Otrais Eiropas Datu aizsardzības uzraudzītāja atzinums par pārskatīto Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju)

(2009/C 128/04)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

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

ņemot vērā Eiropas Savienības Pamattiesību hartu un it 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,

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,

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 it īpaši tās 41. pantu,

IR PIEŅĒMIS ŠO ATZINUMU.

I. IEVADS

Pašreizējais stāvoklis

1. Eiropas Komisija 2007. gada 13. novembrī ierosināja tiesību aktu, ar ko citastarp izdara grozījumus direktīvā par privātumu un elektronisku komunikāciju, ko parasti dēvē par ePrivātuma direktīvu [1] (turpmāk "ierosināts tiesību akts" vai "Komisijas ierosināts tiesību akts"). EDAU 2008. gada 10. aprīlī pieņēma atzinumu par Komisijas ierosināto tiesību aktu un nāca klajā ar ieteikumiem uzlabot ierosināto tiesību aktu, lai palīdzētu nodrošināt to, ka ierosinātie grozījumi cilvēkiem nodrošinātu cik vien iespējams labu privātuma un personas datu aizsardzību ("EDAU pirmais atzinums") [2].

2. EDAU sveica Komisijas ierosinājumu izveidot obligātu aizsargpasākumu pārkāpumu paziņošanas sistēmu, kas uzņēmumiem liktu paziņot cilvēkiem, ka viņu personas dati ir bojāti. Turklāt viņš arī pauda gandarījumu par jaunu noteikumu, kas ļauj juridiskām personām (*piem.*, patērētāju apvienībām un interneta pakalpojumu nodrošinātājiem) celt tiesā prasību pret surogātpasta sūtījumu izplatītājiem, papildinot surogātpasta sūtījumu apkarošanas instrumentus.

3. Parlamenta diskusijās pirms Eiropas Parlamenta pirmā lasījuma EDAU sniedza vēl dažus padomus – un saistībā ar jautājumiem, kas bija aktualizējušies ziņojumos, ar ko nāca klajā vispārējo pakalpojumu direktīvas un ePrivātuma direktīvas [3] pārskatīšanas jautājumos kompetentas Eiropas Parlamenta komitejas – ar piebildēm par dažiem konkrētiem jautājumiem ("piebildes") [4]. Piebildes galvenokārt attiecās uz jautājumiem saistībā ar datu plūsmu datu apstrādi un intelektuālā īpašuma tiesību aizsardzību.

4. Eiropas Parlaments ("EP") 2008. gada 24. septembrī pieņēma normatīvo rezolūciju par ePrivātuma direktīvu ("pirmais lasījums") [5]. EDAU pozitīvi vērtēja vairākus EP ierosinātus grozījumus, kas bija pieņemti pēc EDAU atzinuma un iepriekš minētajām piebildēm. Pie svarīgākiem grozījumiem piederēja pienākumu ziņot par aizsargpasākumu pārkāpumiem attiecināt arī uz informācijas sabiedrības pakalpojumu nodrošinātājiem (t. i., uzņēmumiem, kas darbojas internetā). EDAU sveica arī grozījumu, kas ļauj juridiskām un fiziskām personām celt prasības par visiem ePrivātuma direktīvas pārkāpumiem (ne tikai par

[1] ePrivātuma direktīvas, direktīvu 2002/21/EK, 2002/19/EK, 2002/20/EK, 2002/22/EK un 2002/58/EK, kā arī Regulas (EK) Nr. 2006/2004 pārskatīšana (turpmāk "telekomunikāciju paketes pārskatīšana") pieder pie plašāka pārskatīšanas procesa, veidojot ES telekomunikāciju iestādi.

[2] 2008. gada 10. aprīļa atzinums par ierosināto direktīvu, ar ko, citu starpā, groza Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīvu par privāto dzīvi un elektroniskām komunikācijām), OV C 181, 18.7.2008., 1. lpp.

[3] Direktīva 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (universālo pakalpojumu direktīva), OV L 108., 24.4.2002, 51. lpp.

[4] EDAU piebildes par dažiem jautājumiem sakarā ar IMCO ziņojumu par direktīvas 2002/22/EK (universāli pakalpojumi) & direktīvas 2002/58/EK (ePrivātuma direktīvas), (2008. gada 2. septembris) pārskatīšanu. Tas ir pieejams tīkla vietnē www.EDAU.europa.eu

[5] Eiropas Parlamenta normatīvā rezolūcija (2008. gada 24. septembris) par ierosināto Eiropas Parlamenta un Padomes direktīvu, ar ko groza Direktīvu 2002/22/EK par universāliem pakalpojumiem un lietotāju tiesībām attiecībā uz elektronisko komunikāciju tīkliem, 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 (COM(2007) 698 – C6-0420/2007 – 2007/0248(COD).

surogātpasta sūtījumu noteikumu pārkāpumiem kā Komisijas ierosinātajā tiesību aktā). Pēc Parlamenta pirmā lasījuma Komisija pieņēma grozītu ierosinātu tiesību aktu par ePrivātuma direktīvu (turpmāk "Grozītais ierosinātais tiesību akts") ([6]).

5. Padome 2008. gada 27. novembrī panāca politisku vienošanos pārskatīt noteikumus par telekomunikāciju paketi, arī par ePrivātuma direktīvu, kas kļūs par Padomes Kopējo nostāju ("Kopējā nostāja") ([7]). Kopējo nostāju darīs zināmu Eiropas Parlamentam saskaņā ar Eiropas Kopienas dibināšanas līguma 251. panta 2. punktu, un tas var nozīmēt, ka EP ierosinās grozījumus.

Vispārējs pārskats par Padomes nostāju

6. Padome ir grozījusi būtiskus ierosinātā tiesību akta elementus un nav akceptējusi daudzus EP pieņemtos grozījumus. Tā kā Kopējā nostājā noteikti ir pozitīvi elementi, EDAU ir visnotaļ nobažījies par tās saturu kopumā, it īpaši tāpēc, ka Kopējā nostājā nav iestrādāti daži pozitīvi, EP ierosināti grozījumi, grozītais ierosinātais tiesību akts, un ar 29. panta darba grupas starpniecību publiskoti EDAU un Eiropas Datu aizsardzības iestāžu atzinumi ([8]).

7. Ir noticis pretējais, vairākos gadījumos grozītais ierosinātais tiesību akts un EP ierosinātie grozījumi, kas pilsoņiem dotu aizsardzības līdzekļus, ir svītroti vai būtiski vājināti. Tādējādi tā līmeņa aizsardzība, kas cilvēkiem ir dota Kopējā nostājā, ir būtiski vājināta. Tāpēc EDAU tagad nāk klajā ar otru atzinumu cerībā, ka, ePrivātuma direktīvai atrodoties likumdošanas procesā, pieņems jaunus grozījumus, ar ko datu aizsardzības līdzekļus atjaunos.

8. Otrā atzinumā uzmanība ir pievērsta dažiem būtiskiem aspektiem, un tajā nav atkārtoti visi EDAU pirmā atzinumā vai piebildēs izteiktie argumenti, kas joprojām ir spēkā. Šajā atzinumā konkrēti ir pārrunāti šādi jautājumi –

— noteikumi par aizsargpasākumu pārkāpumu paziņošanu;

— ePrivātuma direktīvas piemērošanas joma privātos un atklātībā pieejamos privātos tīklos;

— datu plūsmu datu apstrāde drošības vajadzībām;

— juridisku personu iespējas celt tiesvedību par ePrivātuma direktīvas pārkāpumiem.

9. Pievēršoties iepriekš minētiem jautājumiem, Padomes Kopējā nostāja šajā atzinumā ir analizēta, salīdzinot ar EP pirmo lasījumu un Komisijas grozīto ierosināto tiesību aktu. Atzinumā ir iekļauti ieteikumi, kā vienkāršot ePrivātuma direktīvu un nodrošināt, lai direktīva arī turpmāk pietiekami aizsargātu cilvēku privātumu un personas datus.

II. **NOTEIKUMI PAR AIZSARGPASĀKUMU PĀRKĀPUMU PAZIŅOŠANU**

10. EDAU ir pārliecināts, ka ir jāizstrādā aizsargpasākumu pārkāpumu paziņošanas sistēma, kā iestādēm un cilvēkiem paziņot par viņu personas datu bojāšanu ([9]). Paziņojumi par aizsargpasākumu pārkāpumiem var palīdzēt cilvēkiem veikt vajadzīgos pasākumus, lai mazinātu iespējamu bojājumu radītos kaitējumus. Turklāt pienākums sūtīt paziņojumus, informējot par aizsargpasākumu pārkāpumiem, mudinās uzņēmumus uzlabot datu drošību un vairot to atbildību tiem uzticēto personas datu jomā.

11. Komisijas grozītais ierosinātais tiesību akts, Eiropas Parlamenta pirmais lasījums un Padomes Kopējā nostāja liecina par trijām dažādām pašlaik izskatāmām pieejām aizsargpasākumu pārkāpumu paziņošanai. Katrai no trijām pieejām ir pozitīvi aspekti. Tomēr EDAU uzskata, ka visas minētās pieejas var uzlabot, un iesaka ņemt vērā še turpmāk aprakstītos ieteikumus, apsverot pēdējos soļus pirms aizsargpasākumu pārkāpumu paziņošanas sistēmas pieņemšanas.

([6]) Grozīta ierosinātā Eiropas Parlamenta un Padomes direktīva, 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, Brisele, 6.11.2008, COM(2008) 723 galīgā redakcija.

([7]) Pieejama atklātībā pieejamā Padomes interneta vietnē.

([8]) Atzinums 2/2008 par direktīvas 2002/58/EK (par privātās dzīves aizsardzību elektronisko komunikāciju nozarē – ePrivātuma direktīvas) pārskatīšanu, kas ir pieejama 29. panta darba grupas tīkla lapā.

([9]) Šajā atzinumā ir lietots vārds "bojāts", runājot par visiem personas datu pārkāpumiem, kas notikuši, nejauši vai nelikumīgi tos iznīcinot, pazaudējot, sagrozot, neatļauti atklājot vai darot atklātībā pieejamus, pārsūtot, glabājot vai citādi apstrādājot.

12. Analizējot trīs minētās aizsargpasākumu pārkāpumu paziņošanas sistēmas, vērā ir jāņem pieci būtiski aspekti i) kāda ir aizsargpasākumu pārkāpumu definīcija; ii) uz kādām struktūrām attiecas paziņošanas pienākums ("pienākuma aptvertās struktūras"); iii) kādi parametri nosaka, ka ir jāīsteno paziņošanas pienākums; iv) kā izvēlēties struktūru, kas noteiks, vai aizsargpasākumu pārkāpums atbilst parametriem, un v) kas saņem paziņojumu.

