I

(Päätöslauselmat, suositukset ja lausunnot)

LAUSUNNOT

EUROOPAN TIETOSUOJAVALTUUTETTU

Euroopan tietosuojavaltuutetun lausunto luottamuksen lisäämisestä tietoyhteiskuntaa kohtaan tietosuojaa ja yksityisyyden suojaa parantamalla

(2010/C 280/01)

EUROOPAN TIETOSUOJAVALTUUTETTU, joka

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

ottaa huomioon Euroopan unionin perusoikeuskirjan ja erityisesti sen 7 ja 8 artiklan,

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

ottaa huomioon henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12 päivänä heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([2]),

ottaa huomioon 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 ([3]) ja erityisesti sen 41 artiklan,

ON ANTANUT SEURAAVAN LAUSUNNON:

I. JOHDANTO

1. Tieto- ja viestintätekniikat (TVT) tarjoavat valtavia mahdollisuuksia lähes kaikilla ihmiselämän osa-alueilla ja vaikuttavat siihen, miten me työskentelemme, toimimme, sosiaalistumme ja kouluttaudumme. Ne ovat välttämättömiä nykypäivän tietoon perustuvan talouden ja yleensä koko yhteiskunnan kannalta.

2. Euroopan unioni on maailmanlaajuisesti vahva toimija kehittyneen tieto- ja viestintätekniikan alalla ja aikoo myös säilyä sellaisena. Euroopan komission odotetaan piakkoin vastaavan tähän haasteeseen hyväksymällä uuden eurooppalaisen digitaalistrategian, jonka komission jäsen Kroes on vahvistanut omaksi ensisijaiseksi tavoitteekseen ([4]).

3. Euroopan tietosuojavaltuutettu toteaa tieto- ja viestintätekniikoista koituvan hyödyn ja sen, että EU:n olisi kaikin tavoin pyrittävä tehostamaan näiden tekniikoiden kehitystä ja laaja-alaista omaksumista. Tietosuojavaltuutettu tukee niin ikään komission jäsenten Kroesin ja Redingin kantoja, joiden mukaan kansalaisten tulisi olla tämän uuden ympäristön keskipisteessä ([5]). Kansalaisten olisi voitava luottaa TVT:n kykyyn säilyttää heidän tietonsa turvassa ja valvoa tietojen käyttöä ja olla varmoja siitä, että kansalaisten yksityisyyttä ja tietosuojaa koskevia oikeuksia noudatetaan digitaalisessa tilassa. Näiden oikeuksien kunnioitus on ehdoton edellytys kuluttajien luottamukselle. Luottamus on puolestaan ratkaiseva tekijä, joka saa kansalaiset käyttämään uusia palveluja ([6]).

([1]) EYVL L 281, 23.11.1995, s. 31.
([2]) EYVL L 201, 31.7.2002, s. 37.
([3]) EYVL L 8, 12.1.2001, s. 1.

([4]) Vastaukset Euroopan parlamentin Neelie Kroesille osoittamaan kyselylomakkeeseen komission jäsenen nimittämistä edeltävän Euroopan parlamentin kuulemisen yhteydessä.

([5]) Vastaukset Euroopan parlamentin komission jäsenelle Neelie Kroesille osoittamaan kyselylomakkeeseen komission jäsenen nimittämistä edeltävän Euroopan parlamentin kuulemisen yhteydessä; komission jäsenen Viviane Redingin puhe Brysselissä 12 päivänä marraskuuta 2009: "A European Digital Agenda for the New Digital Consumer", BEUC Multi-stakeholder Forum on Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives.

([6]) Katso esimerkiksi tietoturvaa, yksityisyyden suojaa ja luottamusta tietoyhteiskunnassa käsittelevän tutkimus- ja innovaationeuvottelukunnan (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society, RISEPTIS) raportti "Trust in the Information Society", joka on luettavissa osoitteessa http://www.think-trust.eu/general/news-events/riseptis-report.html. Katso myös J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1.

4. EU:ssa on vahva tietosuojaa ja yksityisyyttä koskeva lainsäädäntö, jonka periaatteet pysyvät sellaisinaan voimassa myös digitaaliajassa. Meillä ei ole kuitenkaan varaa jäädä lepäämään laakereillamme. TVT tuottaa useissa yhteyksissä aivan uusia huolenaiheita, joita ei ole otettu huomioon nykyisessä sääntelyssä. Näin ollen tarvitaan toimia, joilla varmistetaan, että EU:n laissa vahvistetut kansalaisten oikeudet tarjoavat tehokkaan suojan myös tässä uudessa ympäristössä.

5. Tässä lausunnossa käsitellään toimia, joita Euroopan unioni voi edistää tai toteuttaa taatakseen kansalaisten yksityisyyden suojan ja tietoturvan globaalistuneessa maailmassa, jota teknologian kehitys vie eteenpäin. Lausunnossa käsitellään niin lainsäädännöllisiä kuin muitakin välineitä.

