I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o nevtralnosti omrežja, upravljanju prometa ter varstvu zasebnosti in osebnih podatkov

(2012/C 34/01)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 16 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah ter zlasti členov 7 in 8 Listine,

ob upoštevanju Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]),

ob upoštevanju Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov ([2]) ter zlasti člena 41(2) Uredbe,

ob upoštevanju Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ([3]) –

SPREJEL NASLEDNJE MNENJE:

I. **UVOD**

I.1. **Ozadje**

1. Komisija je 19. aprila 2011 sprejela Sporočilo o odprtem internetu in nevtralnosti omrežja v Evropi ([4]).

2. To mnenje je mogoče razumeti kot odziv na navedeno sporočilo, saj bi ENVP z njim rad prispeval k sedanji politični razpravi v EU o nevtralnosti omrežja, in sicer zlasti glede vidikov, ki so povezani z varstvom podatkov in zasebnostjo.

([1]) UL L 281, 23.11.1995, str. 31; v nadaljnjem besedilu: Direktiva o varstvu podatkov.
([2]) UL L 8, 12.1.2001, str. 1; v nadaljnjem besedilu: Uredba o varstvu podatkov.
([3]) UL L 201, 31.7.2002, str. 37, kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (Prim. opombo 15); v nadaljnjem besedilu: Direktiva o zasebnosti in elektronskih komunikacijah.
([4]) COM(2011) 222 konč.

3. Mnenje temelji na odgovoru ENVP ([5]) v okviru javnega posvetovanja Komisije o odprtem internetu in nevtralnosti omrežja v Evropi, ki je potekalo pred objavo njenega sporočila. ENVP je seznanjen tudi z nedavnim osnutkom sklepov Sveta o nevtralnosti omrežja ([6]).

I.2. **Pojem nevtralnosti omrežja**

4. Nevtralnost omrežja se nanaša na sedanjo razpravo, ali naj se ponudnikom internetnih storitev (v nadaljnjem besedilu: ponudniki ISP ([7])) dovoli, da omejijo, filtrirajo ali blokirajo dostop do interneta ali kako drugače vplivajo na njegovo delovanje. Pojem nevtralnosti omrežja temelji na stališču, da je treba informacije na internetu prenašati nepristransko, ne glede na vsebino, cilj ali vir, ter da morajo imeti uporabniki možnost odločanja, katere uporabniške programe, storitve in strojno opremo hočejo uporabljati. To pomeni, da ponudniki ISP ne morejo samovoljno prednostno obravnavati nekaterih uporabniških programov ali storitev ali upočasniti dostopa do njih, na primer za storitev vsak z vsakim (P2P), itd ([8]).

5. Filtriranje, blokiranje in pregledovanje mrežnega prometa sproža pomembna vprašanja, ki se pogosto spregledajo ali zanemarijo, in sicer so to vprašanja o zaupnosti komunikacij ter spoštovanju zasebnosti posameznikov in njihovih osebnih podatkov pri uporabi interneta. Tako na primer nekatere tehnike pregledovanja vključujejo spremljanje vsebine komunikacij, obiskanih spletnih strani, poslanih in prejetih elektronskih sporočil, časa, ko to poteka, itd., kar omogoča filtriranje komunikacij.

6. Ponudniki ISP lahko s pregledovanjem podatkov o komunikacijah kršijo zaupnost komuniciranja, ki je temeljna pravica, zagotovljena v členu 8 Evropske konvencije o človekovih pravicah in temeljnih svoboščinah (v nadaljnjem besedilu: EKČP) ter členih 7 in 8 Listine Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina). Zaupnost je zaščitena tudi v sekundarni zakonodaji EU, in sicer v členu 5 Direktive o zasebnosti in elektronskih komunikacijah.

I.3. **Usmeritev in struktura mnenja**

7. ENVP meni, da je treba v resni politični razpravi o nevtralnosti omrežja obravnavati zaupnost komunikacij ter druge posledice za zasebnost in varstvo podatkov.

8. To mnenje je prispevek k razpravi o tem, ki poteka v EU. Mnenje ima tri cilje:

— opozarja na pomen zasebnosti in varstva podatkov v sedanjih razpravah o nevtralnosti omrežja. Pri tem zlasti poudarja potrebo po upoštevanju veljavnih pravil o zaupnosti komunikacij. Dovoliti je treba samo prakse, pri katerih se upoštevajo ta pravila;

— nevtralnost omrežja se nanaša na relativno nove tehnološke možnosti, pri katerih ni veliko izkušenj z uporabo pravnega okvira. V tem mnenju so tako podane smernice, kako morajo ponudniki ISP uporabljati in upoštevati pravni okvir varstva podatkov pri morebitnem filtriranju, blokiranju ali pregledovanju omrežnega prometa. To bi moralo biti v pomoč tako ponudnikom ISP kot organom, ki so zadolženi za uveljavitev okvira;

— na področju varstva podatkov in zasebnosti to mnenje določa področja, ki jim je treba posvetiti posebno pozornost in na katerih bo mogoče potrebno ukrepanje na ravni EU. To je zlasti pomembno glede na sedanjo razpravo na ravni EU in politične ukrepe, ki jih lahko v tem okviru sprejme Komisija.

([5]) ENVP je v odgovoru poudaril, kako pomembno je upoštevati vprašanja varstva podatkov in zasebnosti skupaj z drugimi obstoječimi pravicami in vrednotami. Odgovor je na voljo na spletnem naslovu: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Na voljo na spletnem naslovu: http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) To vključuje zagotavljanje fiksnega in mobilnega dostopa do interneta.

([8]) Čeprav se to načelo ne uporablja za pravico ponudnikov ISP, da omejijo hitrost ali količino informacij, ki jih naročnik lahko pošlje ali sprejme v okviru naročniškega razmerja, ki vključuje omejitve pasovne širine ali količine. Tako lahko ponudniki ISP v skladu z načelom nevtralnosti omrežja še vedno ponujajo naročniška razmerja za dostop do interneta, pri katerih je dostop omejen na podlagi meril, kot so hitrost ali količina, če to ne pomeni diskriminacije v prid ali škodo določene vsebine.

9. ENVP se zaveda, da nevtralnost omrežja sproža tudi druga vprašanja, ki so natančneje predstavljena v nadaljevanju, na primer tista, povezana z dostopom do informacij. Obravnavana so samo toliko, kolikor so povezana z varstvom podatkov in zasebnostjo ter vplivajo nanju.

10. Mnenje je sestavljeno, kot je opisano v nadaljevanju. V oddelku II je najprej predstavljen kratek pregled praks, ki jih pri filtriranju uporabljajo ponudniki ISP. V oddelku III je predstavljen pravni okvir EU o nevtralnosti omrežja. Oddelek IV nato vsebuje tehnični opis, ki mu sledi ocena posledic za zasebnost glede na uporabljeno tehniko. V oddelku V so analizirane praktične podrobnosti v zvezi z uporabo sedanjega okvira EU o zasebnosti in varstvu podatkov. Na podlagi te analize oddelek VI vsebuje predloge za nadaljnji razvoj politike, v njem so opredeljena tudi področja, na katerih so mogoče potrebna dodatna pojasnila ali izboljšanje pravnega okvira. Oddelek VII vsebuje sklepne ugotovitve.

II. **NEVTRALNOST OMREŽJA IN POLITIKE UPRAVLJANJA PROMETA**

Vse večja razširjenost politik upravljanja prometa

11. Doslej so ponudniki ISP spremljali omrežni promet in posegali vanj samo v nekaterih redkih okoliščinah. Tako so na primer uporabili tehnike pregledovanja in omejevali pretok informacij zaradi ohranjanja varnosti omrežja, npr. zaradi boja proti virusom. Zato na splošno velja, da je internet rasel in ob tem ohranjal veliko stopnjo nevtralnosti.

12. V zadnjih letih pa je nekaj ponudnikov ISP izrazilo zanimanje za nadzor omrežnega prometa zaradi razlikovanja in uvajanja različnih politik, na primer blokiranja določenih storitev ali zagotavljanja prednostnega dostopa za nekatere. Ta pristop se imenuje tudi „politika upravljanja prometa“ ([9]).

13. Ponudniki ISP imajo najrazličnejše razloge za spremljanje in razlikovanje prometa. Tako jim lahko politika upravljanja prometa na primer pomaga upravljati promet med obdobji prezasedenosti, pri čemer bi na primer prednostno obravnavali nekatere oblike časovno občutljivega prometa, kot je videoprenos, in upočasnili druge vrste prometa, ki niso tako časovno občutljive, kot je storitev P2P ([10]). Poleg tega upravljanje prometa ponudnikom ISP lahko omogoča, da si zagotovijo tok prihodka, ki bi lahko prihajal iz različnih virov. Ponudniki ISP bi tako lahko po eni strani zaračunavali ponudnikom vsebin, na primer tistim, katerih storitve zahtevajo večjo pasovno širino, za zagotovitev prednostne obravnave (in torej hitrosti). To bi pomenilo, da bi bil dostop do nekaterih storitev, na primer storitve videa na zahtevo, hitrejši od dostopa do druge podobne storitve, za katero se ne plačuje visokohitrostni prenos. Prihodek bi bilo mogoče ustvarjati tudi na račun naročnikov, ki so pripravljeni plačevati višjo (ali nižjo) naročnino za nekatere vrste razlikovalnih naročniških razmerij. Tako bi bilo na primer naročniško razmerje, ki ne omogoča dostopa do storitve P2P, cenejše od naročniškega razmerja, ki omogoča neomejen dostop.

