I

(Rezoliucijos, rekomendacijos ir nuomonės)

NUOMONĖS

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl tinklo neutralumo, srauto valdymo ir privatumo bei asmens duomenų apsaugos

(2012/C 34/01)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

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

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

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

atsižvelgdamas į 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių asmenų duomenų judėjimo ([2]), ypač į jo 41 straipsnio 2 dalį,

atsižvelgdamas į 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ([3]),

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS

I.1. Aplinkybės

1. 2011 m. balandžio 19 d. Komisija priėmė komunikatą „Atviras internetas ir tinklo neutralumas Europoje“ ([4]).

2. Šią nuomonę galima laikyti EDAPP reakcija į minėtą komunikatą ir ja siekiama prisidėti prie ES tebevykstančių politinių diskusijų dėl tinklo neutralumo, visų pirma dėl aspektų, susijusių su duomenų apsauga ir privatumu.

([1]) OL L 281, 1995 11 23, p. 31, Duomenų apsaugos direktyva.
([2]) OL L 8, 2001 1 12, p. 1, Duomenų apsaugos reglamentas.
([3]) OL L 201, 2002 7 31, p. 37, su pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB (žr. 15 išnašą), E. privatumo direktyva.
([4]) COM(2011) 222 galutinis.

3. Ši nuomonė paremta EDAPP atsakymu ([5]) į Komisijos viešą konsultaciją dėl atviro interneto ir tinklo neutralumo Europoje, pateiktu prieš priimant Komisijos komunikatą. EDAPP taip pat atsižvelgė į naujausių Tarybos išvadų dėl tinklo neutralumo projektą ([6]).

I.2. **Tinklo neutralumo sąvoka**

4. Tinklo neutralumas susijęs su tebevykstančiomis diskusijomis dėl to, ar interneto paslaugų teikėjams (IPT) ([7]) reikėtų leisti riboti, filtruoti ar blokuoti interneto prieigą arba kitaip veikti jo veikimą. Tinklo neutralumo sąvoka paremta požiūriu, kad internete esanti informacija turi būti perduodama nešališkai, neatsižvelgiant į turinį, paskirtį ar šaltinį, ir kad naudotojai turėtų turėti galimybę nuspręsti, kokias taikomąsias programas, paslaugas ir techninę įrangą jie nori naudoti. Tai reiškia, kad IPT negali savo nuožiūra suteikti pirmenybės prieigai prie tam tikrų programų ar paslaugų, pvz., lygiarangių, arba šią prieigą sulėtinti ir kt. ([8]).

5. Dėl tinklo srauto filtravimo, blokavimo ir patikros kyla svarbių klausimų, į kuriuos dažnai nekreipiama dėmesio arba kurie nustumiami į šalį ir kurie susiję su pranešimų konfidencialumu bei asmenų privatumo paisymu ir pagarba jų asmens duomenims, kai jie naudojasi internetu. Pavyzdžiui, tam tikri patikros metodai yra susiję su susirašinėjimo turinio, interneto svetainių, kuriose lankytasi, išsiųstų ir gautų elektroninių laiškų, laiko, kada tai įvyko, ir kitų dalykų stebėjimu ir leidžia filtruoti pranešimus.

6. Tikrindami ryšių duomenis, IPT gali pažeisti bendravimo konfidencialumą, o tai yra pagrindinė teisė, užtikrinama Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – EŽTK) 8 straipsnyje ir Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 7 ir 8 straipsniuose. Konfidencialumas papildomai saugomas ES antrinės teisės aktais, konkrečiai – E. privatumo direktyvos 5 straipsniu.

I.3. **Pagrindinė nuomonės tema ir struktūra**

7. EDAPP mano, kad vykstant rimtoms diskusijoms dėl tinklo neutralumo reikia aptarti ryšių konfidencialumo klausimą ir kitokį poveikį privatumui ir duomenų apsaugai.

8. Šia nuomone prisidedama prie ES tebevykstančių diskusijų minėta tema. Nuomone siekiama trejopo tikslo:

— joje pažymima privatumo ir duomenų apsaugos svarba vykstančiose diskusijose dėl tinklo neutralumo. Konkrečiai joje pabrėžiamas poreikis paisyti esamų taisyklių, kuriomis reglamentuojamas ryšių konfidencialumas. Turėtų būti leidžiama tik tokia praktika, kuria paisoma minėtų taisyklių,

— tinklo neutralumas susijęs su palyginti naujomis technologinėmis galimybėmis ir yra mažai patirties, susijusios su tuo, kaip taikomi teisės aktai. Todėl šioje nuomonėje pateikiamos rekomendacijos, kaip IPT turėtų taikyti duomenų apsaugos teisės aktus ir jų laikytis, filtruodami, blokuodami ir tikrindami tinklo srautą. Šios rekomendacijos turėtų padėti IPT ir už teisės aktų įgyvendinimo užtikrinimą atsakingoms institucijoms,

— duomenų apsaugos ir privatumo srityje šioje nuomonėje nustatomos sritys, į kurias reikia atkreipti ypatingą dėmesį ir kuriose gali reikėti imtis ES lygmens veiksmų. Tai labai svarbu atsižvelgiant į tebevykstančias ES lygmens diskusijas ir politikos priemones, kurių Komisija šiomis aplinkybėmis gali imtis.

([5]) EDAPP pabrėžė, kad svarbu atsižvelgti į duomenų apsaugos ir privatumo klausimus bei kitas esamas teises ir vertybes. Atsakymą galima rasti http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

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

([7]) Apima ir fiksuotos, ir mobiliosios prieigos prie interneto paslaugų teikimą.

([8]) Nors šis principas netaikomas IPT, ribojantiems informacijos, kurią abonentas gali siųsti ar gauti pagal ribotos siuntimo spartos ar kiekio abonementą, greitį ar kiekį. Todėl pagal tinklo neutralumo principą IPT vis tiek galėtų siūlyti interneto prieigos abonementus, kuriais prieiga ribojama remiantis tokiais kriterijais kaip greitis ar kiekis, jeigu neatsiranda tam tikro turinio atžvilgiu palankios ar nepalankios diskriminacijos.

9. EDAPP yra žinoma, kad dėl tinklo neutralumo kyla kitų klausimų, kurie papildomai aprašyti toliau, pvz., susijusių su galimybe gauti informaciją. Šie klausimai aptariami tik tiek, kiek jie yra susiję su duomenų apsauga ir privatumu arba turi jiems įtakos.

10. Nuomonės struktūra yra tokia: II skyriuje iš pradžių trumpai apžvelgiama IPT filtravimo praktika. III skyriuje apibrėžiami ES teisės aktai dėl tinklo neutralumo. IV skyriuje pateikiamas techninis aprašymas ir vertinamas poveikis privatumui atsižvelgiant į taikomą metodą. V skyriuje analizuojami praktiniai dalykai, susiję su galiojančių ES privatumo ir duomenų apsaugos teisės aktų taikymu. Remiantis atlikta analize, VI skyriuje pateikiami būsimų politikos pokyčių siūlymai ir nustatomos sritys, kuriose gali reikėti patikslinti ir patobulinti teisės aktus. VII skyriuje pateikiamos išvados.

II. **TINKLO NEUTRALUMO IR SRAUTO VALDYMO POLITIKA**

Srauto valdymo politika naudojama vis dažniau

11. Tradiciškai iki šiol IPT tinklo srautą stebėjo ir poveikį jam darė tik ribotomis aplinkybėmis. Pavyzdžiui, IPT taikė patikros metodus ir ribotus informacijos srautus, kad išsaugotų tinklo saugumą, pvz., kovodami su virusais. Todėl apskritai internetas plėtėsi kartu išsaugant nemažą neutralumą.

12. Tačiau pastaraisiais metais kai kurie IPT susidomėjo tinklo srauto tikrinimu, kad jį diferencijuotų ir jam taikytų skirtingą politiką, pavyzdžiui, tam tikras paslaugas blokuotų arba kitoms paslaugoms teiktų pirmenybę. Tai kartais vadinama „srauto valdymo politika“ ([9]).

13. Priežastys, dėl kurių IPT tikrina ir diferencijuoja srautą, yra įvairios. Pavyzdžiui, įgyvendinant srauto valdymo politiką, IPT gali lengviau valdyti srautą didelės perkrovos metu, pavyzdžiui, prioritetizuoti tam tikrą laiko požiūriu svarbų srautą, kaip antai srautinį vaizdų siuntimą, ir prasčiau vertinti kitų rūšių srautą, kuriam laikas nėra toks svarbus, kaip antai P2P ([10]). Be to, srauto valdymas gali būti priemonė IPT gauti potencialų pajamų šaltinį iš įvairių sričių. Kita vertus, IPT galėtų imti mokesčius iš turinio paslaugų teikėjų, pavyzdžiui, iš tų, kurių paslaugoms reikalingas didesnis pralaidumas, ir mainais jiems suteikti pirmenybę (ir kartu greitį). Tai reikštų, kad tam tikrą paslaugą, pvz., vaizdo įrašų pagal pareikalavimą teikimo paslaugą, būtų galima gauti greičiau nei kitą panašią paslaugą, kuriai netaikomas didelio greičio siuntimas. Pajamas būtų galima gauti ir iš abonentų, suinteresuotų mokėti didesnius (arba mažesnius) mokesčius už tam tikrus diferencijuotus abonementus. Pavyzdžiui, abonementas be P2P prieigos galėtų būti pigesnis už neribotos prieigos abonementą.

14. IPT turi savo priežasčių taikyti srauto valdymo politiką, tačiau ir kiti asmenys gali būti suinteresuoti, kad IPT ją taikytų. Jeigu IPT valdo savo tinklus ir tikrina turinį, siunčiamą per jų įrenginius, tikėtina, kad jie didins savo gebėjimą nustatyti tariamai neteisėto naudojimo atvejus, pvz., autorių teisių pažeidimus ar pornografiją.