6. Lausunnossa luodaan yleiskatsaus tieto- ja viestintätekniikkaan uutena kehitysvaiheena, joka tuo mukanaan paitsi mahdollisuuksia myös riskejä, ja käsitellään sitä, miten tietoturva ja yksityisyyden suoja sisällytetään käytännössä osaksi uutta tieto- ja viestintätekniikkaa jo suunnitteluvaiheessa (”sisäänrakennetun yksityisyyden suojan” periaate). Periaatteen toteutumiseksi lausunnossa tarkastellaan, miten ”sisäänrakennetun yksityisyyden suojan” periaate on saatettava osaksi tietosuojalainsäädäntöä ainakin kahdella eri tavalla. Ensiksikin se on sisällytettävä yleisenä, velvoittavana periaatteena, ja toiseksi se on kytkettävä tiettyihin TVT:n aloihin, joilla esiintyviä erityisiä tietoturvan ja yksityisyyden suojan riskejä voidaan vähentää asianmukaisen teknisen arkkitehtuurin ja suunnittelun avulla. Näitä aloja ovat radiotaajuustunnistus (RFID), sosiaaliset verkkoyhteisöt ja selainsovellukset. Lopuksi lausunnossa esitetään ehdotuksia muiksi työkaluiksi ja periaatteiksi, joilla pyritään suojaamaan kansalaisen yksityisyyttä ja tietoja TVT-alalla.

7. Edellä mainittuja aiheita käsiteltäessä lausunnossa kehitellään edelleen eräitä 29 artiklan mukaisen tietosuojatyöryhmän yksityisyyden suojan tulevaisuutta koskevan kuulemisen yhteydessä esittämiä ehdotuksia ([1]). Lisäksi lausunnossa nojaudutaan Euroopan tietosuojavaltuutetun aiempiin lausuntoihin, kuten 25 päivänä heinäkuuta 2007 annettuun lausuntoon tietosuojadirektiivin soveltamisesta ja 20 päivänä joulukuuta 2007 annettuun lausuntoon radiotaajuustunnistuksesta sekä tietosuojavaltuutetun kahteen lausuntoon, jotka koskevat sähköisen viestinnän tietosuojadirektiiviä ([2]).

II. TVT TARJOAA UUSIA MAHDOLLISUUKSIA JA TUO MUKANAAN UUSIA RISKEJÄ

8. Tieto- ja viestintätekniikkaa on verrattu aiempiin merkittäviin keksintöihin, kuten sähköön. TVT:n ja talouskasvun välinen yhteys on selvä kehittyneissä maissa, vaikka TVT:n historiallista vaikutusta voi ollakin vielä vaikea arvioida tässä vaiheessa. TVT on luonut työpaikkoja ja taloudellista hyötyä sekä edistänyt yleistä hyvinvointia. TVT:n vaikutukset ylittävät talouden alueen rajat, koska TVT:llä on tärkeä tehtävä innovaation ja luovuuden tehostajana.

9. Lisäksi TVT on muuttanut ihmisten tapaa tehdä työtä, elää yhteiskunnassa ja vaikuttaa. Ihmiset esimerkiksi hyödyntävät tieto- ja viestintätekniikkaa yhä laajemmin sosiaalisessa ja taloudellisessa vuorovaikutuksessaan. Ihmiset voivat käyttää monipuolista valikoimaa uusia TVT-sovelluksia, kuten sähköistä terveydenhuoltoa, sähköisiä liikennepalveluja ja sähköistä valtionhallintoa sekä innovatiivisia vuorovaikutteisia viihde- ja oppimisjärjestelmiä.

10. Näiden hyötyjen vuoksi kaikki Euroopan unionin toimielimet ovat ilmaisseet sitoutumisensa TVT:n tukemiseen, koska se on tärkeä työkalu Euroopan teollisuuden kilpailukyvyn kohentajana ja Euroopan talouden elpymisen nopeuttajana. Euroopan komissio näet hyväksyi elokuussa 2009 raportin Euroopan digitaalisesta kilpailukyvystä ([3]) ja käynnisti julkisen kuulemismenettelyn TVT-alaa tehostavista tulevista strategioista. Neuvosto julkaisi 7 päivänä joulukuuta 2009 oman panoksensa tähän kuulemiseen nimeltään ”i2010:n jälkeinen strategia – kohti avointa, vihreää ja kilpailukykyistä tietoyhteiskuntaa” ([4]). Euroopan

([1]) 29 artiklan mukaisen tietosuojatyöryhmän lausunto 168: ”The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, annettu 1 päivänä joulukuuta 2009.

([2]) Lausunto komission tiedonannosta Euroopan parlamentille ja neuvostolle tietosuojadirektiivin tehokkaampaa täytäntöönpanoa koskevan työohjelman seurannasta, annettu 25 päivänä heinäkuuta 2007, EUVL C 255, 27.10.2007, s. 1; lausunto komission tiedonannosta Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle ”Radiotaajuustunnistus Euroopassa: Asteittain kohti alan yhteisiä periaatteita” (KOM(2007) 96), annettu 20 päivänä joulukuuta 2007, EUVL C 101, 23.4.2008, s. 1; lausunto ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi, jolla muutetaan muun muassa henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annettua Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi), annettu 10 päivänä huhtikuuta 2008, EUVL C 181, 18.7.2008, s. 1; Euroopan tietosuojavaltuutetun toinen lausunto henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun Euroopan parlamentin ja neuvoston direktiivin (sähköisen viestinnän tietosuojadirektiivi) 2002/58/EY uudelleentarkastelusta, annettu 9 päivänä tammikuuta 2009.

([3]) Raportti Euroopan digitaalisesta kilpailukyvystä – i2010-strategian tärkeimmät saavutukset vuosina 2005-2009 (SEC(2009) 1060).

