I

(Rezolūcijas, ieteikumi un atzinumi)

ATZINUMI

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS

Eiropas datu aizsardzības uzraudzītāja 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)

(2008/C 181/01)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Eiropas Kopienas dibināšanas līgumu un jo īpaši tā 286. pantu,

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

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

ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē [2],

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 un jo īpaši tās 41. pantu [3],

ņemot vērā lūgumu nākt klajā ar atzinumu saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu, kas no Eiropas Komisijas saņemts 2007. gada 16. novembrī,

IR PIEŅĒMIS ŠO ATZINUMU.

I. **IEVADS**

1. Komisija 2007. gada 13. novembrī pieņēma priekšlikumu direktīvai, ar ko groza, citu starpā, Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (še turpmāk "priekšlikums" vai "ierosinātie grozījumi"). Direktīva 2002/58/EK pašreizējā versijā parasti, un tāpat arī šajā atzinumā, tiek saukta par e-privātuma direktīvu.

([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.

2. Priekšlikuma mērķis ir uzlabot personas privātās dzīves un personas datu aizsardzību elektronisko komunikāciju nozarē. To veic nevis pilnībā pārveidojot spēkā esošo e-privātuma direktīvu, bet gan ierosinot tajā *ad hoc* grozījumus, kas galvenokārt vērsti uz to, lai nostiprinātu ar drošību saistītus noteikumus un pilnveidotu izpildes mehānismus.

3. Priekšlikums ir daļa no plašākas piecu ES telekomunikāciju direktīvu reformas ("telekomunikāciju pakete"). Papildus priekšlikumiem pārskatīt telekomunikāciju paketi ([1]) Komisija vienlaikus pieņēma arī priekšlikumu regulai, ar ko izveido Eiropas Elektronisko sakaru tirgus iestādi ([2]).

4. Piezīmes šajā atzinumā attiecas vienīgi uz ierosinātajiem grozījumiem e-privātuma direktīvā, ja vien šādi ierosinātie grozījumi nav balstīti uz jēdzieniem vai noteikumiem, kas ietverti priekšlikumos pārskatīt telekomunikāciju paketi. Turklāt dažas šajā atzinumā iekļautās piezīmes attiecas uz e-privātuma direktīvas noteikumiem, kas ar šo priekšlikumu netiek grozīti.

5. Šajā atzinumā ir aplūkoti šādi temati: i) e-privātuma direktīvas darbības joma, jo īpaši attiecīgie pakalpojumi (ierosināts grozījums 3. panta 1. punktā); ii) ziņošana par drošības pārkāpumiem (ierosināts grozījums, ar ko 4. pantā iekļauj 3. un 4. punktu); iii) noteikumi par sīkdatnēm, spiegprogrammām un citām līdzīgām ierīcēm (ierosināts grozījums 5. panta 3. punktā); iv) tiesiskās darbības, ko uzsāk elektronisko komunikāciju pakalpojumu sniedzēji un citas juridiskas personas (ierosināts grozījums, ar ko iekļauj 13. panta 6. punktu) un v) izpildes noteikumu nostiprināšana (ierosināts grozījums, ar ko iekļauj 15.a pantu).

Konsultācijas ar EDAU un plašāka sabiedriska apspriešana

6. Komisija nosūtīja šo priekšlikumu EDAU 2007. gada 16. novembrī. EDAU šo paziņojumu saprot kā lūgumu konsultēt Kopienas iestādes un struktūras, kā paredzēts 28. panta 2. punktā Regulā (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 (turpmāk tekstā "Regula (EK) Nr. 45/2001").

7. Pirms priekšlikuma pieņemšanas Komisija neoficiāli apspriedās ar EDAU par priekšlikuma projektu, ko EDAU uzņēma atzinīgi, jo tas deva viņam iespēju nākt klajā ar dažiem ierosinājumiem priekšlikuma projektā, kamēr Komisija to vēl nav pieņēmusi. EDAU ar gandarījumu konstatē, ka daži no viņa ierosinājumiem ir iekļauti priekšlikumā.

8. Līdz priekšlikuma pieņemšanai notika plaša sabiedriska apspriešana, ko EDAU uzskata par ļoti svarīgu. Komisija jau 2006. gada jūnijā uzsāka publisku apspriešanu par tās paziņojumu saistībā ar telekomunikāciju paketes pārskatīšanu, kurā Komisija izklāstīja savu viedokli par esošo stāvokli un nāca klajā ar dažiem grozījumu priekšlikumiem ([3]). 29. panta datu aizsardzības darba grupa ("WP 29"), kurai EDAU ir piederīgs, izmantoja šo iespēju, lai paustu savu viedokli par ierosinātajiem grozījumiem atzinumā, kas tika pieņemts 2006. gada 26. septembrī ([4]).

([1]) Ierosinātie grozījumi telekomunikāciju direktīvās ir ietverti šādos priekšlikumos: i) Priekšlikums Eiropas Parlamenta un Padomes direktīvai, ar ko groza Direktīvu 2002/21/EK par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem, Direktīvu 2002/19/EK par piekļuvi elektronisko komunikāciju tīkliem un ar tiem saistītām iekārtām un to savstarpēju savienojumu un Direktīvu 2002/20/EK par elektronisko komunikāciju tīklu un pakalpojumu atļaušanu, 13.11.2007., COM(2007) 697 galīgā redakcija; ii) Priekšlikums Eiropas Parlamenta un Padomes direktīvai, ar ko groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem, Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē un Regulu (EK) Nr. 2006/2004 par sadarbību patērētāju tiesību aizsardzības jomā, 13.11.2007., COM(2007) 698 galīgā redakcija.

([2]) Priekšlikums Eiropas Parlamenta un Padomes Regulai, ar ko izveido Eiropas Elektronisko sakaru tirgus iestādi 13.11.2007., COM(2007) 699 galīgā redakcija.

([3]) Paziņojums par ES tiesisko regulējumu elektronisko sakaru tīkliem un pakalpojumiem {SEC(2006) 816}, pieņemts 2006. gada 29. jūnijā. Paziņojumam pievienots Komisijas Darba dokuments {COM(206) 334 galīgā redakcija}.

([4]) Atzinums 8/2006 par ES tiesiskā regulējuma elektronisko sakaru un pakalpojumu jomā pārskatīšanu, galvenokārt pievēršoties e-privātuma direktīvai, pieņemts 2006. gada 26. septembrī.

EDAU vispārējais viedoklis

9. Kopumā EDAU viedoklis par šo priekšlikumu ir pozitīvs. EDAU pilnībā atbalsta mērķus, kuru vārdā Komisija pieņēmusi priekšlikumu uzlabot personas privātās dzīves un personas datu aizsardzību elektronisko komunikāciju nozarē. EDAU ir īpaši gandarīts par to, ka pieņemta sistēma obligātai ziņošanai par drošības pārkāpumiem (grozījums e-privātuma direktīvas 4. pantā, iekļauj 3. un 4. punktu). Ziņošanai drošības pārkāpumu gadījumā ir neapstrīdamas priekšrocības — tā pastiprina organizāciju atbildību, darbojas kā faktors, kas liek uzņēmumiem ieviest stingrus drošības pasākumus un ļauj konstatēt, kuras ir visuzticamākās tehnoloģijas informācijas aizsardzībai. Turklāt, tā dod iespēju attiecīgām personām veikt pasākumus, lai aizsargātu sevi pret identitātes zādzību vai citādu viņu personiskās informācijas ļaunprātīgu izmantošanu.

10. EDAU pauž gandarījumu par citiem priekšlikuma grozījumiem, piemēram, iespēju juridiskām personām to likumiskās interesēs veikt tiesvedību pret tiem, kas pārkāpj dažus e-privātuma direktīvas noteikumus (grozījums 13. pantā, iekļauj 6. punktu). Tāpat pozitīva ir valsts pārvaldes iestāžu izmeklēšanas pilnvaru stiprināšana, jo tādējādi tās varēs izvērtēt, vai datu apstrāde tiek veikta saskaņā ar tiesību aktu noteikumiem, un atklāt pārkāpējus (iekļauj 15.a panta 3. punktu). Lai aizsargātu personu tiesības un brīvības, ir nepieciešams cik drīz vien iespējams pārtraukt personas datu nelikumīgu apstrādi un privātās dzīves pārkāpumus. Šajā sakarā ierosinātais 15.a panta 2. punkts, kurā valsts pārvaldes iestādēm piešķir pilnvaras pieprasīt izbeigt pārkāpumus, guva plašu atbalstu, jo tādējādi iestādes varēs panākt, ka nopietnas nelikumības datu apstrādē tiek nekavējoties pārtrauktas.