14. Interes, da ponudniki ISP uporabijo politiko upravljanja prometa, pa imajo lahko tudi drugi. Če ponudniki ISP upravljajo svoja omrežja in pregledujejo vsebine, ki se prenašajo prek njihovih zmogljivosti, bodo najbrž lažje odkrivali nezakonito uporabo, npr. kršitev avtorskih pravic ali pornografijo.

([9]) Glej na primer poročilo organa OFCOM z naslovom „Site blocking to reduce online copyright infringement“ (Blokiranje spletnih strani za zmanjšanje kršitev avtorskih pravic na spletu), ki je bilo sprejeto 27. maja 2011 in je na voljo na naslovu: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf:. „Nekateri ponudniki ISP v svojih omrežjih že uporabljajo paketne sisteme za upravljanje prometa in druge namene, zato domnevamo, da bi jih bilo mogoče uporabiti, čeprav to prinaša veliko zapletov in stroškov za tiste, ki še ne uporabljajo takšnih storitev. Mogoče se srednje- ali dolgoročno lahko celo pokaže, da bodo zaradi višine zahtevanega finančnega vložka sisteme DPI lahko uporabljali samo večji ponudniki ISP.“

([10]) Kakovost aplikacij v realnem času, kot je videoprenos, je med drugim odvisna od zakasnitve, tj. zamude, ki lahko nastopi zaradi prezasedenosti omrežja.

Drugi interesi, ki so ogroženi, vključno z varstvom podatkov in zasebnostjo

15. Zaradi tega trenda se je začela razprava, ali so tovrstne prakse upravičene in ali je treba nekatere obveznosti v zvezi z nevtralnostjo omrežja podrobneje opredeliti z zakonom.

16. Če bi ponudniki ISP začeli intenzivneje uporabljati politiko upravljanja prometa, bi lahko omejili dostop do informacij. Če bi takšno ravnanje postalo splošno uveljavljeno in uporabniki ne bi več mogli polno dostopati do interneta (ali pa bi bilo to zelo drago), bi jim omejili dostop do informacij, poleg tega ne bi več mogli pošiljati in prejemati želene vsebine z uporabniškimi programi ali storitvami po lastni izbiri. Tej težavi bi se lahko izognili z zakonsko predpisanim načelom nevtralnosti omrežja.

17. ENVP tako opozarja na vprašanje posledic za varstvo podatkov in zasebnost, kadar ponudniki ISP upravljajo promet. Natančneje:

— kadar ponudniki ISP obdelujejo podatke o prometu samo z namenom usmerjanja toka informacij od pošiljatelja k prejemniku, na splošno poteka omejena obdelava osebnih podatkov ([11]). Tako kot se pri navadnih poštnih storitvah obdelujejo informacije na pisemski ovojnici, ponudnik ISP obdeluje informacije, ki so potrebne za usmerjanje komunikacije k prejemniku. To ni v nasprotju z zakonskimi zahtevami o varstvu podatkov, zasebnosti in zaupnosti komunikacije;

— kadar pa ponudniki ISP pregledujejo podatke o komunikaciji, da bi razbrali vsak posamezni pretok komunikacije in izvajali posebne politike, ki so lahko neugodne za posameznike, so posledice večje. Glede na okoliščine v posameznem primeru in vrsto izvedene analize lahko obdelava močno posega v posameznikovo zasebnost in osebne podatke. To je še bolj očitno, kadar se v okviru politike upravljanja razkriva vsebina posameznikove komunikacije na internetu, vključno s poslanimi in prejetimi elektronskimi sporočili, obiskanimi spletnimi stranmi, datotekami, ki so bile prenesene na računalnik ali z njega, itd.

III. **PREGLED PRAVNEGA OKVIRA EU O NEVTRALNOSTI OMREŽJA IN NADALJNJI RAZVOJ POLITIKE**

III.1. **Kratek opis pravnega okvira**

18. Do leta 2009 zakonodajni instrumenti EU niso vsebovali določb, ki bi ponudnikom ISP izrecno prepovedovale filtriranje ali blokiranje oziroma dodatno zaračunavanje naročnikom za dostop do storitev. Poleg tega niso vsebovali določb, ki bi izrecno urejale tovrstna ravnanja. Položaj je bil tako nekoliko negotov.

19. Sveženj predpisov o telekomunikacijah iz leta 2009 je prinesel spremembo z vključitvijo določb v prid odprtosti interneta. Tako na primer člen 8(4) o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (v nadaljnjem besedilu: okvirna direktiva) nalaga regulativnim organom, da spodbujajo možnost, da končni uporabniki dostopajo do vsebine, uporabniških programov ali storitev po lastni izbiri ([12]). Ta določba se uporablja za omrežje v celoti, ne pa na ravni posameznih ponudnikov. V pred kratkem sprejetem osnutku sklepov Sveta je bila prav tako poudarjena potreba, da se ohrani odprtost interneta ([13]).

([11]) Iz tega so izključene operacije za povečanje varnosti omrežja in odkrivanje škodljivega prometa ter operacije, ki so potrebne za zaračunavanje in medsebojno povezovanje. Izključene so tudi obveznosti, ki izhajajo iz Direktive o hrambi podatkov, Direktive 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13.4.2006, str. 54) (v nadaljnjem besedilu: Direktiva o hrambi podatkov).

([12]) Direktiva 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve, kakor je bila spremenjena z Direktivo 2009/140/ES in Uredbo (ES) št. 544/2009, (UL L 337, 18.12.2009, str. 37).

([13]) Glej točko 3(e), v kateri Svet priznava: „potrebo po ohranitvi odprtosti interneta ob hkratni ohranitvi zagotavljanja visokokakovostnih storitev v okviru, ki spodbuja in spoštuje temeljne pravice, kot sta pravica do svobodnega izražanja in pravica do poslovanja“, in točko 8(d), v kateri poziva države članice, naj bo „cilj njihove politike spodbujanje odprtosti in nevtralnosti interneta“.

20. Direktiva o univerzalnih storitvah ([14]) vsebuje konkretnejše obveznosti. V členih 20 in 21 so določene zahteve po preglednosti v zvezi z omejitvami dostopa in/ali uporabo storitev in uporabniških programov. Zahteva tudi zagotavljanje minimalne ravni kakovosti storitev.

21. V zvezi z ravnanji ponudnikov ISP, ki vključujejo pregledovanje komunikacij posameznikov, uvodna izjava 28 Direktive o spremembi direktiv o univerzalnih storitvah ter zasebnosti in elektronskih komunikacijah ([15]) poudarja, da lahko „glede na uporabljeno tehnologijo in na vrsto omejitve takšne omejitve zahtevajo privolitev uporabnika v okviru Direktive o zasebnosti in elektronskih komunikacijah". Zato je v uvodni izjavi 28 poudarjena potreba po privolitvi v skladu s členom 5(1) Direktive o zasebnosti in elektronskih komunikacijah za vse omejitve na podlagi spremljanja komunikacij. V oddelku IV v nadaljevanju sta dodatno analizirana uporaba člena 5(1) ter splošni pravni okvir o varstvu podatkov in zasebnosti.

22. In nazadnje, člen 22(3) Direktive o univerzalnih storitvah zdaj pooblašča nacionalne regulativne organe, da za ponudnike ISP po potrebi opredelijo zahteve o minimalni kakovosti storitev, da bi preprečili upadanje kakovosti storitev ter oviranje ali upočasnitev prometa prek javnih omrežij.

23. To pomeni, da na ravni EU obstaja splošna tendenca po odprtem internetu (glej člen 8(4) okvirne direktive). Vendar pa ta politični cilj, ki se nanaša na omrežje kot celoto, ni neposredno povezan s prepovedmi ali obveznostmi posameznih ponudnikov ISP. To pomeni, da bi ponudnik ISP lahko uporabljal politiko upravljanja prometa, s katero bi lahko ukinil dostop do nekaterih uporabniških programov, če so končni uporabniki v celoti obveščeni ter so svobodno, izrecno in nedvoumno privolili v to.

24. Pri tem lahko obstajajo razlike med posameznimi državami članicami. V nekaterih lahko ponudniki ISP pod posebnimi pogoji uporabljajo politiko upravljanja prometa, na primer blokirajo uporabniške programe, kot je VoIP (v okviru cenejšega naročniškega razmerja za uporabo interneta), če so posamezniki svobodno, izrecno in nedvoumno privolili v to na podlagi ustrezne obveščenosti. Druge države članice so se odločile okrepiti načelo nevtralnosti omrežja. Tako je na primer nizozemski parlament julija 2011 sprejel zakon, s katerim na splošno prepoveduje ponudnikom, da ovirajo ali upočasnijo uporabniške programe ali storitve na internetu (na primer VoIP), razen če ni to potrebno zaradi omilitve vplivov prezasedenosti, zaradi ohranjanja celovitosti ali varnosti, zaradi boja proti vsiljeni pošti ali je v skladu s sodno odredbo ([16]).

III.2. **Sporočilo o nevtralnosti omrežja**

25. Evropska komisija je v svojem Sporočilu o nevtralnosti omrežja ([17]) ugotovila, da je treba položaj glede nevtralnosti omrežja spremljati in dodatno analizirati. To politiko so poimenovali „počakajmo, pa bomo videli", preden se začne razmišljati o nadaljnjih ureditvenih ukrepih.

