I

(Rezolūcijas, ieteikumi un atzinumi)

ATZINUMI

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS

Eiropas Datu aizsardzības uzraudzītāja atzinums par tīkla neitralitāti, datplūsmas pārvaldību un privātās dzīves un personisko datu aizsardzību

(2012/C 34/01)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

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

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

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

ņemot vērā Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti [2], un jo īpaši tās 41. panta 2. punktu,

ņemot vērā Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē [3],

IR PIEŅĒMIS ŠO ATZINUMU.

I. **IEVADS**

I.1. **Vispārīga informācija**

1. Komisija 2011. gada 19. aprīlī pieņēma paziņojumu par atklāto internetu un tīkla neitralitāti Eiropā [4].

2. Šo atzinumu var uzskatīt par EDAU reakciju uz minēto paziņojumu, un tā mērķis ir dot ieguldījumu ES aktuālajā politiskajā diskusijā par tīkla neitralitāti, jo īpaši attiecībā uz aspektiem, kas saistīti ar datu aizsardzību un privāto dzīvi.

---

[1] OV L 281, 23.11.1995., 31. lpp., "Datu aizsardzības direktīva".
[2] OV L 8, 12.1.2001., 1. lpp., "Datu aizsardzības regula".
[3] OV L 201, 31.7.2002., 37. lpp., kurā grozījumi izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK (skat. 15. atsauci), "e-privātuma direktīva".
[4] COM(2011) 222 galīgā redakcija.

3. Atzinums papildina EDAU atbildi ([5]) Komisijas publiskajai apspriešanai par atklāto internetu un tīkla neitralitāti Eiropā, kas tika rīkota pirms Komisijas paziņojuma pieņemšanas. EDAU ir ņēmis vērā arī neseno Padomes secinājumu projektu par tīkla neitralitāti ([6]).

I.2. **Tīkla neitralitātes jēdziens**

4. Tīkla neitralitātes jēdziens ir saistīts ar šobrīd notiekošajām diskusijām par to, vai interneta pakalpojumu sniedzējiem (IPS ([7])) būtu jāatļauj ierobežot, filtrēt vai bloķēt piekļuvi internetam vai citādi ietekmēt tā darbību. Tīkla neitralitātes jēdziens ir pamatots uz uzskatu, ka informācija internetā būtu jāpārsūta objektīvi, neraugoties uz saturu, galamērķi vai izcelsmes vietu, un ka lietotājiem jāvar izlemt, kādas lietotnes, pakalpojumus un aparatūru tie izmantos. Tas nozīmē, ka IPS nedrīkst pēc pašu iniciatīvas uzskatīt par prioritāriem vai palēināt piekļuvi noteiktām lietotnēm vai pakalpojumiem, piemēram, vienādranga („Peer to Peer — P2P") datu apmaiņai utt ([8]).

5. Tīkla datplūsmas filtrēšana, bloķēšana un pārbaudīšana liek uzdot svarīgus ar saziņas konfidencialitāti un fizisku personu privātās dzīves un personas datu neaizskaramības ievērošanu saistītus jautājumus, kas bieži tiek atstāti otrajā plānā vai atlikti. Piemēram, dažos pārbaudes paņēmienos tiek uzraudzīts saziņas, apmeklēto vietņu un nosūtīto un saņemto e-pasta ziņojumu saturs, laiks, kad veikta attiecīgā darbība, utt., kas sniedz iespēju filtrēt saziņu.

6. Pārbaudot saziņas datus, pastāv iespēja, ka IPS pārkāpj saziņas konfidencialitātes principu, kas ir pamattiesības, ko garantē Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas (*ECHR*) 8. pants un Eiropas Savienības Pamattiesību hartas 7. un 8. pants. Konfidencialitāti aizsargā arī sekundārie ES tiesību akti, respektīvi, E-privātuma direktīvas 5. pants.

I.3. **Atzinuma tematika un struktūra**

7. EDAU uzskata, ka nopietnai politiskai diskusijai par tīkla neitralitāti ir jāskar saziņas konfidencialitāti, kā arī cita veida ietekmi uz privāto dzīvi un datu aizsardzību.

8. Šis atzinums sniedz ieguldījumu pašlaik aktuālajā ES mēroga diskusijā. Tam ir trīskāršs mērķis:

— uzsvērt privātās dzīves un datu aizsardzības svarīgumu pašlaik notiekošajās diskusijās par tīkla neitralitāti. Konkrētāk tas uzsver vajadzību ievērot spēkā esošos noteikumus par saziņas konfidencialitāti. Būtu jāatļauj tikai prakse, kas ņem vērā šos noteikumus;

— tīkla neitralitāte ir saistīta ar salīdzinoši jaunām tehnoloģiskām iespējām, tāpēc ir uzkrāta neliela pieredze par tiesiskā regulējuma piemērošanu. Tāpēc šajā atzinumā ir sniegti norādījumi par to, kā IPS ir jāpiemēro un jāievēro datu aizsardzības tiesiskais regulējums, ja tie filtrē, bloķē un pārbauda tīkla datplūsmu. Šai informācijai jābūt noderīgai IPS un arī iestādēm, kas ir atbildīgas par regulējuma ieviešanu;

— attiecībā uz datu aizsardzību un privāto dzīvi šis atzinums identificē jomas, kurām jāpievērš īpaša uzmanība un kurās, iespējams, būs jāveic ES mēroga pasākumi. Tas ir īpaši svarīgi saistībā ar pašlaik ES līmenī notiekošajām diskusijām un politikas pasākumiem, ko šajā sakarā var sākt Komisija.

([5]) EDAU atbildēja, uzsverot, cik svarīgi ir skatīt ar datu aizsardzību un privātās dzīves neaizskaramību saistītos jautājumus kopā ar citām spēkā esošām tiesībām un vērtībām. Atbilde ir pieejama tīmekļa vietnē: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Pieejams tīmekļa vietnē http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Tas ietver piekļuves nodrošināšanu gan fiksētajam, gan mobilajam internetam.

([8]) Šis princips tomēr neattiecas uz IPS, kuri izmantojot joslas platuma vai apjoma ierobežojumus, nosaka tās informācijas apmaiņas ātruma vai daudzuma ierobežojumus, ko abonents var nosūtīt vai saņemt, abonējot pakalpojumus. Tāpēc saskaņā ar tīkla neitralitātes principu IPS tomēr varētu piedāvāt interneta piekļuves abonementus, kuros tiek ierobežota piekļuve, pamatojoties uz tādiem kritērijiem kā ātrums vai apjoms, ja vien netiek diskriminēta vai par prioritāti izvirzīta noteikta veida informācija.

9. EDAU apzinās, ka tīkla neitralitātes temats aktualizē citus jautājumus, kas sīkāk aprakstīti turpmāk un ir saistīti, piemēram, ar piekļuvi informācijai. Šie jautājumi ir apskatīti tikai tiktāl, ciktāl tie ir saistīti ar datu aizsardzību vai privāto dzīvi vai ietekmē šos aspektus.

10. Šī atzinuma struktūra ir aprakstīta turpmāk. II iedaļas sākumā ir sniegts īss pārskats par to, kā IPS izmanto filtrēšanu. III iedaļas sākumā ir aprakstīts tīkla neitralitātes ES tiesiskais regulējums. Turpmāk IV iedaļā ir tehnisks apraksts, kam seko ietekmes uz privāto dzīvi novērtējums atkarībā no izmantotā paņēmiena. V iedaļā ir analizēta pašreizējā ES privātuma tiesiskā regulējuma praktiskie aspekti. Pamatojoties uz šo analīzi, VI iedaļā ir ietverti ieteikumi turpmāku politikas pasākumu izstrādei un apzinātas jomas, kur varētu būt vajadzīga tiesiskā regulējuma skaidrošana un uzlabošana. VII iedaļā ir ietverti secinājumi.

II. **TĪKLA NEITRALITĀTE UN DATPLŪSMAS PĀRVALDĪBAS POLITIKA**

Arvien izplatītāka datplūsmas pārvaldības politiku izmantošana

11. Parasti IPS uzrauga un ietekmē tīkla datplūsmu tikai ierobežotos apstākļos. Piemēram, IPS ir izmantojuši pārbaudes paņēmienus un ierobežojuši informācijas plūsmu, lai saglabātu tīkla drošību, piemēram, apkarojot vīrusus. Tāpēc, vispārīgi izsakoties, internets ir palielinājies, saglabājot augstu neitralitātes pakāpi.

12. Tomēr pēdējos gados daļa IPS ir izrādījuši interesi par tīkla datplūsmas pārbaudīšanu, lai diferencētu to un piemērotu dažādu politiku, piemēram, bloķētu noteiktus pakalpojumus vai piekļuvi citiem pakalpojumiem noteiktu kā prioritāti. Šādu praksi dažreiz dēvē par datplūsmas pārvaldības politiku ([9]).

13. Ir daudz iemeslu, kāpēc IPS pārbauda un diferencē datplūsmu. Datplūsmas pārvaldības politika var, piemēram, palīdzēt IPS pārvaldīt datplūsmu lielas noslodzes periodos, piemēram, nosakot prioritāti datplūsmai, kas ir atkarīga no nodrošināšanas laika, piemēram, video straumēšanai, un samazinot resursus cita veida datplūsmai, kas ir mazāk atkarīga no nodrošināšanas laika, piemēram, vienādranga datu apmaiņai ([10]). Turklāt datplūsmas pārvaldība IPS var būt ienākumu, kas var nākt no dažādiem avotiem, gūšanas līdzeklis. No vienas puses, IPS var pieprasīt maksu satura nodrošināšanas pakalpojumu sniedzējiem, piemēram, tiem, kuru pakalpojumiem vajadzīgs lielāks joslas platums, par to piešķirot prioritāti to sniegtajiem pakalpojumiem (tādējādi uzlabojot to darbības ātrumu). Tas nozīmē, ka piekļuve noteiktam pakalpojumam, kas, piemēram, nodrošina video pēc pieprasījuma, būtu ātrāka nekā piekļuve līdzīgam pakalpojumam, kura sniedzējs neizmanto ātras datu nosūtīšanas režīmu. Ieņēmumus var gūt arī no abonentiem, kas ir ar mieru maksāt lielāku (vai mazāku) maksu par noteikta veida diferencētu abonementu. Piemēram, abonements, kurā nav ietverta piekļuve vienādranga datu apmaiņai, varētu būt lētāks nekā abonements, kas nodrošina neierobežotu piekļuvi.