([9]) Žr., pvz., OFCOM pranešimą „Svetainių blokavimas siekiant sumažinti autorių teisių pažeidimų internete“, priimtą 2011 m. gegužės 27 d., prieinamą http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: „Kai kurie IPT į savo srauto valdymo tinklą jau yra įdiegę paketines patikros sistemas, todėl darome prielaidą, kad jos gali būti diegiamos, nors tai būtų labai sudėtinga ir brangiai kainuotų tiems, kurie tokių paslaugų dar neteikia. Gali būti, kad, atsižvelgiant į reikalingas kapitalo investicijas, netrukus arba po kurio laiko DAP galės diegti tik didesni IPT.“

([10]) Realiojo laiko programų, pvz., srautinio vaizdų siuntimo programos kokybė, be kitų dalykų, priklauso nuo delsos, t. y. uždelsto laiko, pvz., dėl tinklo perkrovos.

Kiti susiję interesai, įskaitant duomenų apsaugą ir privatumą

15. Dėl šios tendencijos suaktyvėjo diskusija dėl tokio pobūdžio veiklos teisėtumo, o konkrečiau – ar specialūs tinklo neutralumo srities įpareigojimai turėtų būti papildomai teisės aktais plečiami.

16. IPT aktyviau taikant srauto valdymo politiką, gali būti ribojama galimybė gauti informaciją. Jeigu toks elgesys taptų įprasta praktika, o naudotojai negalėtų naudotis visu internetu (arba tai būtų pernelyg brangu), koks jis yra dabar, taip būtų apribota galimybė gauti informaciją ir naudotojų galimybė siųsti bei gauti norimą turinį naudojant pasirinktas programas ar paslaugas. Nustačius teisiškai privalomą principą dėl tinklo neutralumo, šios problemos galima išvengti.

17. Dėl to EDAPP nustatė poveikį duomenų apsaugai ir privatumui, IPT imantis srauto valdymo veiklos. Konkrečiau kalbant:

— kai IPT tvarko srauto duomenis tik tam, kad nukreiptų informacijos srautą iš siuntėjo gavėjui, paprastai jie ribotai tvarko asmens duomenis ([11]). Kaip ir pašto paslaugos atveju, kai tvarkoma ant voko užrašyta informacija, IPT tvarko informaciją, reikalingą pranešimui nukreipti jo gavėjui. Tai neprieštarauja teisiniams duomenų apsaugos, privatumo ir konfidencialumo reikalavimams,

— tačiau kai IPT tikrina ryšių duomenis, kad diferencijuotų kiekvieną ryšių srautą ir taikytų konkrečią politiką, kuri gali būti nepalanki asmenims, poveikis yra daug didesnis. Atsižvelgiant į kiekvieno atvejo aplinkybes ir į atliekamos analizės pobūdį, tvarkymu gali būti labai ribojamas asmens privatumas ir asmens duomenys. Tai yra akivaizdžiau, jeigu taikant valdymo politiką atskleidžiamas asmenų interneto ryšių turinys, įskaitant išsiųstus ir gautus elektroninius laiškus, interneto svetaines, kuriose lankytasi, parsisiųstas ar įkeltas rinkmenas ir kt.

III. **ES TEISĖS AKTŲ, SUSIJUSIŲ SU TINKLO NEUTRALUMU, IR TOLESNĖS POLITIKOS RAIDOS APŽVALGA**

III.1. **Trumpa teisės aktų apžvalga**

18. Iki 2009 m. ES teisės aktuose nebuvo nuostatų, kuriose IPT būtų aiškiai draudžiama vykdyti filtravimo ar blokavimo veiklą arba imti papildomus mokesčius iš abonentų už galimybę gauti paslaugas. Kartu juose nebuvo ir nuostatų, kuriose tokia veikla būtų aiškiai pripažįstama. Padėtis buvo šiek tiek neaiški.

19. 2009 m. telekomunikacijų teisės aktų paketu ši padėtis pakeista, įtraukus nuostatas, kuriose pirmenybė suteikta interneto atvirumui. Pavyzdžiui, Direktyvos dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva) 8 straipsnio 4 dalyje nustatyta reguliavimo institucijų pareiga skatinti galutinių naudotojų galimybę gauti pasirinktą turinį, programas ar paslaugas ([12]). Ši nuostata taikoma visam tinklui, o ne tik atskirų paslaugų teikėjų lygmeniu. Naujausių Tarybos išvadų projekte taip pat pabrėžtas poreikis išlaikyti interneto atvirumą ([13]).

([11]) Tai neapima operacijų, kuriomis siekiama padidinti tinklo saugumą ir nustatyti žalingą srautą, ir operacijų, reikalingų sąskaitoms ir savitarpio jungtims. Be to, neįeina įpareigojimai, kylantys iš Duomenų saugojimo direktyvos, 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvos 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB (OL L 105, 2006 4 13, p. 54) (toliau – Duomenų saugojimo direktyva).

([12]) 2002 m. kovo 7 d. Direktyva 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva), iš dalies pakeista Direktyva 2009/140/EB ir Reglamentu (EB) Nr. 544/2009 (OL L 337, 2009 12 18, p. 37).

([13]) Žr. 3 punkto e papunktį, kuriame Taryba pripažįsta: „Poreikis išlaikyti interneto atvirumą ir kartu užtikrinti, kad ir toliau galėtų būti teikiamos aukštos kokybės interneto paslaugos, kartu skatinant pagrindines teises ir jų paisant, kaip antai nuomonės raiškos laisvės ir laisvės užsiimti verslu“, ir 8 punkto d papunktį, kuriame valstybės narės raginamos kaip vieną iš savo politikos tikslų skatinti interneto atvirumą ir neutralumą.

20. Universaliųjų paslaugų direktyvoje ([14]) numatyti konkretesni įpareigojimai. Jos 20 ir 21 straipsniuose nustatyti skaidrumo reikalavimai, susiję su galimybės gauti paslaugas ir (arba) naudoti programas ribojimais. Be to, joje reikalaujama būtiniausio kokybės lygio.

21. Dėl IPT praktikos, susijusios su asmenų ryšių patikra, direktyvos, kuria iš dalies keičiama Universaliųjų paslaugų direktyva ir E. privatumo direktyva ([15]), 28 konstatuojamojoje dalyje pabrėžiama, kad „priklausomai nuo naudojamų technologijų ir apribojimų, siekiant taikyti šiuos apribojimus, galima reikalauti paslaugų gavėjo sutikimo, kaip numatyta E. privatumo direktyvoje“. Taigi 28 konstatuojamojoje dalyje primenama apie sutikimo dėl bet kokių apribojimų, grindžiamų ryšių stebėjimu, būtinybę pagal E. privatumo direktyvos 5 straipsnio 1 dalį. Toliau IV skyriuje papildomai analizuojama 5 straipsnio 1 dalies taikymas ir bendra duomenų apsaugos ir privatumo teisės aktų sistema.

22. Galiausiai pagal Universaliųjų paslaugų direktyvos 22 straipsnio 3 dalį nacionalinėms reguliavimo institucijoms dabar suteikiami įgaliojimai prireikus taikyti ITP būtinuosius paslaugų kokybės reikalavimus, kad nesuprastėtų paslaugos kokybė, o viešuosiuose tinkluose nebūtų sukliudyta srautui ar jis nesulėtėtų.

23. Tai reiškia, kad ES lygmeniu plačiai siekiama atviro interneto (žr. Pagrindų direktyvos 8 straipsnio 4 dalį). Tačiau šis politikos tikslas, taikomas visam tinklui, nėra tiesiogiai susijęs su draudimais ar įpareigojimais atskiriems IPT. Kitaip tariant, IPT galėtų įgyvendinti srauto valdymo politiką, pagal kurią būtų atimta prieigos prie tam tikrų programų galimybė, jeigu naudotojai yra išsamiai informuojami ir laisvai, konkrečiai bei vienareikšmiškai išreiškia sutikimą.

24. Kiekvienoje valstybėje narėje padėtis gali skirtis. Kai kuriose valstybėse narėse IPT tam tikromis sąlygomis gali įgyvendinti srauto valdymo politiką, pvz., blokuoti tokias programas kaip IP telefonija (pagal pigesnį interneto abonementą), jeigu tik asmuo yra davęs laisvą, konkretų ir vienareikšmį, informacija pagrįstą sutikimą. Kitos valstybės narės yra nusprendusios stiprinti tinklo neutralumo principą. Pavyzdžiui, 2011 m. liepos mėn. Nyderlandų parlamentas priėmė įstatymą, kuriuo paslaugų teikėjams apskritai uždrausta kliudyti interneto programoms ar paslaugoms arba jas lėtinti (pvz., IP telefonija), nebent tai būtų būtina, siekiant kuo labiau sumažinti perkrovos padarinius, dėl vientisumo ar saugumo priežasčių, kovojant su brukalais arba pagal teismo nutartį ([16]).

III.2. **Komunikatas dėl tinklo neutralumo**

25. Komunikate dėl tinklo neutralumo ([17]) Europos Komisija padarė išvadą, kad padėtį tinklo neutralumo srityje reikia stebėti ir papildomai analizuoti. Jos politika pavadinta „palaukime ir pažiūrėsime“ prieš imdamiesi tolesnių reguliavimo veiksmų.

([14]) Direktyva 2002/22/EB su pakeitimais, padarytais 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, iš dalies keičiančia Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo (OL L 337, 2009 12 18, p. 11). Taip pat plg. 1 straipsnio 3 dalį, kurioje nurodyta, kad šioje direktyvoje nei įpareigojama, nei draudžiama taikyti viešųjų elektroninių ryšių tinklų ir paslaugų teikėjų laikantis nacionalinės teisės ir remiantis Bendrijos teise nustatytas galutinių paslaugų gavėjų prieigą prie paslaugų ir programų bei naudojimąsi jomis ribojančias sąlygas, tačiau nustatoma pareiga informuoti apie šias sąlygas.