Pārskats pār Komisijas, Padomes un EP pieeju

13. Gan Eiropas Parlaments, gan Komisija, gan Padome ir izvēlējusies dažādas pieejas, kā paziņot par aizsargpasākumu pārkāpumiem. EP pirmajā lasījumā grozīja sākotnējo Komisijas ierosinātajā tiesību aktā ietverto aizsargpasākumu pārkāpumu paziņošanas sistēmu ([10]). Saskaņā ar EP pieeju paziņošanas pienākums attiecas gan uz atklātībā pieejamu elektronisku komunikāciju pakalpojumu nodrošinātājiem, gan arī uz informācijas sabiedrības pakalpojumu nodrošinātājiem ("PPECS" un "ISSP"). Turklāt tāda pieeja paredz, ka par visiem personas datu režīma pārkāpumiem būtu jāziņo normatīvai vai kompetentai attiecīgas valsts iestādei (kopā – "iestādes"). Ja iestādēm būtu jānosaka, vai pārkāpums ir smags, tās prasītu *PPEC* un *ISSP* to uzreiz paziņot piemeklētajai personai. Ja pārkāpumi radītu tūlītējas un tiešas briesmas, *PPECS* un *ISSP* vispirms to paziņotu cilvēkiem, un tikai tad iestādēm, un negaidītu normatīvas iestādes lēmumu. Struktūrām, kas var iestādēm pierādīt, ka "ir piemēroti attiecīgi tehniskas aizsardzības pasākumi", kas padara datus nelasāmus nevienam, kurš nav pilnvarots tiem piekļūt, nav pienākuma informēt patērētājus.

14. Saskaņā ar Padomes pieeju paziņojumi ir jāsūta gan abonentiem, gan iestādēm, bet tikai tādos gadījumos, ja *struktūra, uz ko attiecas pienākums,* uzskata, ka pārkāpums rada *nopietnu apdraudējumu* abonenta privātumam (t. i., ir notikusi identitātes zādzība vai krāpniecība, miesas bojājumi, smagi pazemojumi vai reputācijas iedragāšana).

15. Komisijas grozītajā ierosinātajā tiesību aktā ir palicis EP pienākums iestādēm paziņot par visiem pārkāpumiem. Tomēr pretstatā EP pieejai grozītajā ierosinātajā tiesību aktā ir iekļauts izņēmums paziņošanas prasībai – tā neattiecas uz attiecīgiem cilvēkiem, ja *PPEC* kompetentai iestādei pierāda, ka i) pārkāpuma dēļ "visnotaļ ir paredzams, ka" neradīsies nekāds ļaunums (t. i., saimnieciski zaudējumi, sociāls ļaunums vai identitātes zādzība) vai ii) datiem, uz ko attiecas pārkāpums, ir piemēroti "attiecīgi tehnoloģiskas aizsardzības pasākumi". Tādējādi Komisijas pieejā ir iekļauta nodarītā ļaunuma analīze saistībā ar individuāliem paziņojumiem.

([10]) EP ierosinātos grozījumos Nr. 187., 124. līdz 127., kā arī 27., 21. un 32. šim jautājumam ir pievērsta īpaša uzmanība.

16. Svarīgi ir ņemt vērā, ka saskaņā ar EP ([11]) un Komisijas pieeju tieši *iestādēm* ir uzlikts pienākums noteikt, vai pārkāpums ir smags un vai visnotaļ ir paredzams, ka tas nodarīs ļaunumu. Saskaņā ar Padomes pieeju lēmums, gluži pretēji, ir atstāts *ieinteresētu struktūru* ziņā.

17. Gan Padomes, gan Komisijas pieeja attiecas tikai uz *PPECS*, un neattiecas uz *ISSPs* – kā paredzēts EP pieejā.

Aizsargpasākumu pārkāpumu definīcijas

18. EDAU priecājas, ka trijos ierosinātos tiesību aktos ir viena un tā pati aizsargpasākumu pārkāpumu paziņošanas definīcija, ar ko saskaņā par pārkāpumiem atzīst "drošības pārkāpumus, kas izraisa nejaušu vai nelikumīgu personas datu iznīcināšanu, zudumu, pārveidi, neatļautu izpaušanu, vai nelikumīgu piekļuvi tiem, tos pārsūtot, glabājot vai citādi apstrādājot (...) " ([12]).

19. Še turpmāk būs norādīts, ka šī definīcija ir apsveicama, ciktāl tā ir pietiekami plaša, lai aptvertu lielāko daļu attiecīgo situāciju, kurās varbūt ir jāziņo par aizsargpasākumu pārkāpumiem.

20. Pirmkārt, definīcijā ir aptverti gadījumi, kad trešā persona ir *neatļauti* piekļuvusi personas datiem, piemēram, ielaužoties serverī ar personas datiem un izgūstot minēto informāciju.

21. Otrkārt, definīcija attiektos arī uz gadījumiem, ja personas dati ir pazaudēti vai darīti atklātībā zināmi, kaut arī neatļauta piekļuve vēl būtu jāpierāda. Pie tādiem gadījumiem piederētu situācijas, kad personas dati var būt pazaudēti (piem., *CD-ROM, USB* datu nesēju vai citu pārnēsājamu ierīču gadījumā), vai parasti lietotāji tos ir darījuši atklātībā pieejamus (darbinieku dati ar interneta starpniecību var nejauši kādu laiku atrasties atklātībā pieejamā vidē). Tā kā bieži vien nebūs pierādījumu, kas liecinātu, ka dati dažkārt var būt pieejami trešām personām, kam tas nav atļauts – vai arī tādas personas varētu tos, lietot, šķiet pareizi definīcijas darbības jomā iekļaut tādus gadījumus. Tātad EDAU iesaka paturēt šo definīciju. EDAU iesaka ietvert aizsargpasākumu pārkāpumu definīciju arī ePrivātuma direktīvas 2. pantā, jo tas labāk saderēs ar visu direktīvas struktūru un nodrošinās lielāku skaidrību.

([11]) Vienīgais izņēmums ir tūlītējas un tiešas briesmas, un tad pienākuma aptvertajām struktūrām vispirms ir jāinformē patērētāji.

([12]) Kopējās nostājas un grozītā ierosinātā tiesību akta 2. panta i) punkts, un EP pirmā lasījuma 3.3. pants.

Struktūras, uz ko vajadzētu attiecināt paziņošanas pienākumu

22. Paziņošanas pienākums saskaņā ar EP pieeju attiecas gan uz *PPECS*, gan *ISSPs*. Tomēr saskaņā ar Padomes un Komisijas sistēmu tikai *PPECS*, piemēram, telekomunikāciju uzņēmumiem un interneta piekļuves nodrošinātājiem, būs pienākums paziņot cilvēkiem, ja aizsargpasākumu pārkāpumi izraisa personas datu bojājumus. Citās darbības jomās, piemēram, tiešsaistes bankām, tiešsaistes vairumtirgotājiem, tiešsaistes veselības aizsardzības nodrošinātājiem un citiem tāda pienākuma nav. Še turpmāk sīkāk aprakstītu iemeslu dēļ EDAU uzskata, ka no valstu politikas perspektīves būtiski svarīgi ir nodrošināt, lai uz informācijas sabiedrības dienestiem, pie kā pieder tiešsaistes uzņēmumi, tiešsaistes bankas, tiešsaistes veselības aizsardzības nodrošinātāji, utt., arī attiektos paziņošanas prasība.

23. Pirmkārt, EDAU norāda, lai gan aizsargpasākumu pārkāpumi, kas uzliktu paziņošanas pienākumu, noteikti ir vērsti pret telekomunikāciju uzņēmumiem, tas pats attiecas uz citu tipu uzņēmumiem/pakalpojumu nodrošinātājiem. Var teikt, ka tiešsaistes vairumtirgotāji, tiešsaistes bankas, tiešsaistes aptiekas no aizsargpasākumu pārkāpumiem cietīs tikpat ļoti, ja ne vairāk kā telekomunikāciju uzņēmumi. Tāpēc apdraudējumu apsvērumi nesveras par labu tam, lai pārkāpumu paziņošanas prasība aprobežotos tikai ar *PPECS*. Vajadzību pēc plašākas pieejas pierāda citu valstu pieredze. Piemēram, gandrīz visos Savienoto Valstu štatos (pašlaik vairāk nekā 40 štatos) ir ieviesti aizsargpasākumu pārkāpumu paziņošanas likumi, kam ir plašāka piemērošanas joma un kas aptver ne tikai *PPECS*, bet visas struktūras, kuru rīcībā ir attiecīgi personas dati.

24. Otrkārt, kaut gan pārkāpumi, kas skar tādus personas datus, ko parasti apstrādā *PPECS*, noteikti var ietekmēt cilvēku privātumu, tas pats – un varbūt pat vēl vairāk – attiecas uz tādu personas informāciju, ko apstrādā *ISSP*. Noteikti banku un citu finanšu iestāžu rīcībā var būt ļoti konfidenciāla informācija (piem., dati par banku kontiem), kuru atklājot, to var izmantot identitātes zādzībai. Tāpat arī ļoti diskrētas veselības stāvokļa informācijas atklāšana tiešsaistes dienestos cilvēkiem var ļoti kaitēt. Tālab tādi personas dati, ko var bojāt, prasa arī plašāku aizsargpasākumu pārkāpumu paziņošanas piemērojumu, un tā obligāti ir jāattiecina vismaz uz *ISSP*.

25. Pret šī panta piemērošanas jomas paplašināšanu, t. i., pret to, lai šī prasība attiektos uz lielāku skaitu struktūru, vēršas, piesaucot dažus juridiskus aspektus. Konkrēti tas, ka ePrivātuma direktīvas darbības joma kopumā attiecas tikai uz *PPECS*, ir uzdots par šķērsli piemērot to arī ISSP.

26. Šādā sakarā EDAU vēlas atgādināt, ka i) nav nekādu juridisku šķēršļu direktīvas darbības jomā iekļaut citus darbību veicējus, ne tikai *PPECS*. Kopienas likumdevējiem šajā ziņā ir pilnīga rīcības brīvība. ii) Ir citi precedenti, kad ePrivātuma direktīva ir piemērota citām struktūrām, ne tikai *PPECS*.