([4]) Neuvoston päätelmät ”i2010:n jälkeinen strategia – kohti avointa, vihreää ja kilpailukykyistä tietoyhteiskuntaa” (17107/09), hyväksytty 18.12.2009.

parlamentti on vastikään hyväksynyt mietinnön ohjeeksi komissiolle digitaalistrategian määrittelyyn ([1]).

11. TVT:n kehittymisen myötä tarjoutuviin mahdollisuuksiin ja hyötyihin liittyy myös uusia riskejä varsinkin yksityisyyden suojan ja kansalaisten henkilötietojen suojelun kannalta. TVT on usein johtanut kerättävien, lajiteltavien, suodatettavien, siirrettävien tai muulla tavoin säilytettävien tietojen määrän valtavaan kasvuun (usein kansalaisilta näkymättömissä), joten myös tietoja koskevat riskit ovat moninkertaistuneet.

12. Esimerkiksi radiotaajuustunnistuksessa käytettävät sirut korvaavat vähitellen viivakoodit (eräissä) kuluttajatuotteissa. Uuden järjestelmän uskotaan hyödyttävän niin elinkeinoelämää kuin kuluttajaakin, koska se parantaa tiedonkulkua toimitusketjussa (ja vähentää samalla tarvetta ”varmuusvarastoihin”, tarkentaa ennusteita jne.). Toisaalta samalla lisätään huolestuttavalla tavalla mahdollisuuksia seurata kansalaisia merkittyjen henkilökohtaisten tavaroiden avulla eri tarkoituksiin ja eri toimijoiden lukuun.

13. Toisena esimerkkinä ovat ns. pilvi- eli etäresurssipalvelut, joilla tarkoitetaan kuluttaja- ja muiden palvelujen tarjoamista etätietokoneilla Internetin kautta. Palvelut ulottuvat valokuvakirjastoista, kalentereista, nettisähköpostipalvelusta ja kuluttajatietokannoista aina monipuolisiin liikeelämän palveluihin. Sekä yritysten että kansalaisten hyödyt ovat selvät: kustannuksia säästyy (kustannukset ovat aiempaan nähden marginaalisia), paikkariippuvuus vähenee (tietoihin on helppo päästä käsiksi kaikkialta), automaatioaste kasvaa (ei tarvita erityisesti tarkoitukseen kohdennettuja tietoteknisiä resursseja eikä ohjelmistopäivityksiä) jne. Samalla turvallisuusongelmien ja tietomurtojen riskit ovat tulleet todellisiksi ja todennäköisiksi. Myös omien tietojen tarkastus- ja hallintaoikeudet luovat epävarmuutta.

14. Muillakin TVT-sovelluksia käyttävillä aloilla on havaittu rinnan hyötyjä ja riskejä. Esimerkiksi sähköinen terveydenhuolto voi parantaa hoidon tehoavuutta, vähentää sen kustannuksia, helpottaa sen saatavuutta ja parantaa terveydenhoitopalvelujen yleistä laatua. Sähköinen terveydenhuolto herättää toisaalta usein kysymyksiä sähköisten terveystietojen muun käytön laillisuudesta, ja mahdollisia muita käyttötarkoituksia onkin tutkittava huolellisesti ([2]). Elektronisten terveyskortistojen yleistyttyä laajalti järjestelmissä on ilmennyt myös useita puutteita, muun muassa elektronisiin terveystietoihin kohdistuneita tietomurtoja.

15. Kaiken kaikkiaan jäljelle jää aina jonkinlainen riski, vaikka tilanne olisikin arvioitu asianmukaisesti ja tarpeelliset toimenpiteet toteutettu. Riskittömyyteen pyrkiminen ei ole realistista. Kuten jäljempänä selvitetään, riskejä kuitenkin voidaan ja tulee vähentää aina asianmukaiselle tasolle.

III. **SISÄÄNRAKENNETTU YKSITYISYYDEN SUOJA KESKEISENÄ TYÖKALUNA KANSALAISTEN LUOTTAMUKSEN PARANTAMISESSA TIETO- JA VIESTINTÄTEKNIIKKAAN**

16. TVT:n mahdolliset hyödyt toteutuvat käytännössä vain, jos ne synnyttävät luottamusta eli niillä pystytään perustelemaan käyttäjän asettuminen riippuvaiseksi TVT:sta sen ominaisuuksien ja hyötyjen ansiosta. Luottamus syntyy ainoastaan silloin, kun TVT on luotettavaa, varmaa ja kansalaisten valvonnassa ja jos henkilötietojen ja yksityisyyden suoja on taattu.

17. Edellä kuvattujen kaltaiset laaja-alaiset riskit ja toimintahäiriöt ovat omiaan vaarantamaan käyttäjien luottamuksen tietoyhteiskuntaan varsinkin silloin, kun ne johtavat henkilötietojen väärinkäyttöön tai anastamiseen ja yksityisyyden vaarantumiseen. Tämä voi vaarantaa merkittävällä tavalla TVT:n kehityksen ja mahdolliset hyödyt.

18. Yksityisyyden ja tietosuojan riskejä ei kuitenkaan voida ratkaista kieltämällä tai estämällä TVT:n käyttöä tai sen puolesta puhumista eikä kieltäytymällä sen käytöstä. Tällainen ratkaisu ei ole toteutettavissa eikä realistinen: se estäisi kansalaisia hyödyntämästä TVT:n hyötyjä ja rajoittaisi voimakkaasti siitä saatavaa yleistä etua.

