītu reklāmu apsvērt tiesību aktus, kas noteiktu, ka pārlūkprogrammās ir noklusējuma iestatījumi trešo personu sīkfailu noraidīšanai un lietotāju pienākumam izskatīt privātuma vedni, pirmoreiz instalējot vai atjauninot pārlūkprogrammu.

117. Visbeidzot EDAU ierosina Komisijai:

a) apsvērt pārskatāmības principa iestrādi esošajā Datu aizsardzības direktīvā un

b) izstrādāt noteikumu un procedūru kopu, lai ieviestu nosacījumus attiecībā uz drošības pārkāpumu paziņošanu atbilstīgi E-privātuma direktīvai, kā arī paplašināt tās piemērošanu, attiecinot to uz visiem datu apstrādātājiem.

Briselē, 2010. gada 18. martā

Peter HUSTINX

Eiropas datu aizsardzības uzraudzītājs