([15]) 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo.

([16]) Pradinį Nyderlandų pakeitimą galima rasti https://zoek.officielebekendmakingen.nl/kst-32549-A.html Tarp spaudoje aprašytų šios politikos galimybės priežasčių buvo paminėti ne duomenų apsaugos ir privatumo motyvai, bet priežastys, susijusios su poreikiu užtikrinti, kad naudotojams nebūtų atimta ar apribota galimybė gauti informaciją. Todėl atrodo, kad šio pakeitimo motyvai buvo klausimai, susiję su galimybe gauti informaciją.

([17]) Žr. 4 išnašą.

26. Komisijos komunikate pripažinta, kad bet kokia priemonė ir tolesni reguliavimo veiksmai būtų išsamiai vertinami duomenų apsaugos ir privatumo požiūriais. Tarybos išvadų projekte taip pat pažymimi kylantys duomenų apsaugos ir privatumo klausimai ([18]).

27. Klausimas, kurį reikia įvertinti duomenų apsaugos ir privatumo požiūriu, yra tas, ar politikos „palaukime ir pažiūrėsime“ pakanka. Nors dabar pagal duomenų apsaugos ir privatumo teisės aktus numatytos tam tikros garantijos, visų pirma pagal ryšių konfidencialumo principą, atrodo, kad būtina atidžiai stebėti reikalavimų vykdymo lygį ir priimti rekomendacijas keliais aspektais, kurie nėra iki galo aiškūs. Be to, reikėtų pateikti kelis pasiūlymus dėl to, kaip būtų galima dar tikslinti ir tobulinti teisės aktus, atsižvelgiant į technologijų pažangą. Jeigu stebint padėtį paaiškėtų, kad rinkoje atsiranda masinių, realiuoju laiku grindžiamų ryšių patikros tendencijų ir iškyla aspektų, susijusių su teisės aktų vykdymu, reikės naujų teisės aktų. Konkretūs siūlymai šiuo atžvilgiu pateikiami VI skyriuje.

IV. **TECHNINĖS APLINKYBĖS IR SUSIJĘS POVEIKIS PRIVATUMUI IR DUOMENŲ APSAUGAI**

28. Prieš pradedant išsamiau analizuoti šią temą, svarbu geriau suvokti patikros metodus, kuriuos IPT gali taikyti, įgyvendindami srauto valdymo politiką, ir kokią įtaką tai gali turėti tinklo neutralumo principui. Dėl tokių metodų atsirandantis poveikis privatumui ir duomenų apsaugai labai skiriasi, atsižvelgiant į taikomą metodą. Būtina suvokti šias technines aplinkybes ir tinkamai taikyti V skyriuje aprašytus duomenų apsaugos teisės aktus. Tačiau reikėtų pažymėti, kad ši sritis nuolat kinta ir yra sudėtinga. Todėl toliau siekiama pateikti ne išsamų ir naujausią aprašymą, o tik techninę informaciją, neišvengiamai būtiną teisiniams motyvams suvokti.

IV.1. **Informacijos perdavimas internetu. Pagrindai**

29. Kai naudotojas perduoda pranešimą internetu, perduodama informacija padalijama į paketus. Šie paketai iš siuntėjo internetu siunčiami gavėjui. Į kiekvieną paketą, be kitų dalykų, įeis informacija apie šaltinį ir paskirtį. Be to, IPT gali šiuos paketus įtraukti į papildomus lygmenis ir protokolus ([19]), kurie bus naudojami įvairiems IPT tinklo srautams valdyti.

30. Pasitelkus paštu siunčiamo laiško analogiją, tinklo perdavimo protokolo naudojimas prilygsta paštu siunčiamo laiško turinio įdėjimui į voką, ant kurio nurodytas paskirties vietos adresas, kurį pašto tarnyba perskaitys ir kuriuo paskui pristatys laišką. Pašto tarnyba savo vidaus vežimams gali naudoti papildomus protokolus, kad sutvarkytų visus persiųstinus laiškus, o tikslas yra toks, kad kiekvienas vokas pasiektų paskirties vietą, kurią iš pat pradžių nurodė siuntėjas. Taikant tokią analogiją, kiekvieną paketą sudaro dvi dalys, *IP naudingieji duomenys*, į kuriuos įeina pranešimo turinys, juos galima prilyginti laiškui. Juose yra tik gavėjui skirta informacija. Antroji paketo dalis – tai *IP antraštė*, į kurią, be kitų dalykų, įeina gavėjo ir siuntėjo adresas, ji prilygsta vokui. IP antraštė leidžia IPT ir kitiems tarpininkams naudinguosius duomenis nukreipti iš siuntimo vietos adreso paskirties vietos adresu.

31. IPT ir kiti tarpininkai užtikrina, kad IP paketai tinkle keliautų mazgais, kurie skaito IP antraštės informaciją, ją tikrina pagal maršrutų lenteles ir paskui persiunčia į kitą mazgą, esantį kelyje į paskirties vietą.

([18]) Žr. 4 punkto e papunktį, kuriame Taryba pažymi: „Tam tikri rūpestį keliantys klausimai, kuriuos dažniausiai mini vartotojai ir duomenų apsaugos institucijos ir kurie susiję su asmens duomenų apsauga.“

([19]) Kaip toliau aprašyta IV skyriaus 2 dalyje, tokie protokolai sutartu būdu koduoja informaciją, perduodamą „nuo pradinio iki galutinio taško“, kad su pranešimu susijusios šalys galėtų viena kitą suprasti, pvz., HTTP, FTP ir kt.

Šis procesas atliekamas visame tinkle, taikant metodą „geriausios pastangos naudojant kuo mažiau atminties“, nes visi per mazgą pereinantys paketai vertinami neutraliai. Persiuntus paketą į kitą mazgą, maršruto parinktuve nebereikia saugoti papildomos informacijos ([20]).

IV.2. **Patikros metodai**

32. Kaip nurodyta pirmiau, IPT perskaito IP antraštes, kad jas nukreiptų į jų paskirties vietą. Tačiau, kaip jau minėta, srauto analizė (apimanti IP antraštes ir IP naudinguosius duomenis) gali būti atliekama ir kitais tikslais, taikant kitokias technologijas. Pagal naujas tendencijas, pvz., gali būti lėtinamos kai kurios naudotojų naudojamos programos, pvz., P2P, arba alternatyviai – privilegijuotiesiems abonentams didinamas tam tikrų paslaugų, pvz., vaizdo rinkmenų pagal pareikalavimą srauto, greitis. Nors taikant bet kuriuos patikros metodus *techniškai* paketinė patikra atliekama, taikomi skirtingi įsikišimo lygiai. Yra dvi pagrindinės patikros metodų kategorijos. Viena grindžiama tik IP antrašte, o kita – ir IP naudingaisiais duomenimis.

Rėmimasis IP antraštės informacija. IP paketo antraštės patikra atskleidžia tam tikras sritis, kurias žinodami, IPT gali taikyti įvairias srauto valdymo politikos kryptis. Taikant šiuos metodus, grindžiamą tik IP antraščių patikra, tvarkomi tik tie duomenys, kurie iš esmės skirti maršruto parinkimo informacijai, kitokiam tikslui (t. y. srauto diferencijavimas). Sužinojęs pirminį IP adresą, IPT gali jį susieti su konkrečiu abonentu ir taikyti konkrečią politiką, pvz., nukreipti paketą per greitesnę arba lėtesnę nuorodą. Sužinojęs paskirties vietos IP adresą, IPT taip pat gali taikyti tam tikrą politiką, pvz., blokuoti arba filtruoti prieigą prie tam tikrų interneto svetainių.

Rėmimasis išsamesne patikra. Taikydamas išsamiąją paketinę patikrą, IPT gali gauti tik pranešimo gavėjui skirtą informaciją. Grįžtant prie pašto paslaugos pavyzdžio, šis metodas prilygsta voko atplėšimui ir jame esančio laiško perskaitymui, siekiant atlikti pranešimo turinio (kuris yra išdėstytas IP paketuose) analizę, kad būtų galima taikyti konkrečią tinklo politiką. Yra įvairių būdų atlikti šią patikrą ir kiekvienas iš jų kelia skirtingų grėsmių duomenų subjektui.

— *Išsamioji paketinė patikra, grindžiama protokolų ir statistikos duomenų analize*. Be IP protokolo, kuris skirtas tam, kad duomenis būtų galima perduoti visame internete, yra papildomi protokolai, sutartu būdu koduojantys perduodamą informaciją (transportas, sesija, pateikimas ir taikymas ir kt.). Šių protokolų tikslas – užtikrinti, kad su pranešimu susijusios šalys galėtų viena kitą suprasti. Pavyzdžiui, kai kurie protokolai susieti su naršymu tinkle ([21]), kiti skirti rinkmenoms perduoti ([22]) ir pan. Todėl protokolų patikra grindžiamais ir kartu su statistikos analize taikomais patikros metodais siekiama nustatyti konkrečius modelius ar pėdsakus, lemiančius tam tikrų protokolų buvimą ([23]). Taikydami tokius patikros metodus, IPT gali suvokti pranešimo pobūdį (e. laiškas, naršymas tinkle, rinkmenų išsiuntimas), o kai kuriais atvejais – nustatyti konkrečią naudojamą paslaugą ar programą, pvz., kai kurių IP telefonijos pranešimų atveju, kai naudojami protokolai yra labai specifiniai konkrečiam pardavėjui ar paslaugų teikėjui. Vien žinodami pranešimo pobūdį, IPT gali įgyti galimybę taikyti konkrečias srauto valdymo politikos kryptis. Pavyzdžiui, jie gali blokuoti tinklo srautą. Be to, tai gali būti pirmas žingsnis leidžiant IPT atlikti papildomą analizę, dėl kurios gali reikėti visiškos prieigos prie metaduomenų ir pranešimo turinio.