19. Tietosuojavaltuutettu pitää myönteisenä ratkaisuna TVT:n suunnittelua ja kehittämistä yksityisyyden ja tietosuojan huomioon ottavalla tavalla. Tämän vuoksi on ratkaisevaa, että yksityisyyden suoja ja tietosuoja kattavat tekniikan koko elinkaaren alustavasta suunnitteluvaiheesta aina lopulliseen hyödyntämis-, käyttö- ja jätevaiheeseen. Tästä käytetään yleensä nimitystä ”sisäänrakennettu yksityisyyden suoja”, ja sitä käsitellään seuraavassa.

20. Sisäänrakennettu yksityisyyden suoja voi sisältää erilaisia tapaus- tai sovelluskohtaisia toimia. Joissain tapauksissa se voi esimerkiksi edellyttää henkilötietojen poistamista/karsimista tai tarpeettoman ja/tai ei-toivotun käsittelyn estämistä. Aika ajoin sisäänrakennettu yksityisyyden tuoja voi tarkoittaa työkalujen antamista kansalaisten käyttöön henkilötietojen valvomiseksi. Tällaisia toimenpiteitä olisi harkittava määriteltäessä standardeja ja/tai parhaita

([1]) Mietintö aiheesta ”Euroopan uusi digitaalinen asialista: i2010-aloitteesta digital.eu:hun” (2009/2225 (INI)), hyväksytty 18.3.2010.

([2]) Esimerkiksi hoitoa varten kerättyjen terveystietojen myynti tai hyödyntäminen ei ole sallittua, kun tarkoituksena on valita uusien sivutoimipisteiden sijaintipaikkoja, perustaa päiväkirurgisia yksiköitä tai suunnitella muulla tavoin tulevaa toimintaa, mihin liittyy taloudellisia seurauksia.

käytäntöjä. Toimenpiteet voidaan sisällyttää myös tieto- ja viestintäjärjestelmien arkkitehtuuriin tai henkilötietoja käsittelevien yksiköiden organisaatiorakenteeseen.

III.1 **Sisäänrakennetun yksityisyyden suojan periaatteen soveltaminen erilaisiin TVT-ympäristöihin ja sen vaikutukset**

21. Sisäänrakennetun yksityisyyden suojan tarvetta esiintyy monissa erilaisissa TVT-ympäristöissä. Esimerkiksi terveydenhoitoalalla nojaudutaan entistä laajemmin TVT-infrastruktuuriin, joka edellyttää usein potilaiden terveyteen liittyvien tietojen varastointia keskitetysti. Sisäänrakennetun yksityisyyden suojan periaatteen soveltaminen terveydenhoitoalalla voi edellyttää eri toimenpiteiden soveltuvuuden arviointia: onko minimoitava keskitetysti tallennetut tiedot tai rajoitettava ne pelkästään hakemistoihin, onko käytettävä salausvälineitä, annettava käyttöoikeuksia yksinomaan tiedonsaantitarpeen perusteella, poistettava tilastotiedoista nimet, kun niitä ei enää tarvita jne.

22. Myös liikennejärjestelmissä on yhä useammin oletusarvoisesti mukana kehittyneitä TVT-sovelluksia, jotka vaikuttavat ajoneuvoon ja sen ympäristöön eri tarkoituksissa ja eri toimintojen yhteydessä. Autoissa on esimerkiksi yhä laajemmin uusia TVT-toimintoja (GPS, GSM, anturiverkostot jne.), jotka kertovat paitsi auton sijainnin myös sen teknisen kunnon tosiaikaisesti. Näiden tietojen avulla esimerkiksi nykyinen tienkäyttövero voidaan korvata käytön mukaan maksettavalla maksulla. Sisäänrakennetun yksityisyyden suojan soveltaminen tällaisten järjestelmien arkkitehtuurisuunnitteluun tarkoittaisi, että henkilötietoja käsitellään ja välitetään eteenpäin mahdollisimman vähän ([1]). Periaatteen mukaisesti olisi suosittava keskitettyjen ratkaisujen sijaan hajautettuja tai osin keskitettyjä arkkitehtuureja, joissa rajoitetaan sijaintitietojen siirtoa yhteen keskitettyyn kohteeseen.

23. Edellä mainitut esimerkit osoittavat, että sisäänrakennetun yksityisyyden suojan periaatteen mukaisesti valmistettuun tieto- ja viestintätekniikkaan sisältyy merkittävästi vähemmän yksityisyyden suojan ja tietosuojan riskejä.

III.2 **Sisäänrakennetun yksityisyyden suojan mukaisen TVT:n rajallinen levinneisyys**

24. On tärkeä selvittää, ovatko taloudelliset toimijat, TVT:n valmistajat/tarjoajat ja rekisterinpitäjät kiinnostuneita markkinoimaan ja toteuttamaan sisäänrakennetun yksityisyyden suojan periaatetta TVT-alalla. Toisaalta on tärkeä arvioida sisäänrakennetun yksityisyyden suojan asiakaskysyntää.

25. Komissio julkaisi vuonna 2007 tiedonannon, jossa se kehotti yrityksiä käyttämään innovaatiokykyään ja kehittämään ja ottamaan käyttöön yksityisyyden suojaa parantavia tekniikoita yhtenä keinona parantaa yksityisyyden suojaa ja henkilötietojen suojelua kehityskaaren alusta alkaen ([2]).