([14]) Direktiva 2002/22/ES, kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov (UL L 337, 18.12.2009, str. 11). Primerjaj tudi člen 1(3), v katerem je navedeno, da direktiva niti ne dovoljuje niti ne prepoveduje, da ponudniki ISP omejujejo končnim uporabnikom dostop do storitev in aplikacij oziroma njihovo uporabo, če to dovoljuje nacionalna zakonodaja in je v skladu z zakonodajo Skupnosti, vendar pa določa obveznost dajanja informacij o teh pogojih.

([15]) Direktiva 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju med nacionalnimi organi, odgovornimi za izvrševanje zakonodaje o varstvu potrošnikov.

([16]) Nizozemska sprememba v izvirniku je na voljo na naslovu: https://zoek.officielebekendmakingen.nl/kst-32549-A.html V javnih občilih se kot razlog za takšno politično možnost niso navajali pomisleki v zvezi z varstvom podatkov in zasebnosti, temveč je bila odločitev utemeljena bolj s potrebo po zagotovitvi tega, da uporabniki ne izgubijo dostopa do informacij ali da ta ni omejen. Tako je ta sprememba očitno nastala zaradi vprašanj, povezanih z dostopom do informacij.

([17]) Prim. opombo 4.

26. Sporočilo Komisije je prineslo ugotovitev, da je treba vsak ukrep in nadaljnje ureditvene ukrepe podrobno proučiti z vidika varstva podatkov in zasebnosti. Tudi osnutek sklepov Sveta opozarja na vprašanja varstva podatkov in zasebnosti, ki jih to sproža ([18]).

27. Vprašanje, ki ga je treba proučiti z vidika varstva podatkov in zasebnosti, je, ali je politika „počakajmo, pa bomo videli", dovolj. Ker so v sedanjem okviru za varstvo podatkov in zasebnost predvideni nekateri zaščitni ukrepi, zlasti na podlagi načela zaupnosti komunikacij, je treba pozorno spremljati stopnjo skladnosti ter objavljati smernice glede več vidikov, ki niso posebno jasni. Poleg tega je treba razmisliti, kako bi bilo mogoče razjasniti in dodatno izboljšati okvir glede na tehnološki razvoj. Če se pri spremljanju pokaže, da se trg nagiba k množičnemu nadzoru komunikacij v realnem času, in se pojavijo vprašanja, povezana s skladnostjo z okvirom, bo treba sprejeti zakonodajne ukrepe. Konkretnejši predlogi v zvezi s tem bodo podani v oddelku VI.

IV. **TEHNIČNO OZADJE TER POSLEDICE ZA ZASEBNOST IN VARSTVO PODATKOV**

28. Pred natančnejšo obravnavo teme se je treba bolje seznaniti s tehnikami pregledovanja, ki jih lahko uporabijo ponudniki ISP pri upravljanju prometa, in vplivom, ki ga imajo lahko na načelo nevtralnosti omrežja. Posledice za zasebnost in varstvo podatkov, ki jih prinašajo te tehnike, se precej razlikujejo glede na uporabljeno(e) tehniko(e). To tehnično ozadje je potrebno za razumevanje in pravilno uporabo pravnega okvira za varstvo podatkov, opisanega v oddelku V. Treba pa je opozoriti, da je področje zapleteno in se stalno spreminja. Zaradi tega spodnji opis ni izčrpen in ne prikazuje najnovejšega stanja, temveč so v njem podane samo tehnične informacije, ki so nujne za razumevanje pravnih utemeljitev.

IV.1. **Prenos informacij prek interneta: osnove**

29. Kadar uporabnik prenaša komunikacijo prek interneta, se informacije, ki se pošiljajo, razdelijo v pakete. Ti paketi se pošiljajo prek interneta od pošiljatelja k prejemniku. Vsak paket med drugim vključuje informacije o viru in cilju. Poleg tega lahko ponudniki ISP v pakete vključijo v dodatne plasti in protokole ([19]), s katerimi se upravljajo različni prometni tokovi v omrežju ponudnika ISP.

30. Če se vrnemo k primerjavi s poštno pošiljko, bi lahko uporabo protokola za omrežni prenos ponazorili s tem, da vsebino pisma damo v ovojnico, nanjo napišemo naslov prejemnika, ki ga bodo prebrali na pošti, in nato pismo damo na pošto, da ga bo dostavila. Pošta lahko pri svojih internih prenosih uporabi dodatne protokole za obvladovanje vseh ovojnic, ki jih je treba poslati, pri čemer je cilj, da vsaka ovojnica doseže cilj v obliki, kot jo je prvotno sestavil pošiljatelj. Če uporabimo to primerjavo, lahko rečemo, da je vsak paket sestavljen iz dveh delov. Prvi je *koristna vsebina* IP, ki vključuje vsebino komunikacije in ustreza pismu. Ta del vsebuje informacije, ki so namenjene samo prejemniku. Drugi del paketa je *glava IP* in med drugim vključuje naslov prejemnika in pošiljatelja ter ustreza ovojnici. Glava IP ponudnikom ISP in drugim posrednikom omogoča, da usmerijo koristno vsebino z naslova vira na naslov cilja.

31. Ponudniki ISP in drugi posredniki zagotavljajo, da paketi IP potujejo po omrežju prek vozlišč, ki berejo informacije z glave IP, jih preverjajo glede na usmerjevalne table in jih nato pošljejo do naslednjega vozlišča na poti proti cilju. Ta proces poteka po celotnem omrežju z uporabo tako imenovanega

([18]) Prim. točko 4(e), v kateri Svet opozarja na „obstoj nekaterih pomislekov v zvezi z varstvom osebnih podatkov, ki jih navajajo predvsem organi za varstvo potrošnikov in podatkov."

([19]) Kot je podrobneje opisano v oddelku IV.2, takšni protokoli na dogovorjen način kodirajo informacije, ki se pošiljajo z enega konca na drugi, tako da se med seboj lahko razumejo stranke, vključene v komunikacijo. Ti protokoli so na primer HTTP, FTP itd.

pristopa „best effort memoryless“, saj se vsi paketi, ki prispejo na vozlišče, obravnavajo nevtralno. Ko se pošljejo na naslednje vozlišče, na usmerjevalniku ni več treba hraniti informacij ([20]).

IV.2. **Tehnike pregledovanja**

32. Kot je bilo prikazano, ponudniki ISP berejo glave IP, da jih usmerijo proti cilju. Prikazano pa je bilo tudi, da je mogoče analizirati promet (kar vključuje glave IP in koristne vsebine IP) za druge namene in z drugačnimi tehnologijami. Nove smernice tako lahko vključujejo upočasnitev nekaterih uporabniških programov, ki jih uporabljajo uporabniki, na primer P2P, po drugi strani pa povečanje hitrosti prometa za nekatere storitve, kot je video na zahtevo, za naročnike, ki plačujejo višjo naročnino. *Formalno gledano*, se pri vseh tehnikah pregledovanja izvaja pregledovanje paketov, vendar posamezne tehnike vključujejo različne stopnje poseganja. Obstajata dve glavni kategoriji tehnik pregledovanja. Ena temelji samo na glavi IP, druga pa tudi na koristni vsebini IP.

Na podlagi informacij v glavi IP. Pregled glave IP na paketu razkrije nekaj polj, ki lahko omogočajo ponudnikom ISP uporabo posebnih politik za upravljanje prometa. Pri teh tehnikah, ki temeljijo samo na pregledu glav IP, se podatki, ki so načeloma namenjeni usmerjanju informacij, obdelujejo za drugačen namen (tj. razlikovanje prometa). Ponudnik ISP lahko z vpogledom v izvorni naslov IP ta naslov poveže s konkretnim naročnikom in uporabi posebne politike, na primer usmerjanje paketa prek hitrejše ali počasnejše povezave. Ponudnik ISP lahko uporabi posebne politike tudi na podlagi vpogleda v ciljni naslov IP, na primer blokiranje ali filtriranje dostopa do nekaterih spletnih strani.

Na podlagi temeljitejšega pregleda. Temeljitejši pregled paketa omogoča ponudniku ISP dostop do informacij, ki so namenjene samo prejemniku komunikacije. Če to spet primerjamo z navadno pošto, bi pristop lahko opisali, kot da bi nekdo odprl kuverto in prebral pismo v njej ter tako analiziral vsebino komunikacije (zajete v paketih IP), da bi uporabil posebno omrežno politiko. Obstaja več načinov pregledovanja, pri čemer vsak pomeni drugačno grožnjo za posameznika, na katerega se nanašajo podatki.

— *Temeljit pregled paketa, ki temelji na analizi protokolov in statističnih evidencah*. Poleg protokola IP, ki naj bi omogočal prenos podatkov po internetu, obstajajo dodatni protokoli za dogovorjeno kodiranje informacij, ki se pošiljajo (prenos, seja, predstavitev in uporabniški program itd.). S temi protokoli se zagotavlja, da se strani, udeležene v komunikaciji, razumejo med seboj. Tako so na primer nekateri protokoli povezani z brskanjem po spletu ([21]), drugi so namenjeni prenosu datotek ([22]) itd. Zaradi tega je cilj tehnik pregledovanja, ki temeljijo na pregledovanju protokolov v kombinaciji s statističnimi analizami, iskanje posebnih vzorcev oziroma prstnih odtisov, ki določajo, kateri protokoli so prisotni ([23]). Te tehnike pregledovanja omogočajo ponudnikom ISP, da poznajo vrsto komunikacije (elektronska pošta, brskanje po spletu, nalaganje datotek) in, v nekaterih primerih, opredelijo posebno storitev ali uporabniški program, ki se uporablja. Tako je na primer pri nekaterih komunikacijah VoIP, pri katerih so uporabljeni protokoli značilni za konkretnega prodajalca ali ponudnika storitve. Ponudniki ISP lahko že samo na podlagi poznavanja vrste komunikacije uporabijo konkretne politike za upravljanje prometa. Tako lahko na primer blokirajo promet na spletu. To je lahko tudi prvi korak, ki ponudnikom ISP omogoča izvajanje nadaljnjih analiz, pri katerih je mogoče potreben poln dostop do metapodatkov in vsebine komunikacije.