14. Papildus datplūsmas pārvaldības politikas izmantošanas iemesliem, kas ir svarīgi pašiem IPS, arī citas personas ir ieinteresētas, lai IPS izmantotu datplūsmas pārvaldības politiku. Ja IPS pārvaldīs savus tīklus un pārbaudīs saturu, kāds tiek pārraidīts ar to infrastruktūras starpniecību, tie palielinās savas spējas konstatēt iespējamus pretlikumīgas lietošanas gadījumus, piemēram, kas saistīti ar autortiesību pārkāpumiem vai pornogrāfiskiem materiāliem.

([9]) Skatīt, piemēram, *OFCOM* 2011. gada 27. maija ziņojumu "Site blocking to reduce online copyright infringement" (Vietņu bloķēšana, lai samazinātu autortiesību pārkāpumu daudzumu tiešsaistē), kas pieejams šajā tīmekļa vietnē: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf "Daži IPS savā tīklā datplūsmas pārvaldības un citos nolūkos jau izvieto pakešu pārbaudes sistēmas, tāpēc mēs pieņemam, ka to var izvietot, tomēr tiem, kas šādus pakalpojumus vēl neizmanto, tas būtu ļoti sarežģīti un dārgi. Ņemot vērā kapitālieguldījumus, kas šādā gadījumā jāveic, iespējams, īstermiņā un vidējā termiņā pakešu padziļinātu pārbaudes funkcionalitāti varētu izvietot tikai lielākie IPS".

([10]) Reāllaika lietojumprogrammu, piemēram, video straumēšanas lietojumprogrammu, darbības kvalitāte cita starpā ir atkarīga no latentuma, t. i., aizkaves, piemēram, tīkla pārblīves dēļ.

Citas ietekmētās intereses, tostarp datu aizsardzība un privātums

15. Šī tendence ir rosinājusi diskusiju par šādu darbību likumību, konkrētāk – vai tiesību aktos būtu turpmāk jānostiprina specifiski tīkla neitralitātes pienākumi.

16. Ja IPS vairāk sāks izmantot datplūsmas pārvaldības politiku, var tikt ierobežota piekļuve informācijai. Ja šāda prakse kļūtu vispārizplatīta, un lietotāji nevarētu pilnībā piekļūt internetam tā pašreizējā izpratnē (vai varētu piekļūt par ļoti lielu maksu), tiktu apdraudēta informācijas pieejamība lietotāja spēja nosūtīt un saņemt vēlamos datus, izmantojot pašu izvēlētas lietotnes vai pakalpojumus. Šo problēmu var novērst, ieviešot juridiski obligātu tīkla neitralitātes principu.

17. Tā EDAU saskaras ar IPS datplūsmas pārvaldības ietekmi uz datu aizsardzību un privāto dzīvi. Tā konkrētāk izpaužas šādi:

— ja IPS apstrādā datus par datplūsmu ar vienīgo nolūku maršrutēt informācijas plūsmu no nosūtītāja saņēmējam, tie parasti veic datu apstrādi ierobežotā apmērā ([11]). Tāpat kā pasts apstrādā informāciju, kas norādīta uz vēstules aploksnes, IPS apstrādā informāciju, kas vajadzīga, lai maršrutētu saziņu līdz saņēmējam. Tas nav pretrunā ar juridiskajām prasībām nodrošināt datu aizsardzību, privātumu un saziņas konfidencialitāti;

— tomēr, ja IPS pārbauda saziņas datus, lai diferencētu saziņas plūsmas un piemērotu konkrētu politiku, kas var būt nelabvēlīga noteiktām personām, sekas ir būtiskākas. Atkarībā no apstākļiem katrā gadījumā un no veiktās analīzes tipa, datu apstrādei var būt ļoti liels iejaukšanās potenciāls attiecībā uz personas privāto dzīvi un personas datiem. Tas ir uzskatamāk jūtams gadījumos, kad pārvaldības politika atklāj personu interneta saziņas saturu, tostarp nosūtītos un saņemtos e-pasta ziņojumus, apmeklētās tīmekļa vietnes, lejupielādētās vai augšupielādētās datnes utt.

III. APSKATS PAR ES TIESISKO REGULĒJUMU TĪKLA NEITRALITĀTES JOMĀ UN TURPMĀKO POLITIKAS ATTĪSTĪBU

III.1. Īsi par tiesisko regulējumu

18. Līdz 2009. gadam ES tiesību aktos nebija noteikumu, kas skaidri aizliegtu IPS filtrēt vai bloķēt, vai pieprasīt papildu samaksu abonentiem par piekļuvi pakalpojumiem. Vienlaikus tajos nebija noteikumu, kas skaidri atzītu šo praksi. Tāpēc situācija zināmā mērā bija neskaidra.

19. Situāciju mainīja 2009. gada telekomunikāciju tiesību aktu pakete, kurā tika iekļauti noteikumi, kas atbalstīja interneta pieejamību. Piemēram, Direktīvas par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem ("pamatdirektīva") ([12]) 8. panta 4. punktā noteikts pārvaldes iestādēm pienākums veicināt lietotāju iespējas piekļūt to izvēlētai informācijai, lietotnēm vai pakalpojumiem. Šis noteikums attiecas uz tīklu kopumā, nevis atsevišķiem nodrošinātājiem. Arī nesenajos Padomes secinājumos tika uzsvērta vajadzība saglabāt interneta pieejamību ([13]).

([11]) Te netiek iekļautas darbības, kuru mērķis ir palielināt tīkla drošību un noteikt kaitīgu datplūsmu, kā arī darbības, kas vajadzīgas rēķinu izrakstīšanai un starpsavienojumu izveidei. Netiek iekļauti arī pienākumi, kas izriet no Datu saglabāšanas direktīvas – Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīva 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK (OV L 105, 13.4.2006., 54. lpp.) (Datu saglabāšanas direktīva).

([12]) 2002. gada 7. marta Direktīva 2002/21/EK par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem, kurā grozījumi izdarīti ar Direktīvu 2009/140/EK un Regulu (EK) Nr. 544/2009 (OV L 337, 18.12.2009., 37. lpp.).

([13]) Skatīt 3. punkta e) apakšpunktu, kur Padome atzīst: "Vajadzība saglabāt interneta atklātumu, vienlaikus nodrošinot, lai tas varētu sniegt kvalitatīvus pakalpojumus saskaņā ar struktūru, kas atbalstītu un ievērotu tādas pamattiesības kā vārda brīvība un uzņēmējdarbības brīvība" un 8. punkta d) apakšpunktu, kas aicina dalībvalstis "atbalstīt interneta atklāto un neitrālo būtību kā politisku mērķi."

20. Universālo pakalpojumu direktīvā ([14]) ir ietverti konkrētāki pienākumi. Tās 20. un 21. pantā ir izklāstītas pārredzamības prasības, kas attiecas uz piekļuves pakalpojumiem un lietotnēm un to lietošanas iespēju ierobežošanu. Tajā ir norādīti arī minimālie pakalpojumu kvalitātes līmeņi.

21. Attiecībā uz IPS darbībām, kas ietver personu saziņas pārbaudi, Direktīvas, ar ko groza Universālo pakalpojumu direktīvu un e-privātuma direktīvu ([15]), 28. apsvērumā ir uzsvērts, ka "atkarībā no izmantotās tehnoloģijas un ierobežojuma veida šādu ierobežojumu piemērošanai var būt vajadzīga patērētāju piekrišana saskaņā ar Direktīvu par privāto dzīvi". Tādējādi 28. apsvērumā tiek atgādināta vajadzība iegūt piekrišanu saskaņā ar E-privātuma direktīvas 5. panta 1. punktu gadījumā, ja tiek piemēroti jebkādi ierobežojumi, kas pamatoti uz saziņas uzraudzību. Turpmāk IV iedaļā ir sīkāk analizēta 5. panta 1. punkta un vispārējā datu aizsardzības un privātuma tiesiskā regulējuma piemērošana.

22. Visbeidzot Universālo pakalpojumu direktīvas 22. panta 3. punkts tagad piešķir valsts regulatīvajām iestādēm pilnvaras vajadzības gadījumā noteikt IPS minimālās pakalpojumu kvalitātes prasības, lai novērstu pakalpojumu kvalitātes pazemināšanos un datu plūsmas kavējumus vai palēninājumus publiskos tīklos.

23. Iepriekšminētais nozīmē, ka ES līmenī ir plaša mēroga centieni panākt atklātu internetu (skatīt Pamatdirektīvas 8. panta 4. punktu). Tomēr šis politiskais mērķis, kas attiecas uz tīklu kopumā, nav tieši saistīts ar atsevišķiem IPS noteiktiem aizliegumiem vai pienākumiem. Citiem vārdiem, IPS var īstenot datplūsmas pārvaldības politiku, kas var izslēgt piekļuvi noteiktām lietotnēm ar nosacījumu, ka lietotāji tiek pilnīgā informēti un ir brīvi, specifiski un viennozīmīgi pauduši savu piekrišanu.

24. Atkarībā no dalībvalsts situācija var būt dažāda. Dažās dalībvalstīs IPS ar zināmiem nosacījumiem var īstenot datplūsmas pārvaldības politiku, lai bloķētu, piemēram, balss pārraides ar interneta protokolu (*VoIP*) lietotnes (lētāka interneta pakalpojumu abonementa gadījumā), ar nosacījumu, ka lietotāji ir devuši brīvu, specifisku un viennozīmīgu, apzinātu piekrišanu. Citas dalībvalstis ir izvēlējušās nostiprināt tīkla neitralitātes principu. Piemēram, Nīderlandes parlaments 2011. gada jūlijā pieņēma likumu, kas vispārēji aizliedz pakalpojumu sniedzējiem kavēt vai palēnināt lietotņu vai pakalpojumu (piemēram, *VoIP*) darbību internetā, ja tas nav vajadzīgs, lai mazinātu pārblīves sekas, integritātes vai drošības apsvērumu dēļ, lai apkarotu surogātpastu vai saskaņā ar tiesas rīkojumu ([16]).

III.2. **Paziņojums par tīkla neitralitāti**

25. Eiropas Komisija paziņojumā par tīkla neitralitāti ([17]) secināja, ka situācija tīkla neitralitātes jomā ir jāuzrauga un tai vajadzīga turpmāka analīze. Tās politika ir raksturota kā "nogaidoša", pirms apsvērt turpmākus regulatīvus pasākumus.