27. Piemēram, 13. pants neattiecas tikai uz *PPECS*, bet uz visām uzņēmējsabiedrībām, kas izsūta nelūgtus paziņojumus, kas prasa, lai iepriekš būtu saņemta piekrišana tādus saņemt. Vēl turklāt ePrivātuma direktīvas 5. panta 3. punkts, kurā *inter alia* ir aizliegts lietotāju datoros glabāt informāciju, piemēram, sīkdatnes, uzliek saistības ne tikai PPECS, bet gan visiem, kas mēģina glabāt informāciju vai gūt piekļuvi informācijai, ko cilvēki glabā datoros. Vēl turklāt Komisija pašreizējā likumdošanas procesā ir ierosinājusi pat paplašināt 5. panta 3. punkta piemērojumu, ja līdzīgas tehnoloģijas (sīkdatnes/spiegu programmas) piegādā, izmantojot ne tikai elektroniskas saziņas sistēmas, bet arī visus citus iespējamus paņēmienus (nosūknējot datus internetā vai pārnesot ārējos datu glabātājos, piemēram, *CD-ROM*, *USB* pirkstiņos jeb ātrdarbīgās atmiņās, utt.). Visi minētie elementi ir labi, un tie būtu jāpatur, turklāt tie arī rada precedentus, kas ir nozīmīgi diskusijās par piemērojuma jomu.

28. Vēl šajā likumdošanas procesā Komisija un EP, un droši vien arī Padome, turklāt ir ierosinājusi jaunu 6.6. panta a) punktu, par ko būs runāts še turpmāk un kas attiektos uz citām struktūrām nekā *PPECS*.

29. Visbeidzot, ņemot vērā pilnībā pozitīvos elementus, kas ir atvasināti no pienākuma paziņot par aizsargpasākumu pārkāpumiem, ir paredzams, ka cilvēki gaidīs ieguvumu no tiem ne tikai tad, kad viņu personas datus būs bojājuši *PPECS*, bet arī *ISSP*. Cilvēki var vilties, ja, piemēram, nesaņems informāciju, kad tiešsaistes banka būs pazaudējusi viņu bankas konta informāciju.

30. Īsi sakot, EDAU ir pārliecināts, ka aizsargpasākumu pārkāpumu paziņošanas jēga pilnībā būs īstenota tikai tad, ja gan *PPECS*, gan *ISSP* būs iekļauti pienākuma aptvertajās struktūrās.

Parastāko paziņojumu parametri

31. Runājot par paziņojumu parametriem, kā būs izskaidrots še turpmāk, EDAU ir pārliecināts, ka grozītā ierosinātā tiesību akta parametrs "ir visnotaļ iespējams kaitēt" ir pareizākais no trijiem ierosinātiem standartiem. Tomēr ir svarīgi nodrošināt, lai "kaitēt" būtu pietiekami plaši izprasts jēdziens, kas attiektos uz visiem gadījumiem, kad vien būtu kaitēts cilvēku privātumam vai citām likumīgām interesēm. Citādā ziņā labāk būtu izveidot jaunu parametru, ar ko saskaņā paziņošana būtu obligāta "ja ir visnotaļ iespējams, ka pārkāpums cilvēkiem rada kaitējumus".

32. Iepriekšējā iedaļā ir ieskicēts, ka nosacījumi, ar ko saskaņā cilvēkiem ir jāsniedz paziņojumi (tos dēvē par "standartiem" jeb "parametriem") EP, Komisijas un Padomes pieejā ir dažādi. Acīmredzot paziņojumu apjoms, ko cilvēki saņems, lielākoties būs atkarīgs no paziņojumu standartu jeb parametru kompleksa.

33. Padomes un Komisijas sistēmā paziņojumi ir jāsūta, ja pārkāpums ir "smags abonenta privātuma pārkāpums" (Padome) un ja "ir visnotaļ iespējams, ka pārkāpuma dēļ notiks kaitējums patērētāju interesēm" (Komisija). EP sistēmā cilvēkiem paziņo tad, ja to nosaka "pārkāpuma smagums" (t. i., cilvēkiem ir jāpaziņo, ja pārkāpumu atzīst par "smagu"). Paziņošana nav vajadzīga, ja pārkāpumu par tādu neatzīst ([13]).

34. EDAU to saprot tā – ja personas dati ir bojāti, var teikt, ka cilvēki, kam pieder dati, jebkādos apstākļos ir tiesīgi uzzināt par notikušo starpgadījumu. Tomēr ir visi iemesli apdomāt, vai tas ir pareizs risinājums, ņemot vērā citas intereses un citus apsvērumus.

35. Ir norādīts, ka pienākums sūtīt paziņojumus ik reizi, kad personas dati ir bojāti, citiem vārdiem sakot, bez kādiem ierobežojumiem, var izraisīt to, ka paziņojumu ir pārāk daudz, un daudzo paziņojumu dēļ iestājas pagurums ("notice fatigue"), un tas varētu radīt intereses zudumu (*desensitization*). Kā še turpmāk būs aprakstīts, EDAU apzinās tāda argumenta svaru; un tomēr viņš grib uzsvērt, ka ir norūpējies par to, ka paziņojumu var būt pārāk daudz, un tas varēs liecināt par informācijas drošības prakses izgāšanos plašos mērogos.

([13]) Skat. 11. zemsvītras piezīmi par šī noteikuma izņēmumiem.

36. Kā iepriekš norādīts, EDAU saskata potenciālas negatīvas sekas tam, ka paziņojumu var būt pārāk daudz, un gribētu palīdzēt, lai tiesiskais regulējums, kas ir izstrādāts aizsargpasākumu pārkāpumu paziņošanai, nodrošinātu, ka tas nenotiek. Ja cilvēki bieži saņems paziņojumus par pārkāpumiem pat tādos gadījumos, ja nekādu negatīvu seku, kaitējuma vai briesmu nav, var izrādīties, ka mēs graujam vienu no svarīgākiem paziņojumu sniegšanas mērķiem, jo cilvēki ironiskā kārtā var ignorēt paziņojumus tādos gadījumos, kad viņiem patiesībā vajadzētu kaut ko darīt, lai aizsargātos. Panākt pareizo līdzsvaru, sniedzot nozīmīgus paziņojumus tālab ir svarīgi, jo, ja cilvēki nereaģēs uz saņemtajiem paziņojumiem, paziņošanas sistēmu efektivitāte būs ļoti maza.

37. Lai pieņemtu pareizus parametrus (kas novērstu to, ka paziņojumu var būt pārāk daudz), līdztekus apsvērumiem par to, kas var izraisīt paziņojumu sūtīšanu, ir jāapsver citi faktori, it īpaši – jādefinē aizsargpasākumu pārkāpumi un tas, uz kādu informāciju attiecas paziņošanas pienākums. Šajā sakarā EDAU norāda, ka saskaņā ar trijām ierosinātām pieejām paziņošanas apjomi var būt lieli, ņemot vērā plašo aizsargpasākumu pārkāpumu definīciju, par ko bija runāts iepriekš. Tādas rūpes par to, ka paziņojumu var būt pārāk daudz, pamato arī tas, ka aizsargpasākumu pārkāpumu definīcija aptver visu tipu personas datus. Lai gan EDAU uzskata, ka tāda pieeja (neaprobežoties ar tāda tipa personas datiem, par ko ir jāpaziņo) ir pareiza – pretstatā citām pieejām, piemēram, ASV likumiem, kuros prasības ir koncentrētas uz informācijas diskrētumu – tas vienalga ir vērā ņemams faktors.

38. Ņemot vērā iepriekš minēto, un neaizmirstot arī dažādos mainīgos lielumus, EDAU atzīst par pareizu izstrādāt tādu standartu vai parametru, kas noteiktu, kādos gadījumos paziņošana vairs nav obligāta.

39. Ierosinātie standarti t. i., ja pārkāpums "nopietni apdraud privātumu" vai "ir visnotaļ paredzams, ka tas nodarīs ļaunumu", rada iespaidu, ka abos gadījumos ir runāts arī, piemēram, par kaitējumu sabiedriskam stāvoklim vai reputācijai un par saimnieciskiem zudumiem. Piemēram, tādi standarti pievērstos gadījumiem, kad identitātes zādzība būtu iespējama atklātībā nepieejamu identifikatoru, piemēram, kāda cilvēka pases numura vai arī privātās dzīves informācijas atklāšanas dēļ. EDAU sveic tādu pieeju. Viņš ir pārliecināts, ka ieguvumi, ko dod aizsargpasākumu pārkāpumu paziņošana, nebūtu pilnīgi, ja paziņošanas sistēma attiektos tikai uz pārkāpumiem, kas rada saimnieciskus kaitējumus.

40. Izvēloties no diviem ierosinātiem standartiem, EDAU dod priekšroku Komisijas standartam "visnotaļ ir paredzams, ka tas nodarīs ļaunumu", jo tāds standarts cilvēkiem nodrošinās pienācīgāku aizsardzību. Paziņot par pārkāpumiem ir daudz pamatotāk, ja par tiem "visnotaļ ir paredzams, ka tie nodarīs ļaunumu" cilvēku privātumam nekā tad, ja tie tikai "radīs nopietnus draudus", ka tāds kaitējums varētu notikt. Tādējādi, ja paziņošana attieksies tikai uz tādiem pārkāpumiem, kas radīs nopietnus draudus cilvēku privātumam, tas jūtami ierobežos tādu pārkāpumu skaitu, par ko būtu jāziņo. Ja paziņošana attieksies tikai uz tādiem pārkāpumiem, tas dotu pārāk lielu rīcības brīvību PPECS un ISSP – no tāda viedokļa, vai vispār ir jāpaziņo – jo tiem daudz vieglāk būtu pamatot secinājumu, ka "nopietni apdraudējumi" nepastāv, un nekāds kaitējums "visnotaļ nav paredzams". Kaut gan noteikti ir jāvairās no tā, ka paziņojumu varētu būt pārāk daudz, kamēr nav pierādīts pretējais, tas būtu jālīdzsvaro ar cilvēku privātuma interešu aizsardzību, un cilvēki būtu jāaizsargā vismaz tad, ja visnotaļ ir paredzams, ka pārkāpums viņiem kaitēs. Vēl turklāt izteiksme "visnotaļ ir paredzams, ka" praksē būs efektīvāka – gan pienākuma aptvertām struktūrām, gan kompetentām iestādēm, jo tā prasa objektīvi izvērtēt katru gadījumu un attiecīgi tā kontekstu.

41. Turklāt personas datu pārkāpumi var nodarīt tādu kaitējumu, ko ir grūti aprēķināt, un kas katrā konkrētā gadījumā var būt citāds. Patiesi, viena un tā paša tipa datu atklāšana atkarībā no individuāliem apstākļiem var nodarīt nopietnu kaitējumu vienam cilvēkam, bet daudz mazāku citam. Nebūtu pareizi noteikt tādus parametrus, kas prasītu, lai kaitējums būtu taustāms, nopietns vai smags. Piemēram, Padomes pieeja, kas prasa, lai pārkāpums *nopietni* skartu kāda privātumu, cilvēkiem nodrošinātu nepietiekamu aizsardzību, jo parametri prasa, lai privātumam nodarītās sekas būtu "nopietnas". Tas arī paver iespējas subjektīviem vērtējumiem.