26. Tähänastisten tietojen perusteella vaikuttaa siltä, etteivät julkisen tai yksityisen sektorin TVT-valmistajat ja rekisterinpitäjät ole onnistuneet ottamaan käyttöön tai markkinoimaan sisäänrakennettua yksityisyyden suojaa. Syitä on esitetty useita, muun muassa taloudellisten kannustimien tai yhteiskunnallisen tuen puuttuminen, riittämätön kysyntä jne ([3]).

27. Samaan aikaan sisäänrakennetun yksityisyyden suojan kysyntä on ollut varsin pientä käyttäjien keskuudessa. TVT-tuotteiden ja -palvelujen käyttäjät voivat oikeutetusti olettaa, että heidän yksityisyytensä ja henkilötietonsa ovat tosiasiassa suojattuja, vaikka näin ei monissakaan tapauksissa ole. Eräissä tapauksissa käyttäjillä ei ole yksinkertaisesti mahdollisuutta toteuttaa tarpeellisia turvaamistoimenpiteitä omien tai muiden henkilötietojen suojaamiseksi. Usein tähän on syynä täydellinen tai osittainen tietämättömyys riskeistä. Esimerkiksi nuoret jättävät yleensä huomiotta riskit, joita henkilötietojen näkyville saattaminen sosiaalisissa verkkoyhteisöissä aiheuttaa, ja useinkaan he eivät määritä yksityisyysasetuksia. Osa käyttäjistä on tosin tietoisia riskeistä, mutta heillä ei välttämättä ole tarvittavaa teknistä asiantuntemusta suojaustekniikan käyttämiseksi, esimerkkeinä Internet-yhteyden suojaaminen tai selaimen asetusten muuttaminen sellaisiksi, että Internetin käytön seurantaan perustuvan profilointi vaikeutuu.

28. Tästä huolimatta yksityisyyden suojaan ja tietosuojaan kohdistuvat riskit ovat hyvin todellisia. Jollei yksityisyyttä ja tietosuojaa oteta huomioon alusta alkaen, järjestelmien muuttaminen jälkikäteen on usein mahdotonta tai taloudellisesti liian raskasta. Sattunutta vahinkoa ei aina voida

([1]) Katso Euroopan tietosuojavaltuutetun lausunto komission tiedonannosta ”Toimintasuunnitelma älykkäiden liikennejärjestelmien käyttöönottamiseksi Euroopassa” ja siihen liittyvästä ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi tieliikennealan älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista, annettu 22 päivänä heinäkuuta 2009, joka on luettavissa osoitteessa http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_FI.pdf

([2]) Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla, KOM(2007) 228 lopullinen, 2.5.2007.

([3]) Tutkimus yksityisyyden suojaa parantavien tekniikoiden käytöstä saatavasta taloudellisesta hyödystä, jls/2008/D4/036.

korvata. Viime vuosina yleistyneet tietomurrot osoittavat selvästi tämän ongelman todelliseksi ja sisäänrakennetun yksityisyyden suojan tarpeelliseksi.

29. Edellä käsitellyn perusteella on selvää, että henkilötietojen käsittelyyn tarkoitetun tieto- ja viestintätekniikan valmistajien ja tarjoajien olisi yhdessä rekisterinpitäjien kanssa kannettava vastuunsa siitä, että järjestelmät suunnitellaan sisältämään sisäänrakennetut tietosuojan ja yksityisyyden takeet. Monissa tapauksissa tämä tarkoittaa järjestelmien suunnittelemista oletusarvoisesti käyttämään yksityisyyden suojaavia asetuksia.

30. Tätä taustaa vasten on pohdittava, millä tavoin poliittisten päättäjien olisi edistettävä sisäänrakennettua yksityisyyden suojaa TVT:n kehittämisessä. Ensimmäiseksi on selvitettävä sisältääkö nykyinen tietosuojalainsäädäntö riittävät säännökset, joilla sekä rekisterinpitäjät että valmistajat/ohjelmistokehittäjät velvoitetaan ottamaan käyttöön sisäänrakennetun yksityisyyden suojan periaatteen. Toiseksi on selvitettävä, miten eurooppalaisessa digitaalistrategiassa voidaan varmistaa, että TVT-sektori lisää kuluttajien luottamusta.

IV. **SISÄÄNRAKENNETUN YKSITYISYYDEN SUOJAN PERIAATTEEN SISÄLLYTTÄMINEN EU:N LAINSÄÄDÄNTÖÖN JA POLITIIKKAAN**

IV.1 **Nykyinen tietosuoja- ja yksityisyyslainsäädäntö**

31. EU:ssa on vankka tietosuoja ja yksityisyyden suoja, jotka on vahvistettu direktiivissä 95/46/EY ([1]), direktiivissä 2002/58/EY ([2]) sekä Euroopan ihmisoikeustuomioistuimen ([3]) ja EY:n tuomioistuimen oikeuskäytännössä.

32. Tietosuojadirektiivi koskee ”kaikenlaisia sellaisia toimintoja tai toimintojen kokonaisuuksia, joita kohdistetaan henkilötietoihin” (kerääminen, säilyttäminen, luovuttaminen jne.). Siinä henkilötietojen käsittelijät (”rekisterinpitäjät”) velvoitetaan noudattamaan tiettyjä periaatteita ja velvollisuuksia. Direktiivissä määritellään yksilön oikeudet, esimerkiksi oikeus päästä käsiksi henkilötietoihin. Sähköisen viestinnän tietosuojadirektiivissä käsitellään erityisesti yksityisyyden suojaa sähköisen viestinnän alalla ([4]).