([20]) V internetni omrežni opremi se kljub temu uporabljajo protokoli za usmerjanje, ki beležijo aktivnost, obdelujejo statistične podatke o prometu in si izmenjujejo informacije z drugo omrežno opremo, kar omogoča usmerjanje paketov IP po najbolj učinkoviti poti. Če je tako na primer povezava prezasedena ali ne deluje ter usmerjevalnik prejme to informacijo, dopolni svojo usmerjevalno tablo z drugo možnostjo, pri kateri ta povezava ni uporabljena. Opozoriti je treba tudi, da zbiranje in obdelava včasih potekata zaradi zaračunavanja pristojbin ali celo v skladu z zahtevami Direktive o hrambi podatkov.

([21]) HTTP – protokol za prenos hiperteksta – ali HTML – jezik za označevanje nadbesedila.

([22]) FTP – protokol za prenos datotek.

([23]) Uporabljene protokole je mogoče ugotoviti na različne načine. Tako je na primer mogoče iskati v posebnih poljih v notranjih protokolih, na primer za opredelitev vrat, ki so bila uporabljena za vzpostavitev komunikacije. Statistično oznako komunikacijskega toka je mogoče ugotoviti tudi na podlagi analize nekaterih posebnih polj, primerjav med protokoli, ki se uporabljajo hkrati med dvema naslovoma IP.

— *Temeljit pregled paketa na podlagi analize vsebine komunikacije.* Nazadnje je mogoče pregledati tudi metapodatke ([24]) in vsebino same komunikacije. Pri tej tehniki se prestrežejo vsi paketi IP, ki so del originalnega komunikacijskega toka, kar omogoča popolno rekonstrukcijo in analizo prvotne vsebine komunikacije. Tako je na primer za odkrivanje škodljivih ali nezakonitih vsebin, kot so virusi, otroška pornografija in podobno, za analizo treba rekonstruirati sámo vsebino. Treba je opozoriti, da udeležene strani včasih lahko izrecno šifrirajo s konca na konec, pri čemer ponudniki ISP ne morejo analizirati vsebine komunikacije.

IV.3. **Posledice za zasebnost in varstvo podatkov**

33. Tehnike pregledovanja, ki temeljijo na glavah IP, in zlasti tiste, ki temeljijo na pregledovanju paketov, vključujejo spremljanje in filtriranje teh podatkov ter imajo resne posledice za zasebnost in varstvo podatkov. Lahko so tudi v nasprotju s pravico do zaupnosti komunikacije.

34. Vpogled v komunikacijo ima že sam po sebi resne posledice za zasebnost in varstvo podatkov. Vendar je vprašanje še širše, saj so glede na cilj spremljanja in prestrezanja posledice za zasebnost lahko še večje. V bistvu ni enako, če kdo zgolj pregleduje komunikacije, da tako na primer zagotavlja delovanje sistema, ali če jih pregleduje zaradi izvajanja politik, ki vplivajo na posameznike. Kadar so politike glede prometa in izbiranja namenjene samo preprečevanju prezasedenosti omrežja, navadno ni večjih posledic za zasebnost posameznika. Politike upravljanja prometa pa so lahko usmerjene v blokiranje nekaterih vsebinskih informacij ali lahko vplivajo na komunikacijo, na primer z vedenjskim oglaševanjem. V takšnih primerih so vplivi bolj občutni. Ta pomislek postane še bolj pereč, če pomislimo, da se tovrstne informacije ne bi zbirale samo za majhno skupino posameznikov, temveč na splošno, za vse stranke ponudnikov ISP ([25]). Če bi vsi ponudniki ISP začeli uporabljati tehnike filtriranja, bi to lahko privedlo do splošnega spremljanja uporabe interneta. Če se poleg tega usmerimo na vrsto informacij, ki se obdelujejo, je očitno, da so tveganja za zasebnost visoka, saj je zelo verjetno, da je veliko informacij, ki se zbirajo, zelo občutljivih ter jih imajo po zbiranju na voljo ponudniki ISP in vsi, ki slednje prosijo za informacije. Poleg tega so te informacije lahko zelo dragocene v komercialnem smislu. To že samo po sebi prinaša visoko tveganje za prikrito spremembo funkcije, pri kateri začeten namen lahko zelo hitro preide v komercialno ali drugačno izkoriščanje zbranih informacij.

35. Pravilna uporaba tehnik spremljanja in pregledovanja in filtriranja mora potekati v skladu z veljavnimi zaščitnimi ukrepi za varstvo podatkov in zasebnost, ki omejujejo, kaj in v katerih okoliščinah je mogoče narediti. V nadaljevanju je predstavljen pregled veljavnih zaščitnih ukrepov v skladu s pravnim okvirom EU za varstvo podatkov in zasebnosti.

V. **UPORABA PRAVNEGA OKVIRA EU O ZASEBNOSTI IN VARSTVU PODATKOV**

36. Pravni okvir EU za varstvo podatkov je tehnološko nevtralen in kot tak ne ureja zgoraj predstavljenih posebnih tehnik pregledovanja. Direktiva o zasebnosti in elektronskih komunikacijah ureja zasebnost pri zagotavljanju storitev elektronskih komunikacij v javnih omrežjih (to sta predvsem dostop do

([24]) Vsak protokol ima v naslovu nekaj posebnih polj, ki zagotavljajo dodatne informacije o komunikaciji, ki se prenaša. Vsebino teh polj lahko poimenujemo metapodatki komunikacije. Primeri takšnih polj so številka uporabljenih vrat. Pri številki 80 je tako precej verjetno, da gre pri komunikaciji za brskanje po spletu.

([25]) Seveda pa zmogljivosti sledenja niso omejene na ponudnike ISP. Tudi ponudniki oglaševalskih mrež lahko sledijo uporabniku na spletnih straneh z uporabo piškotkov tretjih oseb. Glej na primer pred kratkim objavljen znanstveni članek, da je Google prisoten na 97 od 100 najbolj obiskanih spletišč, kar pomeni, da lahko Google sledi uporabnikom, ki niso preklicali piškotkov tretjih oseb, ko brskajo po teh priljubljenih spletiščih. Glej: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (29. julija 2011). Na voljo na SSRN: http://ssrn.com/abstract=1898390. Sledenje uporabnikom prek piškotkov tretjih oseb je obravnavala Delovna skupina iz člena 29. Glej mnenje št. 2/2010 o spletnem vedenjskem oglaševanju, sprejeto 22. junija 2010 (WP 171).

interneta in telefonija) ([26]), Direktiva o varstvu podatkov pa obdelavo podatkov na splošno. Ta pravni okvir na splošno določa različne obveznosti, ki jih morajo upoštevati ponudniki ISP, ki obdelujejo in spremljajo podatke o prometu in komunikacijah.

V.1. **Pravna podlaga za obdelovanje podatkov o prometu in vsebini**

37. V skladu z zakonodajo o varstvu podatkov je treba imeti ustrezno pravno podlago za obdelavo osebnih podatkov, kot je v tem primeru obdelava podatkov o prometu in komunikacijah. Poleg te splošne zahteve se v nekaterih primerih lahko uporabljajo posebne zahteve.

38. Osebni podatki, ki jih v tem primeru obdelujejo ponudniki ISP, se nanašajo na podatke o prometu in vsebino komunikacij. Vsebina komunikacije in podatki o prometu so zaščiteni s pravico do zaupnosti korespondence, ki je zagotovljena v členu 8 EKČP ter členih 7 in 8 Listine. Natančneje, člen 5(1) Direktive o zasebnosti in elektronskih komunikacijah z naslovom „Zaupnost sporočil“ zahteva, da države članice zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev. V členu 5(1) Direktive o zasebnosti in elektronskih komunikacijah je predvideno tudi, da se v nekaterih okoliščinah in s privolitvijo uporabnikov ponudnikom ISP lahko dovoli obdelava podatkov o prometu in vsebini. Tako je vsem osebam razen uporabnikom prepovedano, da „poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo komunikacije (sporočila) in z njimi povezane podatke o prometu, brez privolitve zadevnih uporabnikov, razen kadar je to zakonsko dovoljeno v skladu s členom 15(1)“. To vprašanje je podrobneje obravnavano v nadaljevanju.

39. Poleg privolitve zadevnih uporabnikov so v Direktivi o zasebnosti in elektronskih komunikacijah predvideni še drugi razlogi, na podlagi katerih lahko ponudniki ISP upravičeno obdelujejo podatke o prometu in komunikacijah. Ustrezne pravne podlage za obdelavo v tem primeru so (i) opravljanje storitve; (ii) zagotovitev varnosti storitve in (iii) zmanjševanje prezasedenosti. Drugi razlogi, na podlagi katerih je mogoče legitimizirati politike upravljanja, ki temeljijo na podatkih o prometu ali komunikaciji, so obravnavani v točki (iv) v nadaljevanju.

(i) Pravna podlaga za zagotavljanje storitve

40. Kot je bilo prikazano v oddelku IV, ponudniki ISP obdelujejo podatke o glavah IP za namene, ki vključujejo usmerjanje vsakega paketa IP proti cilju. Člena 6(1) in 6(2) Direktive o zasebnosti in elektronskih komunikacijah dovoljujeta obdelavo podatkov o prometu za namene zagotavljanja komunikacije. Tako ponudniki ISP lahko obdelujejo informacije, ki so potrebne za zagotavljanje storitve.

(ii) Pravna podlaga za zagotavljanje varnosti storitve

41. V skladu s členom 4 Direktive o zasebnosti in elektronskih komunikacijah za ponudnika ISP velja splošna obveznost, da sprejme ustrezne ukrepe za zagotavljanje varnosti svojih storitev. Filtriranje virusov tako lahko vključuje obdelavo glav IP in koristne vsebine IP. Ker člen 4 Direktive o zasebnosti in elektronskih komunikacijah vključuje zahtevo, da ponudniki ISP zagotovijo varnost omrežja, ta določba upravičuje tehnike pregledovanja, ki temeljijo na glavah in vsebini IP in se izvajajo izrecno s tem namenom. V praksi to pomeni, da lahko ponudniki ISP v okviru omejitev zaradi načela sorazmernosti (glej oddelek V.3) spremljajo in filtrirajo podatke o komunikaciji zaradi boja proti virusom in splošnega zagotavljanja varnosti omrežja ([27]).

([26]) Uvodna izjava 10 Direktive o zasebnosti in elektronskih komunikacijah se glasi: „Na področju elektronskih komunikacij se uporablja Direktiva 95/46/ES zlasti za vse zadeve v zvezi z varstvom temeljnih pravic in svoboščin, ki niso izrecno zajete v določbah te direktive, vključno z obveznostmi preglednika in pravicami posameznikov“. Pomembna je tudi uvodna izjava 17, ki se nanaša na privolitev posameznika, na katerega se nanašajo podatki: „Za namene te direktive ima privolitev uporabnika ali naročnika, ne glede na to, ali je ta fizična ali pravna oseba, enak pomen kot privolitev posameznika, na katerega se podatki nanašajo, kakor je opredeljeno in podrobneje opisano v Direktivi 95/46/ES.“

([27]) Mnenje Delovne skupine iz člena 29 št. 2/2006 o vprašanjih zasebnosti pri zagotavljanju storitev pregledovanja elektronske pošte, sprejeto 21. februarja 2006 (WP 118). Delovna skupina meni, da je uporaba filtrov za namene člena 4 lahko združljiva s členom 5 Direktive o zasebnosti in elektronskih komunikacijah.

(iii) Pravna podlaga za zmanjšanje učinkov prezasedenosti

42. Utemeljitev te pravne podlage je mogoče najti v uvodni izjavi 22 Direktive o zasebnosti in elektronskih komunikacijah, v kateri je razložena prepoved shranjevanja komunikacij iz člena 5(1). To ne pomeni prepovedi vsakega samodejnega, vmesnega in prehodnega shranjevanja teh podatkov, dokler se to dogaja samo zaradi izvedbe prenosa in pod pogojem, da podatki niso shranjeni dlje, kot je to potrebno za prenos in upravljanje prometa in da zaupnost podatkov ostane zagotovljena.

43. V primeru prezasedenosti se pojavi vprašanje, ali naj se ponudniki ISP odločijo za naključno prekinitev ali zakasnitev prometa ali naj raje upočasnijo komunikacije, ki niso časovno občutljive, npr. P2P ali promet po elektronski pošti, ter tako na primer omogočijo pretok glasovnega prometa s sprejemljivo kakovostjo.

44. Zaradi splošnega družbenega interesa za zagotovitev uporabnega komunikacijskega omrežja lahko ponudniki ISP trdijo, da je prednostno obravnavanje ali upočasnjevanje prometa zaradi prezasedenosti legitimen ukrep za zagotavljanje ustrezne storitve. To pomeni, da bi v teh primerih in za ta namen obstajala splošna pravna podlaga za obdelavo osebnih podatkov in ne bila potrebna posebna privolitev uporabnikov.

45. Obenem pa možnost takšnega poseganja ni neomejena. Če morajo ponudniki ISP pregledati komunikacije, morajo z vidika zaupnosti in z dosledno uporabo načela sorazmernosti uporabljati najmanj vsiljivo metodo za dosego tega namena (torej se morajo izogibati temeljitemu pregledovanju paketov), ki jo morajo uporabljati, samo dokler je to potrebno za reševanje prezasedenosti.

(iv) Pravna podlaga obdelave podatkov za druge namene

46. Ponudniki ISP bi mogoče želeli pregledovati podatke o vsebini in prometu za druge namene, na primer za ponujanje prilagojenih naročniških razmerij (npr. razmerje z omejenim dostopom do P2P ali razmerje, ki omogoča večjo hitrost pri nekaterih uporabniških programih). Pregledovanje in nadaljnja uporaba podatkov o prometu in komunikacijah za druge namene, kot je zagotavljanje storitve ali njene varnosti ter izogibanje prezasedenosti, je dovoljeno samo pod strogimi pogoji in v skladu s pravnim okvirom.

47. Pravni okvir je predvsem člen 5(1) Direktive o zasebnosti in elektronskih komunikacijah, ki zahteva privolitev zadevnih uporabnikov v poslušanje, prisluškovanje, shranjevanje ali prestrezanje ali nadziranje komunikacij in z njimi povezanih podatkov o prometu na druge načine. V praksi to pomeni, da je za zakonitost obdelave podatkov o komunikacijah in prometu v skladu s členom 5(1) potrebna privolitev uporabnikov, vključenih v komunikacijo.

48. Kot je bilo že pojasnjeno, uporaba tehnik pregledovanja in filtriranja temelji na glavah IP, ki vsebujejo podatke o prometu, ali pa na temeljitem pregledovanju paketov, kar vključuje tudi koristne vsebine IP in sestavlja podatke o komunikaciji. Zaradi tega bi bila uporaba takšnih tehnik načeloma prepovedana za namene, ki niso zagotavljanje storitve ali varnosti, razen če obdelava ni mogoča na podlagi legitimnega razloga, kot je privolitev (člen 5(1)). Tako bi se člen 5(1) na primer uporabljal, kadar se ponudnik ISP odloči ponuditi strankam nižjo naročnino za dostop do interneta v zameno za prejemanje vedenjskega oglaševanja, uporabo temeljitega pregledovanja paketov in torej podatkov o komunikaciji. Zaradi tega je v skladu s členom 5(1) potrebna dejanska in izrecna privolitev na podlagi ustrezne obveščenosti.

49. Poleg tega člen 6 Direktive o zasebnosti in elektronskih komunikacijah z naslovom „Podatki o prometu“ določa nekatera pravila posebej za podatke o prometu. Pri tem zlasti predvideva, da ponudniki ISP

obdelujejo podatke o prometu na podlagi privolitve uporabnikov, da bodo prejemali storitve z dodano vrednostjo ([28]). Ta določba natančneje opredeljuje zahtevo po privolitvi iz člena 5(1), kadar gre za podatke o prometu.

50. V praksi mogoče ni vedno lahko določiti, v katerih primerih je na primer potrebna privolitev in v katerih primerih je obdelava lahko zakonita zaradi varnosti omrežja, zlasti kadar je namen tehnike pregledovanja dvojen (na primer izogibanje prezasedenosti in zagotavljanje storitev z dodano vrednostjo). Treba je poudariti, da privolitev ne sme šteti za lahko in sistematično pot do skladnosti z načeli varstva podatkov.

51. Za zdaj še ni veliko izkušenj z uporabo okvira, kar zlasti velja za vidike, ki so bili predstavljeni zgoraj. Za to področje je nujno pripraviti nadaljnje smernice, kot je podrobneje razloženo v oddelku VI. Poleg tega so s privolitvijo povezani dodatni vidiki, ki tudi zahtevajo ustrezen razmislek in so opisani v nadaljevanju.

V.2. **Vprašanja, povezana s privolitvijo na podlagi ustrezne obveščenosti kot pravno podlago**

52. Privolitev, ki se zahteva v skladu s členoma 5 in 6 Direktive o zasebnosti in elektronskih komunikacijah, ima enak pomen kot privolitev posameznika, na katerega se nanašajo podatki, kot je opredeljena in natančneje razložena v Direktivi 95/46/ES ([29]). V skladu s členom 2(h) Direktive o varstvu podatkov „privolitev posameznika, na katerega se nanašajo osebni podatki“ pomeni „vsako prostovoljno dano posebno in informirano izjavo volje, s katero posameznik, na katerega se osebni podatki nanašajo, izrazi soglasje, da se osebni podatki o njem obdelujejo“. Vloga privolitve in zahteve za njeno veljavnost so bile pred nedavnim obravnavane v mnenju Delovne skupine iz člena 29 št. 15/2011 o privolitvi ([30]).

53. Ponudniki ISP, ki morajo dobiti privolitev, da lahko pregledujejo in filtrirajo podatke o prometu, morajo zato zagotoviti, da je ta privolitev svobodna in izrecna, poleg tega mora biti navedba posameznikovih želja, ki temeljijo na ustrezni informiranosti in s katerimi izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj. To potrjuje uvodna izjava 17 Direktive o zasebnosti in elektronskih komunikacijah: „[…] Privolitev se lahko da na kateri koli primeren način, ki omogoča uporabniku, da navede svoje želje svobodno, izrecno in ozaveščeno, tudi tako, da pri obisku internetne spletne strani označi rubriko s kljukico.“ V nadaljevanju je navedenih nekaj praktičnih primerov, kaj v tem okviru pomeni svobodna, izrecna in ozaveščena privolitev.

Privolitev: Svobodna in izrecna privolitev na podlagi ustrezne obveščenosti

54. *Svobodna privolitev*. Uporabniki ne smejo trpeti omejitev zaradi navezovanja privolitve na naročniško razmerje za uporabo interneta, ki bi ga radi sklenili.

55. Privolitev posameznikov ni svobodna, če morajo privoliti v spremljanje podatkov o njihovi komunikaciji, da dobijo dostop do komunikacijske storitve. To bi bilo še toliko bolj res, če bi *vsi* ponudniki na nekem trgu uvedli upravljanje prometa za namene, ki presegajo varnost omrežja. Tako bi imeli samo še možnost, da sploh ne naročijo internetnih storitev. Ker pa je internet postal nepogrešljivo orodje za

([28]) Uvodna izjava 18 Direktive vsebuje seznam, na katerem so našteti primeri storitev z dodano vrednostjo. Ni pa jasno, ali je mogoča razlaga, da seznam vključuje tudi storitve, za katere se uporabljajo politike upravljanja prometa. Politike upravljanja prometa, ki so namenjene prednostni obravnavi nekaterih vsebin, bi lahko razlagali kot zagotavljanje kakovosti storitve. Tako bi na primer upravljanje prometa, ki vključuje zgolj obdelovanje glav IP in katerega osrednji cilj je zagotavljanje dražjih storitev igranja iger, pri katerih imajo storitve igranja igric v omrežju prednost, lahko razlagali kot storitev z dodano vrednostjo. Po drugi strani pa sploh ni jasno, ali bi lahko tako razlagali tudi upravljanje prometa, namenjeno upočasnitvi nekaterih vrst prometa, na primer prometa P2P.

([29]) Glej uvodno izjavo 17 in člen 2(f) Direktive o zasebnosti in elektronskih komunikacijah.

([30]) Sprejeto 13. julija 2011 (WP 187).

delo in zabavo, možnost, da nekdo ne bi sklenil naročnine, ne pride v poštev. Privedla bi do tega, da posamezniki ne bi imeli dejanske izbire, torej ne bi mogli dati svobodne privolitve. ([31])

56. Po mnenju ENVP obstaja jasna potreba, da Komisija in nacionalni organi spremljajo trg ter se tako zlasti prepričajo, ali možnost, da ponudniki vežejo telekomunikacijske storitve na spremljanje komunikacij, postaja uveljavljena. Ponudniki morajo zagotoviti alternativne storitve, vključno z naročniškim razmerjem za uporabo interneta, pri katerem ni urejanja prometa, ne da bi posamezniki pri tem imeli višje stroške.

57. *Izrecna privolitev*. V obravnavanem primeru je privolitev izrecna, če ponudniki ISP jasno in razločno prosijo za privolitev za spremljanje podatkov o prometu in komunikacijah. Kot navaja Delovna skupina iz člena 29, „… je privolitev izrecna, če je razumljiva: jasno in natančno se mora nanašati na obseg in posledice obdelave podatkov. Ne more se uporabljati za neomejene dejavnosti obdelave. Z drugimi besedami to pomeni, da so okoliščine, v katerih se privolitev uporablja, omejene." Privolitev za pregledovanje podatkov o prometu in komunikacijah verjetno ne bo izrecna, če je vključena „v sveženj" s splošno privolitvijo za naročilo storitve. Izrecnost namreč pomeni, da je treba uporabiti posebna sredstva za pridobitev privolitve, kot je poseben obrazec za privolitev ali poseben okvirček, jasno namenjen spremljanju (ne pa vključitvi te informacije v splošne pogoje pogodbe in zahtevi za podpis pogodbe v obstoječi obliki).

58. *Privolitev na podlagi ustrezne obveščenosti*. Privolitev je legitimna, če je sprejeta na podlagi ustrezne obveščenosti. Predhodna zagotovitev informacij ni potrebna samo na podlagi direktiv o zasebnosti in elektronskih komunikacijah ter varstvu podatkov, temveč tudi na podlagi členov 20 in 21 Direktive o univerzalnih storitvah, kakor je bila spremenjena z Direktivo 2009/136/ES ([32]). Potreba po informacijah in privolitvi je bila izrecno potrjena v uvodni izjavi 28 Direktive 2009/136/ES: „uporabniki morajo biti v vsakem primeru popolnoma obveščeni o vseh omejitvah, ki jih ponudnik storitev in/ali omrežij nalaga pri uporabi elektronskih komunikacijskih storitev. S takšnimi informacijami bi se po izboru ponudnika morala posebej opredeliti zadevna vrsta vsebine, aplikacije ali storitve, individualne aplikacije ali storitve, oziroma oboje." V nadaljevanju je navedeno: „Glede na uporabljeno tehnologijo in na vrsto omejitve lahko takšne omejitve zahtevajo privolitev uporabnika v okviru Direktive 2002/58/ES."

59. Glede na zapletenost teh tehnik spremljanja je eden od glavnih izzivov za pridobitev legitimne privolitve zagotavljanje razumljivih predhodnih informacij. Potrošnike je treba obvestiti tako, da lahko razumejo, katere informacije se obdelujejo, kako bodo uporabljene ter kakšna bosta vpliv na uporabniško izkušnjo in stopnja poseganja v zasebnost pri posameznih tehnikah.

60. To ne pomeni samo, da morajo biti same informacije jasne in razumljive povprečnim uporabnikom, temveč tudi, da se posameznikom zagotovijo neposredno in jasno, da jih ne morejo spregledati.

61. *Navedba želja*. Privolitev v skladu z veljavnim pravnim okvirom zahteva tudi dejanje, s katerim uporabnik potrdi svojo privolitev. Posredna privolitev temu standardu ne ustreza. To potrjuje tudi potrebo po uporabi posebnih sredstev za pridobitev privolitve, ki omogoča ponudniku ISP pregledovanje podatkov o prometu in komunikacijah v okviru izvajanja politik upravljanja prometa. Delovna skupina iz člena 29 je v pred kratkim sprejetem mnenju poudarila potrebo, da so pri pridobivanju privolitve jasno razvidni vsi elementi, ki sestavljajo obdelavo podatkov.

([31]) Podoben je primer PNR, pri katerem je potekala razprava, ali je privolitev potnikov, da se podatki o njihovi rezervaciji posredujejo organom ZDA, upravičena. Delovna skupina je menila, da privolitev potnikov ne more biti svobodna, saj morajo letalske družbe poslati podatke pred vzletom, torej potniki nimajo nobene druge možnosti, če želijo leteti; mnenje št. 6/2002 Delovne skupine iz člena 29 o prenosu očitnih informacij o potnikih in drugih podatkov s strani letalskih družb Združenim državam.

([32]) Direktiva 2009/136/ES z dne 25. novembra 2009 o spremembah Direktive 2002/22/ES o univerzalnih storitvah in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami (Prim. opombo 15).

62. Obstaja tudi argument, da lahko strani, udeležene v komunikaciji, ki nočejo, da ponudniki ISP prestrezajo komunikacijo zaradi izvajanja politike upravljanja prometa, komunikacijo tudi kodirajo. Ta pristop se v praksi sicer lahko obnese, vendar zahteva nekaj truda in tehničnega znanja ter ga ni mogoče enačiti s svobodno in izrecno privolitvijo na podlagi ustrezne obveščenosti. Poleg tega tehnike kodiranja ne zagotavljajo popolne zaupnosti komunikacije, saj imajo ponudniki ISP zaradi usmerjanja komunikacije dostop vsaj do informacij o glavi IP, kar jim omogoča tudi opravljanje statističnih analiz.

63. V skladu s členom 5(1) Direktive o zasebnosti in elektronskih komunikacijah je treba pridobiti privolitev zadevnih uporabnikov. Uporabnik je velikokrat ista oseba kot naročnik, ki je torej dal privolitev, ko je sklenil naročniško razmerje za uporabo telekomunikacijskih storitev. V drugih primerih, tudi tistih, ki vključujejo več kot eno osebo, je treba privolitev zadevnih uporabnikov pridobiti posebej. Pri tem se postavi nekaj praktičnih vprašanj, ki so razložena v nadaljevanju.

Privolitev vseh zadevnih uporabnikov

64. Člen 5(1) predvideva, da je obdelava zakonita, če vanjo privoli uporabnik. Privolitev je treba pridobiti od *vseh* uporabnikov, udeleženih v komunikaciji. Razlog za to je, da komunikacija navadno vključuje vsaj dva posameznika (pošiljatelja in prejemnika). Če tako ponudnik ISP pregleduje koristne vsebine IP, ki se nanašajo na elektronsko sporočilo, pregleduje informacije, ki se nanašajo na pošiljatelja in prejemnika elektronskega sporočila.

65. Pri spremljanju in prestrezanju prometa in komunikacij (na primer pri spletnem prometu) mogoče zadostuje, da ponudniki ISP pridobijo dovoljenje uporabnika, torej naročnika, saj druge strani v komunikaciji, ki je v tem primeru obiskano spletišče, ni mogoče šteti za „zadevnega uporabnika“ ([33]). Položaj pa je lahko bolj zapleten, kadar takšno spremljanje vključuje pregledovanje vsebine elektronskih sporočil in torej osebne informacije pošiljatelja in prejemnika sporočila po elektronski pošti, ki mogoče nimata pogodbenega razmerja z istim ponudnikom ISP. V teh primerih bi ponudnik ISP obdeloval osebne podatke (ime, naslov elektronske pošte in mogoče občutljive vsebinske podatke) oseb, ki niso njegove stranke. Privolitev takšnih posameznikov je mogoče težje pridobiti, saj je potrebna za vsak primer posebej, ne pa že za samo opravljanje telekomunikacijskih storitev. Prav tako ni realno predvidevati, da je uporabnik dal privolitev tudi v imenu drugih uporabnikov, kar pogosto velja za zasebna gospodinjstva.

66. ENVP tako meni, da morajo ponudniki ISP upoštevati veljavne pravne zahteve in izvajati politike, ki ne vključujejo spremljanja in pregledovanja informacij. To je še toliko bolj pomembno pri komunikacijskih storitvah, ki vključujejo tretje strani, ki nimajo možnosti, da bi privolile v spremljanje, kar zlasti velja za poslana in prejeta sporočila po elektronski pošti (to ne velja, če namen temelji na varnostnih pomislekih).

67. Obenem je treba opozoriti, da nacionalni zakoni, s katerimi se uveljavlja člen 5(1) Direktive o zasebnosti in elektronskih komunikacijah, niso vedno zadovoljivi in da se kaže tudi splošna potreba po boljših smernicah v zvezi z zahtevami Direktive o zasebnosti in elektronskih komunikacijah glede tega področja. ENVP zato poziva Komisijo, naj bo bolj dejavna glede tega vprašanja, pri čemer bi si lahko pomagala s prispevkom nadzornih organov, zbranih v Delovni skupini iz člena 29, in drugih zainteresiranih strani. Če bi bilo to potrebno, bi bilo zadevo treba obravnavati pred Sodiščem Evropske unije in v celoti razjasniti pomen in posledice člena 5(1).

([33]) Ne glede na primere, pri katerih spletni promet vključuje prenos osebnih informacij, kot so na primer slike določljivih fizičnih oseb, objavljenih na spletišču. Za obdelavo takšnih informacij je potrebna pravna podlaga, vendar ti primeri niso zajeti v člen 5(1), saj te osebe niso „zadevni uporabniki“.

V.3. **Sorazmernost – načelo zmanjšanja količine podatkov**

68. V členu 6(c) Direktive o varstvu podatkov je določeno načelo sorazmernosti ([34]), ki se uporablja za ponudnike ISP, saj imajo pri spremljanju in filtriranju vlogo nadzornikov podatkov v smislu te direktive.

69. V skladu z navedenim načelom se osebni podatki lahko obdelujejo, če so „primerni, ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali naprej obdelujejo". Uporaba tega načela prinaša potrebo po oceni, ali so sredstva, ki se uporabljajo za obdelavo podatkov, in vrste osebnih podatkov, ki se uporabljajo, primerni in ali je mogoče razumno pričakovati, da bodo dosegli cilje. Če je ugotovljeno, da se zbira več podatkov, kot je potrebno, načelo ni izpolnjeno.

70. Skladnost z načelom sorazmernosti pri nekaterih tehnikah pregledovanja je treba presojati za vsak primer posebej. Pri tem ni mogoče sprejemati ugotovitev na abstraktni podlagi. Je pa mogoče opozoriti na več konkretnih vidikov, ki jih je treba oceniti pri presojanju skladnosti z načelom sorazmernosti.

71. *Količina obdelanih informacij.* Največja stopnja temeljitosti nadzora nad komunikacijami strank ponudnika ISP je večinoma pretirana in nezakonita. Dejstvo, da je nadzor mogoče izvajati s sredstvi, ki jih posamezniki ne opazijo, in da mogoče težko razumejo, kaj se dogaja, še poveča vpliv na njihovo zasebnost. Ponudniki ISP morajo presoditi, katera manj vsiljiva sredstva so na voljo za dosego zahtevanega rezultata. Ali je tako na primer mogoče doseči zahtevani rezultat s spremljanjem glav IP, namesto s temeljitimi pregledi paketov? Celo pri uporabi temeljitih pregledov paketov je mogoče pridobiti zahtevane informacije samo s pregledom nekaterih protokolov. Pri tem je mogoče ustrezna tudi uporaba zaščitnih ukrepov za varstvo podatkov, vključno s psevdoavtomatizacijo. Izid ocene mora potrditi, da je obdelava podatkov sorazmerna.

72. *Učinki obdelave (neposredno povezani z nameni).* Sorazmernost je mogoče premajhna v primerih, ko ponudniki ISP uporabljajo politike upravljanja prometa, ki izključujejo dostop do nekaterih storitev, ne da bi v zameno omogočali ustrezne ugodnosti za uporabnike.

73. Treba je opozoriti, da se načelo sorazmernosti uporablja tudi, če so izpolnjene druge obvezne zakonske zahteve, tudi če je ponudnik ISP na primer pridobil privolitev posameznikov za spremljanje vsebin. To pomeni, da je lahko obdelava podatkov s spremljanjem vsebine vseeno nezakonita, če je v nasprotju s temeljnim načelom sorazmernosti.

V.4. **Varnostni in organizacijski ukrepi**

74. Člen 4 Direktive o zasebnosti in elektronskih komunikacijah izrecno zahteva od ponudnikov ISP, da sprejmejo tehnične in organizacijske ukrepe za zagotovitev, (i) da ima do osebnih podatkov dostop samo pooblaščeno osebje, in to za zakonite namene; (ii) zaščite osebnih podatkov pred naključnim in nezakonitim obdelovanjem ter (iii) izvajanja varnostne politike glede obdelave osebnih podatkov. Nacionalnim pristojnim organom omogoča tudi izvajanje revizij v zvezi s temi ukrepi.

75. Poleg tega morajo ponudniki ISP v skladu s členom 4(3) in (2) Direktive o zasebnosti in elektronskih komunikacijah ustrezno obvestiti pristojne nacionalne organe v primeru kršitve podatkov, prizadete posameznike pa v primeru, da jim razkritje lahko prinese negativne posledice.

76. Obdelava osebnih podatkov, vključenih v komunikacijo, za namene izvajanja politik upravljanja prometa, lahko omogoči ponudnikom ISP dostop do podatkov, ki so celo bolj občutljivi od podatkov o prometu.

([34]) Kot je bilo opisano zgoraj, se Direktiva o varstvu podatkov uporablja za vse zadeve, ki se nanašajo na varstvo temeljnih pravic in svoboščin, ki niso izrecno zajete v Direktivi o zasebnosti in elektronskih komunikacijah.

77. Zaradi tega morajo varnostne politike, ki jih pripravijo ponudniki ISP, vključevati posebne zaščitne ukrepe za zagotovitev, da so sprejeti ukrepi ustrezni za ta tveganja. Poleg tega morajo biti nacionalni pristojni organi, ki pregledujejo te ukrepe, posebno zahtevni. Nazadnje je treba zagotoviti še, da se vzpostavijo učinkoviti postopki obveščanja posameznikov, na katere se nanašajo podatki, katerih podatki so ogroženi in ki lahko utrpijo negativne posledice zaradi tega.

VI. **PREDLOGI ZA POLITIČNE IN ZAKONODAJNE UKREPE**

78. Tehnike pregledovanja, ki temeljijo na podatkih o prometu in pregledovanju koristnih vsebin IP, torej vsebini komunikacij, lahko razkrijejo dejavnost uporabnikov na internetu: obiskana spletna mesta in aktivnost na teh mestih, uporabo uporabniških programov P2P, prenesene datoteke, prejeta in poslana sporočila po elektronski pošti, kdo jih je poslal, na kakšno temo in pod kakšnimi pogoji itd. Ponudniki ISP bi mogoče hoteli uporabiti te informacije za prednostno obravnavanje nekaterih komunikacij, na primer videa na zahtevo. Mogoče bi jih uporabili za prepoznavanje virusov ali oblikovanje profilov za namene vedenjskega oglaševanja. Te dejavnosti posegajo v pravico do zaupnosti komunikacije.

79. Zaradi uporabljene tehnike in značilnosti posameznega primera so lahko posledice za zasebnost še večje. Kolikor več informacij se prestreže in kolikor bolj temeljito se pregledujejo, toliko večje je navzkrižje z načelom zaupnosti komunikacij. Nameni, za katere poteka spremljanje, in uporabljeni zaščitni ukrepi za varstvo podatkov so tudi ključni elementi, s katerimi se določi stopnja poseganja v zasebnost in osebne podatke posameznikov. Blokiranja in spremljanja za boj proti škodljivi programski opremi, s strogimi omejitvami glede hranjenja in uporabe pregledanih podatkov, ni mogoče primerjati z okoliščinami, ko se informacije naložijo za oblikovanje profilov posameznikov v okviru vedenjskega oglaševanja.