11. Pieeja šajā priekšlikumā, kā arī vairums ierosināto grozījumu ir saskaņā ar viedokļiem par nākotnes datu aizsardzības politiku, kas bija izklāstīti iepriekšējos EDAU atzinumos, piemēram, atzinumā par Datu aizsardzības direktīvas īstenošanu ([1]). Pieeja cita starpā ir balstīta uz uzskatu, ka jauni datu aizsardzības principi nav nepieciešami, taču ir vajadzīgi konkrētāki noteikumi, lai risinātu jauno tehnoloģiju, piemēram, interneta, *RFID* utt. izraisītos datu aizsardzības jautājumus, kā arī instrumenti, kas veicinātu tiesību aktu izpildi un efektīvu darbību datu aizsardzības jomā, piemēram, nodrošinot juridiskām personām iespēju uzsākt tiesiskas darbības saistībā ar datu aizsardzības pārkāpumiem un uzliekot datu apstrādātājiem par pienākumu ziņot par drošības pārkāpumiem.

12. Lai gan priekšlikuma pieeja kopumā ir vērtējama pozitīvi, EDAU pauž nožēlu par to, ka priekšlikums nav tik vērienīgs, cik tas varēja būt. Kopš 2003. gada piemērojot e-privātuma direktīvas noteikumus un rūpīgi izanalizējot šo jautājumu, patiesi ir atklājies, ka daži direktīvas noteikumi ir visai neskaidri un tādējādi rada juridiskas neskaidrības un atbilsmes problēmas. Tas attiecas, piemēram, uz to, cik lielā mērā e-privātuma direktīva ir piemērojama elektronisko sakaru tīklu un pakalpojumu sniedzējiem ar valsts kapitāla daļu. Varēja cerēt, ka Komisija izmantotu telekomunikāciju paketes un jo īpaši e-privātuma direktīvas pārskatīšanu, lai atrisinātu dažus problemātiskos jautājumus. Turklāt, attiecībā uz jaunām problēmām, piemēram, sistēmas izveidi obligātai ziņošanai par drošības pārkāpumiem, priekšlikumā sniegts tikai daļējs risinājums, neiekļaujot to organizāciju sarakstā, kuru pienākums ir ziņot par drošības pārkāpumiem, iestādes, kas apstrādā ļoti konfidenciālus datus, piemēram, tiešsaistē funkcionējošas bankas un veselības pakalpojumu sniedzējus. EDAU pauž nožēlu par šādu pieeju.

13. EDAU cer, ka, priekšlikumam veicot likumdošanas procesā noteikto ceļu, likumdevējs ņems vērā šajā atzinumā iekļautās piezīmes un ierosinājumus, lai atrisinātu jautājumus, kuri ir palikuši neatrisināti Komisijas priekšlikumā.

([1]) Eiropas datu aizsardzības uzraudzītāja 2007. gada 25. jūlija atzinums par 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.)

II. PRIEKŠLIKUMA ANALĪZE

II.1. E-privātuma direktīvas darbības joma, jo īpaši attiecīgie pakalpojumi

14. Galvenais jautājums pašreizējā e-privātuma direktīvā attiecas uz tās piemērošanas jomu. Priekšlikumā ir iekļauti daži pozitīvi elementi, lai precizētu un definētu priekšlikuma jomu, jo īpaši pakalpojumus, uz kuriem attiecas šī direktīva, un tie ir aplūkoti turpmāk i) iedaļā. Diemžēl ierosinātie grozījumi neatrisina visas pastāvošās problēmas. Kā iztirzāts turpmāk ii) iedaļā, grozījumos diemžēl nav vēlmes paplašināt direktīvas piemērošanas jomu, lai tajā iekļautu elektronisko komunikāciju pakalpojumus privātajos tīklos.

15. E-privātuma direktīvas 3. pantā ir aprakstīti pakalpojumi, uz kuriem attiecas šī direktīva, citiem vārdiem sakot, pakalpojumi, uz kuriem attiecas šīs direktīvas noteikumu piemērošana: "*Šī direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos*".

16. Tādējādi pakalpojumi, uz kuriem attiecas e-privātuma direktīva, skar publiskajos tīklos pieejamu elektronisko komunikāciju pakalpojumu sniedzējus ("PPEKPS"). PPEKPS definīcija ir dota pamatdirektīvas 2. panta c) apakšpunktā ([1]). Publiskie komunikāciju tīkli ir definēti pamatdirektīvas 2. panta d) apakšpunktā ([2]). PPEKPS darbības, piemēram, ir piekļuves nodrošināšana internetam, informācijas pārraidīšana, izmantojot elektroniskos tīklus, mobilo sakaru un telefonu pieslēgumus utt.

i) *ierosināts grozījums e-privātuma direktīvas 3. pantā: Attiecīgos pakalpojumos iekļaut publiskos komunikāciju tīklus, kuros var izmantot datu vākšanas un identifikācijas ierīces*

17. Priekšlikums groza e-privātuma direktīvas 3. pantu, konkrēti nosakot, ka publiskajos elektronisko komunikāciju tīklos iekļauj "*publiskos komunikāciju tīklus, kuros var izmantot datu vākšanas un identifikācijas ierīces*". Direktīvas 28. apsvērumā paskaidrots, ka attiecībā uz lietojumu izstrādi, kas paredz informācijas, tostarp personas datu, vākšanu, izmantojot radiofrekvences, piemēram, *RFID*, — kad tie darbojas pieslēgumā publiskajiem komunikāciju tīkliem vai pakalpojumiem vai tos izmanto — ir jāpiemēro e-privātuma direktīva.

18. EDAU atzinīgi vērtē šo noteikumu, jo tajā paskaidrots, ka e-privātuma direktīvas darbības joma ir attiecināma uz vairākiem *RFID* lietojumiem, tādējādi mazinot neskaidrības šajā jautājumā un neapšaubāmi likvidējot tiesību aktu nepareizu izpratni vai nepareizu interpretāciju.

19. Patiešām, saskaņā ar e-privātuma direktīvas pašreizējo 3. pantu uz vairākiem *RFID* lietojumiem jau attiecas šī direktīva. Tam ir vairāki kumulatīvi iemesli. Pirmkārt, *RFID* lietojumi ir ietverami elektronisko komunikāciju pakalpojumu definīcijā. Otrkārt, tos nodrošina ar elektronisko komunikāciju tīklu starpniecību, ciktāl to darbībā izmanto pārraides sistēmas, kas pārraida signālus bezvadu ceļā. Visbeidzot tīkls var būt valsts vai privātajā īpašumā. Valsts īpašuma gadījumā *RFID* lietojumi tiks uzskatīti

([1]) Eiropas Parlamenta un Padomes Direktīva 2002/21/EK (2002. gada 7. marts) par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (OV L 108, 24.4.2002., 33. lpp.). Pamatdirektīva nosaka, kas ir jāsaprot ar elektronisko komunikāciju pakalpojumu, proti, i) "elektronisko komunikāciju pakalpojumi" ir pakalpojumi, ko parasti nodrošina par atlīdzību un kas sastāv no signālu pārraidīšanas tīklos, ietverot telekomunikāciju pakalpojumus un pārraidīšanas pakalpojumus tīklos; ii) elektronisko komunikāciju pakalpojumu definīcijā neiekļauj pakalpojumus, kas nodrošina saturu, kas pārraidīts, izmantojot elektronisko komunikāciju tīklus un pakalpojumus; iii) pakalpojumu nodrošināšana nozīmē tīkla izveidi, darbību, kontroli vai padarīšanu par pieejamu; iv) elektronisko komunikāciju pakalpojumos neiekļauj informācijas sabiedrības pakalpojumus, kas e-tirdzniecības direktīvā ir definēti kā pakalpojumi, ko parasti sniedz par atlīdzību no attāluma, ar elektroniskiem līdzekļiem un pēc pakalpojumu saņēmēja individuāla pieprasījuma.