33. Nykyisessä tietosuojadirektiivissä ei nimenomaisesti edellytetä sisäänrakennettua yksityisyyden suojaa. Siihen sisältyy joka tapauksessa säännöksiä, jotka voivat eri tilanteissa velvoittaa noudattamaan sisäänrakennetun yksityisyyden suojan periaatetta. Erityisesti sen 17 artiklassa edellytetään, että rekisterinpitäjät toteuttavat tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi laittomalta käsittelyltä ([5]). Näin ollen sisäänrakennettu yksityisyyden suoja on otettu huomioon varsin yleisesti. Lisäksi direktiivin säännökset ovat suunnattu pääasiassa rekisterinpitäjille ja koskevat näiden suorittamaa henkilötietojen käsittelyä. Niissä ei nimenomaisesti edellytetä, että tieto- ja viestintätekniikan tulee olla yksityisyyden suojan ja tietosuojan mukaista, mikä edellyttäisi myös TVT-alan suunnittelijoiden ja valmistajien sekä standardointivaiheen toiminnan huomioon ottamista.

34. Sähköisen viestinnän alan yksityisyyden suojaa koskeva direktiivi on edellistä sanatarkempi. Sen 14 artiklan 3 kohdassa säädetään, että ”[t]arvittaessa voidaan toteuttaa toimenpiteitä sen varmistamiseksi, että päätelaitteet rakennetaan tavalla, joka on sopusoinnussa käyttäjillä olevan oikeuden kanssa, joka koskee heidän henkilötietojensa käytön suojelua ja valvontaa direktiivin 1999/5/EY ja standardoinnista tietotekniikassa ja televiestinnässä 22 päivänä joulukuuta 1986 tehdyn neuvoston päätöksen 87/95/ETY(10) mukaisesti”. Tätä säännöstä ei ole kuitenkaan koskaan käytetty ([6]).

35. Vaikka direktiivien edellä mainitut säännökset auttavat *edistämään* sisäänrakennettua yksityisyyden suojaa, ne eivät käytännössä ole riittäneet *varmistamaan*, että yksityisyyden suoja sisällytetään tieto- ja viestintätekniikkaan.

36. Edellä kuvatun perusteella lainsäädännössä ei säädetä riittävän tarkasti siitä, että tieto- ja viestintätekniikka on suunniteltava sisäänrakennetun yksityisyyden suojan

([1]) Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, (jäljempänä ’tietosuojadirektiivi’).

([2]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, (jäljempänä ’sähköisen viestinnän tietosuojadirektiivi’).

([3]) Ihmisoikeustuomioistuin tulkitsee Roomassa 4 päivänä marraskuuta 1950 ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn eurooppalaisen yleissopimuksen 8 artiklassa määriteltyjä keskeisiä seikkoja ja edellytyksiä.

([4]) Lissabonin sopimuksessa vahvistettiin tätä suojaa tunnustamalla henkilötietojen yksityisyyden suoja ja perhe-elämän kunnioittaminen ja henkilötietojen suoja erillisiksi perusoikeuksiksi EU:n perusoikeuskirjan 7 ja 8 artiklan mukaisesti. EU:n perusoikeuskirjasta tuli velvoittava Lissabonin sopimuksen tullessa voimaan.

([5]) Direktiivin 17 artiklassa säädetään seuraavasti: ”Jäsenvaltioiden on säädettävä siitä, että rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai tietojen antamiselta, erityisesti jos käsittely muodostuu tietojen siirtämisestä verkossa, sekä kaikelta muulta laittomalta käsittelyltä.” Johdanto-osan 46 kohdassa täydennetään artiklan tekstiä seuraavasti: ”rekisteröityjen oikeuksien ja vapauksien suoja henkilötietojen käsittelyssä edellyttää, että toteutetaan asianmukaiset tekniset ja organisaatiotoimenpiteet sekä käsittelyn suunnittelu- että toteuttamisvaiheessa, erityisesti turvallisuuden takaamiseksi ja siten luvattoman käsittelyn estämiseksi; jäsenvaltioiden on valvottava, että rekisterinpitäjät noudattavat näitä toimenpiteitä; toimenpiteillä on taattava asianmukainen turvallisuustaso ottaen huomioon kehityksen taso ja toimenpiteiden kustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien tietojen luonteeseen”.

([6]) Komissio on ilmoittanut aikomuksestaan saattaa direktiivi 1999/5/EY ajan tasalle vuoden 2010 lopulla.

periaatteen mukaisesti. Myöskään tietosuojaviranomaisilla ei ole riittävästi valtuuksia varmistaa sisäänrakennetun yksityisyyden suojan sisällyttäminen. Tämä johtaa tehottomuuteen. Tietosuojaviranomaiset voivat esimerkiksi määrätä seuraamuksia, jos rekisterinpitäjät eivät vastaa kansalaisten pyyntöihin päästä tietoihin käsiksi, ja niillä on valtuudet edellyttää tiettyjen toimenpiteiden toteuttamista laittoman tietojenkäsittelyn estämiseksi. Sitä vastoin ei ole aina riittävän selvää, voivatko viranomaiset valtuuksiensa perusteella edellyttää, että järjestelmät on suunniteltava helpottamaan henkilötietojen suojeluoikeuksien toteutumista ([1]). Nykyisen lainsäädännön säännösten vuoksi on esimerkiksi epäselvää, voidaanko tietojärjestelmän arkkitehtuuri velvoittaa suunnittelemaan sellaiseksi, että yhtiöt voivat vastata nopeasti kansalaisten esittämiin pyyntöihin saada tiedot nähtäväksi automaattisesti ja nopeasti. Lisäksi yritykset muuttaa kehitettyä ja käyttöön otettua tekniikkaa jälkikäteen voivat aiheuttaa ratkaisujen tilkkutäkin, joka ei toimi täydellisesti ja on lisäksi taloudellisesti raskas.