([20]) Vis dėlto interneto tinklo įranga naudoja maršruto parinkimo protokolus, kurie registruoja veiklą, tvarko eismo statistiką ir keičiasi informacija su kita tinklo įranga, siekiant IP paketus nukreipti veiksmingiausiai. Pavyzdžiui, jeigu nuoroda yra apkrauta arba neveikia ir maršruto parinktuvas gauna šią informaciją, jis atnaujins maršrutų lentelės informaciją ir į ją įtrauks alternatyvą, kuri šios nuorodos nenaudoja. Be to, svarbu pažymėti duomenų rinkimą ir tvarkymą, kuris kartais gali būti atliekamas sąskaitų išrašymo tikslais arba net pagal Duomenų saugojimo direktyvos reikalavimus.

([21]) HTTP – hipertekstų persiuntimo protokolas arba HTML – hiperteksto ženklinimo kalba.

([22]) FTP – rinkmenų persiuntimo protokolas.

([23]) Yra įvairių būdų naudojamiems protokolams nustatyti. Pavyzdžiui, galima ieškoti specialiuose vidaus protokolų laukuose, pvz., identifikuoti pranešimui nustatyti naudojamas jungtis. Pranešimų srauto statistinį apibūdinimą taip pat galima gauti atlikus kai kurių konkrečių laukų analizę, vienu metu tarp dviejų IP adresų naudojamų protokolų koreliaciją.

— *Išsamioji paketinė patikra, grindžiama pranešimo turinio analize*. Galiausiai taip pat galima patikrinti metaduomenis ([24]) ir paties pranešimo turinį. Šį metodą sudaro visų IP paketų, sudarančių pradinio pranešimo srauto dalį, perėmimas, kad būtų galima visiškai atkurti ir išanalizuoti pradinį pranešimo turinį. Pavyzdžiui, siekiant nustatyti žalingą ar neteisėtą turinį, kaip antai virusus, vaikų pornografiją ir kt., reikia atkurti patį turinį, kad jį būtų galima išanalizuoti. Pažymėtina, kad susijusios šalys gali aiškiai užšifruoti pranešimą nuo pradžios iki pabaigos ir tokia praktika kliudys IPT atlikti pranešimo turinio analizę.

IV.3. **Poveikis privatumui ir duomenų apsaugai**

33. IP antraštėmis, o konkrečiau – paketine patikra grindžiami patikros metodai susiję su šių duomenų stebėjimu ir filtravimu ir turi didelį poveikį privatumui ir duomenų apsaugai. Šie metodai taip pat gali neatitikti teisės į bendravimo konfidencialumą.

34. Asmenų pranešimų patikra savaime turi didelį poveikį privatumui ir duomenų apsaugai. Vis dėlto problema yra platesnė, nes, atsižvelgiant į padarinius, kurių siekiama stebėjimu ir perėmimu, poveikis privatumui gali būti dar didesnis. Iš tiesų pranešimų patikra vien tam, kad būtų užtikrintas tinkamas sistemos veikimas, nėra tas pats, kas pranešimų patikra siekiant taikyti politiką, kuri gali turėti poveikį asmenims. Jeigu srauto ir atrankos politika gali būti siekiama išvengti tik tinklo perkrovos, paprastai didelio poveikio asmens privatumui nebus. Tačiau srauto valdymo politika gali būti siekiama blokuoti kai kurią turinio informaciją arba paveikti pranešimą, pvz., elgsena paremta reklama. Tokiais atvejais padariniai yra labiau ribojantys. Problema tampa dar opesnė, suvokus, kad tokio pobūdžio informacija būtų renkama ne nedidelei asmenų grupei, bet veikiau bendrai, iš visų IPT klientų ([25]). Jeigu visi IPT taikytų filtravimo metodus, tai galėtų reikšti bendro pobūdžio interneto naudojimo stebėjimą. Be to, jeigu daugiausia dėmesio būtų kreipiama į tvarkomos informacijos pobūdį, kyla neabejotinai didelė grėsmė privatumui, nes daug renkamos informacijos gali būti visiškai neskelbtina, o surinkta ji tampa prieinama IPT ir tiems asmenims, kurie iš jų prašytų informacijos. Be to, informacija gali būti labai vertinga komerciniu požiūriu. Savaime tai kelia didelę funkcijų iškreipimo grėsmę, jeigu pradiniai tikslai galėtų nesunkiai tapti komerciniais ar surinkta informacija būtų kitaip išnaudojama.

35. Stebėjimo ir patikros bei filtravimo metodai turi būti teisingai taikomi laikantis taikytinų duomenų apsaugos ir privatumo garantijų, kuriose numatyti apribojimai dėl to, ką galima daryti ir kokiomis aplinkybėmis. Toliau apžvelgiamos pagal dabartinius ES duomenų apsaugos ir privatumo teisės aktus taikytinos garantijos.

V. **ES PRIVATUMO IR DUOMENŲ APSAUGOS TEISĖS AKTŲ TAIKYMAS**

36. ES duomenų apsaugos teisės aktai yra technologiškai neutralūs; pirmiau aprašyti konkretūs patikros metodai jais pačiais nereglamentuojama. E. privatumo direktyvoje reglamentuojamas privatumas teikiant

([24]) Kiekvieno protokolo antraštėje yra konkretūs laukai, kuriuose pateikiama papildoma informacija apie perduodamą pranešimą. Todėl šių laukų turinį galima vadinti pranešimo metaduomenimis. Šių laukų pavyzdys galėtų būti naudojamas jungties numeris, ir jeigu tas numeris yra, pvz., 80, gana tikėtina, kad pranešimo pobūdis yra naršymas tinkle.

([25]) Aišku, sekimo galimybes turi ne tik IPT. Ir reklaminių skelbimų tinklo paslaugų teikėjai, naudodami trečiųjų asmenų slapukus, gali sekti naudotojus įvairiose interneto svetainėse. Žr., pvz., neseniai paskelbtą mokslinį straipsnį, kuriame įrodyta, kad *Google* buvimas užfiksuotas 97 iš 100 populiariausių interneto svetainių, o tai reiškia, kad *Google* gali sekti trečiųjų asmenų slapukų neatsisakiusius naudotojus jiems naršant šiose populiariose interneto svetainėse. Žr. Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan ir Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (2011 m. liepos 29 d.). Galima rasti SSRN: http://ssrn.com/abstract=1898390 Naudotojų sekimo naudojant trečiųjų asmenų slapukus nagrinėjo 29 straipsnio darbo grupė. Žr. 2010 m. birželio 22 d. priimtą nuomonę 2/2010 dėl vartotojų elgesiu grindžiamos internetinės reklamos (WP 171).

elektroninių pranešimų paslaugas viešuosiuose tinkluose (paprastai interneto prieigos ir telefonijos) ([26]), o Duomenų apsaugos direktyvoje reglamentuojamas duomenų tvarkymas apskritai. Visuose šiuose teisės aktuose nustatomi skirtingi įpareigojimai, taikomi srauto ir pranešimų duomenis tvarkantiems ir stebintiems IPT.

V.1. **Srauto ir turinio duomenų tvarkymo teisiniai pagrindai**

37. Pagal duomenų apsaugos teisės aktus asmens duomenų tvarkymui, o šiuo atveju – srauto ir pranešimų duomenų tvarkymui reikalingas tinkamas teisinis pagrindas. Be šio bendrojo reikalavimo, tam tikrais atvejais gali būti taikomi specialieji reikalavimai.

38. Šiuo atveju IPT tvarkomų asmens duomenų pobūdis susijęs su srauto duomenimis ir pranešimų turiniu. Pranešimų turinys ir srauto duomenys yra saugomi teisės į susirašinėjimo konfidencialumą, užtikrinamą EŽTK 8 straipsnyje ir Chartijos 7 bei 8 straipsniuose. E. privatumo direktyvos 5 straipsnio „Pranešimų konfidencialumas“ 1 dalyje reikalaujama, kad valstybės narės užtikrintų pranešimų ir susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai prieinamas elektroninių ryšių paslaugas, konfidencialumą. Kartu E. privatumo direktyvos 5 straipsnio 1 dalyje numatyta, kad IPT tam tikromis aplinkybėmis gali būti leidžiama tvarkyti srauto ir turinio duomenis, jeigu naudotojai sutinka. Tuo tikslu nustatytas draudimas „be atitinkamų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti bei stebėti pranešimus ir su jais susijusius srauto duomenis, išskyrus atvejus, kai tai galima teisėtai daryti pagal 15 straipsnio 1 dalį“. Šis klausimas plačiau nagrinėjamas toliau.