([2]) Publiskais komunikāciju tīkls nozīmē elektronisku komunikāciju tīklu, ko pilnībā vai galvenokārt izmanto publiski pieejamu elektronisko komunikāciju pakalpojumu nodrošināšanai.

par "attiecīgiem pakalpojumiem" un tādēļ uz tiem būs attiecināma e-privātuma direktīvas darbības joma. Tomēr ierosinātais grozījums likvidēs jebkādas atlikušās šaubas par to un tādējādi radīs lielāku tiesisko noteiktību.

20. Kā uzsvērts iepriekšējā EDAU atzinumā par *RFID* ([1]), šis noteikums, protams, neizslēdz iespējamo vajadzību ieviest papildu tiesiskos instrumentus saistībā ar *RFID*. Šādi pasākumi tomēr būtu jāpieņem citā kontekstā, un nevis šā priekšlikuma ietvaros.

ii) *nepieciešamība iekļaut elektronisko komunikāciju pakalpojumus privātajos vai daļēji privātajos tīklos*

21. Lai gan EDAU atzinīgi vērtē iepriekš minēto paskaidrojumu, viņš pauž nožēlu par to, ka priekšlikumā nav risināts jautājums saistībā ar nošķīrumu starp publiskajiem un privātajiem tīkliem, kas kļūst arvien neskaidrāks. Turklāt EDAU pauž nožēlu par to, ka pakalpojumu, uz kuriem attiecas e-privātuma direktīva, definīcija nav paplašināta, lai tajā iekļautu privātos tīklus. E-privātuma direktīvas 3. panta 1. punkts pašreizējā redakcijā attiecas tikai uz *publiskajos tīklos sniegtiem elektronisko komunikāciju pakalpojumiem*.

22. EDAU vērš uzmanību uz to, ka publiskajiem un privātajiem pakalpojumiem ir tendence arvien vairāk sajaukties. Piemēram, iedomājieties universitātes, kas tūkstošiem studentu dod iespēju izmantot internetu un e-pastu. Šo daļēji publisko (vai daļēji privāto) tīklu iespējas ietekmēt personu privāto dzīvi ir acīmredzamas un tādēļ ir nepieciešamība šāda veida pakalpojumiem piemērot tādus pašus noteikumus, kādus piemēro tikai publiskajiem tīkliem. Turklāt, privātie tīkli, piemēram, ar ko darba devējs nodrošina darbiniekiem piekļuvi internetam, viesnīcu vai dzīvokļu īpašnieki nodrošina viesiem telefonsakarus un e-pastu, kā arī interneta kafejnīcas, ietekmē lietotāju datu aizsardzību un privāto dzīvi, kas vedina domāt, ka arī uz tiem būtu jāattiecina e-privātuma direktīvas darbības joma.

23. Faktiski dažu dalībvalstu judikatūrā jau ir paredzēts, ka uz elektronisko komunikāciju pakalpojumiem, ko sniedz privātajos tīklos, attiecas tādi paši noteikumi kā uz pakalpojumiem, ko sniedz publiskajos tīklos ([2]). Arī saskaņā ar Vācijas tiesību aktiem datu aizsardzības iestādes ir atklājušas, ka, ja uzņēmumā atļauj lietot privāto e-pastu, tas var nozīmēt, ka uzņēmums ir uzskatāms par publisko telekomunikāciju pakalpojumu sniedzēju, un tādēļ uz to attiecas e-privātuma direktīvas noteikumi.

24. Īsumā, arvien lielāks jaukto (privāto un publisko) un privāto tīklu īpatsvars ikdienas dzīvē, ar attiecīgi palielinātu personas datu un privātās dzīves apdraudējumu, ir pietiekams pamatojums, lai šādiem pakalpojumiem piemērotu tādus pašus noteikumus, kādus piemēro publiskajiem elektronisko komunikāciju pakalpojumiem. Šajā sakarā EDAU uzskata, ka direktīva būtu jāgroza, lai paplašinātu tās darbības jomu, kas ietvertu šāda veida privātos pakalpojumus; šo viedokli atbalsta arī 29. panta darba grupa ([3]).

II.2. **Ziņošana par drošības pārkāpumiem: grozījums 4. pantā**

25. E-privātuma direktīvas 4. pantu groza, iekļaujot tajā divus jaunus punktus (3. un 4. punkts), kuros ir noteikta prasība ziņot par drošības pārkāpumiem. Saskaņā ar 4. panta 3. punktu elektronisko komunikāciju pakalpojumu sniedzējiem (PPEKPS), no vienas puses, bez nepamatotas kavēšanās ir jāziņo valsts pārvaldes iestādei par jebkuru pārkāpumu, kā rezultātā nejauši vai nelikumīgi iznīcināti, zaudēti, izmainīti, neatļauti izpausti vai kļuvuši pieejami personas dati, kas pārraidīti, uzglabāti vai citādi apstrādāti saistībā ar publiski pieejamu komunikāciju pakalpojumu sniegšanu (kolektīvi "datu apdraudējums"), un, no otras puses, tiem ir jāziņo arī saviem klientiem.

([1]) Eiropas datu aizsardzības uzraudzītāja 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.

([2]) Piemēram, Parīzes Apelācijas tiesas 2005. gada 4. februāra spriedumā *BNP Paribas v World Press Online* lietā tika konstatēts, ka nav atšķirības starp interneta pakalpojumu sniedzējiem, kas piedāvā piekļuvi internetam uz komerciāla pamata, un darba devējiem, kas nodrošina interneta piekļuvi saviem darbiniekiem.

([3]) Atzinums 8/2006 par ES tiesiskā regulējuma elektronisko sakaru un pakalpojumu jomā pārskatīšanu, galvenokārt pievēršoties e-privātuma direktīvai, pieņemts 2006. gada 26. septembrī.

Šīs prasības priekšrocības

26. EDAU atzinīgi vērtē šo noteikumu iekļaušanu (4. panta 3. un 4. punkts), ar ko tiek ieviesta obligāta prasība ziņot par drošības pārkāpumiem. Ziņošanai par drošības pārkāpumiem ir pozitīva ietekme saistībā ar personas datu un privātās dzīves aizsardzību; par to ir pārliecinājušies Amerikas Savienotajās Valstīs, kur jau vairākus gadus štatu līmenī ir spēkā tiesību akti attiecībā uz ziņošanu par drošības pārkāpumiem.

27. Pirmkārt, tiesību akti attiecībā uz ziņošanu par drošības pārkāpumiem pastiprina PPEKPS atbildību attiecībā uz informāciju, kas ir tikusi apdraudēta. Saskaņā ar datu aizsardzības vai privātās dzīves politikas normatīvo bāzi, atbildība nozīmē to, ka katra organizācija ir atbildīga par informāciju, ko tā glabā un kontrolē. Prasība par ziņošanu ir līdzvērtīga atkārtotam paziņojumam, ka, no vienas puses, apdraudētie dati atradās PPEKPS kontrolē, un, no otras puses, ka šīs organizācijas atbildība ir veikt vajadzīgos pasākumus saistībā ar šādiem datiem.

28. Otrkārt, fakts, ka pastāv ziņošana par drošības pārkāpumiem, ir bijis svarīgs faktors, kas veicina ieguldījumus drošības pasākumos organizācijās, kas apstrādā personas datus. Tas, ka organizācijām ir publiski jāziņo par drošības pārkāpumiem, jau pats par sevi liek tām ieviest stingrākus drošības standartus, kas aizsargā personisku informāciju un novērš pārkāpumus. Turklāt ziņošana par drošības pārkāpumiem palīdzēs noteikt un īstenot uzticamu statistikas analīzi par visefektīvākajiem drošības risinājumiem un mehānismiem. Ilgu laiku ir pastāvējis uzticamu datu trūkums par nepilnībām informācijas drošības aizsardzībā un vispiemērotākajām tehnoloģijām informācijas aizsardzībā. Šo problēmu varētu atrisināt, ieviešot prasību par drošības pārkāpumu paziņošanu, līdzīgi kā tas bija ASV tiesību aktos par ziņošanu drošības pārkāpumu gadījumos, jo ziņošana darīs pieejamu informāciju par tehnoloģijām, kas ir vairāk pakļautas pārkāpumiem ([1]).