37. Tietosuojavaltuutetun ja 29 artiklan mukaisen tietosuojaryhmän ([2]) kanta on, että nykyisen lainsäädännön sanamuoto mahdollistaa sisäänrakennetun yksityisyyden suojan periaatteen tarkentamisen yksityiskohtaisesti.

IV.2 **Sisäänrakennetun yksityisyyden suojan huomioiminen eri tasoilla**

38. Edellä käsitellyn perusteella Euroopan tietosuojavaltuutettu suosittelee komissiolle neljää toimintalinjaa:

a) Sen olisi sisällytettävä sisäänrakennettua yksityisyyden suojaa koskeva yleinen säännös tietosuojaa koskevaan lainsäädäntöön.

b) Tätä yleistä säännöstä olisi tarkennettava erityissäännöksissä, kun eri aloille ehdotetaan erityisiä oikeudellisia välineitä. erityiset säännökset voitaisiin jo nyt sisällyttää säädöksiin tietosuojadirektiivin 17 artiklan (ja muun olemassa olevan lainsäädännön) nojalla.

c) Sisäänrakennettu yksityisyyden suoja olisi otettava eurooppalaiseen digitaalistrategiaan ohjaavaksi periaatteeksi.

d) Sisäänrakennettu yksityisyyden suoja olisi sisällytettävä periaatteena muihin EU:n aloitteisiin (kuin lainsäädännöllisiin aloitteisiin).

Sisäänrakennettua yksityisyyden suojaa koskeva yleinen säännös

39. Tietosuojavaltuutettu ehdottaa sisäänrakennetun yksityisyyden suojan periaatteen sisällyttämistä yksiselitteisesti ja nimenomaisesti nykyiseen tietosuojalainsäädäntöön. Tämä vahvistaisi sisäänrakennetun yksityisyyden suojan periaatetta ja tekisi sen näkyvämmäksi sekä velvoittaisin sen tosiasialliseen noudattamiseen. Lisäksi se antaisi lainvalvontaviranomaisille legitiimiyden edellyttää sen tosiasiallisesti noudattamista käytännössä. Tämän on erityisen tarpeen edellä käsiteltyjen seikkojen perusteella: sen isäksi, että periaate sinällään lisää luottamusta, se toimii myös sidosryhmiin nähden kannustimena periaatteen toteuttamiseksi ja nykyisessä lainsäädännössä olevien takuiden tehostamiseksi.

40. Tämä ehdotus perustuu 29 artiklan mukaisen tietosuojaryhmän suositukseen, jonka mukaan ”sisäänrakennetun yksityisyyden suojan” periaate olisi otettava yleiseksi periaatteeksi tietosuojalainsäädännössä ja erityisesti tietosuojadirektiivissä. 29 artiklan mukaisen tietosuojaryhmän mukaan ”tämän periaatteen tulisi velvoittaa tekniikan suunnittelijoita ja valmistajia sekä rekisterinpitäjiä, joiden tehtävänä on päättää TVT:n hankinnasta ja käytöstä. Nämä tulisi velvoittaa ottamaan tietosuoja teknisesti huomioon jo tietoteknisten menettelyjen ja järjestelmien suunnitteluvaiheessa. Järjestelmien tai palvelujen tarjoajien sekä rekisterinpitäjien tulisi osoittaa, että ne ovat toteuttaneet kaikki näiden vaatimusten noudattamiseen tarvittavat toimenpiteet”.

41. Tietosuojavaltuutettu suhtautuu myönteisesti siihen, että komission jäsen Viviane Reding tukee sisäänrakennetun yksityisyyden suojan periaatteen huomioon ottamista tietosuojadirektiivin ilmoitetun tarkistamisen yhteydessä ([3]).

42. Tämän jälkeen on pohdittava lainsäädännön sisältöä. Ensimmäisenä ja tärkeimpänä asiana on, että yleisen sisäänrakennettua yksityisyyden suojan periaatteet on oltava teknologisesti neutraali. Periaatteella ei ole tarkoitus säännellä teknologiaa eli määrätä mitään tiettyjä teknisiä ratkaisuja pakollisiksi. Sitä vastoin tarkoituksena on nykyisten yksityisyyden suojan ja tietosuojan periaatteiden integrointi tieto- ja viestintäjärjestelmiin ja -ratkaisuihin. Näin

([1]) Katso Yhdistyneen kuningaskunnan tietosuojavaltuutetun viraston marraskuussa 2008 julkaistu raportti ”Privacy by Design”.

([2]) Katso 29 artiklan mukaisen tietosuojatyöryhmän lausunto 168 ”The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, annettu 1 päivänä joulukuuta 2009.