39. E. privatumo direktyvoje numatytas ne tik atitinkamų naudotojų sutikimas, bet ir kiti pagrindai, kuriems esant IPT srauto ir pranešimų duomenų tvarkymas gali būti laikomas teisėtu. Atitinkami tvarkymo teisiniai pagrindai šiuo atveju yra: i) paslaugos teikimas; ii) paslaugos saugumo užtikrinimas ir iii) kuo didesnis perkrovos mažinimas. Kiti galimi pagrindai srauto ar pranešimų duomenimis grindžiamai valdymo politikai įteisinti aptariami toliau iv punkte.

i) Teisiniai paslaugos teikimo pagrindai

40. Kaip parodyta IV skyriuje, IPT tvarko IP antraščių informaciją, kad nukreiptų kiekvieną IP paketą į jo paskirties vietą. E. privatumo direktyvos 6 straipsnio 1 ir 2 dalyse pranešimui perduoti leidžiama tvarkyti srauto duomenis. Todėl IPT gali tvarkyti informaciją, kuri yra būtina paslaugai suteikti.

ii) Paslaugos saugumo užtikrinimo teisiniai pagrindai

41. Pagal E. privatumo direktyvos 4 straipsnį IPT turi bendrą pareigą imtis atitinkamų priemonių savo teikiamų paslaugų saugumui užtikrinti. Virusų filtravimo praktika gali būti susijusi su IP antraščių ir IP naudingųjų duomenų tvarkymu. Atsižvelgiant į tai, kad E. privatumo direktyvos 4 straipsnyje iš IPT reikalaujama užtikrinti tinklo saugumą, šioje nuostatoje įteisinama IP antraštėmis ir turiniu grindžiami patikros metodai, kuriais siekiama pasiekti griežtai tokį tikslą. Praktiškai tai reiškia, kad per laikotarpį, nustatytą laikantis proporcingumo principo (žr. V skyriaus 3 dalį), IPT gali stebėti ir filtruoti pranešimų duomenis, siekdami kovoti su virusais ir apskritai užtikrinti tinklo saugumą ([27]).

([26]) E. privatumo direktyvos 10 konstatuojamoji dalis suformuluota taip: „Elektroninių ryšių sektoriuje Direktyva 95/46/EB pirmiausia taikoma visiems pagrindinių teisių ir laisvių apsaugos klausimams, kuriems nėra konkrečiai taikomos šios direktyvos nuostatos, įskaitant valdytojo įsipareigojimus ir fizinių asmenų teises. Direktyva 95/46/EB taikoma neviešųjų ryšių paslaugoms.“ Be to, 17 konstatuojamoji dalis yra svarbi duomenų subjekto sutikimo požiūriu: „Šioje direktyvoje abonento ar naudotojo, ir fizinio, ir juridinio asmens, sutikimas turėtų būti apibrėžiamas taip, kaip ir duomenų subjekto sutikimas buvo apibrėžtas ir patikslintas Direktyvoje 95/46/EB.“

([27]) 2006 m. vasario 21 d. priimta 29 straipsnio darbo grupės nuomonė 2/2006 apie privatumo klausimus, susijusius su elektroninio pašto tikrinimo paslaugų teikimu (WP 118). Toje nuomonėje darbo grupė mano, kad filtrų naudojimas taikant 4 straipsnį gali būti suderinamas su E. privatumo direktyvos 5 straipsniu.

iii) Perkrovos padarinių sumažinimo teisiniai pagrindai

42. Šio teisinio pagrindo *motyvas* nurodytas E. privatumo direktyvos 22 konstatuojamojoje dalyje, paaiškinant 5 straipsnio 1 dalyje numatytą pranešimų saugojimo draudimą. Tai nereiškia, kad draudžiamas automatiškas, tarpinis ir laikinas saugojimas, jeigu tai vyksta vieninteliu perdavimo atlikimo tikslu ir netrunka ilgiau nei būtina perdavimo ir tinklo valdymo tikslais ir išlieka užtikrinama pranešimų konfidencialumas.

43. Perkrovos atveju kyla klausimas, ar IPT gali svarstyti galimybę kartais nutraukti ar uždelsti srautą, ar veikiau sulėtinti pranešimus, kuriems laikas nėra toks svarbus, pvz., P2P arba e. laiškų srautą, ir leisti balso srautui būti perduotam priimtinos kokybės.

44. Atsižvelgiant į bendrą visuomeninį interesą užtikrinti naudotiną ryšių tinklą, IPT gali teigti, kad srauto prioritetizavimas arba kliudymas jam sprendžiant perkrovos problemas yra teisėta priemonė, būtina tinkamai paslaugai suteikti. Tai reiškia, kad tokiais atvejais ir tokiam tikslui būtų bendras teisinis pagrindas tvarkyti asmens duomenis ir nereikėtų specialaus naudotojų sutikimo.

45. Kartu tokio kišimosi galimybė nėra neribota. Jeigu IPT reikia patikrinti pranešimus, konfidencialumo požiūriu ir griežtai taikant proporcingumo principą jie privalo taikyti mažiau ribojamą metodą, kuriuo galima pasiekti tikslą (vengdami išsamiosios paketinės patikros) ir privalo jį taikyti tik tiek, kiek reikia perkrovos problemai išspręsti.

iv) Teisiniai pagrindai tvarkyti duomenis kitais tikslais

46. IPT taip pat gali pageidauti tikrinti srauto ir turinio duomenis kitais tikslais, pvz., siūlydami tikslinius abonementus (pvz., abonementą, pagal kurį ribojama prieiga prie P2P, arba abonementą, pagal kurį kai kurioms programoms suteikiamas didesnis greitis). Patikra ir tolesnis srauto ir pranešimų duomenų naudojimas kitais tikslais nei paslaugos teikimas ar jos saugumo užtikrinimas ir perkrovos pašalinimas leidžiamas tik esant griežtoms sąlygoms, laikantis teisės aktų.

47. Teisinis pagrindas iš esmės yra E. privatumo direktyvos 5 straipsnio 1 dalis, kurioje reikalaujama naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti bei stebėti pranešimus ir su jais susijusius srauto duomenis. Praktiškai tai reiškia, kad su pranešimu susijusių naudotojų sutikimas yra būtinas ir srauto, ir pranešimo duomenų tvarkymui pagal 5 straipsnio 1 dalį įteisinti.

48. Kaip jau paaiškinta, patikros ir filtravimo metodų taikymas grindžiamas IP antraštėmis, sudarančiomis srauto duomenis, arba išsamiąja paketine patikra, kuri taip pat apima IP naudinguosius duomenis ir sudaro pranešimo duomenis. Todėl iš esmės tokių metodų taikymas kitais tikslais nei paslaugos suteikimas ar saugumas būtų draudžiamas, nebent tvarkymas galimas esant teisėtam pagrindui, pvz., sutikimui (5 straipsnio 1 dalis). 5 straipsnio 1 dalies taikymo pavyzdys būtų, kai IPT nusprendžia siūlyti klientams mažesnį interneto prieigos tarifą mainais į elgsena grindžiamos reklamos gavimą, šiuo tikslu naudojant išsamiąją paketinę patikrą, taigi, ir pranešimų duomenis. Todėl pagal 5 straipsnio 1 dalį būtinas tikras, konkretus ir informacija pagrįstas sutikimas.

49. Be to, E. privatumo direktyvos 6 straipsnyje „Srauto duomenys“ numatytos tam tikros taisyklės, taikomos būtent srauto duomenims. Konkrečiau kalbant, jame numatyta galimybė IPT tvarkyti srauto

duomenis remiantis naudotojo sutikimu gauti pridėtinės vertės paslaugas ([28]). Šioje nuostatoje nustatytas 5 straipsnio 1 dalyje numatytas sutikimo reikalavimas, jeigu kalbama apie srauto duomenis.

50. Praktiškai gali būti ne visada lengva išsiaiškinti, pvz., kokiais atvejais sutikimas yra būtinas ir kokiais atvejais tinklo saugumas gali būti teisėtas pagrindas tvarkyti duomenis, visų pirma jeigu patikros metodais siekiama dvejopų tikslų (pvz., išvengti perkrovos ir teikti pridėtinės vertės paslaugas). Reikėtų pabrėžti, kad sutikimo negalima laikyti lengvu ir sisteminiu būdu laikytis duomenų apsaugos principo.

51. Kol kas yra mažai teisės aktų taikymo patirties, visų pirma tai susiję su įvairiais pirmiau aprašytais aspektais. Tai yra ta sritis, kurioje reikalingos papildomos rekomendacijos, kaip aprašyta VI skyriuje. Be to, yra papildomų svarbių aspektų, susijusių su sutikimo gavimu, ir juos reikia specialiai apsvarstyti. Jie aprašomi toliau.

V.2. **Klausimai, susiję su informacija pagrįsto sutikimo davimu kaip teisiniu pagrindu**

52. Pagal E. privatumo direktyvos 5 ir 6 straipsnius reikalaujamas sutikimas turi tokią pačią reikšmę kaip duomenų subjekto sutikimas, apibrėžtas ir papildomai detalizuotas Direktyvoje 95/46/EB ([29]). Pagal Duomenų apsaugos direktyvos 2 straipsnio h punktą „duomenų subjekto sutikimas“ reiškia „bet kurį savanoriškai ir žinomai duotą konkretų duomenų subjekto pareiškimą, kuriuo duomenų subjektas nurodo savo sutikimą, kad būtų tvarkomi su juo susiję duomenys“. Neseniai sutikimo vaidmenį ir jo galiojimo reikalavimus savo nuomonėje 15/2011 dėl sutikimo ([30]) nagrinėjo 29 straipsnio darbo grupė.

53. Todėl IPT, reikalaujantys sutikimo tikrinti ir filtruoti srauto bei turinio duomenis, turi užtikrinti, kad sutikimas būtų laisvai duotas ir konkretus, tai turi būti visiškai sąmoningas asmens valios išreiškimas, kuriuo jis išreiškia savo sutikimą dėl su juo susijusių asmens duomenų tvarkymo. Tai patvirtinama E. privatumo direktyvos 17 konstatuojamojoje dalyje: „(…) Sutikimas gali būti duotas bet kuriuo tinkamu būdu, specialiu ir pakankamai informatyviu, leidžiančiu naudotojui laisvai išreikšti savo valią, įskaitant ir atitinkamame interneto tinklavietės langelyje dedamą varnelę.“ Toliau pateikiami kai kurie praktiniai pavyzdžiai, ką šiomis aplinkybėmis reiškia laisvai duotas, konkretus ir informacija pagrįstas sutikimas.