29. Visbeidzot ziņošana par drošības pārkāpumiem palīdz personām apzināties, kādu risku rada situācija, kad tiek apdraudēti viņu personiskie dati, un veikt vajadzīgos pasākumus, lai šādu apdraudējumu mazinātu. Piemēram, ja ir apdraudēta informācija par bankas datiem, persona, kas par to ir informēta, var nolemt veikt izmaiņas piekļuves datos savam bankas kontam, lai nepieļautu, ka kāds var iegūt šo informāciju un to izmantot nelikumīgiem mērķiem (parasti to sauc par "identitātes zādzību"). Īsumā, šī prasība samazina iespējamību, ka persona varētu kļūt par identitātes zādzības upuri, un var palīdzēt upuriem veikt nepieciešamās darbības, lai atrisinātu problēmas.

Ierosinātā grozījuma trūkumi

30. EDAU ir apmierināts ar 4. pantā iekļauto 3. un 4. punktu, kuros izklāstīta sistēma ziņošanai par drošības pārkāpumiem, taču viņš būtu vēlējies, lai to piemērošana būtu plašāka mēroga, iekļaujot tajā arī informācijas sabiedrības pakalpojumu sniedzējus. Tas nozīmētu, ka tiesību akti attiektos arī uz tiešsaistē funkcionējošām bankām, uzņēmumiem, veselības pakalpojumu sniedzējiem u.c. ([2]).

31. Iemesli, kuru dēļ ir pamatojums uzlikt par pienākumu elektronisko komunikāciju pakalpojumu sniedzējiem, t.i. PPEKPS, ieviest ziņošanu par drošības pārkāpumiem, pastāv arī attiecībā uz citām organizācijām, kas arī apstrādā liela apjoma personiskos datus, kuru atklāšana var būt īpaši kaitējoša datu subjektam. Tas attiecas uz tiešsaistē funkcionējošām bankām, datu brokeriem un citiem tiešsaistes pakalpojumu sniedzējiem, piemēram, tādiem, kas apstrādā konfidenciālu informāciju (tostarp datus par veselību, politiskajiem uzskatiem, utt.). Pārkāpumi attiecībā uz informāciju, kas ir tiešsaistē funkcionējošu banku un uzņēmumu rīcībā, kas var ietvert ne tikai bankas konta numurus, bet arī kredītkaršu datus, var novest pie identitātes zādzības, un tādā gadījumā ir būtiski, lai persona būtu par to informēta un varētu veikt vajadzīgos pasākumus. Minētajā gadījumā (attiecībā uz tiešsaistes datiem par veselību), kad tiek izpausta konfidenciāla informācija, personas, ja arī necieš finansiālus zaudējumus, tās neapšaubāmi var ciest no nemateriāla kaitējuma.

([1]) Skatīt ziņojumu "*Drošības ekonomika un iekšējais tirgus*", ko pēc *ENISA* pasūtījuma sagatavojuši *Ross Anderson (Prof.), Rainer Böhme, Richard Clayton* un *Tyler Moore*. Ziņojums ir pieejams: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Informācijas sabiedrības pakalpojumu sniedzēji e-tirdzniecības direktīvā ir definēti kā pakalpojumi, ko parasti sniedz par atlīdzību no attāluma, ar elektroniskiem līdzekļiem un pēc pakalpojumu saņēmēja individuāla pieprasījuma.

32. Turklāt, paplašinot šīs prasības darbības jomu, iepriekš minētie ieguvumi, ko sniegtu šādas prasības ieviešana, nebūtu ierobežoti tikai viena darbības sektora ietvaros, proti, saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem, bet attiektos plašāk uz informācijas sabiedrības pakalpojumiem kopumā. Neapšaubāmi, ieviešot prasību informācijas sabiedrības pakalpojumu sniedzējiem, piemēram, tiešsaistē funkcionējošām bankām ziņot par drošības pārkāpumiem, ne tikai palielinās viņu atbildību, bet arī rosinās šos uzņēmumus stiprināt savus drošības pasākumus un tādējādi izvairīties no potenciāliem drošības pārkāpumiem nākotnē.

33. Pastāv arī citi precedenti, liecinot, ka e-privātuma direktīva jau ir attiecināma uz iestādēm, kas nav PPEKPS, piemēram, 5. pants par komunikāciju konfidencialitāti un 13. pants par surogātpastu (*spam*). Tas apstiprina, ka likumdevējs pagātnē ir rīkojies prātīgi, pieņemot lēmumu paplašināt dažu e-privātuma direktīvas noteikumu piemērošanas jomu, jo uzskatīja, ka tas ir lietderīgi un nepieciešami. EDAU cer, ka arī patlaban likumdevējs lems par tikpat saprātīgu un elastīgu pieeju un paplašinās 4. panta piemērošanas jomu, lai tajā iekļautu arī informācijas sabiedrības pakalpojumu sniedzējus. Šajā sakarā pietiktu ar to, ka 4. panta 3. punktā iekļauj šādu atsauci uz informācijas sabiedrības pakalpojumu sniedzējiem: "*Drošības pārkāpuma gadījumā, kā rezultātā nejauši vai … elektronisko komunikāciju pakalpojumu sniedzējs* un informācijas sabiedrības pakalpojumu sniedzējs *… par to ziņo attiecīgajam abonentam un valsts pārvaldes iestādē*".

34. EDAU uzskata, ka šī prasība un tās piemērošana gan *PPECS*, gan informācijas sabiedrības pakalpojumu sniedzējiem ir pirmais solis, virzībā uz tādu sistēmu, kas ar laiku tiktu vispārēji piemērota attiecībā uz visiem datu kontrolieriem.

Īpašs tiesiskais regulējums attiecībā uz drošības pārkāpumiem, kas jārisina, ar komitoloģijas procedūras palīdzību

35. Priekšlikumā nav risināti vairāki jautājumi, kas saistīti ar prasību ziņot par drošības pārkāpumiem. Risināmie jautājumi ir, piemēram, ziņošanas apstākļi, piemērojamais formāts un procedūras. Turpretī saskaņā ar priekšlikuma 4. panta 4. punktu šo lēmumu pieņemšana ir atstāta "komitoloģijas" komitejai ([1]), proti, Komunikāciju komitejai, kas izveidota ar Pamatdirektīvas 22. pantu, atbilstīgi Padomes 1999. gada 28. jūnija lēmumam. Konkrēti, šādus pasākumus pieņemtu saskaņā ar Padomes 1999. gada 28. jūnija lēmuma 5. pantu, kurā noteikta regulatīvā kontroles procedūra attiecībā uz "*vispārējiem pasākumiem, kas paredzēti, lai ieviestu pamataktos noteiktos svarīgākos noteikumus*".

36. EDAU neiebilst pret izvēli atstāt visu šo jautājumu risināšanu īstenošanas tiesību aktos. Tiesību aktu pieņemšana ar komitoloģijas palīdzību varētu saīsināt likumdošanas procedūru. Komitoloģija arī palīdzētu nodrošināt saskaņošanu, kas ir mērķis, uz kuru gala rezultātā būtu jātiecas.

37. Ņemot vērā plašo jautājumu loku, kas būs jārisina īstenošanas pasākumos, kā arī to svarīgumu, kā minēts iepriekš, liekas, ka būtu atbilstoši tos aplūkot vienkopus vienā tiesību aktā, un nevis izmantojot atsevišķu pieeju, kuras rezultātā daži jautājumi tiktu risināti e-privātuma direktīvā, bet citi attiektos uz īstenošanas tiesību aktiem. Tādēļ apsveicama ir Komisijas pieeja, kas paredz atstāt šo jautājumu risināšanu īstenošanas tiesību aktos, kurus pieņemtu pēc apspriešanās ar EDAU un, cerams, citām ieinteresētajām pusēm (skatīt nākamo punktu).

Jautājumi, kas būs jārisina īstenošanas tiesību aktos

38. Īstenošanas pasākumu nozīme atklājas spilgtāk, ja pietiekami detalizēti iztēlojas jautājumus, kas būs jārisina ar īstenošanas pasākumiem. Piemēram, īstenošanas pasākumos var noteikt standartus, kas jāievēro, sniedzot ziņojumus. Tajos varēs precizēt, kas veido drošības pārkāpumu, nosacījumi, pie kādiem jāsniedz paziņojumi personām un iestādēm, paziņojuma izsūtīšanas laiks.