80. ENVP načeloma meni, da sedanji okvir EU za zasebnost in varstvo podatkov, če se pravilno razlaga, uporablja in uveljavlja, zadošča za zagotovitev, da se spoštuje pravica do zaupnosti ter da na splošno nista ogrožena zasebnost in varstvo podatkov posameznikov ([35]). Ponudniki ISP ne smejo uporabljati takšnih mehanizmov, če ne uporabljajo ustrezno pravnega okvira. Ponudniki ISP morajo upoštevati predvsem naslednje elemente okvira:

— ponudniki ISP lahko v skladu s členoma 4 in 6 Direktive o zasebnosti in elektronskih komunikacijah uporabijo politike upravljanja prometa, ki so namenjene varnosti storitve, zagotavljanju storitve, vključno z omejevanjem prezasedenosti;

— ponudniki ISP potrebujejo še eno izrecno pravno podlago in po možnosti tudi privolitev uporabnikov za izvajanje politik upravljanja prometa, ki vključujejo obdelovanje podatkov o prometu in/ali komunikaciji za druge namene. Tako je na primer potrebna privolitev uporabnikov na podlagi ustrezne obveščenosti za spremljanje in filtriranje komunikacij posameznikov za namene omejevanja (ali omogočanja) dostopa do nekaterih uporabniških programov in storitev, kot sta P2P ali VoIP;

— privolitev mora biti svobodna, izrecna in sprejeta na podlagi ustrezne obveščenosti. Izražena mora biti s pritrdilnim dejanjem. Pri teh zahtevah je močno poudarjena potreba po okrepitvi prizadevanj za zagotovitev, da so posamezniki ustrezno obveščeni, in sicer na neposreden, razumljiv in izrecen način, tako da lahko ocenijo posledice ravnanja in nazadnje sprejmejo odločitev na podlagi ustrezne obveščenosti. Glede na zapletenost teh tehnik je eden od glavnih izzivov za pridobitev legitimne privolitve podajanje razumljivih predhodnih informacij. Poleg tega uporabniki, ki ne privolijo v spremljanje, ne smejo nositi nobenih negativnih posledic (vključno s finančnimi stroški);

([35]) To ne posega v pravico do spremembe zakonodaje na podlagi drugih elementov, zlasti v okviru splošnega pregleda pravnega okvira EU za varstvo podatkov za povečanje njegove učinkovitosti glede na nove tehnologije in globalizacijo.

— kadar ponudniki ISP izvajajo politike upravljanja prometa, ima bistveno vlogo načelo sorazmernosti, in to ne glede na pravno podlago ali namen: zagotavljanje storitve, izogibanje prezasedenosti ali zagotavljanje prilagojenih naročniških razmerij z dostopom do nekaterih storitev in uporabniških programov ali brez njega. To načelo omejuje možnost, da bi ponudniki ISP spremljali vsebino posameznikovih komunikacij, ki vključuje obdelovanje prevelike količine informacij ali od katere imajo korist samo ponudniki ISP. Dejanja ponudnikov ISP, ki so logistično izvedljiva, so odvisna od stopnje poseganja tehnik, zahtevanih rezultatov (ki jim lahko prinesejo prednosti) ter posebnih zaščitnih ukrepov za varovanje zasebnosti in varstva podatkov, ki se uporabijo. Ponudniki ISP morajo pred uporabo tehnik pregledovanja presoditi, ali ustrezajo načelu sorazmernosti.

81. Sedanji pravni okvir sicer vključuje ustrezne pogoje in zaščitne ukrepe, vendar je treba posvetiti posebno pozornost temu, ali ponudniki ISP dejansko izpolnjujejo zakonske zahteve, ali zagotavljajo potrebne informacije, na podlagi katerih potrošniki lahko smiselno izbirajo, in ali spoštujejo načelo sorazmernosti. Na nacionalni ravni so za to področje pristojni nacionalni organi za področje telekomunikacij in organi za varstvo podatkov. Med ustreznimi organi na ravni EU je tudi BEREC. Pri tem ima lahko vlogo tudi ENVP.

82. Zaradi relativno novih možnosti za množično spremljanje komunikacij v realnem času poleg spremljanja sedanje ravni skladnosti zahtevajo bolj poglobljeno analizo in dokončno razjasnitev tudi nekateri vidiki uporabe okvira, ki so bili obravnavani v tem mnenju. Smernice, ki so posebno pomembne na več področjih, vključujejo:

— določiti legitimne prakse pregledovanja, ki zagotavljajo nemoten pretok prometa in pri katerih mogoče ni potrebna privolitev uporabnikov, na primer boj proti vsiljeni pošti. Pri tem je treba poleg stopnje poseganja pri spremljanju upoštevati tudi druge vidike, kot je na primer stopnja motenj glede na siceršnji nemoten pretok prometa;

— določiti, katere tehnike pregledovanja, za katere ni potrebna privolitev uporabnikov, je mogoče uporabiti za namene varnosti;

— določiti, kdaj je za spremljanje potrebna privolitev posameznika, predvsem privolitev vseh zadevnih uporabnikov, in kateri so dovoljeni tehnični parametri, ki zagotavljajo, da tehnika pregledovanja ne vključuje nesorazmerne obdelave podatkov glede na namen;

— poleg tega so v treh primerih zgoraj mogoče potrebne smernice glede uporabe potrebnih zaščitnih ukrepov za varstvo podatkov (omejitev namena, varnost itd.).

83. Ker so za to področje pristojne države in EU, je po mnenju ENVP bistveno, da si obe strani izmenjujeta stališča in izkušnje ter tako poskušata določiti usklajen pristop. Da bi to dosegli, ENVP predlaga ustanovitev platforme ali strokovne skupine, v kateri se morajo zbrati predstavniki nacionalnih regulativnih organov, Delovne skupine iz člena 29, urada ENVP in organa BEREC. Prvi cilj platforme bi bil pripraviti smernice, vsaj glede zgoraj izpostavljenih vprašanj, ter tako zagotoviti trden in usklajen pristop ter enake pogoje za vse. ENVP poziva Komisijo, da poskrbi za izvedbo te pobude.

84. In ne nazadnje, tako nacionalni organi kot ustrezni organi EU, ki vključujejo organ BEREC in Komisijo EU, morajo skrbno spremljati razvoj trga na tem področju. Scenarij, pri katerem bi ponudniki ISP rutinsko izvajali politike upravljanja prometa in ponujali naročniška razmerja na podlagi filtriranja dostopa do vsebin in uporabniških programov, bi bil izredno problematičen z vidika varstva podatkov in zasebnosti. Če bi se kdaj uresničil, je treba sprejeti zakonodajo, ki bi ustrezno obravnavala ta položaj.

VII. **SKLEPNE UGOTOVITVE**

85. Ponudniki ISP vse pogosteje posegajo po tehnikah spremljanja in pregledovanja, s čimer posegajo v nevtralnost interneta in zaupnost komunikacij. To vzbuja resna vprašanja v zvezi z varstvom zasebnosti in osebnih podatkov uporabnikov.

86. Tega vprašanja se sicer bežno dotika sporočilo Komisije o odprtem internetu in nevtralnosti omrežja v Evropi, vendar ENVP meni, da je treba storiti več za oblikovanje zadovoljive prihodnje politike. To mnenje je torej prispevek k sedanji politični razpravi o nevtralnosti omrežja, zlasti glede vidikov, povezanih z varstvom podatkov in zasebnostjo.

87. ENVP meni, da bi morali nacionalni organi in organ BEREC spremljati položaj na trgu ter tako nedvoumno ugotoviti, ali se trg razvija v smeri množičnega pregledovanja komunikacij v realnem času, in opredeliti vprašanja glede skladnosti s pravnim okvirom.

88. Spremljanje trga mora biti pospremljeno z nadaljnjo analizo o učinkih novih praks v zvezi z varstvom podatkov in zasebnosti na internetu. V tem mnenju je opisanih nekaj področij, ki potrebujejo tovrstno razjasnitev. Agencije in organi EU, kot so BEREC, Delovna skupina iz člena 29 in ENVP, sicer lahko razjasnijo pogoje za uporabo okvira, vendar ENVP meni, da mora razpravo usklajevati in usmerjati Komisija. Zaradi tega poziva Komisijo, da sprejme pobudo za oblikovanje platforme ali delovne skupine, ki bi poskušala doseči ta cilj in v kateri bi sodelovale vse navedene zainteresirane strani. Med vprašanji, ki zahtevajo nadaljnjo analizo, je treba obravnavati:

— katere prakse pregledovanja so legitimne za zagotovitev nemotenega pretoka prometa in jih je mogoče izvajati za namene varnosti;

— kdaj je za spremljanje potrebna privolitev posameznika, predvsem privolitev vseh zadevnih uporabnikov, in kateri so dovoljeni tehnični parametri, ki zagotavljajo, da tehnika pregledovanja ne vključuje obdelave podatkov, ki ni sorazmerna glede na namen;

— v teh primerih so mogoče potrebne smernice glede uporabe potrebnih zaščitnih ukrepov za varstvo podatkov (omejitev namena, varnost itd.).

89. Na podlagi teh ugotovitev bo mogoče treba sprejeti dodatne zakonodajne ukrepe. V tem primeru mora Komisija predlagati politične ukrepe, usmerjene v krepitev pravnega okvira in zagotovitev pravne varnosti. Novi ukrepi morajo pojasniti praktične posledice načela nevtralnosti omrežja, kar se že izvaja v nekaterih državah članicah, in zagotoviti, da imajo uporabniki lahko resnično izbiro, pri čemer jim morajo ponudniki ISP predvsem omogočiti dostop do povezav, ki se ne spremljajo.

V Bruslju, 7. oktobra 2011

Peter HUSTINX

Evropski nadzornik za varstvo podatkov