Sutikimas. Laisvas, konkretus ir informacija pagrįstas valios išreiškimas

54. *Laisvai duotas sutikimas*. Naudotojai neturėtų patirti suvaržymų, susiejant sutikimą su interneto paslauga, kuriai gauti jie nori užsiregistruoti.

55. Asmenų sutikimas nebus duotas laisvai, jeigu jiems teko sutikti dėl jų pranešimų duomenų stebėjimo, kad gautų pranešimų paslaugą. Tai juo labiau pasakytina tuo atveju, jeigu *visi* konkrečioje rinkoje veikiantys paslaugų teikėjai įgyvendintų srauto valdymą tikslais, kurie apimtų daugiau nei tinklo saugumo užtikrinimas. Vienintelė prieinama galimybė būtų apskritai nesiregistruoti interneto paslaugos

([28]) Direktyvos 18 konstatuojamojoje dalyje pateikiamas pavyzdinis pridėtinės vertės paslaugų sąrašas. Nėra aišku, ar paslaugos, kurioms taikoma srauto valdymo politika, galėtų būti laikomos įtrauktomis į tą sąrašą. Srauto valdymo politika, kuria siekiama prioritetizuoti tam tikrą turinį, galėtų būti suprantama kaip užtikrinanti paslaugos kokybę. Pavyzdžiui, srauto valdymas, kurį įgyvendinant tvarkomos tik IP antraštės ir kurio tikslas – siūlyti geriausios kainos lošimų paslaugas, kai naudotojų asmeninis lošimų srautas prioritetizuojamas per tinklą, galėtų būti laikomas pridėtinės vertės paslauga. Kita vertus, visai neaišku, ar srauto valdymas tam tikriems srautams stabdyti, pvz., P2P srautui lėtinti, galėtų būti tokiu laikomas.

([29]) Žr. E. privatumo direktyvos 17 konstatuojamąją dalį ir 2 straipsnio f punktą.

([30]) Priimta 2011 m. liepos 13 d. (WP 187).

abonentu. Kadangi internetas yra tapęs esmine darbo ir laisvalaikio priemone, interneto paslaugos abonemento neįsigijimas nėra teisėta alternatyva. Dėl to asmenys neturėtų realaus pasirinkimo, t. y. jie negalėtų laisvai duoti sutikimo ([31]).

56. EDAPP mano, kad Komisijai ir nacionalinėms institucijoms aiškiai reikia stebėti rinką, visų pirma siekiant nustatyti, ar šis scenarijus, t. y. tai, kad paslaugų teikėjai susieja telekomunikacijų paslaugas su pranešimų stebėjimu, tampa bendra tendencija. Paslaugų teikėjai turėtų siūlyti alternatyvias paslaugas, įskaitant interneto abonementą, kuriam nenustatyta srauto valdymo sąlyga, ir dėl to netaikyti asmenims didesnių mokesčių.

57. *Konkretus sutikimas.* Dėl konkretaus sutikimo būtinybės šiuo atveju reikia, kad IPT aiškiai ir matomai gautų sutikimą dėl srauto ir pranešimų tvarkymo. 29 straipsnio darbo grupės teigimu, „(…) kalbant konkrečiai, sutikimas turi būti suprantamas: jis turėtų aiškiai ir tiksliai nurodyti duomenų tvarkymo apimtį ir padarinius. Jis negali būti taikomas neapibrėžtai tvarkymo veiklai. Kitaip tariant, tai reiškia, kad sutikimo taikymo aplinkybės yra ribotos.“ Konkretus sutikimas mažai tikėtinas, jeigu sutikimas atlikti srauto ir pranešimų patikrą yra „susietas“ su bendru sutikimu įsigyti paslaugos abonementą. Kaip tik konkretumas reiškia tikslinių priemonių naudojimą sutikimui gauti, pvz., konkrečios sutikimo formos ar atskiro langelio, aiškiai skirto stebėjimo tikslui, pateikimą (o ne informacijos įtraukimą į bendrąsias sutarties sąlygas ir reikalavimą pasirašyti tokią sutartį, kokia yra).

58. *Informacija pagrįstas sutikimas.* Kad sutikimas galiotų, jis turi būti pagrįstas informacija. Poreikis pateikti tinkamą išankstinę informaciją kyla ne tik iš E. privatumo direktyvos ir Duomenų apsaugos direktyvos, bet ir iš Universaliųjų paslaugų direktyvos, iš dalies pakeistos Direktyva 2009/136/EB ([32]), 20 ir 21 straipsnių. Informacijos ir sutikimo poreikis aiškiai patvirtintas Direktyvos 2009/136/EB 28 konstatuojamojoje dalyje: „Tokia informacija teikėjo pasirinkimu turėtų apimti arba atitinkamo turinio, programos ar paslaugos rūšį, arba atskiras programas ar paslaugas, arba abu šiuos dalykus.“ Paskui joje nurodoma, kad „priklausomai nuo naudojamų technologijų ir apribojimų, siekiant taikyti šiuos apribojimus, galima reikalauti paslaugų gavėjo sutikimo, kaip numatyta Direktyvoje 2002/58/EB“.

59. Atsižvelgiant į tokių stebėjimo metodų sudėtingumą, reikšmingos išankstinės informacijos pateikimas yra viena didžiausių problemų, norint gauti galiojantį sutikimą. Vartotojai turėtų būti informuojami taip, kad galėtų suprasti tvarkomą informaciją, kaip ji naudojama, poveikį naudotojo patirčiai ir su metodais susijusį privatumo ribojimo lygį.

60. Tai reiškia ne tik tai, kad pati informacija turi būti aiški ir suprantama paprastiems naudotojams, bet ir tai, kad informacija turi būti teikiama tiesiogiai asmenims akivaizdžiu būdu, kad jie ją pastebėtų.

61. *Valios išreiškimas.* Pagal taikytinus teisės aktus sutikimui taip pat būtini patvirtinamieji naudotojo veiksmai, kuriais jis išreiškia savo sutikimą. Numanomas sutikimas šio reikalavimo neatitiktų. Tai taip pat patvirtina poreikį taikyti specialias priemones sutikimui gauti, kad taikydami srauto valdymo politiką IPT galėtų tikrinti srauto ir pranešimų duomenis. Neseniai priimtoje nuomonėje dėl sutikimo 29 straipsnio darbo grupė pabrėžė detalumo poreikį gaunant sutikimą, susijusį su įvairiais duomenų tvarkymą sudarančiais elementais.

([31]) Panašus atvejis susijęs su PNR duomenimis, kai buvo diskutuojama, ar keleivių sutikimas perduoti rezervacijos duomenis JAV institucijoms yra galiojantis. Darbo grupės nuomone, keleivių sutikimas negali būti duotas laisvai, nes oro susisiekimo bendrovės privalo siųsti duomenis prieš skrydį, todėl keleiviai neturi realaus pasirinkimo, jeigu nori skristi 29 straipsnio darbo grupės nuomonė 6/2002 dėl akivaizdžios keleivių informacijos ir kitų duomenų siuntimo iš oro susisiekimo bendrovių Jungtinėms Valstijoms.

([32]) 2009 m. lapkričio 25 d. direktyva 2009/136/EB, iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis (žr. 15 išnašą).

62. Būtų galima teigti, kad jeigu su pranešimu susijusios šalys nenori IPT įsikišimo srauto valdymo politikos taikymo tikslu, jos visada gali pranešimą užšifruoti. Šis požiūris gali būti laikomas naudingu praktiniu požiūriu, tačiau jam įgyvendinti reikalingos tam tikros pastangos ir techninės žinios, be to, jo negalima laikyti panašiu į laisvai duotą, konkretų ir informacija pagrįstą sutikimą. Be to, naudojant šifravimo metodus, nėra užtikrinamas visiškas pranešimo konfidencialumas, nes IPT bent jau galės gauti IP antraštės informaciją, kad nukreiptų pranešimą, jie taip pat galės taikyti statistikos analizę.

63. Pagal E. privatumo direktyvos 5 straipsnio 1 dalį sutikimas turi būti gautas iš atitinkamų naudotojų. Daugeliu atvejų naudotojas ir abonentas bus tas pats asmuo, todėl sutikimas galimas įsigyjant telekomunikacijų paslaugos abonentą. Kitais atvejais, įskaitant tuos, kai gali dalyvauti daugiau negu vienas asmuo, atitinkamų naudotojų sutikimą reikės gauti atskirai. Dėl to gali kilti toliau nurodytų praktinių klausimų.

Visų atitinkamų naudotojų sutikimas

64. 5 straipsnio 1 dalyje numatyta, kad naudotojo sutikimas įteisina duomenų tvarkymą. Turi būti gautas *visų* su pranešimu susijusių *naudotojų* sutikimas. Šis reikalavimas *pagrįstas tuo*, kad pranešimas paprastai susijęs bent su dviem asmenimis (siuntėju ir gavėju). Pavyzdžiui, jeigu IPT nuskenuoja IP naudinguosius duomenis, susijusius su e. laišku, jie tikrina informaciją, susijusią ir su e. laiško siuntėju, ir su gavėju.

65. Stebint ir perimant srautą ir pranešimus (pvz., tam tikrą tinklo srautą) IPT gali pakakti gauti naudotojo, t. y. abonento, sutikimą. Taip yra todėl, kad kita pranešimo šalis, šiuo atveju – interneto svetainė, kurioje lankytasi, nelaikoma „atitinkamu naudotoju“ ([33]). Tačiau padėtis gali būti sudėtingesnė, jeigu toks stebėjimas apima e. laiškų turinio, taigi, ir e. laiško siuntėjo ir gavėjo asmeninės informacijos patikrą, o šie abu asmenys gali būti ir nesusiję sutartiniais santykiais su tuo pačiu IPT. Iš tikrųjų tokiais atvejais IPT tvarkytų ne savo klientų asmens duomenis (vardą, e. pašto adresą ir galbūt neskelbtinus turinio duomenis). Praktiniu požiūriu gauti tokių asmenų sutikimą gali būti sunkiau, nes tai turėtų būti daroma kiekvienu konkrečiu atveju, o ne sudarant sutartį dėl telekomunikacijų paslaugos teikimo. Be to, nebūtų realu daryti prielaidos, kad abonentas davė sutikimą ir kitų naudotojų vardu, kaip dažnai gali būti privačiuose namų ūkiuose.