([1]) EK likumdošanas procedūras, kurās iesaistās komitejas, kuru sastāvā ir dalībvalstu valdību pārstāvji civildienesta ierēdņu līmenī.

39. EDAU uzskata, ka e-privātuma direktīvā, konkrēti 4. pantā nebūtu jāiekļauj nekādi izņēmumi attiecībā uz paziņošanas prasību. Šajā sakarā EDAU ar prieku atzīst 4. pantā pausto Komisijas pieeju, kurā ir noteikta ziņošanas prasība, neparedzot nekādus izņēmumus, bet ir atļauts šo un citus jautājumus risināt īstenošanas tiesību aktos. Lai gan EDAU apzinās argumentus, kas varētu būt par pamatu dažu izņēmumu ieviešanai attiecībā uz šo prasību, EDAU atbalsta šī un citu jautājumu risināšanu īstenošanas tiesību aktos, iepriekš veicot rūpīgas un plašas apspriedes par visiem attiecīgajiem jautājumiem. Kā minēts iepriekš, sarežģīto jautājumu dēļ, kas saistīti ar prasību ziņot par drošības pārkāpumiem, tostarp par to, vai būtu pieņemami noteikt izņēmumus vai ierobežojumus, šo problēmu ir nepieciešams risināt vienoti, t.i., ar vienu vienīgu tiesību aktu, kurā būtu aplūkots tikai un vienīgi šis jautājums.

Konsultācijas ar EDAU un nepieciešamība paplašināt apspriešanos

40. Ņemot vērā to, cik lielā mērā īstenošanas pasākumi ietekmēs personas datu aizsardzību, ir svarīgi, lai pirms šo pasākumu pieņemšanas Komisija iesaistītos pienācīgā apspriešanā. Šajā sakarā EDAU pauž gandarījumu par priekšlikuma 4. panta 4. punktu, kurā skaidri noteikts, ka pirms īstenošanas pasākumu pieņemšanas Komisija apspriedīsies ar Eiropas datu aizsardzības uzraudzītāju. Šādi pasākumi ne tikai skars personas datu un privātās dzīves aizsardzību, bet to ievērojami ietekmēs. Tādēļ ir svarīgi lūgt EDAU konsultāciju, kā tas prasīts atbilstīgi Regulas (EK) Nr. 45/2001 41. pantam.

41. Papildus konsultācijām ar EDAU, iespējams, būtu lietderīgi iekļaut noteikumu par to, ka ir jāveic īstenošanas pasākumu projekta sabiedriska apspriešana, lai saņemtu padomus un veicinātu pieredzes un labākās prakses apmaiņu par šiem jautājumiem. Tas būs pareizais ceļš, kas izmantojams ne tikai nozarei, bet arī citām ieinteresētajām pusēm, tostarp citām datu aizsardzības iestādēm un 29. panta darba grupai, lai paustu savus viedokļus. Vajadzība veikt sabiedrisku apspriešanu ir vēl jo svarīgāka, ja ņem vērā, ka likumdošanas pieņemšanas procedūra ir komitoloģija, ar ierobežotu Eiropas Parlamenta līdzdalību.

42. EDAU atzīmē, ka priekšlikuma 4. panta 4. punktā paredzēts, ka pirms īstenošanas noteikumu pieņemšanas Komisija arī apspriedīsies ar Elektronisko sakaru tirgus iestādi. Šajā sakarā EDAU principiāli atbalsta konsultācijas ar Elektronisko sakaru tirgus iestādi kā ETIDA pieredzes un zināšanu uzglabātāju par tīklu un informācijas drošības jautājumiem. Līdz tam, kad tiks izveidota Elektronisko sakaru tirgus iestāde, kā pagaidu risinājumu būtu lietderīgi ierosinātajā grozījumā (4. panta 4. punkts) paredzēt apspriešanos ar ETIDA.

II.3. **Noteikums par sīkdatnēm, spiegprogrammām un līdzīgām ierīcēm: grozījums 5. panta 3. punktā**

43. E-privātuma direktīvas 5. panta 3. punktā risināts jautājums par tehnoloģijām, kas ļauj piekļūt informācijai lietotāja gala iekārtā un to uzglabāt, izmantojot elektronisko komunikāciju tīklus. Piemērs direktīvas 5. panta 3. punkta piemērošanai attiecas uz sīkdatņu izmantošanu ([1]). Citi piemēri ir tehnoloģiju — tādu kā spiegprogrammu (slēptas spiegošanas programmas) un "trojas zirgu" (programmas, kas apslēptas sūtījumos vai citās ārēji nekaitīgās programmās) — izmantošana. Šādu tehnoloģiju mērķis un nolūki mēdz būt ļoti dažādi — daži ir pilnīgi nekaitīgi, vai pat noderīgi lietotājam, turpretim citi ir neapšaubāmi ļoti kaitējoši un rada apdraudējumu.

([1]) *ISSP* (tīmekļa vietnes) ievieto sīkdatnes lietotāja gala iekārtās dažādiem mērķiem, tostarp lai pazītu apmeklētāju, kad viņš atkārtoti apmeklē tīmekļa vietni. Praksē tas nozīmē, ka tad, kad tīmekļa vietne interneta lietotājam nosūta sīkdatni, lietotāja datoram tiek piešķirts vienreizējs numurs (t.i., dators, kas saņēmis sīkdatni no tīmekļa vietnes A kļūst par "datoru, kas uzglabā sīkdatni 111"). Tīmekļa vietne saglabā to kā atsauces numuru. Ja lietotājs, kura dators ir saņēmis sīkdatni 111, to neizdzēš, nākamajā reizē, kad viņš apmeklē to pašu tīmekļa vietni, tā spēs to identificēt kā datoru, kas uzglabā sīkdatni 111. Tīmekļa vietne, protams, secina, ka šis dators ir apmeklējis arī iepriekšējās reizēs. Mehānisms, kas ļauj tīmekļa vietnei pazīt datoru kā atkārtotu apmeklētāju, ir ļoti vienkāršs. Ja apmeklētājā datorā glabājas sīkdatne, piemēram, sīkdatne 111, un tas apmeklē tīmekļa vietni, kura iepriekšējā apmeklējumā izveidoja šo sīkdatni, tā pārmeklēs lietotāja cieto disku, lai atrastu sīkdatnes attiecīgo numuru. Ja lietotāja meklētājs atradīs sīkdatnes numuru, kas atbilst atsauces numuram, kurš glabājas tīmekļa vietnē, tas informēs tīmekļa vietni, ka šis dators glabā sīkdatni 111.

44. E-privātuma direktīvas 5. panta 3. punktā izklāstīti nosacījumi, lai iegūtu piekļuvi lietotāja gala iekārtā uzglabātai informācijai vai tās uzglabāšanai, izmantojot, cita starpā, iepriekš minētās tehnoloģijas. Konkrēti, saskaņā ar 5. panta 3. punktu i) interneta lietotājs ir jānodrošina ar skaidru un visaptverošu informāciju, saskaņā ar Direktīvu 95/46/EK, cita starpā, par apstrādes nolūkiem; un ii) interneta lietotājam jādod tiesības liegt veikt šādu apstrādi, t.i., atteikties no informācijas apstrādes, kas ir iegūta no viņa gala iekārtas.

Ierosinātā grozījuma priekšrocības

45. E-privātuma direktīvas pašreizējā 5. panta 3. punktā tās piemērošana ir ierobežota tikai attiecībā uz situācijām, kur piekļuvi informācijai un tās uzglabāšanai lietotāja gala iekārtā veic, izmantojot *elektronisko komunikāciju tīklus*. Tas ietver iepriekš aprakstīto situāciju attiecībā uz sīkdatnēm un citām tehnoloģijām, piemēram, spiegprogrammām, ko piesūta, izmantojot elektronisko komunikāciju tīklus. Tomēr nebūt nav skaidrs, vai 5. panta 3. punkts attiecas uz tādām situācijām, kad līdzīgas tehnoloģijas (sīkdatnes, spiegprogrammas un tamlīdzīgi) tiek izplatītas ar programmatūru, kas tiek uzglabāta ārējos atmiņas nesējos un lejupielādēta lietotāja gala iekārtā. Ņemot vērā to, ka privātās dzīves apdraudējums pastāv neatkarīgi no komunikāciju kanāla, 5. panta 3. punkta attiecināšana tikai uz vienu komunikāciju kanālu ir diemžēl neveiksmīga.