42. Lai gan formulējums "ir visnotaļ iespējams kaitēt" šķiet piemērots aizsargpasākumu pārkāpumu paziņošanas parametrs, EDAU tomēr ir nobažījies, ka tas var neaptvert visus gadījumus, kad cilvēkiem būtu jāpaziņo par notikušo, t. i., visos gadījumos, kad negatīvas sekas cilvēku privātumam vai citām likumīgām tiesībām ir visnotaļ iespējamas. Tāpēc varētu apsvērt parametrus, kas prasītu paziņošanu, "ja visnotaļ ir paredzams, ka pārkāpums cilvēkiem izraisīs nelabvēlīgas sekas".

43. Tādiem alternatīviem parametriem ir papildu priekšrocība – tie saskan ar ES tiesību aktiem datu aizsardzības jomā. Patiesi, datu aizsardzības direktīvā bieži ir pieminētas nelabvēlīgas sekas datu subjektu tiesībām un brīvībām. Piemēram, 18. pants un 49. apsvērums, kurā ir runāts par pienākumu datu aizsardzības iestādēs reģistrēt datu apstrādes darbības, ļauj dalībvalstīm šo pienākumu nepiemērot gadījumos, ja apstrādē "nav visnotaļ paredzams, ka tā varētu nelabvēlīgi iespaidot datu subjektu tiesības un brīvības". Līdzīgs formulējums ir lietots Kopējās nostājas 16.6. pantā, lai juridiskas personas varētu celt prasības pret surogātpasta sūtījumu izplatītājiem.

44. Turklāt, ņemot vērā iepriekš minēto, varētu arī gaidīt, ka pienākuma aptvertās struktūras, un it īpaši iestādes, kas ir kompetentas īstenot datu aizsardzības tiesību aktus, būtu labāk iepazinušās ar iepriekš minētiem parametriem, un tādējādi palīdzētu tos izvērtēt no viedokļa – vai kāds konkrēts pārkāpums atbilst prasītam parametram.

Struktūra, kas nosaka, vai aizsargpasākumu pārkāpums atbilst parametriem

45. Saskaņā ar EP pieeju (izņemot tiešu briesmu gadījumus) un Komisijas grozīto ierosināto tiesību aktu no dalībvalstu iestādēm būs atkarīgs, kā noteikt, vai aizsargpasākumu pārkāpums atbilst parametriem, kas aktivē pienākumu sūtīt paziņojumus attiecīgiem cilvēkiem.

46. EDAU uzskata, ka iestādes iesaistei ir svarīga nozīme, nosakot, vai parametri ir ievēroti, jo tas savā ziņā garantē pareizu likumu piemērojumu. Tāda sistēma var novērst to, ka uzņēmumi nepareizi izvērtē pārkāpumu un uzskata, ka tas nekaitē/nav smags, un tādējādi izvairās no paziņošanas, lai gan patiesībā par to būtu jāpaziņo.

47. No otras puses, EDAU ir norūpējies par to, ka tāds režīms, kas iestādēm prasītu izvērtējumu, varētu nebūt praktisks, un to būtu grūti piemērot, vai arī izrādītos, ka praksē tas drīzāk kaitē nekā palīdz. Tādējādi tas pat var mazināt cilvēku datu aizsardzības līdzekļu efektivitāti.

48. Patiesi, saskaņā ar tādu pieeju ir paredzams, ka datu aizsardzības iestādes slīks aizsargpasākumu pārkāpumu paziņojumos, un tām var rasties nopietnas grūtības veikt vajadzīgos izvērtējumus. Ir svarīgi atcerēties, ka, lai izvērtētu, vai pārkāpums atbilst parametriem, iestādēm vajadzēs saņemt pietiekami daudz slēptas informācijas, kas bieži ir sarežģīta tehniska informācija, kura būs jāapstrādā ļoti ātri. Ņemot vērā izvērtēšanas grūtības un to, ka dažu iestāžu resursi ir ierobežoti, EDAU ir nobažījies, ka iestādēm ļoti grūti būs veikt šo pienākumu, un tas var atņemt resursus citām svarīgām prioritātēm. Turklāt tāda sistēma var iestādēm uzkraut lieku nastu; patiesi, ja tās nolemj, ka pārkāpums nav smags, un tomēr cilvēkiem ir nodarīts kaitējums, potenciāli no iestādes varētu prasīt atbildību.

49. Iepriekš minētās grūtības kļūst vēl lielākas, ja ņem vērā to, ka laiks ir svarīgs faktors, kā mazināt apdraudējumus, ko rada aizsargpasākumu pārkāpumi. Ja iestādes nespēj izvērtējumu pabeigt ļoti īsā laikā, papildu laiks, kas iestādēm ir vajadzīgs, lai veiktu izvērtējumus, var palielināt attiecīgiem cilvēkiem nodarīto kaitējumu. Tālab tāds papildu pasākums, ar ko ir paredzēts cilvēkiem nodrošināt lielāku aizsardzību, smieklīgā kārtā var samazināt aizsardzību salīdzinājumā ar sistēmām, kas izmanto tiešu paziņošanu.

50. Minēto iemeslu dēļ EDAU uzskata, ka labāk būtu izveidot sistēmu, kā iesaistītām struktūrām izvērtēt, vai pārkāpums atbilst parametriem, kā paredzēts Padomes pieejā.

51. Tomēr, lai izvairītos no iespējamas ļaunprātīgas izmantošanas, piemēram, struktūras neatteiktos no paziņošanas tādos apstākļos, kad noteikti ir jāpaziņo, ir ļoti svarīgi iekļaut dažus še turpmāk aprakstītos datu aizsardzības līdzekļus.

52. Pirmkārt, tas, ka pienākuma aptvertām struktūrām ir jānosaka, vai tām ir jāsūta paziņojums, protams, tām uzliek arī pienākumu prasīt obligāti paziņot iestādēm par visiem pārkāpumiem, kas atbilst prasītajiem parametriem. No ieinteresētām struktūrām tādos gadījumos būtu jāprasa informēt iestādes par notikušo pārkāpumu un iemesliem, kāpēc tās ir pieņēmušas attiecīgu lēmumu par paziņojumu, kā arī paziņojuma saturs.

53. Otrkārt, iestādēm ir jāuztic uzdevums – nopietna pārraudzība. Veicot šo uzdevumu, iestādēm ir jāļauj – bet nevis jāuzliek pienākums – izskatīt pārkāpuma apstākļus un prasīt tādas korektīvas darbības, kas varētu būt vajadzīgas ([14]). Pie tā būtu jāpieder ne tikai paziņojumi cilvēkiem (ja tas nav jau darīts), bet arī spējas uzlikt pienākumu darboties tā, lai novērstu turpmākus pārkāpumus. Iestādēm šajā ziņā būtu jāpiešķir efektīvas pilnvaras un resursi, un iestādēm ir jādod vajadzīgā rīcības brīvība, lai pieņemtu lēmumus, kad reaģēt uz paziņojumiem par aizsargpasākumu pārkāpumiem. Citiem vārdiem sakot, tas ļautu iestādēm būt selektīvām un izmeklēt, piemēram, plašu, patiesi postīgu aizsargpasākumu pārkāpumu, pārbaudīt un nodrošināt likumos ietverto prasību ievērošanu.

54. Lai sasniegtu iepriekš minēto, līdztekus, piemēram, ePrivātuma direktīvas 15.a.3. pantā un datu aizsardzības direktīvā atzītām pilnvarām, EDAU iesaka iespraust šādu formulējumu "Ja abonentiem vai attiecīgiem cilvēkiem vēl nav paziņots, kompetenta attiecīgas valsts iestāde, apsvērusi pārkāpuma būtību, var prasīt, lai to dara *PPECS* vai *ISSP*".

55. Turklāt EDAU iesaka EP un Padomei apliecināt EP ierosinātos pienākumus (122. grozījums, 4.1.a pants) struktūrām savās sistēmās un tajos personas datos, ko tās ir paredzējušas apstrādāt, veikt apdraudējumu ekspertīzi un to identifikāciju. Saskaņā ar šo pienākumu, struktūras izstrādā konkrēti piemērotas un precīzas drošības pasākumu definīcijas, ko īstās reizēs piemērot, un kam būtu jābūt iestāžu rīcībā. Ja notiek aizsargpasākumu pārkāpums, tāds pienākums palīdzēs pienākuma aptvertām struktūrām – un pēc tam arī iestādēm kā pārraudzītājām – noteikt, vai informācijas bojājums var cilvēkiem radīt kaitīgas sekas vai kaitējumu.

56. Treškārt, pienākums, kas ir uzlikts pienākuma aptvertām struktūrām – pieņemt lēmumus par to, vai tām ir jāpaziņo cilvēkiem, ir jāpapildina ar pienākumu uzturēt sīku un pilnīgu iekšēju revīziju uzskaiti, kurā būtu aprakstīti visi notikušie pārkāpumi un visi paziņojumi par tiem, kā arī veiktie pasākumi, lai izvairītos no turpmākiem pārkāpumiem. Iekšēju revīziju uzskaitei ir jābūt iestāžu rīcībā, lai to varētu pārskatīt un, iespējams, izmeklēt. Tas ļaus iestādēm veikt pārraudzību. To varētu nodrošināt, pieņemot apmēram šādu formulējumu – "*PPECS* un *ISSP* patur un uztur pilnīgu un sīku uzskaiti par visiem notikušiem aizsargpasākumu pārkāpumiem, ar tiem saistītu svarīgu tehnisku informāciju un to, kas ir darīts, lai labotu stāvokli. Uzskaita arī atsauces par visiem paziņojumiem, kas ir izdoti abonentiem vai attiecīgiem cilvēkiem un kompetentām attiecīgu valstu iestādēm, arī to datumu un saturu. Pēc lūguma kompetentai attiecīgas valsts iestādei uzrāda uzskaiti."

57. Protams, lai nodrošinātu konsekvenci minēto parametru īstenošanā, kā arī citu svarīgu aizsargpasākumu pārkāpumu paziņošanas sistēmas aspektus, piemēram, paziņojumu formātu un procedūras, pareizi būtu Komisijai, konsultējoties ar EDAU, 29. panta darba grupu un svarīgām ieinteresētām personām, paredzēt tehniskus īstenošanas pasākumus.

([14]) 15a. panta 3. punktā ir atzītas tādas pārraudzības pilnvaras, un noteikts, ka "dalībvalstis kompetentām iestādēm un vajadzības gadījumā citām iestādēm nodrošina visas vajadzīgās izmeklēšanas pilnvaras un resursus, arī iespēju saņemt visu svarīgāko informāciju, kas varētu būt vajadzīga, lai pārraudzītu un īstenotu saskaņā ar šo direktīvu pieņemtos attiecīgu valstu tiesību aktus."