([14]) Direktīva 2002/22/EK, kurā grozījumi izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK 2002/22/EK, 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 starp valstu iestādēm, kas atbildīgas par tiesību aktu īstenošanu patērētāju tiesību aizsardzības jomā (OV L 337, 18.12.2009., 11. lpp.). Salīdzināt arī ar 1. panta 3. punktu, kurā noteikts, ka Direktīva nedz atļauj, nedz aizliedz IPS ierobežot piekļuvi pakalpojumiem vai lietotnēm un/vai to lietošanu, ja to atļauj valsts tiesību akti un šāda rīcība atbilst Kopienas tiesību aktiem, bet Direktīvā tiem ir prasīts sniegt informāciju par šādiem nosacījumiem.

([15]) Direktīvu 2009/136/EK, 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 starp valstu iestādēm, kas atbildīgas par tiesību aktu īstenošanu patērētāju tiesību aizsardzības jomā.

([16]) Sākotnējie Nīderlandes grozījumi ir pieejami šajā tīmekļa vietnē: https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Presē šāda politikas izvēle netika saistīta ar datu aizsardzības un privātās dzīves neaizskaramības apsvērumiem, bet gan ar vajadzību nodrošināt, lai lietotājiem netiktu atņemtas vai piedāvātas ierobežotas iespējas piekļūt informācijai. Tāpēc šķiet, ka šie grozījumi ir pieņemti ar piekļuvi informācijai saistītu apsvērumu dēļ.

([17]) Skat. 4. atsauci.

26. Komisijas paziņojumā tika atzīts, ka jebkuram pasākumam un turpmākiem regulatīviem pasākumiem tiks veikts datu aizsardzības un privātuma aspektu padziļināts novērtējums. Arī Padomes secinājumu projektā ir minēti ietekmētie datu aizsardzības un privātuma jautājumi ([18]).

27. No datu aizsardzības un privātuma viedokļa ir jāizvērtē jautājums, vai pietiek īstenot nogaidošu politiku. Kaut gan datu aizsardzības un privātuma tiesiskajā regulējumā pašlaik ir paredzēti daži aizsardzības pasākumi, jo īpaši saskaņā ar saziņas konfidencialitātes principu, šķiet, ka ir rūpīgi jāuzrauga, cik lielā mērā tas tiek ievērots, un jāizdod vadlīnijas par vairākiem neskaidriem aspektiem. Turklāt ir jāpiedāvā idejas par to, kā skaidrot un turpmāk uzlabot regulējumu, ņemot vērā tehnoloģijas attīstību. Ja uzraudzībā atklāsies, ka tirgū pastāv virzība uz lielapjoma saziņas pārbaudēm reāllaikā un ar regulējuma ievērošanu saistītas problēmas, būs jāpieņem tiesību akti. Konkrēti ieteikumi šajā ziņā tiks izteikti VI iedaļā.

IV. **TEHNISKS RAKSTUROJUMS UN ATTIECĪGĀ IETEKME UZ PRIVĀTUMU UN DATU AIZSARDZĪBU**

28. Pirms temata detalizētāka izklāsta ir svarīgi labāk izprast pārbaudes paņēmienus, ko IPS var lietot, lai īstenotu datplūsmas pārvaldību un tās ietekmi uz tīkla neitralitātes principu. Šo paņēmienu ietekme uz privātumu un datu aizsardzību var ievērojami atšķirties atkarībā no tā, kāds(-i) paņēmiens(-i) tiek izmantots(-i). Šis tehniskais raksturojums ir vajadzīgs, lai izprastu un pareizi piemērotu V iedaļā aprakstīto datu aizsardzības tiesisko regulējumu. Tomēr jānorāda, ka šī joma ir pastāvīgi mainīga un sarežģīta. Tāpēc turpmāk sniegtais apraksts nav uzskatāms par izsmeļošu un pilnībā aktuālu, bet ir paredzēts tikai, lai sniegtu tehnisko informāciju, kas ir neaizstājama, lai izprastu juridisko argumentāciju.

IV.1. **Informācijas pārsūtīšana internetā: pamati**

29. Kad lietotājs internetā sazinās, pārsūtītā informācija tiek sadalīta paketēs. Šīs paketes tiek internetā pārsūtītas no nosūtītāja saņēmējam. Katrā paketē cita starpā tiek iekļauta informācija par izcelsmi un adresātu. Turklāt IPS var iekļaut šīs paketes papildu slāņos un protokolos ([19]), kas tiek izmantoti, lai pārvaldītu dažādo datplūsmu apriti IPS tīklā.

30. Atkārtoti atsaucoties uz salīdzinājumu ar vēstuli, kas tiek nosūtīta pa pastu, tīkla pārraides protokola lietošana ir līdzvērtīga pa pastu sūtītas vēstules satura ievietošanai aploksnē, uz kuras ir saņēmēja adrese, ko izlasa un nosūta pasta nodaļa. Pasta nodaļa savā iekšējā apritē var izmantot papildu protokolus, lai pārvaldītu visas nosūtāmās aploksnes; šīs darbības mērķis ir, lai katra aploksne sasniegtu adresātu, ko sākotnēji norādījis sūtītājs. Atbilstoši šim salīdzinājumam katrai paketei ir divas daļas, no kurām viena ir *IP vērtums*, kurā ir saziņas saturs un kas atbilst salīdzinājumā minētajai vēstulei. Tajā ir informācija, kas adresēta tikai saņēmējam. Paketes otrā daļa ir *IP galvene*, kas cita starpā ietver saņēmēja un sūtītāja adresi un kas atbilst salīdzinājumā minētajai aploksnei. IP galvene nodrošina IPS un citiem starpniekiem maršrutēt vērtumu no tā izcelsmes adreses to uz tās galamērķa adresi.

31. IPS un citi starpnieki nodrošina IP pakešu kustību tīklā pa mezgliem, kas nolasa IP galvenes informāciju, salīdzina to ar maršrutēšanas tabulās ietverto informāciju un pēc tam pārvirza tās uz nākamo mezglu ceļā uz galamērķi. Šis process tiek realizēts visā tīklā, izmantojot labākās piepūles bezatmiņas pieeju, jo

([18]) Skatīt 4. punkta e) apakšpunktu, kur Padome norāda: "Pastāv zināmas bažas saistībā ar personas datu aizsardzību, ko pauž galvenokārt patērētāji un datu aizsardzības jomā strādājošās iestādes."

([19]) Kā aprakstīts turpmāk IV.2. iedaļā, šādi protokoli kodē pārraidāmo informāciju saskaņotā veidā, piemēram, *HTTP*, *FTP* vai citā formātā, lai saziņā iesaistītās personas varētu saprasties.

visas paketes, kas nonāk līdz mezglam, tiek apdarinātas neitrāli. Kad tās ir pārvirzītas uz nākamo mezglu, maršrutētājā nav jāpatur papildu informācija ([20]).

IV.2. **Pārbaudes paņēmieni**

32. Kā norādīts iepriekš, IPS ir vajadzīgi IP lasītāji, lai maršrutētu informāciju uz galamērķi. Tomēr, kā minēts iepriekš, datplūsmas (tostarp IP galvenes un IP vērtuma) analīzi var veikt citos nolūkos un izmantojot dažādu tehnoloģiju. Jaunās tendences ir, piemēram, dažu lietotāju izmantotu lietotņu, piemēram, P2P lietotņu, savienojuma palēninašana, vai noteiktu pakalpojumu, piemēram, video pakalpojumu pēc pieprasījuma, datplūsmas palielināšana augstākas kategorijas pakalpojumu abonentiem. Kaut gan teorētiski pakešu pārbaudi var veikt, izmantojot visus pārbaudes paņēmienus, tiem ir dažādas iejaukšanās pakāpes. Ir divas pārbaudes paņēmienu kategorijas. Saskaņā ar vienu tiek pārbaudīta tikai IP galvene, bet saskaņā ar otru – arī IP vērtums.

Pārbaude, ko veic, pamatojoties uz IP galvenes informāciju. IP paketes galvenes pārbaudē tiek atklāti daži lauki, kas var sniegt iespēju IPS lietot vairākas specifiskas datplūsmas pārvaldes politikas. Izmantojot paņēmienus, kuros tiek pārbaudītas IP galvenes, dati, kuri principā ir paredzēti informācijas maršrutēšanai, tiek apstrādāti citā nolūkā (t. i., lai diferencētu datplūsmu). Avota IP adresi IPS var attiecināt uz konkrētu abonentu un īstenot specifisku politiku, piemēram, maršrutēt paketi pa ātrāku vai lēnāku savienojumu. Arī galamērķa IP adresei IPS var īstenot specifisku politiku, piemēram, bloķēt vai filtrēt piekļuvi noteiktām tīmekļa vietnēm.

Datu padziļināta pārbaude. Pakešu padziļināta pārbaude sniedz iespēju IPS piekļūt informācijai, kas paredzēta tikai saziņas adresātam. Atgriežoties pie salīdzinājuma ar saziņu pa pastu, šo pieeju var salīdzināt ar aploksnes atvēršanu un tajā esošās vēstules izlasīšanu, lai analizētu (IP paketēs ietvertās) saziņas saturu, lai īstenotu specifisku tīkla politiku. Ir dažādi pārbaudes veikšanas veidi, no kuriem katrs rada citādu apdraudējumu datu subjektam.

— *Pakešu padziļināta pārbaude, pamatojoties uz protokolu analīzi un reģistrēto statistiku.* Papildus IP protokolam, kas ir paredzēts, lai nodrošinātu datu pārraidi internetā, ir vēl citi protokoli, kas saskaņotā veidā kodē (transportēšana, sesija, pasniegšana un lietošana utt.) pārraidāmo informāciju. Šo protokolu mērķis ir nodrošināt, lai saziņā iesaistītās personas saprastos. Piemēram, daļa protokolu ir saistīti ar tīmekļa pārlūkošanu ([21]), citi ir paredzēti datņu pārsūtīšanai ([22]) utt. Tāpēc to pārbaudes paņēmienu mērķis, kas pamatoti uz protokolu pārbaudi un apvienoti ar statistikas analīzi, ir meklēt specifiskas sakarības vai raksturīgās pazīmes, kas nosaka, kādi protokoli tiek izmantoti ([23]). Šie pārbaudes paņēmieni ļauj IPS noskaidrot saziņas veidu (e-pasta saziņa, tīmekļa pārlūkošana, datņu augšupielādēšana) un dažos gadījumos identificēt, kāds pakalpojums vai lietotne tiek izmantota, kā ir, piemēram, dažu *VoIP* saziņas veidu gadījumā, kuros izmantotie protokoli ir raksturīgi tieši konkrētam izplatītājam vai pakalpojumu sniedzējam. Ja ir zināms saziņas veids, IPS var piemērot konkrētu datplūsmas pārvaldības politiku, piemēram, bloķēt tīmekļa datplūsmu. Tas var būt arī pirmais posms darbību secībā, kura rezultātā IPS sāk veikt analīzes, kam var būt vajadzīga pilnīga piekļuve saziņas metadatiem un saturam.