66. Tokiomis aplinkybėmis EDAPP mano, kad IPT turėtų laikytis esamų teisinių reikalavimų ir įgyvendinti politiką, neapimančią informacijos stebėjimo ir patikros. Tai dar svarbiau, atsižvelgiant į ryšių paslaugas, susijusias su trečiaisiais asmenimis, negalinčiais duoti sutikimo dėl stebėjimo, visų pirma tai pasakytina apie siunčiamus ir gaunamus e. laiškus (tai netaikoma, jeigu tikslas grindžiamas saugumo motyvais).

67. Kartu reikėtų pažymėti, kad nacionalinė teisė, kuria įgyvendinama E. privatumo direktyvos 5 straipsnio 1 dalis, šiuo atžvilgiu ne visada gali būti tinkama ir kad apskritai atrodo, jog veikiau būtinos geresnės rekomendacijos dėl E. privatumo direktyvos šios srities reikalavimų. Todėl EDAPP ragina Komisiją šioje srityje būti aktyvesnei ir imtis iniciatyvos, prie kurios galėtų prisidėti ir priežiūros institucijos, dalyvaujančios 29 straipsnio darbo grupėje, bei kiti suinteresuotieji subjektai. Prireikus reikėtų kreiptis į Teisingumo Teismą, siekiant iki galo išsiaiškinti 5 straipsnio 1 dalies reikšmę ir padarinius.

([33]) Nepaisant tų atvejų, kai tinklo srautas apima asmeninės informacijos, kaip antai, fizinių asmenų, kurių tapatybę galima nustatyti, nuotraukų, paskelbtų interneto svetainėje, perdavimą. Tokios informacijos tvarkymui reikalingas teisinis pagrindas, tačiau jam nebus taikoma 5 straipsnio 1 dalis, nes šie asmenys nebūtų laikomi „atitinkamais naudotojais“.

V.3. **Proporcingumas, duomenų minimizavimo principas**

68. Duomenų apsaugos direktyvos 6 straipsnio c punkte nustatytas proporcingumo principas ([34]), taikomas IPT, nes jie pagal direktyvą yra duomenų valdytojai, kai vykdo stebėjimo ir filtravimo veiklą.

69. Pagal šį principą asmens duomenys gali būti tvarkomi tik tiek, kiek jie yra „adekvatūs, susiję ir savo apimtimi neviršijantys tikslų, kuriems jie renkami ir (arba) vėliau tvarkomi“. Šio principo taikymas susijęs su poreikiu įvertinti, ar duomenų tvarkymui taikomos priemonės ir naudojami asmens duomenys yra tinkami ir gali būti pagrįstai pasiekti jų tikslai. Jeigu prieinama prie išvados, kad duomenų renkama daugiau nei būtina, šis principas neįgyvendinamas.

70. Tam tikrų patikros metodų rūšių atitiktis proporcingumo principui turėtų būti vertinama kiekvienu konkrečiu atveju. Neįmanoma padaryti abstrakčios išvados. Tačiau galima pažymėti įvairius konkrečius aspektus, kuriuos reikėtų įvertinti vertinant atitiktį proporcingumo principui.

71. *Tvarkomos informacijos kiekis.* IPT klientų pranešimų stebėjimas kuo išsamiausiu būdu daugeliu atvejų bus perteklinis ir neteisėtas. Kadangi tai gali būti daroma taikant priemones, kurios asmenims nėra akivaizdžios, be to, jiems gali būti sunku suprasti, kas vyksta, didėja poveikis jų privatumui. IPT turėtų įvertinti, kokios mažiau ribojančios priemonės gali būti prieinamos reikalingam rezultatui pasiekti. Pavyzdžiui, ar IP antraščių stebėjimu gali būti pasiektas reikiamas rezultatas, užuot ėmusis išsamios paketinės patikros? Net ir taikant išsamią paketinę patikrą, būtiną informaciją galima gauti identifikavus tik tam tikrus protokolus. Reikšmę gali turėti ir duomenų apsaugos garantijų taikymas, įskaitant pseudo-anonimizavimą. Vertinimo rezultatas turi patvirtinti, kad duomenų tvarkymas yra proporcingas.

72. *Tvarkymo padariniai (tiesiogiai susiję su tikslais).* Proporcingumo gali nebūti tais atvejais, IPT taikant srauto valdymo politiką, pagal kurią neleidžiama gauti tam tikrų paslaugų ir kartu dėl to gaunama nauda sąžiningai nesidalijama su naudotojais.

73. Svarbu priminti, kad proporcingumo principas taikomas net ir tada, jeigu yra tenkinami kiti privalomieji teisiniai reikalavimai, įskaitant tai, ar IPT, pavyzdžiui, yra gavęs asmenų sutikimą turinio stebėjimui. Tai reiškia, kad duomenų tvarkymas, atliekamas stebint turinį, gali būti neteisėtas, jeigu juo pažeidžiamas pagrindinis proporcingumo principas.

V.4. **Saugumo ir organizacinės priemonės**

74. E. privatumo direktyvos 4 straipsnyje aiškiai reikalaujama, kad IPT imtųsi techninių ir organizacinių priemonių užtikrinti: i) kad asmens duomenys būtų prieinami tik įgaliotiems darbuotojams ir tik teisėtais tikslais; ii) asmens duomenų apsaugą nuo atsitiktinio ar neteisėto tvarkymo ir iii) įgyvendinti asmens duomenų tvarkymo saugumo politiką. Be to, pagal šį straipsnį nacionalinės kompetentingos institucijos gali atlikti šių priemonių auditą.

75. Be to, pagal E. privatumo direktyvos 4 straipsnio 3 ir 2 dalis IPT taip pat turi pareigą pranešti atitinkamoms kompetentingoms institucijoms duomenų saugumo pažeidimo atveju, taip pat paveiktiesiems asmenims, jeigu atskleidimas gali jiems turėti neigiamų padarinių.

76. Tvarkydami į pranešimus įtrauktą asmeninę informaciją, siekdami taikyti srauto valdymo politiką, IPT gali gauti prieigą prie duomenų, kurie yra dar labiau neskelbtini nei srauto duomenys.

([34]) Kaip nurodyta pirmiau, Duomenų apsaugos direktyva taikoma visiems klausimams, susijusiems su pagrindinių teisių ir laisvių apsauga, jeigu jiems specialiai netaikoma E. privatumo direktyva.

77. Todėl IPT sukurta saugumo politika turėtų apimti konkrečias garantijas, kuriomis būtų užtikrinama, kad taikomos priemonės tinkamos šioms grėsmėms. Kartu nacionalinės kompetentingos institucijos, atliekančios tokių priemonių auditą, turėtų būti itin reiklios. Galiausiai reikėtų užtikrinti, kad būtų įgyvendintos veiksmingos pranešimo procedūros, siekiant informuoti duomenų subjektus, kurių informacijos saugumui pakenkta ir kurie dėl to gali patirti neigiamų padarinių.

VI. **POLITIKOS IR TEISĖKŪROS PRIEMONIŲ SIŪLYMAI**

78. Srauto duomenimis ir IP naudingųjų duomenų, t. y. pranešimo turinio, patikra grindžiama patikros metodai gali atskleisti naudotojų veiklą internete – interneto svetaines, kuriose lankytasi, veiklą jose, P2P programų naudojimą, parsisiųstas rinkmenas, išsiųstus ir gautus e. laiškus, kas juos siuntė, kokia tema ir kokiomis sąlygomis ir pan. IPT gali norėti panaudoti šią informaciją kai kuriems pranešimams, pvz., vaizdo rinkmenoms pagal pareikalavimą prioritetizuoti. Jie gali norėti panaudoti šią informaciją virusams identifikuoti arba profiliams kurti elgsena grindžiamos reklamos tikslais. Tokiais veiksmais ribojama teisė į ryšių konfidencialumą.

79. Atsižvelgiant į taikomus metodus ir atvejo ypatybes, poveikis privatumui didės. Kuo išsamiau perimama ir analizuojama surinkta informacija, tuo labiau tai prieštarauja ryšių konfidencialumo principui. Stebėjimo tikslai ir taikomos duomenų apsaugos garantijos taip pat yra esminiai dalykai nustatant kišimosi į asmenų privatumą ir asmens duomenis. Blokavimo ir stebėjimo, siekiant kovoti su kenkimo programine įranga, taikant griežtus apribojimus tikrinamų duomenų saugojimui ir naudojimui, negalima lyginti su atvejais, kai informacija yra registruojama individualiems profiliams kurti, kad šie būtų naudojami elgsena grindžiamai reklamai.