Paziņojumu saņēmēji

58. Runājot par paziņojumu saņēmējiem, EDAU dod priekšroku EP un Komisijas formulējumiem, nevis Padomes formulējumiem. Patiesi, EP vārda "abonenti" vietā izmanto vārdu "lietotāji". Komisija lieto "abonenti" un "attiecīgi cilvēki". Gan EP, gan Komisijas formulējumos kā paziņojumu saņēmēji ir iekļauti ne tikai konkrētā brīža abonenti, bet arī izbijuši abonenti un trešās personas, piemēram, lietotāji, kas sadarbojas ar dažām pienākuma aptvertām struktūrām, neko neabonējot. EDAU sveic tādu pieeju un aicina EP un Padomi to paturēt.

59. Tomēr EDAU norāda uz vairākām terminoloģiskām nekonsekvencēm EP pirmajā lasījumā, un tās būtu jānovērš. Piemēram, vārds "abonenti" gandrīz visur, bet ne gluži visur ir aizstāts ar vārdu "lietotāji", un citos gadījumos – ar vārdu "patērētāji." Tas būtu jāsaskaņo.

III. **ePRIVĀTUMA DIREKTĪVAS PIEMĒROŠANAS JOMA – VALSTU TĪKLI UN PRIVĀTI TĪKLI**

60. Pašreizējās ePrivātuma direktīvas 3.1 pantā ir paredzēts izveidot struktūras, uz ko direktīva attiecas galvenokārt, t. i., struktūras, kas apstrādā datus "saistībā ar" atklātībā pieejamu elektronisku komunikācijas pakalpojumu sniegšanu valstu tīklos (še iepriekš tie ir dēvēti par "PPECS – public electronic communication services") ([15]). *PPECS* darbības, piemēram, ir piekļuves nodrošināšana internetam, informācijas pārraide pa elektroniskiem tīkliem, mobilie sakari un telefonsakari, utt.

61. EP pieņēma 121. grozījumu, lai grozītu Komisijas ierosinātā tiesību akta 3. pantu, ar ko saskaņā ePrivātuma direktīvas piemērošanas joma ir paplašināta, tajā iekļaujot "personas datu apstrādi saistībā ar atklātībā pieejamu Kopienas elektronisko komunikāciju pakalpojumu sniegšanu valstu tīklos un privātos komunikāciju tīklos, kā arī atklātībā pieejamos privātos tīklos, (...)" (ePrivātuma direktīvas 3.1. pants). Diemžēl Padome un Komisija nav uzskatījusi par iespējamu pieņemt šo grozījumu, un tālab nav iestrādājusi šo pieeju Kopējā nostājā un grozītajā ierosinātajā tiesību aktā.

ePrivātuma direktīvas piemērojums atklātībā pieejamos privātos tīklos

62. Še turpmāk izskaidrotu iemeslu dēļ un palīdzot veidot konsensu, EDAU aicina paturēt 121. grozījuma būtību. Turklāt EDAU ierosina iekļaut tādu grozījumu, kas vēl vairāk palīdzētu skaidrot to, uz kādu tipu pakalpojumiem attiektos paplašinātā darbības joma.

([15]) "Šī direktīva attiecas uz personas datu apstrādi saistībā ar atklātībā pieejamu elektronisko komunikāciju pakalpojumu sniegšanu atklātībā pieejamos komunikāciju tīklos".

63. Privātus tīklus bieži lieto, lai nodrošinātu elektroniskus komunikāciju pakalpojumus, piemēram interneta piekļuvi nenoteiktam skaitam cilvēku, kas potenciāli varētu būt liels. Tā notiek, piemēram, interneta kafejnīcu nodrošinātā interneta piekļuvē, kā arī viesnīcās, restorānos, lidostās, vilcienos un citādos atklātībā pieejamos iestādījumos iekārtotos *Wi-Fi* punktos, kur tādus pakalpojumus bieži vien sniedz kā papildinājumu citiem pakalpojumiem (dzērieniem, miteklim, utt.).

64. Visos iepriekš minētos piemēros komunikāciju pakalpojumi, t. i., interneta piekļuve, ir darīti atklātībā pieejami nevis kādas valsts tīklos, bet gan tīklos, ko var uzskatīt par privātiem, t. i., privāti apsaimniekotos tīklos. Turklāt, lai gan iepriekš minētos gadījumos komunikāciju pakalpojumus sniedz sabiedrībai, tā kā lietotais tīkls ir privāts, nevis atklātībā pieejams, uz tādu pakalpojumu sniegšanu *droši vien* neattiecas visa ePrivātuma direktīva vai vismaz daži tās panti ([16]). Tādējādi tādos gadījumos nav aizsargātas cilvēku pamattiesības, kas ir garantētas ePrivātuma direktīvā, un lietotājiem rodas dažāds juridisks stāvoklis, no kuriem vieni interneta piekļuves pakalpojumiem piekļūst pa attiecīgu valstu telekomunikāciju līdzekļiem, bet citi – pa privātiem tīkliem. Tā notiek, lai gan cilvēku privātumam un personas datiem visos šajos gadījumos apdraudējums ir tikpat liels kā tad, kad pakalpojumu sniegšanai izmanto kādas valsts tīklus. Īsi sakot, nešķiet, ka būtu kāds *pamatojums*, kas saskaņā ar komunikāciju pakalpojumu direktīvu attaisnotu to, ka attieksme pret privātos tīklos sniegtiem pakalpojumiem ir citāda salīdzinājumā ar tādiem, ko sniedz valstu tīklos.

65. Tālab EDAU atbalstītu grozījumu, piemēram, EP ierosināto 121. grozījumu, ar ko saskaņā ePrivātuma direktīva attiektos arī uz personas datu apstrādi saistībā ar atklātībā pieejamu elektronisku komunikāciju pakalpojumu sniegšanu *privātos* komunikāciju tīklos.

66. EDAU tomēr apzinās, ka tāds formulējums varētu izraisīt neparedzamas un, iespējams, negribētas sekas. Patiesi, to vien, ka privāti tīkli ir pieminēti, varētu interpretēt tā, lai aptvertu gadījumus, kādos direktīvas piemērojums noteikti nav paredzēts. Piemēram, varētu apgalvot, ka tieša vai stingra šāda formulējuma interpretācija varētu attiecināt direktīvu uz tādu māju īpašniekiem, kurās ir uzstādīts *Wi-Fi* ([17]).– kas ļauj tīklam pievienoties visiem, kuri ir

([16]) *A contrario*, varētu teikt – tāpēc, ka komunikāciju pakalpojumus sniedz sabiedrībai, kaut arī tīkls ir privāts, uz tādu pakalpojumu attiecas esošais tiesiskais regulējums, kaut gan tīkls ir privāts. Patiesībā, piem., Francijā darba devējus, kas darbiniekiem nodrošina piekļuvi internetam, pielīdzina tādiem interneta piekļuves nodrošinātājiem, kas komerciāli nodrošina interneta piekļuvi. Tāda interpretācija nav vispāratzīta par pareizu.

([17]) Parasti – vietēji bezvadu tīkli (*Local Area Network – LAN*).

iekārtas darbības rādiusā (parasti – ir mājās) – kaut arī 121. grozījumā tas nav iecerēts. Lai no tā izvairītos, EDAU ierosina pārfrāzēt 121. grozījumu, ePrivātuma direktīvas piemērošanas jomā iekļaujot "personas datu apstrādi saistībā ar atklātībā pieejamu Kopienas elektronisko komunikāciju pakalpojumu sniegšanu valstu tīklos vai atklātībā pieejamos privātos komunikāciju tīklos, ..."

67. Tas palīdzētu padarīt skaidrāku to, ka ePrivātuma direktīva attieksies tikai uz tādiem privātiem tīkliem, kas ir atklātībā pieejami. Piemērojot ePrivātuma direktīvu *tikai atklātībā pieejamiem privātiem tīkliem* (nevis jebkuram privātam tīklam), ir noteikts robežlielums, lai direktīva aptvertu tikai komunikācijas pakalpojumus, ko sniedz privātos tīklos, kas ir ar nodomu darīti pieejami sabiedrībai. Tāds formulējums vēl vairāk palīdzēs uzsvērt to, ka privātu tīklu *pieejamība sabiedrības locekļiem* ir svarīgākais faktors, lai noteiktu, uz ko direktīva attiecas (līdztekus noteikumam par atklātībā pieejamiem komunikāciju pakalpojumiem). Citiem vārdiem sakot, neatkarīgi no tā, vai tīkls ir valsts vai privāts tīkls, ja tas ir apzināti darīts sabiedrībai pieejams, lai nodrošinātu atklātībā pieejamus komunikāciju pakalpojumus, piemēram, piekļuvi internetam – kaut arī tāds pakalpojums papildina kādu citu (*piem.*, mitekli viesnīcā), uz tāda tipa pakalpojumiem/tīkliem attiektos ePrivātuma direktīva.

68. EDAU norāda, ka še iepriekš atbalstītā pieeja, ar ko saskaņā ePrivātuma direktīvu piemēro *atklātībā pieejamiem privātiem tīkliem*, atbilst pieejai, ko ir pieņēmušas vairākas dalībvalstis, kur iestādes tāda tipa pakalpojumus, kā arī pakalpojumus, ko sniedz gluži privāti tīkli, jau uzskata par ePrivātuma direktīvas piemērošanas jomā īstenojamiem attiecīgas valsts noteikumiem ([18]).

69. Vairojot juridisku skaidrību par struktūru, ko aptver jaunā darbības joma, varbūt vajadzētu ePrivātuma direktīvā iekļaut grozījumu, lai definētu "atklātībā pieejamus privātus tīklus", un tas varētu būt šāds – "atklātībā pieejami privāti tīkli ir privāti apsaimniekoti tīkli, kam sabiedrības locekļi, pieņemot attiecīgus noteikumus, parasti var neierobežoti piekļūt vai nu par maksu, vai arī kopā ar citiem pakalpojumiem vai piedāvājumiem."

([18]) Skat. 16. zemsvītras piezīmi.

70. Praksē iepriekš minētā pieeja nozīmētu to, ka būtu aptverti arī privāti tīkli viesnīcās un citās iestādēs, kur sabiedrības locekļu piekļuvi internetam nodrošina ar privātu tīklu starpniecību. Un otrādi, nebūtu aptverta komunikāciju pakalpojumu sniegšana gluži privātos tīklos, kur pakalpojumi ir ierobežoti mazām, konkrētām cilvēku grupām. Tālab, piemēram, direktīva neattiektos uz virtuāliem privātiem tīkliem un patērētāju mājām, kur ir uzstādītas *Wi-Fi* iekārtas. Tāpat tā neattiektos uz pakalpojumiem, ko sniedz gluži korporatīvi tīkli.

Privāti tīkli ePrivātuma direktīvas piemērošanas jomā

71. Še iepriekš ierosināto privāto tīklu svītrošanu per se vajadzētu uzskatīt par pagaidu pasākumu, par ko vēl vajadzētu debatēt. Patiesi, tā kā direktīva no vienas puses rada sekas privātumam, jo tā neattiecas ne uz vienu gluži privātu tīklu un, no otras puses, tā skar daudzus cilvēkus, kas parasti piekļūst internetam pa korporatīviem tīkliem, nākotnē to vajadzētu apsvērt atkārtoti. Tāpēc, un lai veicinātu debates par šo tematu, EDAU iesaka ePrivātuma direktīvā iekļaut apsvērumu, ar ko saskaņā Komisija atklāti konsultētos par ePrivātuma direktīvas piemērojumu visiem privātiem tīkliem – ņemot vērā EDAU, datu aizsardzības iestāžu un citu svarīgu ieinteresētu personu devumu. Turklāt apsvērumā varētu īpaši norādīt, ka pēc atklātajām konsultācijām Komisijai vajadzētu ierosināt attiecīgu tiesību aktu, lai paplašinātu vai ierobežotu to struktūru tipu skaitu, uz ko vajadzētu attiekties ePrivātuma direktīvai.

72. Līdztekus iepriekš minētajam dažādi ePrivātuma direktīvas panti būtu attiecīgi jāgroza, lai līdztekus valstu tīkliem visos noteikumos par darbībām būtu skaidri piesaukti atklātībā pieejami privāti tīkli.

IV. **DATU PLŪSMU APSTRĀDE DROŠĪBAS VAJADZĪBĀM**

73. Likumdošanas procesā, kas ir saistīts ar ePrivātuma direktīvas pārskatīšanu, uzņēmumi, kuri sniedz drošības pakalpojumus, apgalvoja, ka ePrivātuma direktīvā ir jāiestrādā pants, ar ko likumīgi būtu atļauts vākt datu plūsmu datus, lai tiešsaistē garantētu efektīvu drošību.

74. Tāpēc EP iekļāva 181. grozījumu, radot jaunu – 6.6. panta a) punktu – kurā būtu skaidri atļauts apstrādāt datu plūsmu datus drošības vajadzībām – "neskarot atbilstību citiem noteikumiem, kas nav ietverti Direktīvas 95/46/EK 7. pantā un šīs direktīvas 5. pantā, likumīgās datu apstrādātāju interesēs var apstrādāt datu plūsmu datus, lai īstenotu tehniskus tīklu un informācijas drošības pasākumus saskaņā ar 4. panta c) apakšpunktu Eiropas Parlamenta un Padomes Regulā (EK) Nr. 460/2004 (2004. gada 10. marts), ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru, lai garantētu atklātībā pieejamu elektronisko sakaru pakalpojumu, atklātībā pieejamu vai privātu elektronisku sakaru tīklu, informācijas sabiedrības pakalpojumu vai ar tiem saistītu termināliekārtu vai elektronisku sakaru sistēmu drošību, izņemot gadījumus, ja datu subjektu pamattiesības un brīvības ir svarīgākas par tādām interesēm. Datu apstrādei ir jāaprobežojas ar to, kas obligāti ir vajadzīgs tādām aizsardzības darbībām."

75. Komisijas grozītā ierosinātā tiesību aktā šis grozījums būtībā ir pieņemts, bet no tā ir svītrota svarīga klauzula, ar ko paredzēts nodrošināt to, ka citi direktīvas panti būtu jārespektē – ir svītrota klauzula, kas skan – "neskarot (...) šīs direktīvas ..."). Padome pieņēma pārstrādātu versiju, sperot vēl soli tālāk svarīgu aizsargpasākumu atšķaidīšanā un atsverot 181. grozījumā iestrādātās intereses ar šādu formulējumu "datu plūsmu datus var apstrādāt, ciktāl tas ir obligāti vajadzīgs, lai nodrošinātu (...) tīklu un informācijas drošību, kā noteikts 4.(c) pantā Eiropas Parlamenta un Padomes Regulai (EK) Nr. 460/2004 (2004. gada 10. marts), ar ko izveido Eiropas Tīklu un informācijas drošības aģentūru."

76. Še turpmāk būs sīkāk skaidrots, kāpēc 6.6. panta a) punkts nav vajadzīgs un to var izmantot ļaunprātīgi, it īpaši, ja to pieņem tādā formā, kurā nav iekļauti svarīgi aizsardzības līdzekļi, klauzulas par citu direktīvas pantu respektēšanu un interešu līdzsvarošanu. Tāpēc EDAU iesaka atteikties no šī panta vai vismaz nodrošināt, lai visos pantos, kas attiecas uz šo jautājumu, būtu iekļauti to pašu tipu aizsardzības līdzekļi, kuri ir iekļauti EP ierosinātajā 181. grozījumā.

Juridisks pamatojums datu plūsmu datu apstrādei, ko saskaņā ar pašreizējiem datu aizsardzības jomā pieņemtiem tiesību aktiem piemēro elektroniskiem komunikāciju pakalpojumiem un citiem datu apstrādātājiem

77. Tas, ciktāl atklātībā pieejamu elektronisku komunikāciju pakalpojumu nodrošinātāji var likumīgi apstrādāt datu plūsmu datus, ir normēts ePrivātuma direktīvas 6. pantā, kurā datu plūsmu datu apstrāde ir ierobežota ar dažām vajadzībām, piemēram, rēķiniem, savstarpējiem savienojumiem un jaunu pakalpojumu laišanu tirgū. Apstrāde var notikt vienīgi īpašos apstākļos, piemēram, ar cilvēku piekrišanu – gadījumos, kad tirgū laiž jaunus pakalpojumus. Turklāt citi datu apstrādātāji, piemēram informācijas sabiedrības pakalpojumu nodrošinātāji, var apstrādāt datu plūsmu datus saskaņā ar datu aizsardzības direktīvas 7. pantu, kurā ir noteikts, ka datu apstrādātāji var apstrādāt personas datus, ja to ļauj vismaz viena no vairākām uzskaitītām tiesiskām bāzēm, ko dēvē arī par tiesiskiem pamatojumiem.

78. Tāda tiesiska pamatojuma piemērs ir datu aizsardzības direktīvas 7. panta a) punkts, kurā ir prasīta datu subjekta piekrišana. Piemēram, ja kāds tiešsaistes vairumtirgotājs vēlas apstrādāt datu plūsmu datus, lai sūtītu reklāmas materiālus vai jaunu pakalpojumu tirgū laišanas materiālus, viņam ir jāsaņem attiecīgā cilvēka piekrišana. Cits 7. pantā ietverts tiesisks pamatojums dažos gadījumos var ļaut, piemēram, drošības uzņēmumiem, kas sniedz drošības pakalpojumus, apstrādāt datu plūsmu datus drošības vajadzībām. Tā pamatā ir 7. panta f) punkts, kurā ir noteikts, ka datu apstrādātāji var apstrādāt personas datus, ja tas ir "vajadzīgs datu apstrādātāju vai trešo personu likumīgām interesēm – vai tādu personu likumīgām interesēm, kurām datus atklāj, izņemot gadījumus, ja datu subjektu pamattiesības un brīvības ir svarīgākas par tādām interesēm ..." Datu aizsardzības direktīvā nav konkrēti uzskaitīti gadījumi, kad personas datu apstrāde atbilstu tādai prasībai. Lēmumus toties pieņem datu apstrādātāji, katru gadījumu izskatot konkrēti, bieži vien ar attiecīgas valsts datu aizsardzības iestāžu un citu iestāžu piekrišanu.

79. Būtu jāizskata datu aizsardzības direktīvas 7. panta mijiedarbība ar ierosināto ePrivātuma direktīvas 6.6. panta a) punktu. Ierosinātajā 6.6. panta a) punktā ir norādīti konkrēti norādīti apstākļi, kādos būtu ievērotas iepriekš aprakstītās 7. panta f) punkta prasības. Patiesi, atļaujot apstrādāt datu plūsmu datus, lai palīdzētu nodrošināt tīklu un informācijas drošību, 6.6. panta a) punkts paver iespēju datus apstrādāt likumīgās datu apstrādātāja interesēs.

80. Še turpmāk būs sīkāk izskaidrots, kāpēc EDAU uzskata, ka ierosinātais 6.6 panta a) punkts nav nedz vajadzīgs, nedz izmantojams. Patiesi, no juridiskā viedokļa nav jānoskaidro, vai konkrēta tipa datu apstrāde, šajā gadījumā datu plūsmu datu apstrāde drošības vajadzībām, atbilst datu aizsardzības direktīvas 7. panta f) punkta prasībām, un tādā gadījumā var būt vajadzīga attiecīgā cilvēka piekrišana – *ex* 7. panta a) punkts. Kā norādīts iepriekš, īstenošanas mērogos to parasti izvērtē datu apstrādātāji, t. i., uzņēmumi – saziņā ar datu aizsardzības iestādēm – un vajadzības gadījumā tiesas. Visumā EDAU uzskata, ka konkrētos gadījumos likumīga datu plūsmu datu apstrāde drošības vajadzībām, ko veic, neapdraudot cilvēku pamattiesības un pamatbrīvības, atbildīs datu aizsardzības direktīvas 7. panta f) punkta prasībām, un tāpēc to varēs veikt.

Vēl turklāt datu aizsardzības un ePrivātuma direktīvā nav citu precedentu, kā atlasīt dažu tipu datu apstrādes darbības vai citādi pret tām izturēties – darbības, kas atbilst 7. panta f) punkta prasībām – un nekas nav darīts, lai pierādītu, ka dažas darbības būtu jāveic citādi. Gluži pretēji, kā iepriekš norādīts, šķiet, ka daudzos apstākļos tāda tipa darbības ļoti labi sadzīvotu ar pašreizējo formulējumu. Tāpēc nav vajadzīgs juridisks noteikums, ar ko būtu paredzēts apstiprināt piekrišanu.

EP, Padomes, un Komisijas versija 6.6. panta a) punktam

81. Iepriekš, lai gan tas nebija vajadzīgs, jau ir paskaidrots – ir svarīgi izcelt, ka EP ierosinātais 181. grozījums tomēr bija izstrādāts, mazliet ņemot vērā privātuma un datu aizsardzības principus, kas ir ietverti datu aizsardzības tiesību aktos. EP ierosinātais 181. grozījums varētu vēl vairāk pievērsties datu aizsardzības un privātuma interesēm, piemēram, iespraužot vārdus "īpašos gadījumos", lai nodrošinātu selektīvu šī panta piemērojumu vai paredzot īpašu iesaldēšanas termiņu.

82. Grozījumā Nr. 181 ir daži pozitīvi elementi. Tajā ir apstiprināts, ka apstrādei vajadzētu atbilst visiem citiem datu aizsardzības principiem, ko piemēro personas datu apstrādei ("neskarot .... atbilstību direktīvas 95/46/EK un (..) neskarot atbilstību (..) Direktīvai 95/46/EK (..) un šai direktīvai"). Turklāt, lai gan 181. grozījums ļauj apstrādāt datu plūsmu datus drošības vajadzībām, tajā ir līdzsvarotas to struktūru intereses, kuras apstrādā datu plūsmu datus, un tādu cilvēku intereses, kā datus apstrādā, lai datu apstrāde varētu notikt tikai tad, ja cilvēku pamattiesības un pamatbrīvības nav svarīgākas par datu apstrādes struktūras interesēm ("izņemot gadījumus, ja datu subjektu pamattiesības un brīvības ir svarīgākas par tādām interesēm"). Šāda prasība ir būtiski svarīga, jo īpašos gadījumos tā var atļaut apstrādāt datu plūsmu datus; tomēr tā neļautu struktūrai apstrādāt nevienu datu plūsmu kopumā.

83. Padomes pārstrādātā grozījuma versijā ir slavējami elementi, piemēram, tas, ka ir saglabāts termins "obligāti vajadzīgs", kas uzsver to, ka šī panta piemērošanas joma ir ierobežota. Tomēr Padomes versijā ir pazuduši iepriekš minētie datu aizsardzības un privātuma aizsardzības līdzekļi. Lai gan spēkā joprojām ir vispārēji datu aizsardzības noteikumi, neatkarīgi no tā, vai katrā gadījumā ir dota konkrēta atsauce, Padomes 6.6. panta a) punkta versiju tomēr var interpretēt kā tādu, kas dod visas datu plūsmu datu apstrādes pilnvaras, nepiemērojot nekādus datu aizsardzības un privātuma aizsardzības līdzekļus, kuri vienmēr ir spēkā, apstrādājot datu plūsmu datus. Tālab var teikt, ka datu plūsmu datus var vākt, glabāt, un izmantot arī turpmāk, neievērojot datu aizsardzības principus un īpašus pienākumus, kas citādi attiecas uz atbildīgām personām – piemēram, kvalitātes principu vai pienākumu godīgi un likumīgi apstrādāt datus, un turēt tos slepenībā un drošībā. Turklāt, tā kā pantā nav atsauces uz attiecīgiem datu aizsardzības principiem, kas uzliek informācijas glabāšanas termiņus vai konkrētus termiņus, Padomes versiju var interpretēt kā tādu, kas neierobežoti ilgi ļauj drošības vajadzībām vākt datus un apstrādāt datu plūsmu datus.

84. Turklāt Padome ir vājinājusi privātuma aizsardzību dažās dokumenta daļās, izmantojot pēc iespējas aptuvenu izteiksmi. Piemēram, atsauce uz "likumīgām datu apstrādātāja interesēm" ir svītrota, un tas liek apšaubīt to, kādu tipu struktūras varētu izmantot šo izņēmumu. Ir būtiski svarīgi censties nepavērt durvis tam, lai kāds lietotājs vai juridiska persona sāktu izmantot šo grozījumu.

85. Svaigākā EP un Padomes pieredze rāda, ka ir grūti tiesību aktos definēt, ciktāl un kādos apstākļos datu apstrāde drošības vajadzībām var būt likumīga. Nav domājams, ka jelkāds spēkā esošs pants – vai tāds, kas nākotnē stāsies spēkā – likvidētu acīmredzamos apdraudējumus, ko radītu tas, ka izņēmumu pārlieku plaši piemērotu citu iemeslu dēļ, nevis tāpēc, ka tas būtu tikai saistīts ar drošību, vai to darītu struktūras, uz ko izņēmumam nevajadzētu attiekties. Tas nenozīmē, ka apstrāde nedrīkstētu notikt vispār. Tomēr to, vai apstrāde var notikt, un ciktāl tā varētu notikt, īstenošanas līmenī būtu labāk izvērtēt. Struktūrai, kas vēlas iesaistīties datu apstrādē, vajadzētu ar datu aizsardzības iestādēm un, iespējams, ar 29. panta darba grupu pārrunāt apstrādes mērogus un nosacījumus. Savukārt ePrivātuma direktīvā varētu iekļaut pantu, kurā būtu ļauts apstrādāt datu plūsmu datus drošības vajadzībām, ja to skaidri ir atļāvušas datu aizsardzības iestādes.

86. Ņemot vērā no vienas puses apdraudējumu, ko 6.6. panta a) punkts rada cilvēku pamattiesībām uz datu aizsardzību un privātumu, un, no otras puses – kā šajā atzinumā skaidrots – to, ka no juridiska viedokļa šis pants nav vajadzīgs, EDAU ir secinājis, ka labākais iznākums būtu pilnībā svītrot ierosināto 6.6. panta a) punktu.

87. Ja pretēji EDAU ieteikumam pieņem kādu tekstu, kas aptuveni saskan ar kādu no pašreizējām 6.6. panta a) punkta versijām, tajā būtu jāiestrādā iepriekš aplūkotie datu aizsardzības līdzekļi. Tas būtu arī pareizi jāintegrē pašreizējā 6. panta struktūrā, ieteicams – kā jauns, 2.a punkts.

V. **JURIDISKU PERSONU SPĒJAS CELT PRASĪBAS PAR ePRIVĀTUMA DIREKTĪVAS PĀRKĀPUMIEM**

88. EP ir pieņēmis 133. grozījumu, ar ko interneta piekļuves nodrošinātājiem un citām juridiskām personām, piemēram, patērētāju apvienībām, celt tiesvedību par kura katra ePrivātuma direktīvas panta pārkāpumiem ([19]). Nelaimīgā kārtā ne Komisija, ne Padome to nav pieņēmusi. EDAU uzskata šo grozījumu par ļoti labu un iesaka to saglabāt.

89. Lai saprastu to, cik svarīgs ir šis grozījums, ir jāaptver, ka ar cilvēkam privātuma un datu aizsardzības jomā nodarītu, atsevišķi ņemtu kaitējumu vien parasti nepietiek, lai celtu prasību tiesā. Cilvēki parasti paši neiet tiesā tāpēc vien, ka viņiem ir piesūtīts surogātpasta sūtījums vai tāpēc, ka viņu vārdi būtu kļūdas pēc iekļauti telefongrāmatā. Šis grozījums ļautu patērētāju apvienībām un arodbiedrībām, kas kolektīvi pārstāv patērētāju intereses, viņu vārdā celt prasības tiesās. Ir paredzams, ka lielāka īstenošanas mehānismu dažādība veicinās lielāku atbilsmi ePrivātuma direktīvas prasībām, un tātad lielāku ieinteresētību efektīvā tās piemērošanā.

90. Dažu dalībvalstu juridiskās sistēmās ir precedenti – tajās jau ir paredzēta iespēja prasīt kolektīvu kompensāciju, lai ļautu patērētājiem vai interešu grupām celt kompensācijas prasības pret personām, kas ir izraisījušas kaitējumu.

91. Vēl turklāt daži dalībvalstu konkurences likumi ([20]) pilnvaro patērētājus, interešu grupas (līdztekus *piemeklētiem konkurentiem*) celt tiesvedību pret struktūrām, kas ir izdarījušas pārkāpumus. Domu gaita, ar ko tāda pieeja ir pamatota, paredz, ka uzņēmumi, kas pārkāpj konkurences likumus, visticamāk gūst peļņu, jo patērētāji, kam nodarīts mazs kaitējums, parasti nelabprāt ceļ prasību. Tādu domu gaitu *mutantis mutandi* var piemērot datu aizsardzības un privātuma jomā.

92. Vēl svarīgāk, kā iepriekš norādīts, ir tas, ka juridisku personu, piemēram patērētāju apvienību un *PPECS*, padarīšana par tiesīgām celt prasības tiesās stiprina patērētāju pozīcijas un kopumā veicina datu aizsardzības jomā pieņemtu tiesību aktu ievērošanu. Ja pastāv lielāka iespējamība, ka tiesā sūdzēs uzņēmumus, kas pārkāpj konkurences likumus, ir paredzams, ka tie vairāk investēs datu aizsardzības jomā pieņemtu tiesību aktu ievērošanā, un tas beigu beigās radīs lielāku privātumu un patērētāju aizsardzību. Visu minēto iemeslu dēļ EDAU aicina EP un Padomi pieņemt noteikumu, kas ļautu juridiskām personām celt tiesvedību par visiem ePrivātuma direktīvas pārkāpumiem.

VI. **SECINĀJUMI**

93. Padomes Kopējā nostājā, EP pirmā lasījumā un Komisijas grozītā ierosinātā tiesību aktā ir dažādā pakāpē ietverti pozitīvi elementi, kas palīdzētu stiprināt cilvēku privātuma un personas datu aizsardzību.

94. Tomēr EDAU uzskata, ka uzlabojumi ir iespējami, it īpaši Padomes Kopējā nostājā, kurā diemžēl nav paturēti daži EP ierosināti grozījumi, kas ir iecerēti, lai palīdzētu cilvēkiem nodrošināt pietiekamu privātuma un personas datu aizsardzību. EDAU aicina EP un Padomi atjaunot privātuma aizsardzības līdzekļus, kas ir iestrādāti EP pirmajā lasījumā.

95. Turklāt EDAU uzskata, ka pareizi būtu vienkāršot dažus direktīvas pantus. Tas ir it īpaši patiesi aizsargpasākumu pārkāpumiem veltīto pantu gadījumā, jo EDAU uzskata, ka visus pārkāpumu paziņošanas dotos labumus vislabāk varēs īstenot, ja jau pašā sākumā ir izveidota pareiza sistēma. Visbeidzot, EDAU uzskata, ka pareizi būtu uzlabot un skaidrāk formulēt dažus direktīvas pantus.

96. Ņemot vērā iepriekš minēto, EDAU aicina EP un Padomi pielikt visas pūles, lai uzlabotu un padarītu skaidrākus dažus ePrivātuma direktīvas pantus, reizē atjaunojot EP pirmajā lasījumā ierosinātos grozījumus, ar ko paredzēts nodrošināt attiecīga līmeņa privātumu un datu aizsardzību. Lai to nodrošinātu, 97., 98., 99. un 100. še turpmāk dotajā punktā ir apkopoti uz spēles liktie jautājumi un nākts klajā ar dažiem ieteikumiem un ierosinātiem priekšlikumiem. EDAU aicina visas iesaistītās personas tos ņemt vērā, ePrivātuma direktīvai virzoties pretī pieņemšanai galīgā variantā.