([20]) Tomēr interneta tīkla iekārtas izmanto maršrutēšanas protokolus, kas reģistrē darbību, apstrādā datplūsmas statistiku un apmainās ar informāciju ar citām tīkla iekārtām, lai maršrutētu IP paketes pa visefektīvāko ceļu. Piemēram, ja savienojums ir pārblīvēts vai sarauts un ja maršrutētājs saņem šo informāciju, tas atjauninās maršrutēšanas tabulu, kurā šī savienojuma vietā tiks izmantots cits. Jāpiemin arī datu vākšana un apstrāde, kas dažos gadījumos var tikt veikta norēķinu vajadzībām vai pat saskaņā ar Datu saglabāšanas direktīvas prasībām.

([21]) *HTTP* – hiperteksta pārsūtīšanas protokols, HTML – hiperteksta iezīmēšanas valoda.

([22]) *FTP* – datņu pārsūtīšanas protokols.

([23]) Ir dažādi veidi, kā noteikt izmantotos protokolus. Piemēram, var iekšējos protokolos meklēt noteiktus laukus, lai noteiktu portus, kas tiek lietoti, lai izveidotu saziņu. Saziņas plūsmas statistisku raksturojumu var izsecināt arī, analizējot specifiskus laukus un vienlaikus divās IP adresēs izmantoto protokolu korelāciju.

— *Pakešu padziļinātā pārbaude, kas pamatota uz saziņas satura analīzi*. Visbeidzot var arī pārbaudīt pašas saziņas metadatus ([24]) un saturu. Izmantojot šo paņēmienu, tiek pārtvertas visas sākotnējās saziņas plūsmas IP paketes, lai pilnībā varētu rekonstruēt un analizēt saziņas sākotnējo saturu. Piemēram, lai konstatētu tādu kaitīgu vai pretlikumīgu saturu kā vīrusi, bērnu pornogrāfija utt., ir jārekonstruē saziņas saturs, lai to varētu analizēt. Jānorāda, ka dažreiz saziņā iesaistītās personas visā datu pārraides ceļā var būt saziņu atklāti šifrējušas, un šāda rīcība traucē IPS analizēt saziņas saturu.

IV.3. **Ietekme uz privāto dzīvi un datu aizsardzību**

33. Izmantojot pārbaudes paņēmienus, kas pamatoti uz IP galveņu pārbaudi, konkrētāk – kas pamatoti uz pakešu pārbaudi, šie dati tiek uzraudzīti un filtrēti, kas var nopietni ietekmēt privāto dzīvi un datu aizsardzību. Šīs darbības, iespējams, ir pretrunā arī ar saziņas konfidencialitātes tiesībām.

34. Personu saziņas apskatei pašai par sevi jau ir ievērojama ietekme uz privāto dzīvi un datu aizsardzību. Taču šajā gadījumā problēmas mērogs ir lielāks, jo atkarībā no uzraudzības un pārtveršanas paredzētā mērķa šo darbību ietekme uz privāto dzīvi var būt vēl lielāka. Jāatzīst, ka saziņas pārbaudīšana, lai nodrošinātu sistēmas sekmīgu darbību nav salīdzināma ar saziņas pārbaudīšanu, kuras mērķis ir piemērot politiku, kas var ietekmēt privātpersonas. Ja datplūsmas un atlases politikas mērķis ir tikai izvairīšanās no tīkla pārblīves, šīs darbības būtiski neietekmēs personas privāto dzīvi. Tomēr datplūsmas pārvaldības politiku mērķis var būt saziņas saturā ietvertās informācijas daļas bloķēšana vai saziņas ietekmēšana, piemēram, izmantojot paradumorientēto reklamēšanu. Šajos gadījumos veiktajām darbībām ir lielāks iejaukšanās potenciāls. Šī problēma kļūst vēl akūtāka, ja apzināmies, ka šāda informācija tiktu apkopota nevis par nelielu personu grupu, bet vispārēji, par visiem IPS klientiem ([25]). Ja visi IPS sāktu izmantot filtrēšanas paņēmienus, varētu aizsākties interneta lietojuma vispārējas uzraudzības tendence. Turklāt, ja ņem vērā apstrādātās informācijas veidu, privātumam radītais risks nepārprotami ir liels, jo liela daļa vāktās informācijas var būt ļoti sensitīva un pēc savākšanas būtu pieejama visiem IPS un personām, kuras no tiem mēģinātu iegūt informāciju. Turklāt šai informācijai var būt arī ļoti liela komerciāla vērtība. Šīm darbībām ir liels funkciju nobīdes risks, kā rezultātā savāktā informācija vairs netiktu lietota sākotnējos nolūkos, bet izmantota komerciālām vajadzībām vai citā neparedzētā nolūkā.

35. Lai pareizi lietotu uzraudzības, pārbaudes un filtrēšanas paņēmienus, tiem jāatbilst piemērojamajiem datu aizsardzības un privātās dzīves neaizskaramības aizsardzības pasākumiem, kas nosaka veicamo darbību ierobežojumus un apstākļus. Turpmāk ir sniegts pārskats par piemērojamajiem aizsardzības pasākumiem saskaņā ar spēkā esošo ES tiesisko regulējumu datu aizsardzības un privātuma jomā.

V. **ES PRIVĀTĀS DZĪVES NEAIZSKARAMĪBAS UN DATU AIZSARDZĪBAS TIESISKĀ REGULĒJUMA PIEMĒROŠANA**

36. ES datu aizsardzības tiesiskais regulējums ir tehnoloģiski neitrāls, tāpēc tas nereglamentē tādus specifiskus pārbaudes paņēmienus kā iepriekš aprakstītie. E-privātuma direktīva reglamentē privātumu

([24]) Katra protokola galvenē ir specifiski lauki, kas papildus sniedz neformālu informāciju par pārraidīto saziņu. Tāpēc šo lauku saturu var dēvēt par saziņas metadatiem. Šie lauki var būt, piemēram, izmantotā porta numurs – ja tas ir 80, ir ļoti iespējams, ka saziņas veids ir tīmekļa pārlūkošana.

([25]) Protams, izsekošanai vajadzīgie resursi ir ne tikai IPS rīcībā. Arī reklāmas tīklu nodrošinātāji, izmantojot trešo personu sīkdatnes, spēj izsekot lietotāju darbībām tīmekļa vietnēs. Skatīt, piemēram, nesen publicētu zinātnisku rakstu, kurā minēts, ka uzņēmuma *Google* reklāmas tīkls darbojas 97 no 100 visbiežāk apmeklētajām vietnēm, kas nozīmē, ka *Google* var izsekot to lietotāju darbībām, kuri nav atteikušies no trešo personu sīkdatņu izmantošanas, pārlūkojot šīs populārās vietnes. Skatīt: *Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning* (*Flash* sīkdatnes un privātums, II daļa: tagad arī HTML5 formātā un ar entītiju tagu atkārtotu ģenerēšanu) (2011. gada 29. jūlijs). Pieejams *SSRN* tīmekļa vietnē: http://ssrn.com/abstract=1898390 Jautājumu par lietotāju izsekošanu, izmantojot trešo personu sīkdatnes, ir izskatījusi 29. panta darba grupa. Skatīt Atzinumu 2/2010 par paradumorientēto reklamēšanu tiešsaistē, kas pieņemts 2010. gada 22. jūnijā (WP 171).

elektroniskās saziņas pakalpojumu jomā publiskos tīklos (parasti piekļuve internetam un telefonija) ([26]), bet Datu aizsardzības direktīva reglamentē datu apstrādi vispārīgi. Kopumā šis tiesiskais regulējums nosaka dažādus pienākumus, kas attiecas uz IPS, kuri apstrādā un uzrauga datplūsmas un saziņas datus.

V.1. **Datplūsmas un satura datu apstrādes juridiskais pamatojums**

37. Saskaņā ar datu aizsardzības tiesību aktiem personas datu apstrādei kā šajā datplūsmas un saziņas datu apstrādes gadījumā ir vajadzīgs pietiekams juridisks pamatojums. Papildus šai vispārīgajai prasībai noteiktos gadījumos var būt spēkā specifiskas prasības.

38. Šajā gadījumā personiskie dati, ko apstrādā IPS, ir datplūsmas dati un saziņas saturs. Gan saziņas saturu, gan datplūsmas datus aizsargā sarakstes konfidencialitātes princips, ko garantē ECHR 8. pants un Hartas 7. un 8. pants. Konkrētāk, e-privātuma direktīvas 5. panta 1. punktā "komunikāciju konfidencialitāte" ir ietverta prasība dalībvalstīm nodrošināt komunikāciju un saistītās informācijas par datu plūsmu konfidencialitāti ar publisko komunikāciju tīkla un publiski pieejamu elektronisko komunikāciju pakalpojumiem. Vienlaikus e-privātuma direktīvas 5. panta 1. punkts paredz, ka IPS zināmos apstākļos ar lietotāju piekrišanu drīkst apstrādāt datus par datu plūsmu un saziņas saturu. Šis noteikums ir formulēts, paredzot aizliegumu "komunikāciju un saistītās informācijas par datu plūsmu noklausīšanos, ierakstīšanu, uzglabāšanu vai cita veida aizturēšanu vai pārraudzību personām, kas nav lietotāji, bez attiecīgo lietotāju piekrišanas, izņemot gadījumus, kad to darīt ir ar likumu atļauts saskaņā ar 15. panta 1. punktu". Šis noteikums ir sīkāk izskaidrots turpmāk.

39. Papildus attiecīgo lietotāju piekrišanai E-privātuma direktīva paredz citu pamatojumu, kas padara likumīgu IPS veiktu datu apstrādi par datplūsmu un saziņu. Piemērojamais datu apstrādes juridiskais pamatojums šajā gadījumā ir i) pakalpojuma sniegšana; ii) pakalpojuma drošības aizsardzība un iii) pārblīves mazināšana. Citi iespējamie pamatojuma veidi, kas padara likumīgu pārvaldības politiku, kura pamatota uz datiem par datplūsmu vai saziņas datiem, ir turpmāk apspriesti iv) apakšpunktā.

i) ar pakalpojumu sniegšanu saistītais juridiskais pamatojums

40. Kā parādīts IV iedaļā, IPS apstrādā IP galvenēs ietverto informāciju, lai maršrutētu katru IP paketi uz tās galamērķi. E-privātuma direktīvas 6. panta 1. un 2. punkts atļauj apstrādāt datus par datplūsmu, lai nodrošinātu saziņu. Tādējādi IPS drīkst apstrādāt informāciju, kas ir vajadzīga, lai sniegtu pakalpojumu.

ii) ar pakalpojuma drošības aizsardzību saistītais juridiskais pamatojums

41. Atbilstīgi E-privātuma direktīvas 4. pantam IPS ir vispārējs pienākums veikt attiecīgus pasākumus, lai nodrošinātu savu pakalpojumu drošību. Lai filtrētu vīrusus, var būt jāapstrādā gan IP galvenes, gan IP vērtums. Ņemot vērā to, ka E-privātuma direktīvas 4. pants pieprasa, lai IPS garantētu to tīkla drošību, šis noteikums padara likumīgus pārbaudes paņēmienus, kas pamatoti uz IP galveņu un satura pārbaudi un kas ir paredzēti tieši šāda mērķa sasniegšanai. Praksē tas nozīmē, ka IPS, atbilstoši proporcionalitātes principa paredzētajiem ierobežojumiem skatīt V.3. iedaļu), drīkst uzraudzīt un filtrēt saziņas datus, lai apkarotu vīrusus un nodrošinātu tīkla vispārējo drošību ([27]).

([26]) E-privātuma direktīvas 10. apsvērums: "Telekomunikāciju nozarē, jo īpaši uz visiem ar pamattiesību un pamatbrīvību aizsardzību saistītajiem jautājumiem, uz ko konkrēti neattiecas šīs direktīvas noteikumi, tostarp uz personas datu apstrādātāju pienākumiem un fizisku personu tiesībām, attiecas Direktīva 95/46/EK." Būtisks ir arī 17. apsvērums par datu subjekta piekrišanu. "Šajā direktīvā jēdzienam lietotāja vai abonenta piekrišana, neatkarīgi no tā, vai tas ir fiziska vai juridiska persona, jābūt tādai pašai nozīmei, kāda tā ir jēdzienam informācijas objekta piekrišana, kā noteikts un precizēts Direktīvā 95/46/EK."

([27]) 29. panta darba grupas atzinumu 2/2006 par privātuma jautājumiem saistībā ar e-pasta pārbaudīšanas pakalpojumu nodrošināšanu, kas pieņemts 2006. gada 21. februārī (WP 118). Šajā atzinumā darba grupa norāda, ka filtru lietošana 4. panta nolūkā var būt saderīga ar E-privātuma direktīvas 5. pantu.

iii) ar pārblīves seku mazināšanu saistītais juridiskais pamatojums

42. Šī juridiskā pamatojuma *motivācija* ir atrodama E-privātuma direktīvas 22. apsvērumā, kas izskaidro 5. panta 1. punktā paredzēto aizliegumu uzglabāt saziņas datus. Šis noteikums neaizliedz automātisku, pastarpinātu un īslaicīgu uzglabāšanu, ciktāl tās vienīgais nolūks ir nodrošināt datu pārraidi, tā nav ilgāka, nekā vajadzīgs datu pārraides un datplūsmas pārvaldības nodrošināšanai, un tiek saglabāta saziņas konfidencialitātes garantija.

43. Pārblīves gadījumā rodas jautājums, vai IPS var apsvērt iespēju pēc nejaušības principa atmest vai aizkavēt datplūsmu vai palēināt saziņu, kas nav atkarīga no nodrošināšanas laika, piemēram, vienādranga datu apmaiņas vai e-pasta saziņas datplūsmu, lai nodrošinātu, piemēram, balss datplūsmas pieņemamu kvalitāti.

44. Ņemot vērā sabiedrības vispārējo ieinteresētību, lai tai tiktu garantēts lietojams sakaru tīkls, IPS var argumentēt, ka datplūsmas prioritāšu noteikšana vai droselēšana, lai risinātu pārblīves problēmu, ir likumīgs pasākums, kas ir vajadzīgs, lai pienācīgi sniegtu pakalpojumus. Tas nozīmē, ka šajos gadījumos un šajā nolūkā personisko datu apstrādei būtu vispārējs juridisks pamatojums, un nebūtu vajadzīga atsevišķa lietotāju piekrišana.

45. Vienlaikus spēja šādi iejaukties nav neierobežota. Ja IPS ir jāpārbauda saziņa, no konfidencialitātes viedokļa un stingri piemērojot proporcionalitātes principu, lai sasniegtu šo mērķi, tiem jāizmanto metode ar vismazāko iespējamo iejaukšanās pakāpi (izvairoties no pakešu padziļinātas pārbaudes), un viņi drīkst šo metodi izmantot tikai tik ilgi, cik vajadzīgs, lai novērstu pārblīvi.

iv) ar citiem nolūkiem saistītas datu apstrādes juridiskais pamatojums

46. IPS, iespējams, vēlēsies pārbaudīt datus par datplūsmu un saziņas datus citos nolūkos, piemēram, lai piedāvātu specializētu abonementu (piemēram, abonementu, kas ierobežo piekļuvi vienādranga datu apmaiņai, vai abonementu ar lielāku savienojuma ātrumu noteiktām lietotnēm). Pārbaudīt un turpmāk izmantot datus par datplūsmu un saziņas datus citos nolūkos, nevis lai sniegtu pakalpojumu vai nodrošinātu tā drošību un novērstu pārblīvi, ir atļauts tikai saskaņā ar stingriem noteikumiem atbilstoši tiesiskajam regulējumam.

47. Tiesiskais regulējums ir galvenokārt E-privātuma direktīvas 5. panta 1. punkts, kurā pieprasīts iegūt attiecīgo lietotāju piekrišanu, lai noklausītos, ierakstītu, uzglabātu vai citādi aizturētu vai pārraudzītu saziņas un saistītās datplūsmas datus. Praksē tas nozīmē, ka, lai atbilstoši 5. panta 1. punktam padarītu likumīgu datplūsmas vai saziņas datu apstrādi, ir vajadzīga saziņā iesaistīto lietotāju piekrišana.

48. Kā izskaidrots iepriekš, pārbaudes un filtrēšanas paņēmieni ir pamatoti uz IP galveņu pārbaudi, kurās ir dati par datplūsmu, vai uz pakešu padziļinātu pārbaudi, pārbaudot IP vērtumus, kuros ir saziņas dati. Tāpēc principā šādu paņēmienu lietošana citos nolūkos, nevis lai sniegtu pakalpojumu vai nodrošinātu tā drošību, būtu aizliegta, ja nav likumīga pamatojuma, kas atļautu veikt datu apstrādi, piemēram, iegūta piekrišana (5. panta 1. punkts). 5. panta 1. punkts tiktu piemērots, piemēram, ja IPS izlemtu piedāvāt klientiem piekļuvi internetam par zemāku tarifu, pretī saņemot tiesības rādīt paradumorientētas reklāmas, to nodrošināšanai izmantojot pakešu padziļināto pārbaudi, respektīvi, saziņas datus. Tāpēc saskaņā ar 5. panta 1. punktu ir jāiegūst īsta, konkrēta un apzināta piekrišana.

49. Turklāt E-privātuma direktīvas 6. pantā "Informācija par datu plūsmu" ir paredzēti daži noteikumi, kas attiecas īpaši uz datiem par datu plūsmu. Konkrētāk, tajā ir paredzēta iespēja IPS apstrādāt datus par

datplūsmu, pamatojoties uz lietotāju piekrišanu, lai saņemtu pievienotās vērtības pakalpojumus ([28]). Šajā noteikumā ir ietverta 5. panta 1. punktā paredzētā prasība iegūt piekrišanu, ja ir paredzēts apstrādāt datus par datplūsmu.

50. Praksē, iespējams, vienmēr nebūs viegli noteikt, piemēram, kuros gadījumos ir vajadzīga piekrišana un kuros gadījumos tīkla drošības apsvērumi padara apstrādi likumīgu, jo īpaši, ja pārbaudes paņēmieniem ir divējādi mērķi (piemēram, novērst pārblīvi un sniegt pievienotās vērtības pakalpojumus). Jāuzsver, ka piekrišanu nevar uzskatīt par vienkāršu un sistēmisku ceļu uz atbilstību datu aizsardzības principiem.

51. Tiesiskā regulējuma piemērošanas jomā, konkrētāk, attiecībā uz dažādajiem iepriekš aprakstītajiem aspektiem, trūkst pieredzes. Šajā jomā ir vajadzīgas papildu vadlīnijas, kā turpmāk aprakstīts VI iedaļā. Turklāt ir vēl citi ar piekrišanas iegūšanu saistīti svarīgi aspekti, kam arī vajadzīga īpaša uzmanība. Šie aspekti ir aprakstīti turpmāk.

V.2. **Ar apzinātas piekrišanas kā juridiska pamata sniegšanu saistītie jautājumi**

52. E-privātuma direktīvas 5. un 6. pantā prasītā piekrišana nozīmē to pašu, ko datu subjekta piekrišana, kā definēts un turpmāk precizēts Direktīvā 95/46/EK ([29]). Saskaņā ar Datu aizsardzības direktīvas 2. panta h) apakšpunktu datu subjekta piekrišana ir "jebkurš labprātīgi sniegts šīs personas vēlmju konkrēts un paziņots norādījumu, ar kuru datu subjekts izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei". Piekrišanas lomu un prasības tās spēkā esamībai nesen savā atzinumā 15/2011 par piekrišanu ([30]) apskatīja 29. panta darba grupa.

53. Tāpēc IPS, kas pieprasa lietotāju piekrišanu datplūsmas pārbaudei un filtrēšanai, jānodrošina, lai piekrišana būtu labprātīga un konkrēta, un tai jābūt pilnībā apzinātam personas vēlmju norādījumam, ar ko tā izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei. To atkārtoti apstiprina E-privātuma direktīvas 17. apsvērums: "(…) Piekrišanu var sniegt ar jebkuru pienācīgu metodi, kas ļauj lietotājam brīvi sniegt konkrētu un informētu norādi par savu vēlmi, tostarp atzīmēšanu ar ķeksīti interneta tīmekļa vietnē." Turpmāk izklāstīti daži praktiski piemēri tam, ko šajā kontekstā nozīmē labprātīga, konkrēta un apzināta piekrišana.

Piekrišana: labprātīgs, konkrēts un apzināts vēlmju norādījums

54. *Labprātīga piekrišana*. Lietotājiem nedrīkstētu uzlikt ierobežojumus, kas saista piekrišanu ar to interneta pakalpojumu abonēšanu, kuru tie vēlas.

55. Personas piekrišana nebūtu sniegta labprātīgi, ja, lai saņemtu sakaru pakalpojumus, tiem būtu jāpiekrīt viņu saziņas datu uzraudzībai. Šī situācija būtu vēl uzskatāmāka, ja *visi* pakalpojumu sniedzēji noteiktā tirgū veiktu datplūsmas pārvaldību citos nolūkos, ne tikai lai nodrošinātu tīkla drošību. Vienīgā alternatīva būtu vispār neabonēt interneta pakalpojumus. Ņemot vērā to, ka internets ir kļuvis par būtisku

([28]) Direktīvas 18. apsvērumā ir ietverts saraksts, kurā minēti pievienotās vērtības pakalpojumu piemēri. Nav skaidrs, vai var uzskatīt, ka pakalpojumi, kuru sniegšanai tiek piemērota datplūsmas pārvaldības politika, ietilpst šajā sarakstā. Datplūsmas pārvaldības politika, kuras mērķis ir piešķirt prioritāti noteiktam saturam, var uzskatīt par kvalitātes uzlabošanas nolūkā veiktu darbību. Piemēram, datplūsmas pārvaldību, kas tiek īstenota, apstrādājot tikai IP galvenes, un kuras mērķis ir sniegt sakaru pakalpojumus spēļu spēlēšanas vajadzībām par augstāku tarifu, lai tīklā par prioritāru tikta uzskatīta lietotāja personiskā spēļu datplūsma, var uzskatīt par pievienotās vērtības pakalpojumu. No otras puses, ne tuvu nav skaidrs, vai datplūsmas pārvaldība, lai droselētu zināma veida datplūsmu, piemēram, lai palēninātu vienādranga datu apmaiņas datplūsmu, par tādu var uzskatīt.

([29]) Skatīt E-privātuma direktīvas 17. apsvērumu un 2. panta f) apakšpunktu.

([30]) Pieņemts 2011. gada 13. jūlijā (WP 187).

instrumentu gan darba vajadzībām, gan brīvā laika pavadīšanas vajadzībām, interneta pakalpojumu neabonēšana nav uzskatāma par pilnvērtīgu alternatīvu. Rezultātā personām nebūtu reālas izvēles, t. i., tās nevarētu labprātīgi dot piekrišanu ([31]).

56. EDAU uzskata, ka ir nepārprotami vajadzīgs, lai Komisija un valstu iestādes uzraudzītu tirgu, jo īpaši, lai pārliecinātos, vai šī tendence, t. i., telesakaru pakalpojumu saistīšana ar saziņas pārraudzību, nekļūst vispārēja. Pakalpojumu sniedzējiem jāpiedāvā alternatīvi pakalpojumi, tostarp interneta pieslēgums, kas nav pakļauts datplūsmas pārvaldībai, neradot privātpersonām lielākas izmaksas.

57. *Konkrēta piekrišana*. Prasība, lai piekrišana būtu konkrēta šajā gadījumā nozīmē, ka IPS ir jāiegūst skaidra un izteikta piekrišana datplūsmas un saziņas uzraudzībai. Pēc 29. panta darba grupas domām, "… lai piekrišana būtu konkrēta, tai jābūt saprotamai: tai skaidri jānorāda uz datu apstrādes apjomu un sekām. Tā nedrīkst attiekties uz vispārīgu apstrādes darbību kopu. Citiem vārdiem, tas nozīmē, ka piekrišanai jābūt spēkā ierobežotā kontekstā." Konkrētu piekrišanu visticamāk nevarēs iegūt, ja piekrišana datplūsmas un saziņas datu pārbaudei ir "apvienota" ar vispārīgu piekrišanu pakalpojumu abonēšanai. Lai piekrišana būtu konkrēta, tās iegūšanai ir mērķtiecīgi jāizmanto specifisks līdzeklis, piemēram, specifiska piekrišanas veidlapa vai atsevišķs lodziņš, kas skaidri paredzēts tam, lai sniegtu piekrišanu datu uzraudzībai (nevis vienkārši iekļaujot informāciju līguma vispārīgajos nosacījumos un pieprasot parakstīt piedāvāto līgumu).

58. *Apzināta piekrišana*. Lai piekrišana būtu spēkā, tai jābūt apzinātai. Vajadzība iepriekš sniegt pietiekamu informāciju izriet ne tikai no E-privātuma un Datu aizsardzības direktīvas, bet arī no Universālo pakalpojumu direktīvas, kurā grozījumi izdarīti ar Direktīvu 2009/136/EK ([32]), 20. un 21. pantā. Informācijas un piekrišanas vajadzība tika skaidri apstiprināta Direktīvas 2009/136/EK 28. apsvērumā: "lietotāji jebkurā gadījumā būtu pilnībā jāinformē par jebkādiem ierobežojošiem apstākļiem, ko elektronisko komunikāciju pakalpojumu izmantošanas jomā nosaka tīkla operators un/vai pakalpojumu sniedzējs. Šādā informācijā pēc pakalpojumu sniedzēja ieskatiem būtu jāprecizē vai nu attiecīgā satura, lietotnes vai pakalpojuma veids, vai atsevišķas lietotnes vai pakalpojumi, vai arī abi minētie." Tajā turpmāk noteikts: "Atkarībā no izmantotās tehnoloģijas un ierobežojuma veida šādu ierobežojumu piemērošanai var būt vajadzīga patērētāju piekrišana saskaņā ar Direktīvu 2002/58/EK".

59. Ņemot vērā šo uzraudzības paņēmienu sarežģītību, jēgpilnas iepriekšējas informācijas sniegšana ir viens no sarežģītākajiem uzdevumiem, kas jāveic, lai iegūtu derīgu piekrišanu. Patērētājus jāinformē tā, lai viņi varētu izprast, kāda informācija tiek apstrādāta, kā tā tiek lietota, un šo darbību ietekmi uz lietojamību un ar paņēmienu saistīto iejaukšanās potenciālu privātajā dzīvē.

60. Tas nozīmē, ka informācijai jābūt ne tikai skaidrai un parastam lietotājam saprotamai, bet informācija arī jāsniedz personām tieši un uzskatāmi, lai to nevarētu neievērot.

61. *Norādījums par vēlmēm*. Piemērojamais tiesiskais regulējums pieprasa, lai, dodot piekrišanu, lietotājs veiktu apstiprinošu darbību, kas norādītu uz viņa/viņas piekrišanu. Netieša piekrišana šai prasībai neatbilst. Šī prasība arī apstiprina vajadzību izmantot īpaši atvēlētu līdzekli, lai iegūtu piekrišanu tam, ka IPS pārbauda datplūsmas un saziņas datus, piemērojot datplūsmas pārvaldības politiku. 29. panta darba grupa savā nesenajā atzinumā par piekrišanu uzsvēra vajadzību nodrošināt detalizētību attiecībā uz dažādajiem datu apstrādes elementiem, iegūstot piekrišanu.

([31]) Līdzīgs gadījums ir PDR, attiecībā uz ko tika apspriests, vai pasažieru piekrišana rezervējumu datu pārsūtīšanai ASV iestādēm ir uzskatāma par spēkā esošu. Darba grupa uzskata, ka pasažieri nevar dot labprātīgu piekrišanu, jo aviosabiedrībām ir pienākums nosūtīt datus pirms reisa izlidošanas, tāpēc pasažieriem nav reālas izvēles lidot vai nelidot; 29. panta darba grupas atzinums 6/2002 par aviosabiedrību pasažieru un ekipāžas locekļu datu un citu datu pārsūtīšanu Amerikas Savienotajām Valstīm.

([32]) 2009. gada 25. novembra Direktīva 2009/136/EK, ar ko groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem (skat. 15. atsauci).

62. Var argumentēt, ka, ja saziņā iesaistītās personas nevēlas, lai IPS to pārtvertu ar nolūku piemērot datplūsmas pārvaldības politiku, tās jebkurā laikā var saziņu šifrēt. Šo pieeju var uzskatīt par praktiski noderīgu, tomēr, lai to izdarītu, ir vajadzīga zināma piepūle un tehniskās zināšanas, un to nevar uzskatīt par līdzīgu labprātīgai, konkrētai un apzinātai piekrišanai. Turklāt šifrēšanas paņēmienu lietošana negarantē saziņas pilnīgu konfidencialitāti, jo IPS varēs piekļūt vismaz IP galvenēs ietvertajai informācijai, lai maršrutētu saziņu, tātad varēs arī veikt statistisku analīzi.

63. Saskaņā ar E-privātuma direktīvas 5. panta 1. punktu, piekrišana jāiegūst no attiecīgajiem lietotājiem. Daudzos gadījumos lietotājs un abonents būs viena un tā pati persona, tādējādi piekrišanu var iegūt telesakaru pakalpojuma abonēšanas brīdī. Citos gadījumos, tostarp tādos, kuros iesaistītas vairākas personas, attiecīgo lietotāju piekrišana jāiegūst atsevišķi. No tā izriet turpmāk apspriestie praktiskie jautājumi.

Visu attiecīgo lietotāju piekrišana

64. Direktīvas 5. panta 1. punktā paredzēts, ka, lai apstrādi padarītu likumīgu, vajadzīga lietotāju piekrišana. Tā jāiegūst no *visiem* saziņā iesaistītajiem lietotājiem. Šīs prasības *motivācija* ir tāda, ka saziņa parasti attiecas vismaz uz divām personām (sūtītājs un saņēmējs). Piemēram, ja IPS skenē IP vērtumus, kas attiecas uz e-pasta ziņojumu, viņš pārbauda informāciju, kas attiecas gan uz e-pasta ziņojuma sūtītāju, gan saņēmēju.

65. Uzraugot un pārtverot datplūsmu un saziņu (piemēram, daļu tīmekļa datplūsmas), IPS var pietikt ar lietotāja, tas ir, abonenta, piekrišanu. Tas tāpēc, ka otru saziņas pusi, šajā gadījumā, apmeklētu tīmekļa vietni, nevar uzskatīt par "attiecīgu lietotāju" ([33]). Tomēr situācija kļūst sarežģītāka, ja šāda uzraudzība ietver e-pasta ziņojumu satura pārbaudi, tādējādi, e-pasta ziņojuma sūtītāja un saņēmēja personisko informāciju, kam abiem var nebūt līgumattiecības ar vienu un to pašu IPS. Šādos gadījumos IPS apstrādātu lietotāju, kas nav tā klienti, personas datus (vārds, e-pasta adrese un iespējami sensitīvi saziņas satura dati). No praktiskā viedokļa šādu personu piekrišanu var būt grūtāk iegūt, jo tas jādara katrā gadījumā individuāli, nevis slēdzot līgumu par telesakaru pakalpojumu sniegšanu. Nav arī reālistiski pieņemt, ka abonenta piekrišana ir sniegta arī citu lietotāju vārdā, piemēram, kā bieži ir privātās mājsaimniecībās.

66. Šajā kontekstā EDAU uzskata, ka IPS jāievēro spēkā esošās juridiskās prasības, un jāīsteno politika, kas neietver informācijas uzraudzību un pārbaudi. Tas ir vēl būtiskāk attiecībā uz sakaru pakalpojumiem, kas ietver trešās personas, kuras nevar sniegt piekrišanu informācijas uzraudzībai, jo īpaši attiecībā uz nosūtītajiem un saņemtajiem e-pasta ziņojumiem (šī situācija neattiecas uz gadījumiem, kad tas tiek darīts drošības apsvērumu dēļ).

67. Vienlaikus jānorāda, ka valstu tiesību akti, ar ko īsteno E-privātuma direktīvas 5. panta 1. punktu, šajā ziņā var nebūt apmierinoši, un ka kopumā šķiet, ka būtu vajadzīgas labākas vadlīnijas par E-privātuma direktīvas prasībām šajā kontekstā. Tāpēc EDAU aicina Komisija šajā ziņā būt aktīvākai un uzņemties iniciatīvu, kurā vērtīgu ieguldījumu varētu dot 29. panta darba grupā iesaistītās uzraudzības iestādes un citas ieinteresētās personas. Ja vajadzīgs, jāceļ prasība Eiropas Tiesā, lai iegūtu pilnīgu noteiktību par 5. panta 1. punkta nozīmi un sekām.

([33]) Neņemot vērā gadījumus, kad tīmekļa datplūsmā tiek pārsūtīta tāda personiska informācija, kā, piemēram, identificējamu fizisku personu fotoattēli, kas publicēti tīmekļa vietnē. Šādas informācijas apstrādei ir vajadzīgs juridiskais pamats, bet uz to neattiektos 5. panta 1. punkts, jo šīs personas nebūtu "attiecīgie lietotāji".

V.3. **Proporcionalitāte – datu minimizācijas princips**

68. Datu aizsardzības direktīvas 6. panta c) apakšpunktā ir noteikts proporcionalitātes princips ([34]), kas attiecas uz IPS, jo, veicot uzraudzību un filtrēšanu, tie minētās direktīvas izpratnē ir personas datu apstrādātāji.

69. Atbilstīgi minētajam principam, personas datus drīkst apstrādāt tikai tiktāl, ciktāl tie ir "adekvātiem, attiecīgiem un ne pārmērīgā apjomā attiecībā uz nolūkiem, kādiem tie savākti un/vai tālāk apstrādāti". No šī principa piemērošanas izriet vajadzība novērtēt, vai datu apstrādē izmantoti līdzekļi un izmantotie personas datu veidi ir piemēroti šīs darbības mērķu sasniegšanai un vai ir pamatoti uzskatīt, ka ar tiem šos mērķus var sasniegt. Ja tiek konstatēts, ka ir savākts vairāk datu nekā vajadzīgs, princips nav ievērots.

70. Dažādu pārbaudes paņēmienu veidu atbilstība proporcionalitātes principam jāvērtē katrā gadījumā individuāli. Secinājumus nevar izdarīt *abstrakti*. Tomēr var norādīt uz dažādiem konkrētiem aspektiem, kas jāvērtē, lai novērtētu, vai tiek ievērots proporcionalitātes princips.

71. *Apstrādātās informācijas daudzums*. Maksimāli dziļa IPS klientu saziņas uzraudzība lielākajā daļā gadījumu ir pārmērīga un pretlikumīga. Ietekmi uz privātpersonu privāto dzīvi palielina apstāklis, ka to var īstenot ar līdzekļiem, kas nav tām redzami un ka tām šis process var būt grūti saprotams. IPS jānovērtē, kuram no vajadzīgā rezultāta sasniegšanai pieejamajiem līdzekļiem ir vismazākais iejaukšanās potenciāls. Piemēram, vai vajadzīgo rezultātu var sasniegt, uzraugot IP galveņu informāciju, nevis veicot pakešu padziļinātu pārbaudi? Arī tad, ja tiek lietota pakešu padziļinātā pārbaude, vajadzīgās informācijas ieguvei var pietikt tikai ar to, ka tiek identificēti noteikti protokoli. Būtiska var būt arī datu aizsardzības pasākumu, tostarp pseidoanonimizācijas lietošana. Novērtējuma rezultātā ir jāgūst apstiprinājums tam, ka datu apstrāde ir proporcionāla.

72. *Apstrādes sekas (tieši saistītas ar nolūkiem)*. Proporcionalitātes princips, iespējams, netiek ievērots gadījumos, kad IPS izmanto datplūsmas pārvaldības politiku, kas neļauj lietotājiem piekļūt noteiktiem pakalpojumiem, un neļauj lietotājiem izmantot pietiekamu daļu rezultātā iegūto priekšrocību.

73. Ir būtiski atgādināt, ka proporcionalitātes princips ir jāpiemēro, pat ja citas obligātās juridiskās prasības ir izpildītas, tostarp ja IPS ir, piemēram, ieguvis personu piekrišanu satura uzraudzībai. Tas nozīmē, ka datu apstrāde, kas tiek veikta, īstenojot satura uzraudzību, joprojām var tikt uzskatīta par pretlikumīgu, ja tā pārkāpj proporcionalitātes pamatprincipu.

V.4. **Drošības un organizatoriskie pasākumi**

74. E-privātuma direktīvas 4. pants skaidri pieprasa IPS veikt tehniskus un organizatoriskus pasākumus, lai nodrošinātu i) ka personas datiem piekļūst tikai pilnvaroti darbinieki likumīgiem mērķiem; ii) personas datu aizsardzību pret nejaušu vai pretlikumīgu apstrādi un iii) ka attiecībā uz personas datu apstrādi tiek īstenota drošības politika. Šis pants arī pilnvaro kompetentās valsts iestādes veikt šo pasākumu revīziju.

75. Turklāt saskaņā ar E-privātuma direktīvas 4. panta 2. un 3. punktu IPS ir arī pienākums paziņot par pārkāpumiem, kas saistīti ar personas datiem, attiecīgi kompetentajām valsts iestādēm, kā arī personām, kuras ietekmē šie pārkāpumi, gadījumā, ja datu izpaušanas sekas šīm personām var būt negatīvas.

76. Saziņā ietverto personas datu apstrādes rezultātā, kas tiek veikta ar mērķi piemērot datplūsmas pārvaldības politikas, IPS var iegūt piekļuvi datiem, kas ir sensitīvāki nekā datplūsmas dati.

([34]) Kā izskaidrots iepriekš, Datu aizsardzības direktīva attiecas uz visiem ar pamattiesību un pamatbrīvību aizsardzību saistītajiem jautājumiem, kas nav atsevišķi reglamentēti E-privātuma direktīvā.

77. Tāpēc IPS izstrādātajās drošības politikās ir jāparedz specifiski aizsardzības pasākumi, lai garantētu, ka veiktie pasākumi ir atbilstīgi šiem apdraudējumiem. Vienlaikus kompetentajām valsts iestādēm, kas veic šo pasākumu revīziju, jābūt īpaši prasīgām. Visbeidzot, ir jānodrošina, lai tiktu ieviestas efektīvas paziņošanas procedūras to datu subjektu informēšanai, kuru informācija ir kompromitēta un kurus tas var negatīvi ietekmēt.

VI. **POLITISKO UN LIKUMDOŠANAS PASĀKUMU IETEIKUMI**

78. Izmantojot pārbaudes paņēmienus, kas pamatoti uz datplūsmas datu un IP vērtumu, t. i., saziņas satura, pārbaudi, var noskaidrot lietotāju internetā veiktās darbības: apmeklētās tīmekļa vietnes un šajās vietnēs veiktās darbības, vienādranga datu apmaiņas lietotņu izmantošanu, lejupielādētās datnes, nosūtītos un saņemtos e-pasta ziņojumus, to adresātus, tematus un nosūtīšanas laiku utt. IPS šo informāciju var izmantot, lai piešķirtu prioritāti noteiktiem saziņas veidiem, piemēram, video pakalpojumiem pēc pieprasījuma, salīdzinājumā ar citiem. Tie var lietot šo informāciju, lai identificētu vīrusus vai izstrādātu lietotāju profilus ar nolūku rādīt paradumorientētas reklāmas. Šīs darbības ir tiesību uz saziņas konfidencialitāti pārkāpums.

79. Atkarībā no izmantotajiem paņēmieniem un gadījuma specifikas ietekme uz privāto dzīvi var palielināties. Jo dziļāk sniedzas datu pārtveršana un savāktās informācijas analīze, jo vairāk tā ir pretrunā ar saziņas konfidencialitātes principu. Būtiski elementi, pēc kā var noteikt iejaukšanās pakāpi privātpersonu privātajā dzīvē, ir uzraudzības veikšanas nolūks un īstenotie datu aizsardzības pasākumi. Datplūsmas bloķēšanu un uzraudzību, kas tiek veikta ļaunprātīgas programmatūras apkarošanas nolūkos, ievērojot stingrus pārbaudīto datu saglabāšanas un lietošanas ierobežojumus, nevar salīdzināt ar situācijām, kad iegūtā informācija tiek reģistrētu, lai veidotu individuālus profilus ar nolūku rādīt paradumorientētas reklāmas.

80. Principā EDAU uzskata, ka spēkā esošais ES regulējums privātuma un datu aizsardzības jomā, ja to pareizi interpretē, piemēro un ievieš, ir pietiekams, lai garantētu, ka tiek ievērotas tiesības uz konfidencialitāti un ka netiek apdraudēta privātpersonu privātā dzīve un datu aizsardzība ([35]). IPS nebūtu jāizmanto šādi mehānismi, ja tie nav pienācīgi piemērojuši tiesisko regulējumu. Konkrētāk, IPS jāapsver un jāievēro šādi būtiski regulējuma elementi:

— IPS var īstenot datplūsmas pārvaldības politiku, kas paredzēta, lai garantētu pakalpojuma drošību, nodrošinātu pakalpojuma sniegšanu, tostarp ierobežojot pārblīvi, saskaņā ar E-privātuma direktīvas 4. un 6. pantu;

— lai īstenotu datplūsmas pārvaldības politiku, kas ietver datplūsmas un/vai saziņas datu apstrādi citos, nevis iepriekš minētajos nolūkos, IPS ir vajadzīgs cits specifisks juridisks pamatojums un, iespējams, lietotāju piekrišana. Piemēram, lai uzraudzītu un filtrētu privātpersonu saziņu piekļuves ierobežošanas (vai atļaušanas) nolūkā noteiktām lietotnēm un pakalpojumiem, piemēram, P2P vai *VoIP*, ir jāiegūst apzināta lietotāju piekrišana;

— piekrišanai jābūt labprātīgai, skaidrai un apzinātai. Tā jānorāda ar apstiprinošu darbību. Šīs prasības ievērojami uzsver vajadzību aktīvāk strādāt, lai nodrošinātu, ka privātpersonas tiek pienācīgi, tieši, saprotami un konkrēti informētas, lai novērtētu šo darbību sekas un spētu pieņemt apzinātu lēmumu. Ņemot vērā šo paņēmienu sarežģītību, jēgpilnas iepriekšējas informācijas sniegšana ir viens no sarežģītākajiem uzdevumiem, kas jāveic, lai iegūtu derīgu piekrišanu. Turklāt lietotāji, kuri nepiekrīt uzraudzībai nedrīkst tikt nelabvēlīgi ietekmēti (tostarp finansiāli);

([35]) Neskarot vajadzību ieviest izmaiņas tiesību aktos, pamatojoties uz citiem apsvērumiem, jo īpaši ES tiesiskā regulējuma vispārējās pārskatīšanas kontekstā, lai uzlabotu tā efektivitāti, ņemot vērā jauno tehnoloģiju un globalizācijas ietekmi.

— proporcionalitātes principam ir izšķirīga loma gadījumos, kad IPS īsteno datplūsmas pārvaldības politiku, neatkarīgi no apstrādes juridiskā pamatojuma un nolūka: pakalpojuma sniegšana, pārblīves novēršana vai specifisku pieslēguma abonementu piedāvāšana, kuros ir vai nav ietverta piekļuve noteiktiem pakalpojumiem vai lietotnēm. Šis princips ierobežo IPS iespējas veikt tādu privātpersonu saziņas uzraudzību, kas ietver pārmērīga informācijas daudzuma apstrādi vai sniedz priekšrocības tikai IPS. No loģistikas viedokļa IPS iespējas ir atkarīgas no paņēmienu iejaukšanās potenciāla, vajadzīgajiem rezultātiem (no kuriem tie var gūt labumu) un īstenotajiem specifiskajiem privātās dzīves un datu aizsardzības pasākumiem. Pirms pārbaudes paņēmienu lietošanas IPS ir jāveic novērtējums, vai tie atbilst proporcionalitātes principam.

81. Kaut gan spēkā esošajā tiesiskajā regulējumā ir ietverti attiecīgi nosacījumi un aizsardzības pasākumi, ir jāpievērš īpaša uzmanība tam, vai IPS reāli atbilst juridiskajām prasībām, vai viņi sniedz patērētājiem vajadzīgo informāciju, lai tie varētu izdarīt jēgpilnu izvēli, un vai viņi ievēro proporcionalitātes principu. Valsts līmenī pie iepriekš minētajā jomā kompetentajām iestādēm pieder valsts telesakaru iestādes no vienas puses, un valsts datu aizsardzības iestādes no otras puses. ES līmenī attiecīgās ES līmeņa iestādes ir, piemēram, *BEREC*. Arī EDAU šajā kontekstā, iespējams, ir zināma loma.

82. Papildus šībrīža atbilstības līmeņa uzraudzībai, ņemot vērā, ka iespēja reālā laikā veikt saziņas lielapjoma pārbaudi ir salīdzinoši jauna, daži ar regulējuma piemērošanu saistītie aspekti, kas apspriesti šajā atzinumā, ir detalizētāk jāanalizē un turpmāk jāskaidro. Jo īpaši būtiskas vairākās jomās ir turpmāk minētās vadlīnijas:

— tādu likumīgu pārbaudes paņēmienu noteikšana, kas paredzēti netraucētas datplūsmas nodrošināšanai un kuru īstenošanai var nebūt vajadzīga lietotāju piekrišana, piemēram, cīņa ar surogātpastu. Papildus lietotās uzraudzības iejaukšanās potenciālam būtiski ir tādi aspekti kā, piemēram, traucējumu līmenis datplūsmas netraucētai apritei, kāda tā būtu, ja minētie paņēmieni netiktu īstenoti;

— to pārbaudes paņēmienu noteikšana, kurus drīkst īstenot drošības apsvērumu dēļ un kuru īstenošanai var nebūt vajadzīga lietotāju piekrišana;

— to gadījumu noteikšana, kad uzraudzības veikšanai vajadzīga privātpersonas piekrišana, jo īpaši visu attiecīgo lietotāju piekrišana, un pieļaujamie tehniskie parametri, lai nodrošinātu, ka, īstenojot pārbaudes paņēmienu, netiek apstrādāts šī paņēmiena mērķa sasniegšana nesamērīgs datu apjoms;

— turklāt trijos iepriekš minētajos gadījumos var būt vajadzīgas vadlīnijas par vajadzīgo datu aizsardzības pasākumu piemērošanu (nolūka ierobežošana, drošība utt.).

83. Ņemot vērā to, ka šī joma ir gan valstu, gan ES kompetencē, EDAU uzskata, ka būtiski svarīgi ir apmainīties ar viedokli un pieredzi, lai atrastu saskaņotu pieeju. Lai to sasniegtu EDAU ierosina izveidot platformu vai ekspertu grupu, kurā apvienotos valstu regulatīvo iestāžu, 29. panta darba grupas, EDAU un *BEREC* pārstāvji. Šīs platformas pirmais mērķis būtu izstrādāt vadlīnijas vismaz iepriekš apzinātajos jautājumos, lai izveidotu stabilu un saskaņotu pieeju un vienlīdzīgus apstākļus. EDAU aicina Komisiju uzņemties šo iniciatīvu.

84. Pēdējais, bet ne mazāk svarīgais aspekts ir tāds, ka gan valstu, gan ES iestādēm, tostarp BEREC un ES Komisijai ir jāpievērš īpaša uzmanība aktualitātēm tirgū šajā jomā. No datu aizsardzības un privātās dzīves skatupunkta, situācijas attīstība, kuras rezultātā IPS sāktu ikdienā īstenot datplūsmas pārvaldības politiku, piedāvājot abonēt pakalpojumus, kas pamatoti uz piekļuves saturam un lietotnēm filtrēšanu, būtu ļoti problemātiska. Ja tā notiktu, lai atrisinātu situāciju, būtu jāpieņem tiesību akti.

VII. **SECINĀJUMI**

85. Arvien pieaugošā uzraudzības un pārbaudes paņēmienu lietošanas apmēri IPS vidū apdraud interneta neitralitāti un saziņas konfidencialitāti. No šīs situācijas izriet nopietni ar lietotāju privātās dzīves un personas datu aizsardzību saistīti jautājumi.

86. Kaut gan šie jautājumi ir īsi apskatīti Komisijas paziņojumā par atklāto internetu un tīkla neitralitāti Eiropā, EDAU uzskata, ka ir jādara vairāk, lai izstrādātu apmierinošu nākotnes rīcības politiku. Tāpēc šajā atzinumā viņš ir devis savu ieguldījumu aktuālajā politiskajā diskusijā par tīkla neitralitāti, jo īpaši ar datu aizsardzību un privāto dzīvi saistītajos aspektos.

87. EDAU uzskata, ka valstu iestādēm un BEREC ir jāuzrauga situācija tirgū. Šīs uzraudzības rezultātā jāiegūst skaidrs priekšstats par to, vai tirgū ir vērojama tendence pāriet uz liela apjoma saziņas pārbaudi reāllaikā un par jautājumiem, kas saistīti ar tiesiskā regulējuma ievērošanu.

88. Veicot tirgus uzraudzību, nedrīkst iztikt bez jauno paņēmienu ietekmes uz datu aizsardzību un privātumu internetā turpmākas analīzes. Šajā atzinumā ir apzinātas dažas jomas, kurās būtu noderīgs skaidrojums. Kaut gan tādas ES aģentūras un struktūras kā *BEREC*, 29. panta darba grupa un EDAU, iespējams, varētu sekmīgi izskaidrot regulējuma piemērošanas nosacījumus, EDAU uzskata, ka Komisijas pienākums ir koordinēt un vadīt diskusiju. Tāpēc viņš aicina Komisiju uzņemties iniciatīvu, apvienojot visas šīs ieinteresētās personas platformā vai darba grupā ar šādu mērķi. Kopā ar citiem jautājumiem, kam vajadzīga turpmāka analīze, ieteicams apskatīt turpmāk minētos:

— tādu likumīgu pārbaudes paņēmienu noteikšana, kas paredzēti netraucētas datplūsmas nodrošināšanai un kurus var īstenot drošības nolūkos;

— to gadījumu noteikšana, kad uzraudzības veikšanai vajadzīga privātpersonas piekrišana, jo īpaši visu attiecīgo lietotāju piekrišana, un pieļaujamie tehniskie parametri, lai nodrošinātu, ka, īstenojot pārbaudes paņēmienu, netiek apstrādāts šī paņēmiena mērķa sasniegšana nesamērīgs datu apjoms;

— iepriekš minētajos gadījumos var būt vajadzīgas vadlīnijas par vajadzīgo datu aizsardzības pasākumu piemērošanu (nolūka ierobežošana, drošība utt.).

89. Atkarībā no konstatējumiem iepriekš minētajās jomās var būt vajadzīgi papildu tiesību akti. Šādā gadījumā Komisijai jāpiedāvā politiski pasākumi, kuru mērķis būs stiprināt tiesisko regulējumu un nodrošināt juridisko noteiktību. Jāīsteno jauni pasākumi, lai skaidrotu tīkla neitralitātes principa praktiskās sekas, kā tas jau ir darīts dažās dalībvalstīs, un jānodrošina, lai lietotājiem būtu reāla izvēle, jo īpaši, piespiežot IPS piedāvāt pieslēgumus, kas netiek uzraudzīti.

Briselē, 2011. gada 7. oktobrī

Eiropas datu aizsardzības uzraudzītājs

Peter HUSTINX