46. Tādēļ EDAU ir gandarīts par grozījumu 5. panta 3. punktā, kas atceļ atsauci uz "elektronisko komunikāciju tīkliem" un tādējādi faktiski paplašina 5. panta 3. punkta piemērošanas jomu. Tiešām 5. panta 3. punkta grozītā versija ietver abas situācijas — kad piekļuve informācijai un informācijas uzglabāšana lietotāja gala iekārtā tiek veikta gan ar elektronisko komunikāciju tīklu, gan arī citu ārējo atmiņas nesēju, piemēram, kompaktdisku, lasāmatmiņas kompaktdisku (CD-ROM), USB atslēgu utt., starpniecību.

Tehniska uzglabāšana, lai veicinātu komunikāciju pārraidīšanu

47. Pēdējais teikums 5. panta 3. punktā e-privātuma direktīvas grozītajā versijā paliek bez izmaiņām. Atbilstīgi pēdējam teikumam, nosacījumi 5. panta 3. punkta pirmajā teikumā "*neliedz jebkādu tehnisku uzglabāšanu vai vienīgi pieeju, lai veiktu vai veicinātu komunikāciju pārraidīšanu elektronisko komunikāciju tīklā, vai kas nepieciešama, lai sniegtu informācijas sabiedrības pakalpojumu…*". Tādēļ 5. panta 3. punkta pirmajā daļā minētie obligātie nosacījumi (nepieciešamība sniegt informāciju un piedāvāt iespēju atteikties) nav jāpiemēro, ja vienīgais nolūks piekļūt lietotāja gala iekārtai vai informācijas uzglabāšanai ir lai *veicinātu* komunikāciju pārraidīšanu, vai kad tas ir noteikti nepieciešams, lai sniegtu informācijas sabiedrības pakalpojumu, ko pieprasa lietotājs.

48. Direktīva nepaskaidro, kad vienīgais nolūks piekļuvei vai informācijas uzglabāšanai ir veicināt komunikāciju pārraidīšanu vai sniegt informāciju. Viena situācija, uz kuru skaidri attiektos šis izņēmums, ir interneta savienojuma izveidošana. Tas ir tādēļ, ka, lai veiktu interneta savienojumu, ir nepieciešams iegūt IP adresi ([1]). Gala lietotāja datoram tiks vaicāta noteikta informācija, kas tam par sevi jāsniedz interneta piekļuves pakalpojumu sniedzējam, kurš tam apmaiņā piešķirs IP adresi. Šajā gadījumā lietotāja gala iekārtā uzglabāta informācija tiks pārsūtīta interneta piekļuves pakalpojumu sniedzējam, lai lietotājam nodrošinātu piekļuvi internetam. Šajā gadījumā interneta piekļuves pakalpojumu sniedzējs ir atbrīvots gan no prasības paziņot par šo informācijas ievākšanu, gan nodrošināt tiesības atteikt, ciktāl tas ir nepieciešams pakalpojuma sniegšanai.

49. Kad lietotājs ir pieslēdzies internetam un vēlas apskatīt kādu tīmekļa vietni, viņam jānosūta pieprasījums uz serveri, kas šo vietni apkalpo. Atbilde no tīmekļa vietnes pienāks, ja būs zināms, kur sūtīt informāciju, t.i., ja būs zināma lietotāja IP adrese. Saistībā ar to, kā tiek uzglabāta šī adrese, ir atkal nepieciešams, lai tīmekļa vietnei, kuru lietotājs vēlas apmeklēt, būtu piekļuve interneta lietotāja gala iekārtai. Neapšaubāmi uz šo operāciju arī attiektos minētais izņēmums. Šajos gadījumos, šķiet, patiešām būtu pareizi, ka tie paliktu ārpus 5. panta 3. punkta noteikumu piemērošanas jomas.

([1]) IP (interneta protokola) adrese ir unikāla adrese, ko lieto dažas elektroniskās iekārtas, lai identificētu cita citu un veiktu savstarpēju komunikāciju datoru tīklā, izmantojot interneta protokola standartu (IP) — vienkāršāk sakot, datora adrese. Jebkurai tīkla iekārtai, kas tajā ir iesaistīta — tostarp, rūterim, pārslēgumam, datoram, infrastruktūras serverim (piemēram, NTP, DNS, DHCP, SNMP utt.), printerim, inetrneta faksa aparātam un dažiem telefoniem — var būt sava adrese, kas ir unikāla šī konkrētā tīkla ietvaros. Dažas IP adreses ir veidotas tā, lai tās būtu unikālas visaptverošā interneta mērogā, bet citas ir unikālas tikai attiecīga uzņēmuma mērogā.

50. EDAU uzskata, ka ir piemēroti atbrīvot no prasības sniegt informāciju un dot iespēju atteikt iepriekš aprakstītajās situācijās, kad tehniska uzglabāšana vai piekļuve interneta lietotāja gala iekārtai ir *nepieciešama* ar nolūku vienīgi pārraidīt komunikācijas elektronisko komunikāciju tīklā. Tas pats attiecas uz gadījumiem, kad tehniska uzglabāšana vai piekļuve ir nepieciešama vienīgi, lai sniegtu informācijas sabiedrības pakalpojumu. Tomēr EDAU nesaskata vajadzību atbrīvot no prasības sniegt informāciju un dot tiesības atteikt situācijās, kad tehniska uzglabāšana vai piekļuve ir nepieciešama ar nolūku vienīgi *veicināt* komunikāciju pārraidīšanu elektronisko komunikāciju tīklā. Piemēram, saskaņā ar šā panta pēdējo teikumu datu subjekts var nespēt izmantot informāciju un tiesības iebilst pret savu datu apstrādi, ja sīkdatne ievāc ziņas par valodu izvēli vai viņa atrašanās vietu (piemēram, Beļģijā, Ķīnā), jo šāda veida sīkdatnes var raksturot kā tādas, kuru mērķis ir veicināt komunikāciju pārraidīšanu. EDAU apzinās, ka programmatūras līmenī datu subjektam praksē ir dota iespēja atteikties no sīkdatņu uzglabāšanas vai to regulēt. Tomēr tam nav sniegts pietiekami skaidrs atbalsts ne ar vienu noteikumu, kurā datu subjekts būtu formāli pilnvarots aizstāvēt savas tiesības iepriekš minētajā kontekstā.

51. Lai izvairītos no šāda iznākuma, EDAU ierosina veikt nelielu grozījumu 5. panta 3. punkta pēdējā daļā, proti, svītrot no teikuma vārdu "*veicinātu*": "*neliedz jebkādu tehnisku uzglabāšanu vai vienīgi pieeju, lai veiktu vai veicinātu komunikāciju pārraidīšanu elektronisko komunikāciju tīklā, vai kas nepieciešama, lai sniegtu informācijas sabiedrības pakalpojumu…*".

II.4. **Tiesiskās darbības, ko uzsāki elektronisko komunikāciju pakalpojumu sniedzēji un juridiskas personas: 13. pantā iekļauj 6. punktu**

52. Ierosinātais 13. panta 6. punkts nosaka civiltiesiskās aizsardzības līdzekļus jebkurai privātpersonai vai juridiskai personai, kuras likumiskās interesēs, — jo īpaši elektronisko komunikāciju pakalpojumu sniedzējiem, kuru uzņēmējdarbības interesēs — ir cīnīties ar tiem, kas pārkāpj e-privātuma direktīvas 13. pantu. Šis pants attiecas uz jautājumu par nevēlamu komerciālu komunikāciju sūtīšanu.

53. Ierosinātais grozījums dos iespēju, piemēram, interneta pakalpojumu sniedzējiem vērsties pret surogātpasta izplatītājiem par tīklu ļaunprātīgu izmantošanu, iesūdzēt tiesā sūtītāja adrešu viltotājus vai hakerus, kas veic nelikumīgu piekļuvi serveriem nolūkā tos izmantot kā surogātpasta relejus utt.

54. E-privātuma direktīvā nebija skaidri noteikts, vai tā dod PPEKPS tiesības veikt darbības pret surogātpasta izplatītājiem, un tikai ļoti retos gadījumos elektronisko komunikāciju pakalpojumu sniedzēji ir cēluši prasības tiesā par pārkāpumiem saistībā ar 13. pantu, kā tas īstenots dalībvalstu tiesību aktos ([1]). Atzīstot elektronisko komunikāciju pakalpojumu sniedzēju tiesības veikt tiesvedību, lai aizstāvētu savas likumīgās uzņēmējdarbības intereses, priekšlikumā ir apstiprināts, ka e-privātuma direktīva paredz aizsargāt ne tikai individuālos abonentus, bet arī elektronisko komunikāciju pakalpojumu sniedzējus.

55. EDAU ir apmierināts, ka priekšlikumā ir iekļauta iespēja uzņēmējdarbībā interesētiem elektronisko komunikāciju pakalpojumu sniedzējiem veikt darbības pret surogātpasta izplatītājiem. Individuāliem abonentiem, izņemot atsevišķus gadījumus, nav ne naudas, ne stimulu uzsākt šāda veida tiesiskas darbības. Turpretim interneta piekļuves sniedzējiem un citiem PPEKPS ir finanšu līdzekļi un tehnoloģiskās spējas, lai izmeklētu surogātpasta kampaņas un identificētu to autorus, un šķiet, būtu tikai atbilstoši, ka tiem dotu tiesības veikt tiesiskas darbības pret surogātpasta izplatītājiem.

56. EDAU ierosinātajā grozījumā īpaši novērtē to, ka tas arī ļautu patērētāju apvienībām un arodbiedrībām, kas pārstāv no surogātpasta cietušo patērētāju intereses, celt tiesā prasību viņu vārdā. Kā izklāstīts iepriekš, surogātpasta dēļ datu subjektam nodarītais kaitējums, izvērtējot individuāli, parasti nav pats par sevi pietiekami būtisks, lai celtu prasību tiesā. Faktiski EDAU jau ir ierosinājis šo pasākumu attiecībā uz privātās dzīves un datu aizsardzības pārkāpumiem, vispārējā tekstā to iekļaujot savā atzinumā

([1]) Viens šāds gadījums ir lieta *Microsoft corporation v Paul McDonald t/a Bizards UK* (2006 All Er (D) 153).

par pasākumiem, kas veikti saskaņā ar Darba programmu labākai Datu aizsardzības direktīvas īstenošanai ([1]). EDAU uzskata, ka priekšlikumā varēja iet vēl tālāk un ierosināt kolektīvas prasības, kas dotu iespēju pilsoņu grupām kopīgi izmantot tiesvedību jautājumos, kas attiecas uz personas datu aizsardzību. Attiecībā uz surogātpastu, ko saņem liels personu skaits, pastāv iespēja, ka atsevišķu personu grupas apvienotos un kolektīvi uzsāktu tiesiskas darbības pret surogātpasta izplatītājiem.

57. EDAU īpaši nožēlo to, ka priekšlikumā iespējas juridiskām personām veikt tiesiskas darbības ir ierobežotas, — tikai situācijās, kad tiek pārkāpts direktīvas 13. pants, t.i., situācijās, kad pārkāpj noteikumu par nevēlamām e-pasta komunikācijām. Tiešām saskaņā ar ierosināto grozījumu juridiskām personām nebūtu iespējas veikt tiesiskas darbības saistībā ar pārējo e-privātuma direktīvas noteikumu pārkāpumiem. Piemēram, pašreizējos noteikumos nav paredzēts ļaut juridiskām personām, tādām kā patērētāju apvienības, veikt tiesiskas darbības pret interneta piekļuves pakalpojumu sniedzēju, kas būtu izpaudis miljoniem patērētāju personas datus. E-privātuma direktīvas izpilde kopumā, ne tikai kāda atsevišķa tās panta izpilde, ievērojami uzlabotos, ja 13. panta 6. punkta noteikums tiktu pārveidots uz vispārīgu noteikumu, lai ļautu juridiskām personām veikt tiesiskas darbības saistībā ar jebkura e-privātuma direktīvas noteikuma pārkāpumu.

58. Lai atrisinātu šo problēmu, EDAU ierosina pārveidot 13. panta 6. punktu par atsevišķu pantu (14. pantu). Turklāt būtu jāveic šāds neliels grozījums 13. panta 6. punkta formulējumā: Teksts "*saskaņā ar šo pantu*" būtu jālasa "saskaņā ar šo direktīvu".

II.5. **Izpildes noteikumu nostiprināšana: pievieno 15.a pantu**

59. E-privātuma direktīvā nav iekļauti skaidri formulēti izpildes noteikumi. Tā vietā ir dota atsauce uz iedaļu par izpildes noteikumiem datu aizsardzības direktīvā ([2]). EDAU pauž gandarījumu par priekšlikumā iekļauto jauno 15.a pantu, kurā skaidri pievēršas šajā direktīvā paredzētajiem izpildes noteikumiem.

60. Pirmkārt, EDAU norāda, ka efektīvas izpildes politika šajā jomā paredz, kā tas prasīts saskaņā ar ierosināto 15.a panta 3. punktu, lai valsts iestādēm piešķirtu izmeklēšanas pilnvaras vajadzīgās informācijas vākšanai. Visai bieži būs situācija, ka pierādījumi par e-privātuma direktīvas noteikumu pārkāpumiem pēc būtības ir elektroniski un tos var saglabāt dažādos datoros un iekārtās vai tīklos. Šajā sakarā ir svarīgi, lai izpildes iestādēm tiktu dota iespēja iegūt kratīšanas orderi, kas piešķir tiesības ierasties un veikt meklēšanu un arestu.

61. Otrkārt, EDAU īpaši priecājas par ierosināto grozījumu, t.i., 15.a panta 2. punktu, saskaņā ar kuru valsts pārvaldes iestādēm jābūt pilnvarotām izdot pavēles, t.i., pieprasīt pārkāpumu izbeigšanu, un rīkoties ar vajadzīgām izmeklēšanas pilnvarām un resursiem. Valsts pārvaldes iestādēm, tostarp datu aizsardzības iestādēm, būtu jādod tiesības izdot pavēles ar pieprasījumu, lai likumpārkāpēji pārtrauc darbības, ar ko tiek pārkāpti e-privātuma direktīvas noteikumi. Pavēle vai pilnvarojums pieprasīt pārkāpuma izbeigšanu ir lietderīgs līdzeklis pret darbībām, kas notiek nepārtraukti, pārkāpjot personas tiesības. Pavēles būtu ļoti lietderīgas, lai pārtrauktu e-privātuma direktīvas noteikumu pārkāpumus, piemēram, 13. panta par nevēlamām komerciālām komunikācijām pārkāpšanu, kas pati par sevi ir nepārtraukta darbība.

62. Treškārt, priekšlikums ļauj Komisijai ieviest tehniskus īstenošanas pasākumus, lai nodrošinātu efektīvu pārrobežu sadarbību valsts tiesību aktu izpildē (ierosināts grozījums 15.a panta 4. punkts). Līdzšinējā sadarbības pieredze ietver vienošanos, kas panākta pēc Komisijas ierosmes, ar ko izveido kopīgu procedūru, kā risināt pārrobežu sūdzības par surogātpastu.

([1]) Eiropas datu aizsardzības uzraudzītāja atzinums saistībā ar 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.).

([2]) Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

63. EDAU uzskata, ka tiesību aktos paustais atbalsts tam, lai pārvaldes iestādes palīdzētu savām partnerēm citās dalībvalstīs, neapšaubāmi sekmēs to ievērošanu pārrobežu mērogā. Tādēļ ir piemēroti, ka ar šo priekšlikumu ļautu Komisijai izveidot nosacījumus, lai nodrošinātu pārrobežu sadarbību, tostarp procedūras informācijas apmaiņai.

III. **SECINĀJUMI UN IETEIKUMI**

64. EDAU pauž nedalītu gandarījumu par šo priekšlikumu. Ierosinātie grozījumi nostiprina personas privātās dzīves un personas datu aizsardzību elektronisko komunikāciju nozarē, un tas darīts ar viegliem paņēmieniem, neuzliekot organizācijām nepamatotus un nevajadzīgus slogus. Konkrēti, EDAU uzskata, ka ierosinātie grozījumi lielākoties nebūtu jāgroza, ciktāl tie pienācīgi izpilda noteiktos mērķus. 69. punktā ir uzskaitīti grozījumi, ko EDAU vēlētos saglabāt negrozītā versijā.