80. Iš esmės EDAPP mano, kad esami ES privatumo ir duomenų apsaugos teisės aktai, tinkamai aiškinami, taikomi ir įgyvendinami, būtų tinkami užtikrinti, kad teisė į konfidencialumą būtų išsaugota ir apskritai kad nebūtų pakenkta asmenų privatumo ir duomenų apsaugai ([35]). IPT neturėtų taikyti tokių mechanizmų, nebent jie tinkamai taiko teisės aktus. Konkrečiau kalbant, atitinkami teisės aktų elementai, į kuriuos IPT turėtų atsižvelgti ir kurių turėtų paisyti, apima tokius dalykus:

— IPT gali taikyti srauto valdymo politiką, kuria siekiama užtikrinti paslaugos saugumą ir suteikti paslaugą, įskaitant perkrovos ribojimą, pagal E. privatumo direktyvos 4 ir 6 straipsnius,

— IPT reikia dar vieno konkretaus teisinio pagrindo ir galbūt naudotojų sutikimo taikyti srauto valdymo politiką, susijusią su srauto ir (arba) pranešimų duomenų tvarkymu kitais tikslais nei pirmiau nurodytieji. Pavyzdžiui, informacija pagrįstas naudotojų sutikimas reikalingas asmenų pranešimams stebėti ir filtruoti, siekiant riboti (arba) leisti naudotis tam tikromis programomis ir paslaugomis, kaip antai P2P arba IP telefonijos,

— sutikimas turi būti duotas laisvai, aiškus ir pagrįstas informacija. Jis turėtų būti išreikštas patvirtinamaisiais veiksmais. Šie reikalavimai ypač susiję su poreikiu didinti pastangas užtikrinti, kad asmenys būtų tinkamai tiesiogiai, suprantamai ir konkrečiai informuojami, kad jie galėtų įvertinti veiklos padarinius ir galiausiai priimti informacija pagrįstą sprendimą. Atsižvelgiant į šių metodų sudėtingumą, reikšmingos išankstinės informacijos suteikimas naudotojams yra vienas svarbiausių uždavinių galiojančiam sutikimui gauti. Be to, neturėtų kilti žalingų padarinių (įskaitant finansines išlaidas) naudotojams, neišreiškusiems sutikimo stebėjimui,

([35]) Tai nepažeidžia poreikio keisti teisės aktus, remiantis kitais motyvais, visų pirma kai ES duomenų apsaugos teisės aktai yra bendrai persvarstomi siekiant, kad jie taptų veiksmingesni, atsižvelgiant į naujas technologijas ir globalizaciją.

— proporcingumo principui tenka esminis vaidmuo, IPT įgyvendinant srauto valdymo politiką, nepaisant duomenų tvarkymo teisinio pagrindo ir tikslo: teikiant paslaugą, vengiant perkrovos ar registruojant tikslinius abonementus, pagal kuriuos suteikiama arba nesuteikiama galimybė gauti tam tikras paslaugas ir programas. Pagal šį principą ribojama IPT galimybė stebėti asmenų pranešimų turinį ir taip tvarkyti perteklinę informaciją arba naudą gauti tik patiems IPT. Tai, ką logistiniu požiūriu galės daryti IPT, priklausys nuo naudojamų metodų įsibrovimo lygio, reikalaujamų rezultatų (dėl kurių jie gali gauti naudą) ir konkrečių taikomų privatumo ir duomenų apsaugos garantijų. Prieš diegdami patikros metodus, IPT privalo įvertinti, ar jie atitinka proporcingumo principą.

81. Nors dabar teisės aktuose yra numatytos atitinkamos sąlygos ir garantijos, ypatingą dėmesį reikia atkreipti į tai, ar IPT iš tikrųjų atitinka teisinius reikalavimus, ar jie teikia vartotojams būtiną informaciją, kad šie reikšmingai pasirinktų, ir ar jie paiso proporcingumo principo. Nacionaliniu lygmeniu pirmiau aprašytoje srityje kompetentingos institucijos apima nacionalines telekomunikacijų institucijas ir nacionalines duomenų apsaugos institucijas. ES lygmeniu tarp atitinkamų ES lygmens institucijų yra EERRI.

82. Be esamo reikalavimų įgyvendinimo lygio stebėjimo, atsižvelgiant į tai, kad masinė realiuoju laiku atliekama pranešimų patikra yra palyginti naujas dalykas, kai kuriuos šioje nuomonėje aptartus aspektus, susijusius su teisės aktų taikymu, reikia papildomai, išsamiau analizuoti ir labiau tikslinti. Ypač svarbios kelių sričių rekomendacijos apima:

— patikros praktikos, kuri yra teisėta sklandžiam srautui užtikrinti, kai gali nereikėti naudotojų sutikimo, pvz., kovojant su brukalais, nustatymą. Be to, svarbu yra ne tik tai, kiek taikomas stebėjimas riboja privatumą, bet ir tokie aspektai, kaip, pvz., kitu atveju atsirasiančių sklandaus srauto trukdžių lygis,

— nustatymą, kokie patikros metodai galėtų būti taikomi saugumo sumetimais, galbūt nereikalaujant naudotojų sutikimo,

— nustatymą, kada stebėjimui reikalingas asmens sutikimas, visų pirma visų atitinkamų naudotojų sutikimas, ir leistini techniniai parametrai, siekiant užtikrinti, kad taikant patikros metodus nereikėtų tvarkyti duomenų, kurių tvarkymas nėra proporcingas siekiamiems tikslams,

— be to, pirmiau aprašytais trimis atvejais gali reikėti rekomendacijų dėl būtinųjų duomenų apsaugos garantijų taikymo (tikslo ribojimo, saugumo ir kt.).

83. Kadangi šioje srityje kompetenciją turi ir valstybės narės, ir ES, EDAPP mano, kad dalijimasis nuomonėmis ir patirtimi, siekiant surasti suderintą požiūrį į pirmiau nurodytus dalykus turi esminę reikšmę. Kad tai būtų pasiekta, EDAPP siūlo sukurti platformą arba ekspertų grupę, kurioje dalyvautų nacionalinių reguliavimo institucijų, 29 straipsnio darbo grupės, EDAPP ir EERRI atstovai. Pirmasis tokios platformos tikslas būtų parengti rekomendacijas, bent jau pirmiau aprašytais klausimais, siekiant užtikrinti patikimą ir suderintą požiūrį bei vienodas veiklos sąlygas. EDAPP ragina Komisiją imtis šios iniciatyvos.

84. Ir galiausiai, nors tai ne mažiau svarbu, ir nacionalinės institucijos, ir ES institucijos bei įstaigos, įskaitant EERRI ir ES Komisiją, turi atidžiai analizuoti rinkos pokyčius šioje srityje. Duomenų apsaugos ir privatumo požiūriu scenarijus, pagal kurį IPT įprastai taikytų srauto valdymo politiką ir siūlytų abonementus, grindžiamus prieigos prie turinio ir programų filtravimu, būtų labai problemiškas. Jeigu kada nors taip nutiktų, reikėtų priimti teisės aktus tokiai padėčiai sureguliuoti.

VII. **IŠVADOS**

85. Tai, kad IPT vis dažniau taiko stebėjimo ir patikros metodus, turi įtakos interneto neutralumui ir ryšių konfidencialumui. Dėl to kyla svarbių klausimų, susijusių su naudotojų privatumo ir asmens duomenų apsauga.

86. Nors Komisijos komunikate dėl atviro interneto ir tinklo neutralumo Europoje šie klausimai trumpai aptariami, EDAPP mano, kad reikėtų imtis papildomų veiksmų, kad būtų pradėta taikyti tinkamesnė politika dėl to, kaip elgtis toliau. Todėl šioje nuomonėje jis prisidėjo prie tebevykstančių politinių diskusijų dėl tinklo neutralumo, visų pirma aspektais, susijusiais su duomenų apsauga ir privatumu.

87. EDAPP mano, kad nacionalinėms institucijoms ir EERRI reikia stebėti rinkos padėtį. Atliekant šį stebėjimą turėtų būti sudarytas aiškus vaizdas, apibūdinantis, ar rinkoje linkstama prie masinės, realiuoju laiku grindžiamos pranešimų patikros ir klausimų, susijusių su teisės aktų vykdymu.

88. Rinka neturėtų būti stebima neatlikus papildomos naujosios praktikos padarinių duomenų apsaugai ir privatumui internete analizės. Šioje nuomonėje apibrėžiamos kai kurios sritys, kurias reikėtų patikslinti. Nors tokios ES agentūros ir įstaigos, kaip EERRI, 29 straipsnio darbo grupė ir EDAPP, gali gerai patikslinti teisės aktų taikymo sąlygas, EDAPP mano, kad Komisija turi pareigą koordinuoti ir valdyti diskusijas. Todėl jis ragina Komisiją imtis iniciatyvos ir visus šiuos suinteresuotuosius subjektus suburti į platformą ar darbo grupę, kuri siektų tokio tikslo. Tarp tolesnei analizei skirtų klausimų reikėtų sureguliuoti tokius dalykus:

— nustatyti patikros praktiką, kuri yra teisėta, siekiant užtikrinti sklandų srautą ir kuri galėtų būti įgyvendinama saugumo sumetimais,

— nustatyti, kada stebėjimui reikalingas asmens sutikimas, visų pirma visų atitinkamų naudotojų sutikimas, ir leistinus techninius parametrus, siekiant užtikrinti, kad taikant patikros metodus nereikėtų tvarkyti asmens duomenų, kurių tvarkymas nėra proporcingas numatytam tikslui,

— pirmiau aprašytais atvejais gali reikėti rekomendacijų dėl būtinųjų duomenų apsaugos garantijų taikymo (tikslo ribojimo, saugumo ir kt.).

89. Atsižvelgiant į šias išvadas, gali reikėti papildomų teisėkūros priemonių. Tokiu atveju Komisija turėtų pateikti politikos priemones, kuriomis būtų siekiama stiprinti teisės aktus ir užtikrinti teisinį saugumą. Naujomis priemonėmis reikėtų patikslinti praktinius tinklo neutralumo padarinius, kaip tai jau yra padaryta keliose valstybėse narėse, ir užtikrinti, kad naudotojai galėtų iš tikrųjų pasirinkti, visų pirma priverčiant IPT siūlyti nestebimą sujungimą.

Priimta Briuselyje 2011 m. spalio 7 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas