I

(Päätöslauselmat, suositukset ja lausunnot)

LAUSUNNOT

EUROOPAN TIETOSUOJAVALTUUTETTU

Euroopan tietosuojavaltuutetun lausuntoverkon neutraliteetista, verkkoliikenteen hallinnasta sekä yksityisyyden ja henkilötietojen suojelusta

(2012/C 34/01)

EUROOPAN TIETOSUOJAVALTUUTETTU

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 16 artiklan,

Euroopan unionin perusoikeuskirjan ja erityisesti sen 7 ja 8 artiklan,

yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY ([1]),

yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 ([2]), erityisesti sen 41 artiklan 2 kohdan, sekä

henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) 12 päivänä heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([3]), ja

ON ANTANUT SEURAAVAN LAUSUNNON:

I **JOHDANTO**

I.1 **Taustaa**

1. Komissio antoi 19. huhtikuuta 2011 tiedonannon avoimesta internetistä ja verkon neutraliteetista Euroopassa ([4]).

2. Tämä lausunto voidaan katsoa Euroopan tietosuojavaltuutetun reaktioksi kyseiseen tiedonantoon, ja sen tarkoituksena on osallistua Euroopan unionissa parhaillaan käytävään periaatekeskusteluun verkon neutraliteetista etenkin tietosuojaan ja yksityisyyteen liittyvistä näkökohdista.

([1]) EYVL L 281, 23.11.1995, s. 31, tietosuojadirektiivi.
([2]) EYVL L 8, 12.1.2001, s. 1, tietosuoja-asetus.
([3]) EYVL L 201, 31.7.2002, s. 37, sellaisena kuin se on muutettuna 25 päivänä marraskuuta 2009 annetulla Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EY (katso alaviite 15), sähköisen viestinnän tietosuojadirektiivi.
([4]) KOM(2011) 222 lopullinen.

3. Lausunto perustuu vastaukseen ([5]), jonka tietosuojavaltuutettu antoi komission järjestämässä julkisessa kuulemisessa avoimesta internetistä ja verkon neutraliteetista Euroopassa ennen komission tiedonannon julkistamista. Tietosuojavaltuutettu on ottanut huomioon myös neuvoston äskettäiset päätösluonnokset verkon neutraliteetista ([6]).

I.2 **Verkon neutraliteetin käsite**

4. Verkon neutraliteetti liittyy meneillään olevaan keskusteluun siitä, tulisiko internet-palveluntarjoajille ([7]) sallia mahdollisuus rajoittaa, suodattaa tai estää pääsyä internetiin tai muulla tavoin vaikuttaa sen toimintakykyyn. Verkon neutraliteetin käsite perustuu näkemykseen, jonka mukaan internetissä olevaa tietoa tulisi välittää puolueettomasti sisällöstä, kohteesta tai lähteestä riippumatta ja että käyttäjien tulisi voida päättää, mitä sovelluksia, palveluja ja laitteistoa he haluavat käyttää. Tämä tarkoittaa sitä, etteivät internet-palveluntarjoajat voi päättää oma-aloitteisesti ensisijaistaa tai hidastaa pääsyä tiettyihin sovelluksiin tai palveluihin, kuten vertaisverkkopalveluihin jne. ([8]).

5. Verkkoliikenteen suodattaminen, estäminen ja valvonta herättää kysymyksiä, jotka on usein jätetty huomiotta tai siirretty syrjään mutta jotka ovat tärkeitä viestinnän luottamuksellisuuden sekä yksilöiden ja heidän henkilötietojensa yksityisyyden kannalta, kun he käyttävät internetiä. Esimerkiksi tiettyihin valvontatekniikkoihin kuuluu viestinnän sisällön sekä selailtujen verkkosivujen, lähetettyjen ja vastaanotettujen sähköpostiviestien ja näiden toimintojen ajankohdan ym. seurantaa, mikä mahdollistaa viestien suodattamisen.

6. Kun internet-palveluntarjoajat valvovat viestintätietoja, ne saattavat rikkoa viestinnän luottamuksellisuutta, joka on Euroopan ihmisoikeussopimuksen 8 artiklan sekä Euroopan perusoikeuskirjan 7 ja 8 artiklan takaama perusoikeus. Luottamuksellisuuden suojasta säädetään myös johdetussa Euroopan unionin oikeudessa, nimittäin sähköisen viestinnän tietosuojaa koskevan direktiivin 5 artiklassa.

I.3 **Lausunnon tavoite ja jäsennys**

7. Tietosuojavaltuutettu katsoo, että vakavassa keskustelussa verkon neutraliteetista on käsiteltävä viestinnän luottamuksellisuutta sekä sen muita seurauksia yksityisyydelle ja tietosuojalle.

8. Tämä lausunto on osa Euroopan unionissa käytävää keskustelua. Lausunnon tavoite on kolmitahoinen:

— Siinä tähdennetään yksityisyyden ja tietosuojan merkitystä parhaillaan käytävissä keskusteluissa verkon neutraliteetista. Erityisesti lausunnossa korostetaan, että nykyisiä viestinnän luottamuksellisuutta koskevia sääntöjä on noudatettava. Vain sellaisia käytäntöjä tulisi sallia, jotka kunnioittavat näitä sääntöjä.

— Verkon neutraliteetti liittyy suhteellisen uusiin teknisiin mahdollisuuksiin, joten säädöskehyksen sovellettavuudesta on vain vähän kokemusta. Sen vuoksi tässä lausunnossa annetaan ohjeita siitä, miten internet-palveluntarjoajien tulee soveltaa ja noudattaa tietosuojalainsäädäntöä, jos ne osallistuvat verkkoliikenteen suodattamiseen, estämiseen ja valvontaan. Tästä on tarkoitus olla apua internet-palveluntarjoajille ja myös lainsäädännön täytäntöönpanosta vastaaville viranomaisille.

— Tietosuojan ja yksityisyyden osalta tässä lausunnossa määritetään, mihin alueisiin on kiinnitettävä erityistä huomiota ja mitkä saattavat edellyttää toimenpiteitä EU:n tasolla. Tämä on erityisen tärkeää EU-tasolla parhaillaan käytävän keskustelun sekä niiden poliittisten toimien osalta, jotka komission on mahdollisesti käynnistettävä.

([5]) Vastauksessaan tietosuojavaltuutettu korosti, että on tärkeää ottaa tietosuojaan ja yksityisyyteen liittyvät seikat huomioon muiden oikeuksien ja arvojen ohella. Lausunto on luettavissa osoitteessa http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

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

([7]) Tämä koskee sekä kiinteää että mobiilia internetyhteyttä.

([8]) Periaatetta ei kuitenkaan sovelleta siihen, että Internet-palveluntarjoajat rajoittavat nopeutta tai sen tiedon määrää, jota tilaaja voi lähettää tai vastaanottaa tilauksensa mukaisen kaistanleveyden tai määrällisten rajojen perusteella. Näin ollen verkon neutraliteettiperiaatetta sovellettaessakin internet-palveluntarjoajat voisivat edelleen tarjota internet-yhteystilauksia, joissa pääsyä on rajoitettu esimerkiksi nopeuden tai määrän perusteella, mikäli se ei ole syrjivää tietyn sisällön puolesta tai sitä vastaan.

9. Tietosuojavaltuutettu on tietoinen siitä, että verkon neutraliteetti herättää myös muita kysymyksiä, esimerkiksi tietojen käytettävyyteen liittyviä; niitä käsitellään jäljempänä. Näitä kysymyksiä käsitellään vain siltä osin kuin ne liittyvät tietosuojaan ja yksityisyyteen tai vaikuttavat niihin.

10. Tämä lausunto on jäsennetty seuraavasti: Luku II alkaa lyhyellä yhteenvedolla internet-palveluntarjoajien harjoittamista suodattamiskäytännöistä. Luvussa III luodaan katsaus verkon neutraliteettia koskevaan EU-lainsäädäntöön. Luvussa IV esitetään tekninen kuvaus ja arviointi suodattamiskäytäntöjen yksityisyyteen kohdistuvista seurauksista, jotka määräytyvät käytetyn tekniikan perusteella. Luvussa V analysoidaan EU:n nykyisen yksityisyys- ja tietosuojalainsäädännön soveltamisen käytännölliset yksityiskohdat. Analyysin perusteella luvussa VI esitetään ehdotuksia politiikan kehittämiseksi ja määritetään, millä alueilla lainsäädännön selventäminen ja parantaminen voivat olla tarpeen. Luvussa VII esitetään päätelmät.

II **VERKON NEUTRALITEETIN JA VERKKOLIIKENTEEN HALLINNAN PERIAATTEET**

Verkkoliikenteen hallinnan periaatteiden käyttö lisääntyy

11. Perinteisesti internet-palveluntarjoajat ovat osallistuneet verkon liikenteen valvontaan ja siihen vaikuttamiseen vain rajoitetuissa olosuhteissa. Internet-palveluntarjoajat ovat esimerkiksi soveltaneet valvontatekniikoita ja rajoittaneet tietovirtoja varmistaakseen verkon turvallisuuden vaikkapa virusten torjumiseksi. Yleisesti ottaen voidaankin sanoa, että internet on kasvanut säilyttäen silti hyvin suuren neutraliteetin.

12. Viime vuosina jotkin internet-palveluntarjoajat ovat kuitenkin osoittaneet kiinnostusta verkkoliikenteen valvontaan eriyttääkseen verkkoa ja soveltaakseen siihen erilaisia periaatteita esimerkiksi estääkseen tiettyjä palveluja tai asettaakseen tiettyjä palveluja toisiin nähden etusijalle. Tätä kutsutaan joskus ”verkkoliikenteen hallintaperiaatteiksi” ([9]).

13. Internet-palveluntarjoajilla on moninaisia syitä valvoa ja eriyttää verkkoliikennettä. Hallintaperiaatteiden avulla internet-palveluntarjoajat voivat esimerkiksi hallita verkkoliikennettä vilkkaan liikenteen aikana esimerkiksi ensisijaistamalla tiettyä aikakriittistä liikennettä, kuten suoratoistovideopalveluja, ja toissijaistamalla muuntyyppistä verkkoliikennettä, joka ei ole niin aikakriittistä, kuten vertaisverkot ([10]). Lisäksi verkkoliikenteen hallinta voi olla internet-palveluntarjoajille keino hankkia mahdollista tuottovirtaa, joka voi olla peräisin eri lähteistä. Toisaalta internet-palveluntarjoajat voivat myös periä maksuja sisältöpalvelujen tuottajilta, esimerkiksi niiltä, joiden palvelut edellyttävät suuremman kaistanleveyden käyttämistä, ja antavat siitä vastineeksi ensisijaistetun aseman (eli siis nopeutta). Tämä tarkoittaa sitä, että tietyn, esimerkiksi tilausvideoita tarjoavan palvelun käyttäminen on nopeampaa kuin jonkin vastaavan palvelun, jota varten ei ole tilattu suurempaa välitysnopeutta. Tuottoja voidaan hankkia myös tilaajilta, jotka haluavat maksaa suurempia (tai pienempiä) maksuja tietyntyyppisistä eriytetyistä tilauksistaan. Esimerkiksi tilaus ilman vertaisverkon käyttömahdollisuutta voi olla halvempi kuin tilaus, jossa pääsyä ei ole rajoitettu.

14. Internet-palveluntarjoajien omien verkkoliikenteen hallinnan periaatteiden käyttöä koskevien syiden lisäksi myös muut osapuolet voivat olla kiinnostuneita internet-palveluntarjoajasta, joka käyttää verkkoliikenteen hallinnan periaatteita. Jos internet-palveluntarjoajat hallinnoivat verkkojaan ja osallistuvat laitteidensa läpi kulkevan sisällön valvontaan, ne todennäköisesti myös lisäävät valmiuksiaan havaita laittoman käytön, esimerkiksi tekijänoikeuksien rikkomisen tai pornografisen käytön.

([9]) Katso esimerkiksi 27. toukokuuta 2011 hyväksytty OFCOMin raportti ”Site blocking to reduce online copyright infringement” (sivustojen estäminen tekijänoikeusloukkauksien vähentämiseksi verkossa), joka on saatavana osoitteessa http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: ”Jotkin internet-palveluntarjoajat käyttävät verkossaan jo pakettivalvontajärjestelmiä liikenteen valvontaan ja muihin tarkoituksiin. On siis oletettavaa, että niitä voidaan käyttää, vaikka se olisikin erittäin monimutkaista ja vaikka siitä aiheutuisikin kustannuksia niille, jotka eivät vielä tarjoa tällaisia palveluita. Voi olla, että lyhyellä tai keskipitkällä aikavälillä internet-tietoliikennepakettien syvätarkastusta (deep packet inspection, DPI) voivat toteuttaa vain suuremmat internet-palveluntarjoajat, jos niillä on tarvittavaa pääomaa.”

([10]) 10 Tosiaikaisten sovellusten, kuten suoratoistovideoiden, laatu määräytyy muun muassa latenssiajan perusteella, eli esimerkiksi verkon kuormituksesta johtuvan viiveen perusteella.

Muut edut sekä tietosuoja ja yksityisyys

15. Tämä suuntaus on käynnistänyt keskustelun tämäntyyppisten käytäntöjen laillisuudesta eritoten sen kannalta, olisiko kehitettävä nimenomaisia lakisääteisiä verkon neutraliteettia koskevia velvoitteita.

16. Jos internet-palveluntarjoajat lisäävät verkkoliikenteen hallinnan periaatteiden käyttöä, se mahdollisesti rajoittaa tiedon saatavuutta. Jos tällaisesta toiminnasta tulee yleinen käytäntö ja jos käyttäjät eivät voi käyttää internetiä kokonaisuudessaan sillä tavoin kuin olemme tottuneet (tai jos se on hyvin kallista), tiedon saatavuus sekä käyttäjän kyky lähettää ja vastaanottaa haluamaansa sisältöä valitsemiensa sovellusten tai palvelujen avulla vaarantuu. Tämä ongelma saatetaan välttää verkon neutraliteettia koskevan lakisääteisen pakollisen periaatteen avulla.

17. Tähän liittyvät tietosuojavaltuutetun käsittelemät tietosuojaan ja yksityisyyteen kohdistuvat seuraukset, joita koituu internet-palveluntarjoajien toteuttaessa verkkoliikenteen hallintaa. Asiaan liittyvät etenkin seuraavat seikat:

— Kun internet-palveluntarjoajat käsittelevät verkkoliikennetietoja ainoana tarkoituksenaan tietovirran reititys lähettäjältä vastaanottajalle, ne periaatteessa toteuttavat rajoitettua henkilötietojen käsittelyä ([11]). Samalla tavoin kuin postitoimistot käsittelevät kirjekuoreen kirjoitettuja tietoja, internet-palveluntarjoajat käsittelevät tietoja, joita tarvitaan viestin reitittämiseksi vastaanottajalle. Tämä ei ole ristiriidassa tietosuojaa, yksityisyyttä ja viestinnän luottamuksellisuutta koskevan lainsäädännön kanssa.

— Kun internet-palveluntarjoajat valvovat viestintätietoja eriyttääkseen kutakin tietovirtaa ja soveltaakseen tiettyjä periaatteita, jotka voivat olla yksilöiden kannalta epäsuotuisia, seuraukset ovat kuitenkin merkittävämpiä. Kunkin tapauksen olosuhteiden ja toteutetun analyysin tyypin mukaan käsittelyllä voidaan puuttua yksilön yksityisyyteen ja henkilötietoihin hyvinkin paljon. Tämä on sitäkin selvempää, jos hallinnan periaatteet johtavat yksilöiden internet-viestinnän sisällön paljastumiseen, mukaan luettuina lähetetyt ja vastaanotetut sähköpostiviestit, selatut verkkosivut, internetistä tai internetiin ladatut tiedostot jne.

III YHTEENVETO EUROOPAN UNIONIN VERKON NEUTRALITEETTIA KOSKEVASTA LAINSÄÄDÄNNÖSTÄ JA MUISTA PERIAATTEISTA

III.1 Tiivistelmä lainsäädännöstä

18. Vuoteen 2009 saakka Euroopan unionin säädöksissä ei ollut sellaisia nimenomaisia määräyksiä, joilla internet-palveluntarjoajia kiellettäisiin suodattamasta tai estämästä palveluja tai perimästä ylimääräisiä maksuja tilaajilta palvelujen saatavuudesta. Säädöksissä ei tuolloin ollut myöskään nimenomaisia määräyksiä tätä käytäntöä varten. Tilanne oli siis jossain määrin epäselvä.

19. Vuoden 2009 Telecom-paketti muutti tilanteen, sillä se sisälsi internetin avoimuutta puoltavia määräyksiä. Esimerkiksi sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä annetun direktiivin (”puitedirektiivi”) 8 artiklan 4 kohdassa sääntelyviranomaisille asetetaan velvoite edistää loppukäyttäjien mahdollisuuksia käyttää haluamiaan sisältöjä, sovelluksia ja palveluja ([12]). Tätä määräystä sovelletaan koko verkkoon, ei siis pelkästään yksittäisiin palveluntarjoajiin. Myös neuvoston äskettäisessä päätösluonnoksessa korostettiin, että internetin avoimuus on säilytettävä ([13]).

([11]) Tähän eivät kuulu operaatiot, joiden tavoitteena on lisätä verkon turvallisuutta ja havaita haitallinen liikenne, eivätkä laskutukseen ja yhteenliittämiseen tarvittavat operaatiot. Tähän eivät kuulu myöskään tietojen säilyttämistä koskevan direktiivin (Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta (EYVL L 105, 13.4.2006, s. 54.)) nojalla syntyneet velvoitteet.

([12]) Direktiivi 2002/21/EY, annettu 7 päivänä maaliskuuta 2002, sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä, sellaisena kuin se on muutettuna direktiivillä 2009/140/EY ja asetuksella (EY) N:o 544/2009 (EUVL L 337, 18.12.2009, s. 37).

([13]) Katso 3 kohdan e alakohta, jossa neuvosto toteaa näin: ”Internetin avoimuus on säilytettävä ja varmistettava, että se voi edelleen tuottaa laadukkaita palveluita sananvapauden ja elinkeinovapauden kaltaisia perusoikeuksia edistäen ja kunnioittaen” sekä 8 kohdan d alakohta, jossa jäsenvaltioita kehotetaan ”edistämään internetin avoimuutta ja neutraaliutta poliittisena tavoitteenaan”.

20. Yleispalveludirektiivissä ([14]) on konkreettisempia velvoitteita. Direktiivin 20 ja 21 artiklassa säädetään avoimuusvaatimuksista, jotka koskevat palvelujen ja sovellusten saatavuuden ja/tai käytön rajoituksia. Niissä säädetään myös tarjottavien palvelujen laadun vähimmäistasosta.

21. Niiden internet-palveluntarjoajien käytäntöjen osalta, joihin liittyy yksilön tietoliikenteen valvontaa, yleispalveludirektiivin ja sähköisen viestinnän tietosuojasta annetun direktiivin muuttamisesta annetun direktiivin johdanto-osan 28 kappaleessa ([15]) korostetaan, että ”käytetyn tekniikan ja rajoituksen tyypin mukaan tällaiset rajoitukset saattavat edellyttää käyttäjän suostumusta direktiivin 2002/58/EY (sähköisen viestinnän tietosuojaa koskeva direktiivi) mukaisesti”. Johdanto-osan 28 kappaleessa muistutetaan siis, että tarvitaan sähköisen viestinnän tietosuojaa koskevan direktiivin 5 artiklan 1 kohdan mukainen suostumus rajoituksille, jotka perustuvat viestinnän valvontaan. Viidennen artiklan 1 kohdan soveltamista sekä tietosuojaa ja yksityisyyttä koskevaa lainsäädäntöä kokonaisuudessaan analysoidaan jäljempänä luvussa IV.

22. Yleispalveludirektiivin 22 artiklan 3 kohdassa säädetään, että kansalliset sääntelyviranomaiset voivat asettaa palvelun laatuun liittyviä vähimmäisvaatimuksia yleisiä viestintäverkkoja tarjoaville yrityksille estääkseen palvelun heikkenemisen ja liikenteen rajoittumisen tai hidastumisen verkoissa.

23. Edellä esitetty tarkoittaa sitä, että EU:n tasolla avointa internetiä kannatetaan laajalti (katso puitedirektiivin 8 artiklan 4 kohta). Tämä poliittinen tavoite, jota sovelletaan koko verkkoon, ei kuitenkaan liity suoraan yksittäisiä internet-palveluntarjoajia koskeviin kieltoihin tai velvoitteisiin. Toisin sanoen internet-palveluntarjoaja voi toteuttaa verkkoliikenteen hallinnan periaatteita, jotka voivat estää tiettyjen sovellusten saatavuuden, jos loppukäyttäjät ovat siitä täysin tietoisia ja jos nämä ovat antaneet asiaan vapaaehtoisen, nimenomaisen ja yksiselitteisen suostumuksensa.

24. Tilanne voi vaihdella eri jäsenvaltioissa. Joissakin jäsenvaltioissa internet-palveluntarjoajat voivat tietyillä ehdoilla toteuttaa verkkoliikenteen hallinnan periaatteita esimerkiksi estääkseen sellaisia sovelluksia kuin internetpuhelut (VoIP) (jolloin internetyhteys on edullisempi), jos henkilö on antanut siihen vapaaehtoisen, nimenomaisen ja yksiselitteisen tietoisen suostumuksensa. Toisissa jäsenvaltioissa on taas päätetty vahvistaa verkon neutraliteetin periaatetta. Esimerkiksi Alankomaiden parlamentti hyväksyi heinäkuussa 2011 lain, jolla yleisesti kielletään palveluntarjoajia estämästä tai hidastamasta internetin sovelluksia tai palveluja (kuten internetpuheluja), ellei se ole ehdottoman välttämätöntä verkon ruuhkautumisen vaikutusten lieventämiseksi, verkon eheyden tai turvallisuuden vuoksi tai roskapostin torjumiseksi tai tuomioistuimen päätöksen mukaista ([16]).

III.2 **Verkon neutraliteettia koskeva tiedonanto**

25. Verkon neutraliteettia koskevassa tiedonannossaan ([17]) Euroopan komissio totesi, että verkon neutraliteetin tilannetta on seurattava ja analysoitava lisää. Sen toimintaperiaatetta on kuvattu ilmauksella ”katsotaan, mitä tapahtuu” ennen muihin lainsäädännöllisiin toimiin ryhtymistä.

([14]) Direktiivi 2002/22/EY, sellaisena kuin se on muutettuna Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta (EUVL L 337, 18.12.2009, s. 11). Vertaa myös 1 artiklan 3 kohtaa, jossa todetaan, että ”tässä direktiivissä ei määrätä pakollisiksi eikä rajoiteta yleisesti saatavilla olevien sähköisten viestintäverkkojen ja -palvelujen tarjoajien asettamia ehtoja, joilla rajoitetaan loppukäyttäjille tarjottavien palvelujen ja sovellusten saatavuutta ja käyttöä, jos ne ovat sallittuja kansallisen ja yhteisön lainsäädännön mukaisesti, mutta siinä säädetään velvollisuus antaa tällaisia ehtoja koskevat tiedot.”

([15]) Euroopan parlamentin ja neuvoston direktiivi 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta.

([16]) Alkuperäinen hollanninkielinen muutos on saatavana osoitteessa https://zoek.officielebekendmakingen.nl/kst-32549-A.html Tiedotusvälineiden ilmoittamissa syissä tämän toimintalinjan valintaan ei viitattu tietosuojan ja yksityisyyden näkökohtiin vaan pikemminkin sen varmistamiseen, etteivät käyttäjät jää vaille tietoa tai ettei tiedon saatavuutta rajoiteta. Näyttää siis siltä, että tämän muutoksen perusteina olivat tiedon saatavuuteen liittyvät seikat.

([17]) Katso alaviite 4.

26. Komission tiedonannossa todettiin, että kaikki tämän alan mahdolliset lainsäädäntöehdotukset arvioitaisiin perusteellisesti sen suhteen, millaisia vaikutuksia niillä on tietosuojaan ja yksityisyyteen. Neuvoston päätelmien luonnoksessa tietosuojaan ja yksityisyyteen liittyvät seikat on niin ikään otettu huomioon. ([18])

27. Tietosuojan ja yksityisyyden kannalta arvioitava kysymys kuuluu, onko ”katsotaan, mitä tapahtuu” -toimintaperiaate riittävä. Vaikka tietosuojaa ja yksityisyyttä koskeva lainsäädäntö antaa tällä hetkellä tiettyjä takeita etenkin viestinnän luottamuksellisuuden periaatteen kautta, näyttää olevan tarpeen seurata säännösten noudattamista tarkemmin ja antaa ohjeita monista seikoista, jotka eivät ole kovin selviä. Lisäksi olisi kehitettävä ideoita siitä, miten lainsäädäntöä voitaisiin selventää ja parantaa teknisen kehityksen kannalta. Jos seuranta osoittaa, että markkinoilla ollaan siirtymässä kohti laaja-alaista, tosiaikaista viestinnän valvontaa ja että lainsäädännön noudattamiseen liittyy ongelmia, tarvitaan lainsäädännöllisiä toimia. Tämän lausunnon luvussa VI esitetään asiaan liittyviä konkreettisia ehdotuksia.

IV **TEKNINEN TAUSTA JA SIIHEN LIITTYVÄT VAIKUTUKSET YKSITYISYYTEEN JA TIETOSUOJAAN**

28. Ennen kuin aihetta aletaan käsitellä perusteellisemmin, on tärkeää saada parempi käsitys valvontatekniikoista, joita internet-palveluntarjoajat voivat käyttää verkkoliikenteen hallinnassa, sekä niiden mahdollisista vaikutuksista verkon neutraliteetin periaatteeseen. Näiden tekniikkojen vaikutus yksityisyyteen ja tietosuojaan vaihtelee huomattavasti sen mukaan, mitä tekniikkaa tai tekniikkoja käytetään. Tämä tekninen taustatieto on tarpeen, jotta luvussa V kuvattua tietosuojalainsäädäntöä voitaisiin ymmärtää ja soveltaa asianmukaisesti. On kuitenkin todettava, että asia on monimutkainen ja jatkuvasti muuttuva. Sen vuoksi jäljempänä esitettyä kuvausta ei ole tarkoitettu kattavaksi ja täysin ajantasaiseksi, vaan sillä on tarkoitus antaa sellaista teknistä tietoa, joka on välttämätöntä oikeudellisen perustelun ymmärtämiseksi.

IV.1 **Tiedon siirto internetin kautta: perusperiaatteet**

29. Kun käyttäjä siirtää tietoa internetin kautta, välitettävä tieto jaetaan paketteihin. Nämä paketit välitetään internetin kautta lähettäjältä vastaanottajalle. Kussakin paketissa on tietoa esimerkiksi lähteestä ja määränpäästä. Lisäksi internet-palveluntarjoajat saattavat laittaa nämä paketit lisäkerroksiin ja -käytäntöihin ([19]), joita käytetään eri liikennevirtojen hallintaan internet-palveluntarjoajien verkossa.

30. Edellä esitettyyn kirje-esimerkkiin viitaten: verkon siirtokäytännön käyttäminen vastaa sitä, että kirjekuoreen kirjoitetun osoitteen lisäksi myös kuoreen laitetun kirjeen sisältö luetaan postitoimistossa, ja kirje toimitetaan vasta sitten perille. Postitoimisto voi käyttää lisäkäytäntöjä sisäisissä siirroissaan hoitaakseen kaikki siirrettävät kirjekuoret, ja tavoitteena on, että kukin kirjekuori pääsee määränpäähänsä sellaisena kuin lähettäjä on alun perin laatinut sen. Tätä analogiaa käyttäen kussakin paketissa on kaksi osaa: *IP-hyötykuorma*, joka sisältää viestinnän sisällön ja joka vastaa kirjettä. Se sisältää tietoa, joka on tarkoitettu vain vastaanottajalle. Paketin toinen osa on *IP-otsikko*, joka sisältää esimerkiksi vastaanottajan ja lähettäjän osoitteen. Se vastaa kirjekuorta. IP-otsikon avulla internet-palveluntarjoajat ja muut välittäjät voivat reitittää hyötykuorman sen lähdeosoitteesta sen määränpääosoitteeseen.

31. Internet-palveluntarjoajat ja muut välittäjät varmistavat, että IP-paketit kulkevat verkossa solmujen kautta, jotka lukevat IP-otsikon tiedot, vertaavat sitä reititystaulukoihin ja välittävät paketit sitten eteenpäin seuraavaan solmuun matkalla määränpäähän. Tämä menettely toteutetaan verkossa käyttämällä

([18]) Katso 4 kohdan e alakohta, jossa neuvosto toteaa: ”Henkilötietojen suojeluun liittyy joitakin huolenaiheita, joita ovat esittäneet pääasiassa kuluttajat ja tietosuojaviranomaiset”.

([19]) Kuten jäljempänä luvussa IV.2 kuvataan, nämä käytännöt koodaavat siirrettävän tiedon sovitulla tavalla niin, että viestinnän osapuolet ymmärtävät toisiaan, kuten HTTP, FTP jne.

best effort memoryless -toimintatapaa, sillä kaikkia solmuun saapuvia paketteja käsitellään neutraalilla tavalla. Kun ne on välitetty seuraavaan solmuun, tietoja ei tarvitse enää säilyttää reitittimessä ([20]).

IV.2 **Valvontatekniikat**

32. Kuten edellä on kuvattu, internet-palveluntarjoajat lukevat IP-osoitteet, jotta he voivat reitittää paketit eteenpäin määränpäähänsä. Kuten edellä on esitetty, liikennettä (mukaan luettuina IP-osoitteet ja IP-hyötykuormat) voidaan analysoida myös muita tarkoituksia varten ja erityyppisillä tekniikoilla. Uusia suuntauksia voivat olla esimerkiksi, että tiettyjä käyttäjien käyttämiä sovelluksia kuten vertaisverkkoja hidastetaan tai että liikennenopeutta lisätään tiettyjä palveluja, esimerkiksi tilausvideoita varten kalliimpien palvelujen tilaajille. Vaikka kaikilla valvontatekniikoilla paketin tarkastus toteutetaan *teknisesti*, niiden yksityisyyteen puuttumisen aste vaihtelee. On olemassa kaksi pääasiallista valvontatekniikkaa. Toinen perustuu vain IP-otsikkoon, toinen IP-hyötykuormaan.

IP-otsikon tietoihin perustuva järjestelmä: IP-paketin otsikon tarkastuksessa paljastuu muutamia kenttiä, joihin internet-palvelujen tarjoajat voivat soveltaa monenlaisia verkkoliikenteen hallinnan periaatteita. Nämä tekniikat perustuvat ainoastaan IP-otsikoiden käsittelytietojen tarkastukseen. Nämä tiedot on periaatteessa tarkoitettu reititystiedoiksi eri tarkoituksiin (esimerkiksi verkkoliikenteen eriyttämiseen). Lähtöpaikan IP-osoitteen perusteella internet-palveluntarjoaja voi liittää sen tiettyyn tilaajaan ja soveltaa tiettyjä periaatteita, esimerkiksi reitittää paketin nopeamman tai hitaamman linkin kautta. Määränpään IP-osoitteen perusteella internet-palveluntarjoaja voi myös soveltaa tiettyjä periaatteita, esimerkiksi estää tai suodattaa pääsyn tietyille verkkosivustoille.

Syvätarkastukseen perustuva järjestelmä: Paketin syvätarkastuksen avulla internet-palveluntarjoaja pääsee käsiksi ainoastaan viestin vastaanottajalle tarkoitettuihin tietoihin. Postitoimistoesimerkkiä käyttääksemme tämä toimintatapa vastaa kirjekuoren avaamista ja kirjeen lukemista viestin sisällön (kapseloituna IP-pakettien sisään) analysoimiseksi, jotta tiettyä verkkoperiaatetta voitaisiin soveltaa. Tarkastus voidaan toteuttaa monin eri tavoin, joista kukin aiheuttaa erilaisia uhkia sille, jota tiedot koskevat.

— *Paketin syvätarkastus perustuu käytäntöjen ja tilastollisten tallenteiden analyysiin.* IP-yhteyskäytännön tehtävänä on mahdollistaa tietojen siirto internetin kautta. Sen lisäksi on myös muita käytäntöjä, joilla koodataan siirrettävä tieto sovitulla tavalla (siirto, yhteysjakso, esitys, sovellus jne.) Näiden käytäntöjen tarkoituksena on varmistaa, että viestinnän osapuolet voivat ymmärtää toisiaan. On olemassa esimerkiksi web-selailuun tarkoitettuja käytäntöjä ([21]), tiedoston siirtoon tarkoitettuja käytäntöjä ([22]) jne. Siksi käytäntöjen tarkastukseen perustuvien tarkastustekniikoiden, joihin on yhdistetty tilastollinen analyysi, tavoitteena on havaita tiettyjä malleja tai sormenjälkiä, jotka määrittävät, mitkä käytännöt ovat käytössä ([23]). Näiden tarkastustekniikoiden avulla internet-palveluntarjoajat voivat ymmärtää viestinnän tyypin (sähköposti, web-selailu, tiedostojen lataus) ja joissakin tapauksissa määrittää tietyn palvelun tai käytetyn sovelluksen. Näin on esimerkiksi tiettyjen internetpuheluviestien osalta, joissa käytännöt ovat vahvasti myyjä- tai palveluntarjoajakohtaisia. Viestinnän tyyppiä koskevan tiedon avulla internet-palveluntarjoajat voivat soveltaa konkreettisia verkkoliikenteen hallinnan periaatteita. He voivat esimerkiksi estää verkkoliikenteen. Se voi myös olla ensimmäinen vaihe siinä, että internet-palvelutarjoaja voi toteuttaa muita analyyseja, joita varten saatetaan tarvita täyttä pääsyä metatietoihin ja viestinnän sisältöön.

([20]) Internetin verkkolaitteet käyttävät kuitenkin reitityskäytäntöjä, joihin tallennetaan toimintatietoja, joissa käsitellään liikennetilastoja ja joissa vaihdetaan tietoja muiden verkkolaitteiden kanssa IP-pakettien reitittämiseksi tehokkainta reittiä pitkin. Kun jokin linkki on ruuhkautunut tai rikki ja kun reititin saa tästä tiedon, se päivittää reititystaulukkoon vaihtoehtoja, jotka eivät käytä tätä linkkiä. Kannattaa myös muistaa tietojen keruu ja käsittely, jota voidaan tehdä tietyissä tapauksissa laskutustarkoituksiin tai jopa tietojen säilyttämistä koskevan direktiivin nojalla.

([21]) HTTP – Hypertext transfer protocol eli verkkosivujen korkean tason yhteyskäytäntö, tai HTML – Hypertext Markup Language eli hypertekstin merkintäkieli, jota käytetään verkkosivujen laatimisessa.

([22]) FTP – File transfer protocol eli TCP-yhteyskäytäntöön perustuva verkkoasemien välisen tiedostonsiirron käytäntö.

([23]) Käytetyn käytännön määrittämiseen on erilaisia tapoja. Voidaan esimerkiksi etsiä sisäisten käytäntöjen tiettyjä kenttiä esimerkiksi viestin laatimiseen käytettyjen porttien määrittämiseksi. Viestivirran tilastollinen luonnehdinta voidaan myös päätellä tiettyjen kenttien analyysista tai kahden IP-osoitteen välillä samanaikaisesti käytettyjen yhteyskäytäntöjen korrelaatiosta.

— *Paketin syvätarkastus perustuu viestinnän sisällön analyysiin.* On myös mahdollista tarkastaa metatietoja ([24]) sekä itse viestinnän sisältö. Tässä tekniikassa siepataan kaikki alkuperäisen viestivirran osana olevat IP-paketit, jotta viestinnän alkuperäinen sisältö voidaan rekonstruoida kokonaan ja analysoida. Esimerkiksi haitallisen tai laittoman sisällön, kuten virusten tai lapsipornon havaitsemiseksi sisältö itsessään on rekonstruoitava, jotta sisältö voidaan analysoida. Todettakoon, että joskus viestinnän osapuolet voivat nimenomaisesti salata viestinnän. Tämä estää internet-palveluntarjoajia suorittamasta viestinnän sisällön analyysia.

IV.3 **Vaikutukset yksityisyyden suojaan ja tietosuojaan**

33. IP-otsikoihin ja etenkin pakettitarkastuksiin perustuviin tekniikoihin kuuluu näiden tietojen valvontaa ja suodatusta, joista on vakavia seurauksia yksityisyyden ja tietosuojan kannalta. Ne voivat olla myös ristiriidassa viestinnän luottamuksellisuutta koskevan oikeuden kanssa.

34. Yksilöiden viestinnän tarkastelusta on jo sinällään vakavia yksityisyyteen ja tietosuojaan liittyviä seurauksia. Ongelma on kuitenkin laajempi, sillä valvonnan ja tietojen sieppauksen vaikutusten mukaan yksityisyyteen liittyvät seuraukset saattavat lisääntyä entisestään. On aivan eri asia pelkästään valvoa viestintää esimerkiksi sen varmistamiseksi, että järjestelmä toimii hyvin, kuin valvoa viestintää sellaisten periaatteiden soveltamiseksi, jotka voivat vaikuttaa yksilöihin. Se, että verkkoliikenteeseen ja valintaan sovellettavilla periaatteilla pyritään välttämään ainoastaan verkon ruuhkautumista, ei yleensä vaikuta merkittävästi yksilön yksityisyyteen. Verkkoliikenteen hallinnan periaatteilla voidaan kuitenkin pyrkiä myös estämään joitakin sisältötietoja tai vaikuttaa viestintään esimerkiksi verkkokäyttäytymiseen perustuvalla mainonnalla. Näissä tapauksissa yksityisyyteen puututaan enemmän. On huolestuttavampaa, jos havaitaan, ettei tämäntyyppistä tietoa kerättäisi pienestä ryhmästä yksilöitä, vaan pikemminkin yleisesti kaikilta internet-palveluntarjoajien asiakkailta ([25]). Jos kaikki internet-palveluntarjoajat käyttävät suodatustekniikoita, se voi johtaa internetin käytön valvonnan yleistymiseen. Ja jos tarkastellaan käsiteltävän tiedon tyyppiä, yksityisyyteen kohdistuvat riskit ovat luonnollisesti suuret, koska kerättävästä tiedosta suuri osa on todennäköisesti arkaluontoista, ja keruun jälkeen se on internet-palveluntarjoajien ja muiden sellaisten tahojen saatavilla, jotka pyrkisivät saamaan tietoa niiltä. Lisäksi tiedot voivat olla arvokkaita myös kaupallisessa mielessä. Tässä piilee myös suuri riski, että tietoja käytetään myös muihin tarkoituksiin, jolloin alkuperäisen tarkoituksen lisäksi voisi syntyä kerättyjen tietojen kaupallista tai muuta hyväksikäyttöä.

35. Valvonta-, tarkastus- ja suodatustekniikkoja on käytettävä sovellettavan tietosuojan ja yksityisyyden suojan mukaisesti. Niitä koskevissa säännöksissä määritetään rajat sille, mitä voidaan tehdä milläkin ehdoilla. Seuraavaksi tässä lausunnossa esitetään yhteenveto EU:n nykyisen tietosuojaa ja yksityisyyden suojaa koskevan lainsäädännön nojalla sovellettavista suojatoimenpiteistä.

V **EUROOPAN UNIONIN YKSITYISYYS- JA TIETOSUOJALAINSÄÄDÄNNÖN SOVELTAMINEN**

36. Euroopan unionin tietosuojalainsäädäntö on tekniikan kannalta neutraali, eli siinä ei säädetä tietyistä, edellä kuvattujen kaltaisista tarkastustekniikoista. Sähköisen viestinnän tietosuojaa koskevassa direktiivissä säädetään yksityisyydestä sähköisten viestintäpalvelujen alalla julkisissa verkoissa (tyypillisesti

([24]) Kunkin käytännön otsikossa on tiettyjä kenttiä, jotka antavat epämuodollista lisätietoa siirrettävästä viestinnästä. Siksi näiden kenttien sisältöä voidaan kutsua viestinnän metatiedoiksi. Esimerkki näistä kentistä voi olla vaikkapa käytetyn portin numero, ja jos se on esimerkiksi 80, on todennäköistä, että viestinnän tyyppi on web-selailu.

([25]) Tietojen seurantaan pystyvät toki muutkin kuin vain internet-palveluntarjoajat. Myös verkkomainonnan tarjoajat pystyvät seuraamaan käyttäjiä verkkosivustoilla käyttämällä kolmannen osapuolen evästeitä. Lue esimerkiksi hiljattain julkaistu akateeminen artikkeli, joka osoittaa, että Google on läsnä 97:ssä sadasta suosituimmasta verkkosivustosta. Tämä tarkoittaa sitä, että Google voi seurata käyttäjiä, jotka eivät ole poistaneet kolmannen osapuolen evästeitä käytöstä näitä suosittuja verkkosivustoja selaillessaan. Ks. Ayenson Mika, Wambach Dietrich James, Soltani Ashkan, Good Nathan ja Hoofnagle Chris Jay: Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (29.7.2011). Saatavana osoitteessa http://ssrn.com/abstract=1898390 29 artiklan työryhmä on käsitellyt käyttäjien seurantaa kolmannen osapuolen evästeitä käyttämällä. Katso lausunto 2/2010 verkkokäyttäytymiseen perustuvasta mainonnasta, hyväksytty 22. kesäkuuta 2010 (WP 171).

internet ja puhelin) ([26]), ja tietosuojadirektiivissä säädetään tietojen käsittelystä yleensä. Kaiken kaikkiaan lainsäädännössä asetetaan erilaisia velvoitteita, jotka koskevat liikenne- ja viestintätietoja käsitteleviä ja valvovia internet-palveluntarjoajia.

V.1 **Liikenne- ja sisältötietojen käsittelemisen oikeudelliset perusteet**

37. Tietosuojalainsäädännön nojalla henkilötietojen käsittelylle (tässä tapauksessa liikenne- ja viestintätietojen käsittelylle) on oltava asianmukaiset oikeudelliset perusteet. Tämän yleisen vaatimuksen lisäksi tiettyihin tapauksiin voidaan soveltaa erityisvaatimuksia.

38. Tässä tapauksessa internet-palveluntarjoajien käsittelemillä henkilötiedoilla tarkoitetaan verkkoliikennetietoja ja viestien sisältöä. Viestien luottamuksellisuutta ja liikennetietoja suojaa oikeus luottamukselliseen kirjeenvaihtoon, joka taataan Euroopan ihmisoikeussopimuksen 8 artiklassa ja perusoikeuskirjan 7 ja 8 artiklassa. Sähköisen viestinnän tietosuojaa koskevan direktiivin 5 artiklan, jonka otsikko on ”Viestinnän luottamuksellisuus”, 1 kohdassa jäsenvaltioita vaaditaan varmistamaan yleisen viestintäverkon ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen välityksellä tapahtuvan viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuus. Samalla sähköisen viestinnän tietosuojadirektiivin 5 artiklan 1 kohdan mukaan internet-palveluntarjoajat saavat käsitellä liikenne- ja sisältötietoja tietyillä ehdoilla käyttäjien suostumuksella. Tämä tehdään kieltämällä se, että ”muut henkilöt kuin käyttäjät ilman kyseisten käyttäjien nimenomaista suostumusta kuuntelevat, salakuuntelevat, tallentavat tai muulla tavalla sieppaavat tai valvovat viestintää ja siihen liittyviä liikennetietoja, jollei se ole laillisesti sallittua 15 artiklan 1 kohdan mukaisesti”. Tätä selostetaan tarkemmin jäljempänä.

39. Käyttäjien suostumuksen lisäksi sähköisen viestinnän tietosuojaa koskevassa direktiivissä luetellaan muita perusteita, joiden nojalla internet-palveluntarjoajat voivat käsitellä liikenne- ja viestintätietoja perustellusti. Tässä tapauksessa oleelliset käsittelyn oikeudelliset perusteet ovat i) palvelun toimittaminen, ii) palvelun turvallisuuden takaaminen ja iii) ruuhkautumisen minimoiminen. Muita mahdollisia perusteita, jotka oikeuttavat liikenne- ja viestintätietoihin pohjautuvia hallinnan periaatteita, käsitellään jäljempänä kohdassa iv).

i) Oikeudelliset perusteet palvelun toimittamiselle

40. Kuten luvussa IV on kuvattu, internet-palveluntarjoajat käsittelevät IP-otsikoissa olevia tietoja reitittääkseen kunkin IP-paketin kohti määränpäätään. Sähköisen viestinnän tietosuojadirektiivin 6 artiklan 1 kohdan ja 6 artiklan 2 kohdan mukaan liikennetietojen käsittely on sallittua viestinnän välittämiseksi. Internet-palveluntarjoajat voivat siis käsitellä tietoja, joita tarvitaan palvelun tuottamiseen.

ii) Oikeudelliset perusteet palvelun turvallisuuden takaamiselle

41. Sähköisen viestinnän tietosuojaa koskevan direktiivin 4 artiklan nojalla internet-palveluntarjoajalla on yleinen velvollisuus ryhtyä asianmukaisiin toimiin palvelujensa turvallisuuden takaamiseksi. Virusten suodattamiskäytänteisiin saattaa liittyä IP-otsikoiden ja IP-hyötykuorman käsittelyä. Ottaen huomioon, että sähköisen viestinnän tietosuojaa koskevan direktiivin 4 artiklassa internet-palveluntarjoajien edellytetään varmistavan verkon turvallisuuden, tällä määräyksellä oikeutetaan tarkastustekniikat, jotka perustuvat IP-otsikoihin ja sisältöön ja joiden tavoitteena on nimenomaan täyttää tämä velvoite. Käytännössä tämä tarkoittaa sitä, että suhteellisuusperiaatteen asettamien rajojen mukaisesti (katso luku V.3) internet-palveluntarjoajat voivat osallistua viestintätietojen valvontaan ja suodattamiseen torjuakseen viruksia ja varmistaakseen verkon turvallisuuden yleisesti ([27]).

([26]) Sähköisen viestinnän tietosuojaa koskevan direktiivin johdanto-osan 10 kappale: ”Sähköisen viestinnän alalla direktiiviä 95/46/EY sovelletaan erityisesti kaikkien sellaisten perusoikeuksien ja -vapauksien turvaamista koskevien kysymysten osalta, jotka eivät nimenomaisesti sisälly tämän direktiivin säännöksiin, rekisterinpitäjän velvoitteet ja yksilöiden oikeudet mukaan lukien.” Myös johdanto-osan 17 kappale on oleellinen rekisteröidyn suostumuksen osalta: ”Tässä direktiivissä käyttäjän tai tilaajan suostumuksella olisi, siitä riippumatta, onko kyseessä luonnollinen vai oikeushenkilö, tarkoitettava samaa kuin rekisteröidyn suostumuksella direktiivissä 95/46/EY määritellyn ja tarkennetun mukaisesti.”

([27]) 29 artiklan työryhmän lausunto 2/2006 yksityisyyteen liittyvistä seikoista, jotka koskevat sähköpostien tarkastuspalvelusta annettua määräystä, annettu 21. helmikuuta 2006 (WP 118). Tässä lausunnossa työryhmä katsoo, että suodattimien käyttö 4 artiklan mukaiseen tarkoitukseen voi olla sähköisen viestinnän tietosuojaa koskevan direktiivin 5 artiklan mukainen.

iii) Oikeudelliset perusteet ruuhkautumisen vaikutusten minimoimiselle

42. Tämä oikeudellinen peruste *perustuu* sähköisen viestinnän tietosuojadirektiivin johdanto-osan 22 kappaleeseen, joka selittää myös 5 artiklan 1 kohdassa tarkoitetun viestien tallentamiskiellon. Tämä ei kuitenkaan estä automaattista, tilapäistä ja ohimenevää tallennusta, joka on tarpeen viestinnän välittämiselle ja joka ei kestä pidempään kuin on tarpeen viestien välittämisen ja liikenteen hallinnan kannalta ja jos viestinnän luottamuksellisuus on taattu.

43. Jos verkko ruuhkautuu, herää kysymys, voivatko internet-palveluntarjoajat porrastaa tai viivyttää liikennettä satunnaisesti tai hidastaa sitä viestintää, joka ei ole aikakriittistä, esimerkiksi vertaisverkko- tai sähköpostiliikenne, jolloin esimerkiksi ääniliikenne voidaan välittää hyväksyttävän laatuisena.

44. Koska viestintäverkon käytettävyyden takaaminen on yleisen yhteiskunnallisen edun mukaista, internet-palveluntarjoajat kenties väittävät, että liikenteen ensisijaistaminen tai hidastaminen ruuhkautumisen selvittämiseksi on perusteltu toimenpide, joka on tarpeen asianmukaisen palvelun tuottamiseksi. Tämä tarkoittaa sitä, että näissä tapauksissa ja tätä tarkoitusta varten henkilötietojen käsittelylle olisi olemassa yleinen oikeudellinen peruste, eikä käyttäjien nimenomaista suostumusta tällöin tarvittaisi.

45. Samalla mahdollisuus puuttua yksityisyyteen tällä tavoin ei kuitenkaan ole rajoittamaton. Jos internet-palveluntarjoajien on tarkastettava viestejä, luottamuksellisuuden kannalta ja suhteellisuusperiaatetta tiukasti noudattaen heidän on käytettävä sitä saatavilla olevaa menetelmää, jolla yksityisyyteen puututaan vähiten tarkoituksen täyttämiseksi (välttäen syväpakettitarkastusta), ja he saavat soveltaa menetelmää vain niin kauan kuin on tarpeen ruuhkan selvittämiseksi.

iv) Oikeudelliset perusteet tietojen käsittelylle muihin tarkoituksiin

46. Internet-palveluntarjoajat saattavat haluta tarkastaa verkkoliikenne- ja sisältötietoja myös muita tarkoituksia varten, esimerkiksi kohdistettujen tilausten tarjoamiseksi (esimerkiksi tilaus, jossa vertaisverkkojen käyttö on rajoitettu, tai tilaus, jossa nopeutta lisätään tiettyjä sovelluksia varten). Verkkoliikenne- ja viestintätietojen tarkastus ja käyttö muihin tarkoituksiin kuin palvelun tuottamiseen tai sen turvallisuuden takaamiseen ja ruuhkautumisen välttämiseen on sallittua ainoastaan tiukkojen ehtojen vallitessa lainsäädännön mukaisesti.

47. Lainsäädäntö tarkoittaa pääasiassa sähköisen viestinnän tietosuojaa koskevan direktiivin 5 artiklan 1 kohtaa, jossa edellytetään kyseisten asiakkaiden suostumusta viestinnän ja siihen liittyvien liikennetietojen kuuntelua, salakuuntelua, tallentamista tai muulla tavoin sieppaamista tai valvomista varten. Käytännössä tämä tarkoittaa sitä, että viestintään osallistuvien käyttäjien suostumus tarvitaan sekä liikenne- että viestintätietojen käsittelyn perustelemiseksi 5 artiklan 1 kohdan mukaisesti.

48. Kuten edellä on selostettu, tarkastus- ja suodatustekniikoiden soveltaminen perustuu joko IP-otsikoihin, joista muodostuu liikennetietoja, tai syväpakettitarkastuksiin, joissa käsitellään myös IP-hyötykuormia, joista puolestaan muodostuu viestintätietoja. Sen vuoksi tällaisten tekniikoiden käyttö muihin tarkoituksiin kuin palvelun välittämiseen tai turvallisuuden takaamiseen on periaatteessa kiellettyä, ellei käsittelylle ole oikeutettua perustetta, kuten esimerkiksi suostumus (5 artiklan 1 kohta). Direktiivin 5 artiklan 1 kohtaa sovellettaisiin esimerkiksi silloin, kun internet-palveluntarjoaja päättää tarjota asiakkaille edullisempaa internetyhteyttä vastineeksi verkkokäyttäytymiseen liittyvän mainonnan vastaanottamisesta, ja jotta mainoksia voitaisiin lähettää, on käytettävä syväpakettitarkastusta ja siis viestintätietoja. Sen vuoksi todellinen, nimenomainen ja tietoinen suostumus on tarpeen 5 artiklan 1 kohdan mukaisesti.

49. Sähköisen viestinnän tietosuojaa koskevan direktiivin 6 artiklassa, jonka otsikko on ”Liikennetiedot”, esitetään tiettyjä sääntöjä, jotka koskevat nimenomaan liikennetietoja. Artiklassa internet-palveluntarjoajille annetaan mahdollisuus käsitellä liikennetietoja, jos se perustuu käyttäjien suostumukseen

lisäarvopalvelujen vastaanottamiseksi ([28]). Tässä määräyksessä määritetään 5 artiklan 1 kohdassa tarkoitettu suostumusvaatimus liikennetietojen osalta.

50. Käytännössä ei ole kuitenkaan aina helppoa varmistaa, missä tapauksissa suostumus on tarpeen ja missä tapauksissa verkon turvallisuus riittää käsittelyn perusteeksi, etenkin jos tarkastustekniikoilla on useampia tarkoituksia (esimerkiksi ruuhkautumisen välttäminen ja lisäarvopalvelujen tarjoaminen). Korostettakoon, että suostumusta ei voida pitää helppona ja järjestelmällisenä keinona noudattaa tietosuojaperiaatteita.

51. Lainsäädännön soveltamisesta on vain vähän kokemusta varsinkin edellä esitettyjen erilaisten näkökohtien osalta. Tälle alueelle tarvitaan lisää ohjeistusta, kuten jäljempänä luvussa VI todetaan. On myös muita oleellisia suostumuksen hankkimiseen liittyviä näkökohtia, joita on pohdittava tarkkaan. Näitä kuvataan jäljempänä.

V.2 **Seikkoja, jotka liittyvät tietoisen suostumuksen esittämiseen oikeudellisena perusteena**

52. Sähköisen viestinnän tietosuojaa koskevan direktiivin 5 ja 6 artiklassa edellytetyn tietoisen suostumuksen tarkoitus on sama kuin rekisteröityä koskevan tietoisen suostumuksen siten kuin se on määritetty ja täsmennetty direktiivissä 95/46/EY ([29]). Tietosuojadirektiivin 2 artiklan h kohdan mukaisesti ”rekisteröidyn suostumuksella’ tarkoitetaan ’kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn’. Hiljattain 29 artiklan mukainen työryhmä on käsitellyt suostumuksen merkitystä ja vaatimuksia, jotta se olisi pätevä, suostumusta käsittelevässä lausunnossaan 15/2011 ([30]).

53. Internet-palveluntarjoajien, jotka tarvitsevat suostumuksen verkkoliikenne- ja sisältötietojen tarkastukseen ja suodatukseen, on siis varmistettava, että suostumus on vapaaehtoinen ja yksilöity ja että se on täysin tietoinen tahdon ilmaus, jolla yksilö hyväksyy henkilötietojensa käsittelyn. Sähköisen viestinnän tietosuojaa koskevan direktiivin johdanto-osan 17 kappale vahvistaa tämän: ”(...) Suostumus voidaan antaa käyttäen mitä tahansa soveltuvaa tapaa, joka mahdollistaa vapaasti esitetyn täsmällisen ja tietoon perustuvan ilmoituksen käyttäjän toiveista, mukaan lukien ruudun rastittaminen vierailtaessa internetsivustolla.” Jäljempänä esitetään muutamia käytännön esimerkkejä siitä, mitä vapaa, yksilöity ja tietoinen suostumus tarkoittaa tässä asiayhteydessä.

Suostumus: vapaa, yksilöity ja tietoinen tahdon ilmaus

54. *Vapaa suostumus.* Käyttäjien ei tulisi joutua kärsimään rajoituksista, jotka liittävät suostumuksen siihen internet-tilaukseen, jonka he haluavat tilata.

55. Yksilön suostumus ei ole vapaasti annettu, jos hänen täytyy suostua viestintätietojensa valvontaan päästäkseen käyttämään jotakin viestintäpalvelua. Tämä pitäisi paikkansa etenkin, jos *kaikki* palveluntarjoajat tietyllä markkina-alueella toteuttaisivat verkkoliikenteen valvontaa sellaisiin tarkoituksiin, jotka eivät liity verkon turvallisuuteen. Ainoa jäljelle jäävä vaihtoehto olisi olla tilaamatta internetpalvelua lainkaan. Koska internetistä on tullut olennainen väline niin työssä kuin vapaa-ajallakin, internetpalvelun

([28]) Direktiivin johdanto-osan 18 kappaleessa on lueteltu esimerkkejä lisäarvopalveluista. On epäselvää, voidaanko palvelut, joihin sovelletaan liikenteen hallinnan periaatteita, tulkita osaksi luetteloa. Liikenteen hallintapalvelujen, joiden tavoitteena on tietyn sisällön ensisijaistaminen, voitaisiin katsoa tuottavan palvelun laatua. Esimerkiksi sellaiset liikenteen hallintapalvelut, joihin kuuluu pelkästään IP-otsikoiden käsittelyä ja joiden tavoitteena on tarjota kalliimmin hinnoiteltuja pelipalveluita, joissa käyttäjien henkilökohtaista peliliikennettä ensisijaistetaan verkossa, voitaisiin katsoa lisäarvopalveluksi. Toisaalta ei ole lainkaan selvää, voitaisiinko tietyntyyppisen liikenteen hidastamiseen tähtäävä liikenteen hallintapalvelu esimerkiksi vertaisverkkoliikenteen osalta katsoa sellaiseksi.

([29]) Katso sähköisen viestinnän tietosuojadirektiivin johdanto-osan 17 kappale ja 2 artiklan f kohta.

([30]) Hyväksytty 13. heinäkuuta 2011 (WP 187).

tilaamatta jättämistä ei voida pitää todellisena vaihtoehtona. Koska yksilöillä ei siis olisi todellista valinnanvapautta, he eivät myöskään voisi antaa suostumusta vapaaehtoisesti ([31]).

56. Tietosuojavaltuutettu katsoo, että komission ja kansallisten viranomaisten on ehdottomasti seurattava markkinoita etenkin sen varmistamiseksi, yleistyykö tämä skenaario (eli liittävätkö palveluntarjoajat tietoliikennepalvelut viestinnän valvontaan). Palveluntarjoajien tulisi tarjota vaihtoehtoisia palveluja, mukaan lukien internet-tilaus, johon ei liity verkkoliikenteen hallintaa, ilman, että niistä aiheutuu yksilöille lisäkustannuksia.

57. *Yksilöity suostumus.* Jotta suostumus olisi yksilöity, tässä tapauksessa internet-palveluntarjoajien on pyydettävä suostumus liikenne- ja viestintätietojen valvontaan selkeästi ja selvästi erottuvalla tavalla. 29 artiklan tietosuojaryhmän mukaan ”jotta suostumus olisi yksilöity, sen on oltava ymmärrettävä: siinä on viitattava selvästi ja tarkasti tietojen käsittelyn laajuuteen ja seurauksiin. Sitä ei voida soveltaa avoimesti kaikenlaisiin käsittelytoimiin. Tämä tarkoittaa, että käyttöyhteys, jossa suostumusta voidaan soveltaa, on rajattu.” Yksilöityä suostumusta ei todennäköisesti hankita, jos liikenne- ja viestintätietojen tarkastus on kytketty yleiseen suostumukseen, joka koskee palvelun tilausta. Sen sijaan yksilöitävyys edellyttää suostumuksen hankintaa kohdennettujen keinojen avulla; on esimerkiksi oltava erillinen suostumuslomake tai erillinen valintaruutu tietojen valvontaa varten (sen sijaan, että tieto asiasta lisätään yleisiin sopimusehtoihin ja sopimus vaaditaan allekirjoitettavaksi sellaisenaan).

58. *Tietoinen suostumus.* Jotta suostumus olisi pätevä, sen on oltava tietoinen. Tarve antaa asianmukaiset tiedot etukäteen on määritetty sähköisen viestinnän tietosuojadirektiivin ja tietosuojadirektiivin lisäksi myös yleispalveludirektiivin, sellaisena kuin se on muutettuna direktiivillä 2009/136/EY ([32]), 20 ja 21 artiklassa. Tiedottamisen ja suostumuksen tarve on perusteltu nimenomaisesti direktiivin 2009/136/EY johdanto-osan 28 kappaleessa: ”Ottaen huomioon sähköisen viestinnän kasvavan merkityksen kuluttajille ja yrityksille käyttäjille olisi joka tapauksessa tiedotettava kattavasti kaikista rajoituksista, joita palvelun ja/tai verkon tarjoaja on mahdollisesti asettanut sähköisten viestintäpalvelujen käytölle. Tällaisissa tiedoissa olisi palveluntarjoajan valinnan mukaan määritettävä joko asianomaisen sisällön, sovelluksen tai palvelun tyyppi, yksittäiset sovellukset tai palvelut taikka molemmat.” Lisäksi kohdassa määritetään, että ”käytetyn tekniikan ja rajoituksen tyypin mukaan tällaiset rajoitukset saattavat edellyttää käyttäjän suostumusta direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) mukaisesti.”

59. Näiden valvontatekniikoiden monimutkaisuuden vuoksi mielekkään etukäteistiedon antaminen on yksi keskeisistä haasteista pätevän suostumuksen hankkimisessa. Kuluttajille on tiedotettava asiasta siten, että he kykenevät ymmärtämään, mitä tietoja käsitellään, miten niitä käytetään, mikä sen vaikutus on käyttäjäkokemukseen ja missä määrin tekniikoilla puututaan yksityisyyteen.

60. Tämä tarkoittaa, että sen lisäksi, että tiedon on oltava selvää ja ymmärrettävää keskivertokäyttäjille, se on annettava suoraan yksilöille huomiota herättävällä tavalla, jotta kuluttajat eivät voi olla huomaamatta sitä.

61. *Tahdon ilmaus.* Sovellettavan lainsäädännön nojalla annettava suostumus edellyttää myös, että käyttäjä vahvistaa suostumuksensa ilmoittamalla siitä. Epäsuora suostumus ei täytä tätä vaatimusta. Tämä myös vahvistaa tarpeen käyttää tiettyjä keinoja suostumuksen hankkimiseksi, jotta internet-palveluntarjoajat voivat tarkastaa liikenne- ja viestintätietoja soveltaessaan liikenteen hallinnan periaatteita. Äskettäisessä suostumusta koskevassa lausunnossaan 29 artiklan työryhmä korosti selkeyden tarvetta suostumuksen hankkimisessa tietojen käsittelyyn kuuluvien eri elementtien osalta.

([31]) Vastaava esimerkki on matkustajarekisterijärjestelmä (PNR), jonka osalta keskusteltiin siitä, oliko matkustajien suostumus varaustietojen välittämiseen Yhdysvaltojen viranomaisille pätevä. Työryhmä katsoi, että matkustajien suostumusta ei voida antaa vapaaehtoisesti, koska lentoyhtiöillä on velvollisuus lähettää tiedot ennen lentokoneen lähtöä, joten matkustajilla ei näin ollen ole todellista valinnanvapautta, jos he haluavat lentää (29 artiklan mukaisen työryhmän lausunto 6/2002 matkustajatietojen ja muiden tietojen välittämisestä lentoyhtiöiltä Yhdysvaltoihin).

([32]) Direktiivi 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY muuttamisesta (katso alaviite 15).

62. Voidaan ajatella, että jos viestinnän osapuolet eivät halua internet-palveluntarjoajien sieppaavan viestejä soveltaakseen liikenteen hallinnan periaatteita, he voivat aina salata viestinsä. Tällaista toimintatapaa voidaan pitää käyttökelpoisena käytännöllisyyden kannalta, mutta se vaatii kuitenkin jonkin verran ponnisteluja ja teknistä tietämystä, eikä sitä voida rinnastaa vapaaehtoiseen, yksilöityyn ja tietoiseen suostumukseen. Salaustekniikoiden käyttö ei myöskään tee viestinnästä täysin luottamuksellista, sillä internet-palveluntarjoaja pääsee käsiksi ainakin IP-otsikkotietoihin reitittääkseen viestejä, ja se voi myös toteuttaa tilastollisia analyyseja.

63. Sähköisen viestinnän tietosuojaa koskevan direktiivin 5 artiklan 1 kohdan mukaan suostumus on hankittava ”kyseisiltä käyttäjiltä”. Monissa tapauksissa käyttäjä on sama henkilö kuin tilaaja, jolloin suostumus voidaan pyytää tietoliikennepalvelun tilausta tehtäessä. Toisissa tapauksissa – esimerkiksi jos kyseessä on useampi kuin yksi henkilö – käyttäjien suostumus on taas hankittava kultakin erikseen. Tästä voi aiheutua käytännön ongelmia, joita käsitellään jäljempänä.

Kaikkien asianosaisten käyttäjien suostumus

64. Direktiivin 5 artiklan 1 kohdassa säädetään, että tietojen käsittelyn oikeuttamiseksi tarvitaan käyttäjän suostumus. Suostumus on hankittava *kaikilta käyttäjiltä*, jotka osallistuvat viestintätapahtumaan. Tämän *perusteena* on se, että viestintä koskee yleensä vähintään kahta yksilöä (lähettäjää ja vastaanottajaa). Jos internet-palveluntarjoaja esimerkiksi tutkii IP-hyötykuormia, jotka koskevat jotakin sähköpostiviestiä, hän tutkii tietoa, joka koskee sekä sähköpostiviestin lähettäjää että vastaanottajaa.

65. Kun liikennettä ja viestintää valvotaan ja siepataan (esimerkiksi web-liikennettä), voi riittää, että internet-palveluntarjoajat hankkivat käyttäjän, eli tilaajan, suostumuksen. Tämä johtuu siitä, että viestinnän toista osapuolta, eli tässä tapauksessa selattua verkkosivua, ei välttämättä pidetä ”kyseisenä käyttäjänä” ([33]). Tilanne voi olla kuitenkin monimutkaisempi, jos valvontaan liittyy sähköpostiviestien sisällön tarkastusta, jolloin kyse on siis sähköpostiviestin lähettäjän ja vastaanottajan henkilökohtaisista tiedoista, eikä näillä henkilöillä ole välttämättä sopimussuhdetta saman internet-palveluntarjoajan kanssa. Näissä tapauksissa internet-palveluntarjoaja käsittelisi siis muiden kuin omien asiakkaidensa henkilötietoja (nimi, sähköpostiosoite ja mahdollisesti arkaluonteiset sisältötiedot). Käytännössä suostumuksen hankkiminen näiltä yksilöiltä voi olla oletettua vaikeampaa, koska se pitäisi tehdä ennemminkin tapauskohtaisesti kuin tietoliikennepalvelusta sopimisen hetkellä. Ei olisi myöskään realistista olettaa, että tilaajan suostumus annettaisiin muiden käyttäjien puolesta, kuten voi usein olla yksityistalouksissa.

66. Tältä osin tietosuojavaltuutettu katsoo, että internet-palveluntarjoajien olisi noudatettava nykyisiä lakisääteisiä vaatimuksia ja toteutettava periaatteita, joihin ei liity tietojen valvontaa ja tarkastusta. Tämä on sitäkin tärkeämpää sellaisten viestintäpalvelujen kannalta, joihin liittyy kolmansia osapuolia, jotka eivät voi antaa suostumustaan valvontaan etenkään lähetettyjen ja vastaanotettujen sähköpostiviestien osalta (tämä ei koske tilannetta, jossa syy perustuu turvallisuusnäkökohtiin).

67. Samalla on kuitenkin todettava, että sähköisen viestinnän tietosuojaa koskevan direktiivin 5 artiklan 1 kohdan täytäntöönpano ei välttämättä ole tyydyttävällä tasolla tältä kannalta ja että vaikuttaa siltä, että kyseisen direktiivin vaatimuksista tarvitaan parempaa ohjeistusta tältä osin. Sen vuoksi tietosuojavaltuutettu kehottaa komissiota olemaan tässä asiassa aktiivisempi ja tekemään aloitteita. Tässä työssä 29 artiklan työryhmään osallistuvien valvontaviranomaisten ja muiden sidosryhmien osallistumisesta voi olla paljon apua. Tarvittaessa jokin tapaus on vietävä unionin tuomioistuimeen, jotta saadaan täydellinen selvyys 5 artiklan 1 kohdan merkityksestä ja seurauksista.

([33]) Tästä huolimatta on tapauksia, joissa verkkoliikenteessä siirretään henkilökohtaista tietoa, jos esimerkiksi verkkosivulle lähetetään kuvia tunnistettavista luonnollisista henkilöistä. Tällaisen tiedon käsittely edellyttää oikeusperustaa, mutta siihen ei sovelleta 5 artiklan 1 kohtaa, koska nämä henkilöt eivät ole ”kyseisiä henkilöitä”.

V.3 **Oikeasuhteisuus – tiedon minimoinnin periaate**

68. Tietosuojadirektiivin 6 artiklan c kohdassa säädetään suhteellisuusperiaatteesta ([34]), joka koskee internet-palveluntarjoajia, koska he ovat tässä direktiivissä tarkoitettuja rekisterinpitäjiä toteuttaessaan valvontaa ja suodatusta.

69. Tämän periaatteen mukaisesti henkilötietoja saa käsitellä vain, jos ”ne ovat asianmukaisia, olennaisia eivätkä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään”. Tämän periaatteen soveltamiseen kuuluu sen arvioiminen, ovatko tietojen käsittelyyn käytetyt keinot ja käytettyjen henkilötietojen tyypit sopivia ja perusteltuja asetettujen tavoitteiden saavuttamiseen nähden. Jos arvioinnin tulos on se, että tietoa on kerätty enemmän kuin tarpeen, periaatetta ei ole tällöin noudatettu.

70. Suhteellisuusperiaatteen noudattaminen tietyntyyppisten tarkastustekniikoiden osalta on arvioitava aina tapauskohtaisesti. *Yleisiä* päätelmiä ei ole mahdollista tehdä. On kuitenkin mahdollista määrittää erilaisia konkreettisia näkökohtia, joita olisi pohdittava suhteellisuusperiaatteen noudattamista arvioitaessa.

71. *Käsiteltävän tiedon määrä*: Viestinnän mahdollisimman laaja valvonta Internet-palveluntarjoajien toimesta on useimmiten liiallista ja laitonta. Se, että sitä voidaan tehdä tavoilla, joita yksilöt eivät voi havaita, ja että yksilöiden voi olla vaikea ymmärtää, mitä tapahtuu, on omiaan lisäämään yksityisyyteen puuttuvaa vaikutusta. Internet-palveluntarjoajien olisi arvioitava, millaisia vähemmän yksityisyyteen puuttuvia keinoja olisi saatavilla vaaditun tuloksen saavuttamiseksi. Voitaisiinko esimerkiksi IP-otsikoiden valvonnalla saavuttaa vaadittu tulos syväpakettitarkastuksen toteuttamisen sijasta? Myös syväpakettitarkastuksen osalta vain tiettyjen käytäntöjen määrittäminen voi riittää tarvittavien tietojen saamiseksi. Tietosuojatakeiden ja näennäisen anonymisoinnin soveltaminen voi myös olla aiheellista. Arviointituloksen on vahvistettava, että tietojen käsittely on oikeasuhteista.

72. *Käsittelyn vaikutukset (jotka liittyvät suoraan tarkoituksiin)*. Oikeasuhteisuus voi olla puutteellista tapauksissa, joissa internet-palveluntarjoajat käyttävät liikenteen hallinnan periaatteita sulkeakseen pääsyn tiettyihin palveluihin ilman, että saavutetusta hyödystä reilu osuus koituu käyttäjien hyväksi.

73. On tärkeää muistaa, että suhteellisuusperiaatetta on sovellettava silloinkin, kun muut pakolliset lakisääteiset vaatimukset täyttyvät, kuten esimerkiksi silloin, kun internet-palveluntarjoaja on hankkinut yksilöltä suostumuksen sisällön valvontaan. Tämä tarkoittaa sitä, että sisällön valvontana toteutettu tietojen käsittely saattaa olla laitonta, jos se loukkaa oikeasuhteisuuden perusperiaatetta.

V.4 **Turvallisuus ja organisatoriset toimet**

74. Sähköisen viestinnän tietosuojaa koskevan direktiivin 4 artiklassa nimenomaisesti edellytetään, että internet-palveluntarjoajien on toteutettava teknisiä ja organisatorisia toimia varmistaakseen, i) että henkilötietoja käsittelee vain valtuutettu henkilöstö laillisiin tarkoituksiin, ii) henkilötietoja suojataan vahingossa tapahtuvalta tai laittomalta käsittelyltä ja iii) henkilötietojen käsittelyssä toteutetaan turvallisuusperiaatteita. Artiklan perusteella myös kansalliset toimivaltaiset viranomaiset voivat toteuttaa näihin toimenpiteisiin kohdistuvia tarkastuksia.

75. Sähköisen viestinnän tietosuojaa koskevan direktiivin 4 artiklan 3 kohdan ja 2 kohdan mukaisesti internet-palveluntarjoajilla on myös velvollisuus ilmoittaa tietoturvaloukkauksista asianomaiselle toimivaltaiselle kansalliselle viranomaiselle sekä kaikille yksilölle, joille tietojen paljastumisesta voi olla haitallisia seurauksia.

76. Käsiteltäessä viestintään liittyviä henkilötietoja liikenteen hallintaperiaatteiden soveltamisen tavoitteen osalta internet-palveluntarjoajat voivat päästä käsiksi tietoihin, jotka ovat arkaluonteisempia kuin liikennetiedot.

([34]) Kuten edellä on korostettu, tietosuojadirektiivi koskee kaikkia niitä perusoikeuksien ja –vapauksien suojeluun liittyviä asioita, joita sähköisen viestinnän tietosuojaa koskeva direktiivi ei nimenomaisesti kata.

77. Sen vuoksi internet-palveluntarjoajien kehittämien turvallisuusperiaatteiden tulisi sisältää tiettyjä takeita sen varmistamiseksi, että toteutetut toimet ovat asianmukaisia näihin riskeihin nähden. Näitä tarkastuksia toteuttavien kansallisten toimivaltaisten viranomaisten tulisi olla erityisen vaativia tältä osin. Olisi myös varmistettava, että käytössä on tehokkaita ilmoitusmenettelyjä, joiden avulla rekisteröidyille ilmoitetaan siitä, kenen tiedot ovat vaarantuneet ja kenelle siitä voi siis aiheutua haitallisia vaikutuksia.

VI **EHDOTUKSIA POLIITTISIKSI JA LAINSÄÄDÄNNÖLLISIKSI TOIMENPITEIKSI**

78. Liikennetietoihin ja IP-hyötykuormien, eli siis viestien sisällön, tarkastukseen perustuvat valvontatekniikat saattavat paljastaa, mitä käyttäjät tekevät internetissä: millä verkkosivuilla he ovat käyneet ja mitä he ovat niillä tehneet, mitä vertaisverkkosovelluksia he ovat käyttäneet, mitä tiedostoja he ovat ladanneet, mitä sähköposteja he ovat lähettäneet ja vastaanottaneet (keneltä, mistä aiheesta ja minkä vuoksi) jne. Internet-palveluntarjoajat saattavat haluta käyttää näitä tietoja ensisijaistaakseen tietyntyyppistä viestintää, esimerkiksi tilausvideoita, muihin tyyppeihin nähden. Palveluntarjoajat voivat haluta käyttää tietoja virusten tunnistamiseen tai profiilien luomiseen käyttäytymiseen liittyvää mainontaa varten. Nämä toimet rikkovat oikeutta luottamukselliseen viestintään.

79. Yksityisyyteen kohdistuvat seuraukset lisääntyvät käytettyjen tekniikoiden ja kunkin tapauksen erityispiirteiden perusteella. Mitä perusteellisempaa kerättyjen tietojen sieppaus ja analysointi on, sitä suurempi konflikti syntyy viestinnän luottamuksellisuuden periaatteeseen nähden. Valvonnan toteuttamisen tarkoitus sekä sovelletut tietosuojatoimenpiteet ovat myös keskeisiä elementtejä sen määrittämisessä, miten suuresti yksilöiden yksityisyyteen ja henkilötietoihin puututaan. Palvelujen käytön estämistä ja valvontaa haittaohjelmien torjumiseksi (jolloin tarkastettujen tietojen säilyttäminen ja käyttö on tarkasti rajattu) ei voida verrata tilanteisiin, joissa tietoja tallennetaan, jotta voidaan luoda yksilöllisiä profiileja käyttäytymiseen perustuvaa mainontaa varten.

80. Periaatteessa tietosuojavaltuutettu katsoo, että asianmukaisesti tulkittuna, sovellettuna ja täytäntöönpantuna EU:n nykyinen yksityisyys- ja tietosuojalainsäädäntö riittää takaamaan, että oikeus luottamukselliseen viestintään säilyy ja että yksilöiden yksityisyyden suojelu ja tietosuoja eivät yleisesti ottaen vaarannu ([35]). Internet-palveluntarjoajien ei tule käyttää valvontamekanismeja, elleivät ne ole soveltaneet lainsäädäntöä asianmukaisesti. Lainsäädännön oleelliset elementit, jotka internet-palveluntarjoajien tulee erityisesti ottaa huomioon ja joita niiden tulee noudattaa, ovat seuraavat:

— Internet-palveluntarjoajat voivat soveltaa sellaisia verkkoliikenteen hallinnan periaatteita, joiden tarkoituksena on taata palvelun turvallisuus, tuottaa palvelu tai rajoittaa palvelun ruuhkautumista sähköisen viestinnän tietosuojadirektiivin 4 ja 6 artiklan nojalla.

— Internet-palveluntarjoajilla on oltava jokin muu tietty oikeudellinen peruste ja mahdollisesti käyttäjien suostumus soveltaakseen sellaisia liikenteen hallinnan periaatteita, joihin kuuluu liikenne- ja/tai viestintätietojen käsittelyä muihin kuin edellä lueteltuihin tarkoituksiin. Käyttäjien tietoinen suostumus tarvitaan esimerkiksi yksilöiden viestien valvomiseen ja suodattamiseen, jos tarkoituksena on rajoittaa (tai sallia) tiettyjen sovellusten ja palvelujen, kuten vertaisverkkojen tai internetpuhelujen, käytettävyyttä.

— Suostumuksen on oltava vapaaehtoinen, yksilöity ja tietoinen. Suostumus on ilmaistava vahvistavalla toimenpiteellä. Nämä vaatimukset korostavat vahvasti sitä, että on pyrittävä tehokkaammin varmistamaan, että yksilöille tiedotetaan asianmukaisesti, suorasti, ymmärrettävästi ja nimenomaisesti siten, että he voivat arvioida käytäntöjen vaikutuksia ja tehdä lopulta tietoisen päätöksen. Valvontatekniikoiden monimutkaisuuden vuoksi mielekkään etukäteistiedon antaminen on yksi keskeisistä haasteista pätevän suostumuksen hankkimisessa. Haitallisia seurauksia (mukaan luettuina taloudelliset kustannukset) ei myöskään saisi koitua niille käyttäjille, jotka eivät suostu valvontaan.

([35]) Tämä ei kuitenkaan vaikuta siihen, että lainsäädäntöä on tarpeen muuttaa muiden seikkojen vuoksi etenkin EU:n tietosuojalainsäädännön yleisen tarkistuksen osalta, jonka tarkoituksena on tehostaa sitä uusien tekniikoiden ja globalisaation kannalta.

— Suhteellisuusperiaate on ratkaisevan tärkeä internet-palveluntarjoajien toteuttaessa liikenteen hallinnan periaatteita siitä riippumatta, mikä käsittelyn oikeudellinen perusta ja tarkoitus on: palvelun tuottaminen, ruuhkautumisen välttäminen vai sellaisten kohdistettujen tilausten tarjoaminen, joihin kuuluu tai ei kuulu pääsy tiettyihin palveluihin ja sovelluksiin. Tämä periaate rajoittaa internet-palveluntarjoajien mahdollisuuksia toteuttaa yksilöiden viestinnän sisällön valvontaa, johon kuuluu liiallisen tiedon käsittelyä tai jolla hankitaan hyötyä ainoastaan palveluntarjoajille. Se, mitä internet-palveluntarjoajat voivat logistisesti tehdä, määräytyy sen mukaan, missä määrin tekniikat puuttuvat yksityisyyteen, millaisia tuloksia saadaan (joiden osalta heille voi koitua etuja) ja mitä yksityisyyden suojelua ja tietosuojaa koskevia toimenpiteitä on sovellettu. Ennen valvontatekniikoiden käyttämistä internet-palveluntarjoajien on arvioitava, ovatko ne suhteellisuusperiaatteen mukaisia.

81. Vaikka nykyinen lainsäädäntö sisältää oleellisia ehtoja ja takeita, on kiinnitettävä erityistä huomiota siihen, täyttävätkö internet-palveluntarjoajat lakisääteiset vaatimukset, tarjoavatko ne kuluttajille tarvittavaa tietoa, jotta nämä voivat tehdä mielekkäitä valintoja, ja noudattavatko ne suhteellisuusperiaatetta. Kansallisella tasolla edellä esitetystä vastaaviin toimivaltaisiin viranomaisiin kuuluvat yhtäältä myös kansalliset tietoliikenneviranomaiset ja toisaalta kansalliset tietosuojaviranomaiset. EU:n tasolla oleellisiin EU-tason tahoihin kuuluu BEREC (Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin). Myös tietosuojavaltuutettu voi osallistua tähän työhön.

82. Sen lisäksi, että vaatimustenmukaisuuden tämänhetkistä noudattamista valvotaan ottaen huomioon, että viestinnän laaja-alaisen tosiaikaisen valvonnan mahdollisuus on suhteellisen tuore asia, jotkin lainsäädännön soveltamiseen liittyvät seikat, joita on käsitelty tässä lausunnossa, edellyttävät perusteellisempaa analyysia, ja niitä on selvennettävä analyysin perusteella myöhemmin. Monilla aloilla erityisen tärkeään ohjeistukseen kuuluvat esimerkiksi seuraavat seikat:

— Sellaisten valvontakäytäntöjen määrittäminen, jotka ovat perusteltuja sujuvan liikennevirran varmistamiseksi ja joihin ei tarvita käyttäjien suostumusta (esimerkiksi roskapostin torjunta). Sen lisäksi, missä määrin sovellettu valvonta puuttuu yksityisyyteen, myös esimerkiksi se, miten paljon häiriöitä sujuvassa liikennevirrassa muuten esiintyisi, on olennaista.

— Sellaisten valvontatekniikoiden määrittäminen, joita voidaan toteuttaa turvallisuustarkoituksiin ilman käyttäjien suostumusta.

— Sen määrittäminen, milloin valvonta edellyttää yksilön suostumusta ja etenkin kaikkien asianosaisten käyttäjien suostumusta ja mitkä ovat sallitut tekniset parametrit sen varmistamiseksi, että valvontatekniikkaan ei sisälly sellaista tietojen käsittelyä, joka ei ole oikeasuhtaista aiottuihin tarkoituksiin nähden.

— Kolmen edellä esitetyn seikan lisäksi ohjeistusta saatetaan tarvita myös tarvittavien tietosuojatakeiden soveltamisesta (käyttötarkoituksen rajoittamisen periaate, turvallisuus jne.).

83. Koska tällä alalla on sekä kansallisia että EU:n toimivaltuuksia, tietosuojavaltuutettu katsoo, että näkemysten ja kokemusten jakaminen yhtenäisten toimintatapojen löytämiseksi edellä esitetystä on tärkeää. Tähän pääsemiseksi tietosuojavaltuutettu ehdottaa, että luodaan yhteistyöelin tai asiantuntijaryhmä, johon kootaan kansallisten sääntelyviranomaisten, 29 artiklan mukaisen työryhmän, tietosuojavaltuutetun ja BERECin edustajia. Tämän yhteistyöelimen ensimmäinen tavoite olisi laatia ohjeistusta ainakin edellä määritetyistä seikoista vahvojen ja yhtenäisten toimintatapojen ja toimintaedellytysten varmistamiseksi. Tietosuojavaltuutettu kehottaa komissiota ryhtymään toimiin tämän aloitteen osalta.

84. Lisäksi sekä kansallisten viranomaisten että niiden EU-kumppaneiden, mukaan luettuina BEREC ja Euroopan unionin komissio, on seurattava markkinoiden kehitystä tällä saralla hyvin tarkkaan. Tietosuojan ja yksityisyyden kannalta se skenaario, jossa internet-palveluntarjoajat toteuttavat liikenteen hallinnan periaatteita rutiininomaisesti tarjoamalla tilauksia, jotka perustuvat sisällön ja sovelluksien käytettävyyden suodattamiseen, olisi erittäin ongelmallinen. Jos näin joskus käy, tarvitaan uutta lainsäädäntöä tilanteen käsittelemiseksi.

VII **PÄÄTELMÄT**

85. Internet-palveluntarjoajien lisääntyvä tukeutuminen valvonta- ja tarkastustekniikkoihin vaikuttaa internetin neutraliteettiin ja viestinnän luottamuksellisuuteen haitallisesti. Tästä syntyy vakavia ongelmia käyttäjien yksityisyyden ja henkilötietojen suojelun kannalta.

86. Vaikka komission tiedonanto avoimesta internetistä ja verkon neutraliteetista Euroopassa käsittelee myös näitä asioita lyhyesti, tietosuojavaltuutettu katsoo, että tarvitaan lisää toimenpiteitä tyydyttävän politiikan luomiseksi tulevaisuudessa. Tämän lausunnon myötä hän on sen vuoksi osallistunut meneillään olevaan periaatekeskusteluun verkon neutraliteetista eritoten tietosuojaan ja yksityisyyteen liittyvien seikkojen osalta.

87. Tietosuojavaltuutettu katsoo, että kansallisten viranomaisten ja BERECin on seurattava tilannetta markkinoilla. Seurannan perusteella olisi voitava luoda selvä kuva siitä, ollaanko markkinoilla siirtymässä kohti laaja-alaista, tosiaikaista viestinnän valvontaa ja liittyykö lainsäädännön noudattamiseen ongelmia.

88. Markkinoiden seurantaan tulisi kuulua myös uusien käytäntöjen vaikutusten tarkempi analyysi internetiin liittyvän tietosuojan ja yksityisyyden osalta. Tässä lausunnossa määritetään muutamia aloja, joita olisi tarpeen selventää. Vaikka EU:n virastot ja sellaiset elimet kuin BEREC, 29 artiklan työryhmä ja tietosuojavaltuutettu voivatkin selventää lainsäädännön soveltamisen ehtoja, tietosuojavaltuutettu katsoo, että komission velvollisuus on koordinoida ja ohjata keskustelua. Sen vuoksi hän kehottaa komissiota tekemään aloitteen yhteistyöelimestä tai työryhmästä, johon kuuluisivat kaikki nämä sidosryhmät, tämän tavoitteen saavuttamiseksi. Tarkempaa analyysia edellyttävien seikkojen osalta olisi käsiteltävä etenkin seuraavia kohtia:

— Sellaisten valvontakäytäntöjen määrittäminen, jotka ovat perusteltuja sujuvan liikennevirran varmistamiseksi ja turvallisuuteen liittyvien tarkoitusten toteuttamiseksi.

— Sen määrittäminen, milloin valvonta edellyttää yksilön suostumusta ja etenkin kaikkien asianosaisten käyttäjien suostumusta, ja mitkä ovat sallitut tekniset parametrit sen varmistamiseksi, että valvontatekniikkaan ei sisälly sellaista tietojen käsittelyä, joka ei ole oikeasuhteista aiottuihin tarkoituksiin nähden.

— Näiden seikkojen lisäksi ohjeistusta saatetaan tarvita myös tarvittavien tietosuojatoimenpiteiden soveltamisesta (käyttötarkoituksen rajoittamisen periaate, turvallisuus jne.).

89. Nämä havainnot saattavat osoittaa lainsäädännöllisten lisätoimenpiteiden tarvetta. Siinä tapauksessa komission tulisi kehittää poliittisia toimenpiteitä, joiden tavoitteena on lainsäädännön vahvistaminen ja oikeusvarmuuden varmistaminen. Uusilla toimenpiteillä olisi voitava selventää verkon neutraliteetin periaatteen käytännön seurauksia, kuten joissakin jäsenvaltioissa on jo tehty, ja varmistaa, että käyttäjillä on todellista valinnanvapautta, eritoten pakottamalla internet-palveluntarjoajat tarjoamaan valvomattomia yhteyksiä.

Tehty Brysselissä 7 päivänä lokakuuta 2011.

Peter HUSTINX

Euroopan tietosuojavaltuutettu