Aizsargpasākumu pārkāpumi

97. Gan Eiropas Parlaments, gan Komisija, gan Padome ir izvēlējusies dažādas pieejas, kā paziņot par aizsargpasākumu pārkāpumiem. Atšķirības trijos modeļos pastāv, *inter alia*, attiecībā uz struktūrām, uz ko attiecas pienākums, paziņojumu sūtīšanas parametriem jeb standartiem, uz datu subjektiem, kas ir tiesīgi saņemt paziņojumus, utt. EP un Padomei ir jādara viss iespējamais, lai izstrādātu stabilu juridisku sistēmu aizsargpasākumu pārkāpumu novēršanai. Lai to panāktu, EP un Padomei vajadzētu –

([19]) EP pirmā lasījuma 13.6. pants.

([20]) Skat., piemēram, UWG 8. pantu – Vācijas negodīgas konkurences likumu.

— *paturēt* aizsargpasākumu pārkāpumu definīciju EP, Padomes un Komisijas dokumentos, jo tā ir pietiekami plaša, lai aptvertu lielāko daļu attiecīgo gadījumu, kad būtu jāpaziņo par aizsargpasākumu pārkāpumiem.

— Informācijas sabiedrības pakalpojumu nodrošinātājus *iekļaut* to struktūru vidū, uz ko attiecas ierosinātā paziņošanas prasība. Var teikt, ka tiešsaistes vairumtirgotāji, tiešsaistes bankas, tiešsaistes aptiekas no aizsargpasākumu pārkāpumiem cietīs tikpat ļoti, ja ne vairāk kā telekomunikāciju uzņēmumi. Pilsoņi cerēs, ka viņiem paziņos ne tikai tad, ja no aizsargpasākumu pārkāpumiem cietīs interneta piekļuves nodrošinātāji, bet it īpaši, ja tas notiks viņu tiešsaistes bankām un tiešsaistes aptiekām.

— Runājot par paziņošanas ierosināšanu, grozītā ierosinātā tiesību akta parametrs "visnotaļ iespējams kaitēt" ir pareizs parametrs, kas nodrošina sistēmas funkcionēšanu. Tomēr ir svarīgi nodrošināt, lai "kaitēt" būtu pietiekami plaši izprasts jēdziens, kas attiektos uz visiem gadījumiem, kad vien būtu kaitēts cilvēku privātumam vai citām likumīgām interesēm. Citādā ziņā labāk būtu izveidot jaunu parametru, ar ko saskaņā paziņošana būtu obligāta "ja ir visnotaļ iespējams, ka pārkāpums cilvēkiem rada kaitējumus". Padomes pieeja, kas prasa, lai pārkāpums *nopietni* skartu kāda privātumu, cilvēkiem nodrošinātu nepietiekamu aizsardzību, jo parametri prasa, lai privātumam nodarītās sekas būtu "nopietnas". Tas arī paver iespējas subjektīviem vērtējumiem.

— Lai gan iestāžu iesaiste, nosakot, vai attiecīgām struktūrām ir jāpaziņo cilvēkiem, noteikti ir pozitīvas sekas, tā varētu būt nerentabla un grūti piemērojama, un tā varētu arī atņemt resursus citām svarīgām prioritātēm. Ja iestādes nevar reaģēt ļoti strauji, EDAU ir nobažījies, ka tāda sistēma var pat mazināt cilvēku aizsardzību un iestādēm uzkraut lieku nastu. Tādējādi, EDAU kopumā iesaka *izveidot* sistēmu, kurā no attiecīgām struktūrām ir atkarīgs izvērtējums, vai paziņojumi būtu jāsūta.

— Lai iestādes varētu pārraudzīt pienākuma aptverto struktūru veiktos izvērtējumus, vai tām būtu jāsūta paziņojumi, *ir jāīsteno* šādi aizsardzības līdzekļi –

  — *Jānodrošina*, ka tādām struktūrām ir jāpaziņo iestādēm par visiem pārkāpumiem, kas atbilst prasītiem parametriem.

  — *Jādod* iestādēm pārraudzības uzdevums, kas ļautu tām būt selektīvām, lai būtu efektīvas. Lai sasniegtu iepriekš minēto, ir jāiekļauj šāds formulējums – "Ja abonentiem vai attiecīgiem cilvēkiem vēl nav paziņots, kompetenta attiecīgas valsts iestāde, apsvērusi pārkāpuma būtību, var prasīt, lai to dara *PPECS* vai *ISSP*".

  — *Jāpieņem* jauns pants, kurā būtu prasīts, lai struktūras uzturētu sīku un pilnīgu iekšēju revīziju uzskaiti. To varētu nodrošināt, pieņemot apmēram šādu formulējumu – "*PPECS* un *ISSP* patur un uztur pilnīgu un sīku uzskaiti par visiem notikušiem aizsargpasākumu pārkāpumiem, ar tiem saistītu svarīgu tehnisku informāciju un to, kas ir darīts, lai labotu stāvokli. Uzskaita arī atsauces par visiem paziņojumiem, kas ir izdoti abonentiem vai attiecīgiem cilvēkiem un kompetentām attiecīgu valstu iestādēm, arī to datumu un saturu. Pēc lūguma kompetentai attiecīgas valsts iestādei uzrāda uzskaiti."

— Lai nodrošinātu konsekvenci aizsargpasākumu pārkāpumu paziņošanas sistēmas īstenošanā, Komisijai, pēc iepriekšējām apspriedēm ar EDAU, 29. panta darba grupu un citām svarīgām ieinteresētām personām ir *jādod* spējas paredzēt tehniskus īstenošanas pasākumus.

— Runājot par to, kādiem cilvēkiem ir jāpaziņo, *izmantot* Komisijas vai EP terminoloģiju "attiecīgi cilvēki" vai "piemeklēti lietotāji", kas aptver visus cilvēkus, kā personas dati ir bojāti.

Atklātībā pieejami privāti tīkli

98. Komunikāciju pakalpojumus bieži vien dara sabiedrībai pieejamus nevis ar atklātībā pieejamiem tīkliem, bet gan ar privāti apsaimniekotu tīklu starpniecību, uz kuriem direktīva droši vien neattiecas (piem., *Wi-Fi* punkti viesnīcās un lidostās). EP ir pieņēmis 121. grozījumu (3. pants), ar ko ir paplašināta direktīvas piemērošanas joma, iekļaujot tajā valstu un privātus komunikāciju tīklus, kā arī atklātībā pieejamus privātus tīklus. Šajā sakarā EP un Padomei vajadzētu –

— *Paturēt* 121. grozījuma būtību, bet izteikt to citādi, lai ePrivātuma direktīvas piemērošanas jomā iekļaujot "personas datu apstrādi saistībā ar atklātībā pieejamu Kopienas elektronisko komunikāciju pakalpojumu sniegšanu valstu tīklos vai atklātībā pieejamos privātos komunikāciju tīklos". Tā skaidri neatteiktos uz gluži privāti apsaimniekotiem tīkliem (salīdzinājumā ar atklātībā pieejamiem privātiem tīkliem).

— Attiecīgi *grozīt* visus darbības noteikumus, lai skaidri piesauktu atklātībā pieejamus privātus tīklus līdztekus attiecīgu valstu tīkliem.

— *Iekļaut* grozījumu, kurā būtu definēts, ka "atklātībā pieejami privāti tīkli ir privāti apsaimniekoti tīkli, kam parasti var neierobežoti piekļūt sabiedrības locekļi neatkarīgi no tā vai tas notiek par maksu, vai saziņā ar citiem pakalpojumiem, vai piedāvājumiem, atkarībā no tā, vai viņi pieņem attiecīgus noteikumus". Tas nodrošinās lielāku juridisku skaidrību par struktūrām, uz ko attiecas jaunā darbības joma.

— *Pieņemt* jaunu apsvērumu, kas ļautu Komisijai atklāti konsultēties par ePrivātuma direktīvas piemērojumu visiem privātiem tīkliem, ņemot vērā EDAU, 29. panta darba grupas un svarīgu ieinteresētu personu ieguldījumu. Īpaši norādīt, ka pēc atklātajām konsultācijām Komisijai vajadzētu ierosināt attiecīgu priekšlikumu, lai paplašinātu vai ierobežotu to struktūru tipu skaitu, uz ko vajadzētu attiekties ePrivātuma direktīvai.

Datu plūsmu apstrāde drošības vajadzībām

99. EP pirmā lasījumā pieņēma 181. grozījumu (6.6. panta a) punkts), kurā ir paredzēts atļaut datu plūsmu datus apstrādāt drošības vajadzībām. Padomes Kopējā nostājā ir pieņemta jauna versija, kurā daži privātuma aizsardzības līdzekļi ir atšķaidīti. Šajā sakarā EDAU iesaka EP un Padomei –

— *Atteikties no* šī panta pilnībā, jo tas nav vajadzīgs – un, ja to lietotu ļaunprātīgi, tas varētu lieki apdraudēt cilvēku datu aizsardzību un privātumu.

— Savukārt, ja ir jāpieņem kāds pašreizējā 6.6. panta a) punkta variants, *iestrādāt* šajā atzinumā pārrunātos datu aizsardzības līdzekļus (līdzīgus EP ierosinātajiem grozījumiem).

Tiesvedība par ePrivātuma direktīvas pārkāpumiem

100. Parlaments ir pieņēmis 133. grozījumu (13.6. pants), kurā juridiskām personām ir dotas spējas celt tiesvedību par visu direktīvas pantu pārkāpumiem. Diemžēl Padome to nav paturējusi. Padomei un EP vajadzētu –

— *Atbalstīt* pantu, kas dod iespēju juridiskām personām, piemēram, patērētāju apvienībām un arodbiedrībām, tiesības celt tiesvedību par visu direktīvas pantu pārkāpumiem (ne tikai par noteikumiem, kas attiecas uz surogātpasta sūtījumiem kā pašreizējā Kopējā nostājā un grozītā ierosinātā tiesību aktā). Lielāka īstenošanas mehānismu dažādība palīdzēs kopumā nodrošināt labāku ePrivātuma direktīvas ievērošanu un efektīvāku piemērojumu.

Problēmas un risinājumi

101. Visos iepriekš minētos jautājumos EP un Padomei ir jārisina problēma, kā izstrādāt pareizus likumus un noteikumus, kas ir gan izmantojami un funkcionāli, un respektētu cilvēku tiesības uz privātumu un datu aizsardzību. EDAU cer, ka iesaistītās personas darīs visu, kas ir viņu spēkos, lai uzveiktu šo pārbaudījumu, un cer, ka šis atzinums palīdzēs.

Briselē, 2009. gada 9. janvārī

Peter HUSTINX

Eiropas Datu aizsardzības uzraudzītājs