65. Lai gan kopumā priekšlikums ir vērtējams pozitīvi, EDAU uzskata, ka dažus grozījumus tajā vajadzētu uzlabot, lai nodrošinātu, ka tie efektīvi garantē pienācīgu personas datu un privātās dzīves aizsardzību. Tas īpaši attiecas uz noteikumiem par ziņošanu saistībā ar drošības pārkāpumiem un noteikumiem par tiesiskām darbībām, ko uzsāk elektronisko komunikāciju pakalpojumu sniedzēji par noteikumu pārkāpumiem attiecībā uz surogātpastu. Turklāt EDAU pauž nožēlu par to, ka priekšlikumā nav aplūkoti daži jautājumi, kas nebija pienācīgi risināti spēkā esošajā e-privātuma direktīvā, tādējādi atstājot neizmantotu šo iespēju, ko deva pārskatīšana, lai atrisinātu problemātiskos jautājumus.

66. Lai atrisinātu abas problēmas, proti, jautājumus, kas priekšlikumā nav aplūkoti pienācīgi un tos, kas nav risināti vispār, šajā atzinumā ir izklāstīti daži teksta priekšlikumi. 67. un 68. punktā ir rezumētas šīs problēmas un ierosināts konkrēts formulējums. EDAU aicina likumdevēju ņemt tos vērā, kamēr priekšlikums darba variantā veic likumdošanas procesā noteikto ceļu.

67. Priekšlikumā ietvertie grozījumi, kurus, EDAU stingri uzskata, vajadzētu grozīt, ir šādi:

i) **ziņošana par drošības pārkāpumiem** Kā formulēts, ierosinātais grozījums, iekļaujot 4. panta 4. punktu attiecas uz publiskajos tīklos pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem (interneta pakalpojumu sniedzējiem un tīkla operatoriem), kuriem ir jāziņo valsts pārvaldes iestādēm un saviem klientiem par drošības pārkāpumiem. EDAU pilnībā atbalsta šo prasību. Tomēr EDAU uzskata, ka šāda prasība būtu jāpiemēro arī informācijas sabiedrības pakalpojumu sniedzējiem, kas bieži apstrādā konfidenciālu personisku informāciju. Tādējādi šī prasība attiektos arī uz tiešsaistē funkcionējošām bankām un apdrošināšanas kompānijām, veselības pakalpojumu sniedzējiem un citiem uzņēmumiem.

Šajā sakarā EDAU ierosina 4. panta 3. punktā iekļaut šādu atsauci uz informācijas sabiedrības pakalpojumu sniedzējiem: "*Drošības pārkāpuma gadījumā … publiski pieejamu komunikāciju pakalpojumu sniedzējs* un informācijas sabiedrības pakalpojumu sniedzējs *… par to ziņo attiecīgajam abonentam un valsts pārvaldes iestādei*".

ii) **tiesiskās darbības, ko uzsāk publiskajos tīklos pieejamu elektronisko sakaru pakalpojumu sniedzēji** Kā formulēts, ierosinātais grozījums, iekļaujot 13. panta 6. punktu, nosaka civiltiesiskās aizsardzības līdzekļus jebkurai privātpersonai vai juridiskai personai, jo īpaši elektronisko komunikāciju pakalpojumu sniedzējiem, apkarot e-privātuma direktīvas 13. panta noteikumu pārkāpumus saistībā ar nevēlamām e-pasta komunikācijām. EDAU šis noteikums ir pieņemams. Tomēr EDAU nesaskata pamatu, kāpēc šīs jaunās spējas būtu jāierobežo, attiecinot tikai uz 13. panta pārkāpumiem. EDAU ierosina ļaut juridiskām personām veikt tiesiskas darbības saistībā ar jebkura e-privātuma direktīvas noteikuma pārkāpumu.

Lai to panāktu, EDAU ierosina pārveidot 13. panta 6. punktu par atsevišķu pantu (14. pantu). Turklāt būtu jāveic šāds neliels grozījums 13. panta 6. punkta formulējumā: Teksts "*saskaņā ar šo pantu*" būtu jālasa "saskaņā ar šo direktīvu".

68. E-privātuma direktīvas piemērošanas joma, kas patlaban attiecas tikai uz publiskajos tīklos pieejamu elektronisko sakaru pakalpojumu sniedzējiem, ir viens no problemātiskākajiem jautājumiem, kas priekšlikumā ir palicis neatrisināts. EDAU uzskata, ka direktīva būtu jāgroza, lai paplašinātu tās piemērošanas jomu, tajā iekļaujot elektronisko komunikāciju pakalpojumu sniedzējus arī jauktajos (privātajos un publiskajos) un privātajos tīklos.

69. Grozījumi, kurus, EDAU stingri uzskata, vajadzētu saglabāt negrozītā versijā, ir šādi:

i) ***RFID***: Ierosinātais grozījums 3. pantā, saskaņā ar kuru publiskajos elektronisko komunikāciju tīklos iekļauj "*publiskos komunikāciju tīklus, kuros var izmantot datu vākšanas un identifikācijas ierīces*" ir pilnībā pieņemams. Šis noteikums ir ļoti pozitīvi vērtējams, jo tajā paskaidrots, ka vairākiem *RFID* lietojumiem ir jābūt saskaņā ar e-privātuma direktīvas noteikumiem, tādējādi mazinot juridiskas neskaidrības šajā jautājumā.

ii) **Sīkdatnes/spiegprogrammas**: Ierosinātais grozījums 5. panta 3. punktā ir jāvērtē atzinīgi, jo no tā izriet, ka prasība ziņot par sīkdatņu/spiegprogrammu uzglabāšanu lietotāja gala iekārtā un dot tiesības iebilst pret šādu uzglabāšanu attieksies arī uz gadījumiem, kad šādas ierīces tiek ievietotas ar ārējo atmiņas nesēju, piemēram, lasāmatmiņas kompaktdisku (CD-ROM), USB atslēgu starpniecību. Tomēr EDAU ierosina veikt nelielu grozījumu 5. panta 3. punkta pēdējā daļā, proti, svītrot no teikuma vārdu "*veicinātu*".

iii) **EDAU lēmums par komitoloģijas procedūru un apspriešanos un nosacījumi/ierobežojumi attiecībā uz paziņošanas prasību**: Ierosinātajā grozījumā, iekļaujot 4. panta 4. punktu attiecībā uz paziņošanas prasību, pēc apspriešanās ar EDAU, komitoloģijas pārziņā ir atstāta lēmumu pieņemšana par sarežģītiem jautājumiem saistībā ar sistēmu ziņošanai par drošības pārkāpumiem — tās apstākļiem, formātu un piemērojamām procedūrām. EDAU stingri atbalsta šo vienoto pieeju. Tiesību akti par drošības pārkāpumu paziņošanu ir temats pats par sevi, un tas jāizskata pēc tam, kad veiktas rūpīgas debates un analīze.

Ar šo jautājumu ir saistīts dažu ieinteresēto pušu aicinājums 4. panta 4. punktā noteikt izņēmumus attiecībā uz prasību ziņot par drošības pārkāpumiem. EDAU stingri iebilst pret šādu pieeju. Viņš drīzāk atbalsta to, lai vispārējais jautājums par ziņošanu — kā to veikt, kādos apstākļos to var saīsināt vai kaut kā ierobežot, tiktu analizēts kopumā, pēc tam, kad notikušas pienācīgas debates.

iv) **Izpilde**: Ierosinātais grozījums, iekļaujot 15.a pantu, satur daudzus derīgus elementus, kas būtu saglabājami, lai veicinātu efektīvu ievērošanu, tostarp valsts pārvaldes iestāžu izmeklēšanas pilnvaru stiprināšanu (15.a panta 3. punkts) un pilnvaru piešķiršanu valsts pārvaldes iestādēm pieprasīt izbeigt pārkāpumus.

Briselē, 2008. gada 10. aprīlī

Peter HUSTINX

Eiropas datu aizsardzības uzraudzītājs