([3]) ”Sisäänrakennettu yksityisyyden suoja on niin kansalaisten kuin yritystenkin etujen mukainen periaate. Sisäänrakennettu yksityisyyden suoja parantaa kansalaisten suojaa sekä luottamusta ja uskoa uusiin palveluihin ja tuotteisiin, jotka puolestaan vaikuttavat myönteisesti talouteen. Kannustavia esimerkkejä on paljon, mutta paljon on myös tehtävää.” Pääpuhujan puhe Euroopan parlamentissa Brysselissä tietosuojapäivänä 28 päivänä tammikuuta 2010.

sidosryhmät, valmistajat, rekisterinpitäjät ja tietosuojaviranomaiset pystyvät tulkitsemaan periaatteen merkitystä yksittäistapauksissa. Toiseksi periaatteen noudattamisen tulisi olla pakollista eri vaiheissa standardien suunnittelusta ja arkkitehtuurisuunnittelusta aina käyttöönottoon rekisterinpitäjän toimesta.

Säännökset erityissäädöksissä

43. Nykyisiin ja tuleviin säädöksiin on sisällytettävä sisäänrakennetun yksityisyyden suojan periaate nykyisen lainsäädännön pohjalta sen jälkeen, kun edellä ehdotettu yleinen säännös on hyväksytty. Esimerkiksi älykkäitä liikennejärjestelmiä koskevien nykyisten aloitteiden mukaisesti komissio on aluksi erityisessä vastuussa toimenpiteiden, standardointialoitteiden, menettelyjen ja käytäntöjen määrittelyssä. Näissä tehtävissä sisäänrakennettua yksityisyyden suojaa olisi noudatettava ohjaavana periaatteena.

44. Lisäksi tietosuojavaltuutettu toteaa, että sisäänrakennetun yksityisyyden suojan periaate on erityisen tärkeä vapauteen, turvallisuuteen ja oikeuteen liittyvällä alueella, varsinkin Tukholman ohjelmassa määritellyn tietohallintostrategian yhteydessä ([1]). Lausunnossaan kyseisestä Tukholman ohjelmasta tietosuojavaltuutettu korosti, että tietojenvaihdossa käytettävä arkkitehtuuri olisi perustettava sisäänrakennettuun yksityisyyden suojaan ([2]): ”Tämä merkitsee käytännössä, että yleisen turvallisuuden tarkoituksiin suunnitellut tietojärjestelmät olisi aina suunniteltava ’sisäänrakennetun yksityisyyden suojan’ periaatteen mukaisesti.”

45. 29 artiklan mukaisen tietosuojatyöryhmän lausunnossa yksityisyyden tulevaisuudesta ([3]) korostetaan vielä käytännönläheisemmin käsittein, että vapauteen, turvallisuuteen ja oikeuteen liittyvällä alueella – jolla julkisviranomaiset ovat pääasiallisia toimijoita ja valvontaa lisäävät toimenpiteet vaikuttavat suoraan yksityisyyden suojan ja tietosuojan perusoikeuksiin – sisäänrakennetun yksityisyyden suojan vaatimuksista olisi tehtävä pakollisia. Ottamalla nämä vaatimukset käyttöön tietojärjestelmiin liittyen valtiot edistäisivät sisäänrakennettua yksityisyyden suojaa myös aloitteellisina asiakkaina.

Sisäänrakennettu yksityisyyden suoja eurooppalaisen digitaalistrategian ohjaavana periaatteena

46. Tieto- ja viestintätekniikka kehittyy yhä monimutkaisemmaksi ja aiheuttaa entistä suurempia yksityisyyden ja tietosuojan riskejä. Yleensä helpommin käyttöön saatava, kopioitava ja siirrettävä digitoitu tieto altistuu paperitietoa paljon suuremmille riskeille. Kun siirrytään kohti keskenään linkitettyjen kohteiden verkkoja, riskit vain lisääntyvät. Mitä suuremmat yksityisyyden ja tietosuojan riskit ovat, sitä suuremmaksi kasvaa pitkälle kehittyneen tietosuojan ja yksityisyyden suojan järjestelmien kysyntä. Tämän vuoksi sisäänrakennetun yksityisyyden suojan käyttöönottotarvetta perustelevat syyt koskevat TVT-alaa entistä velvoittavammin. Lisäksi kansalaisten luottamus TVT-alaan on ratkaiseva edellytys, kuten edellä todetaan, uusien palvelujen käyttöönotolle, ja yksityisyyden suoja ja tietosuoja ovat avaintekijöitä luottamuksen luomisessa.

47. Edellä sanotun perusteella TVT:n kehitysstrategiassa on vahvistettava, että suunnitteluun on sisällytettävä yksityisyyden suojan ja tietosuojan varmistava tekijä eli otettava huomioon sisäänrakennetun yksityisyyden suojan periaate.

48. Tämän vuoksi eurooppalaisessa digitaalistrategiassa olisi nimenomaisesti tuettava sisäänrakennetun yksityisyyden suojan periaatetta välttämättömänä välineenä, kun varmistetaan kansalaisten luottamusta tieto- ja viestintätekniikkaan ja verkkopalveluihin. Siinä olisi todettava, että yksityisyyden suoja ja luottamus ovat sidoksissa toisiinsa ja että sisäänrakennettua yksityisyyden suojaa olisi käytettävä ohjaavan tekijänä luottamuksen ansaitsevan TVT-alan kehityksessä.

Sisäänrakennettu yksityisyyden suoja periaatteena muissa EU:n aloitteissa

49. Komission tulisi käyttää sisäänrakennettua yksityisyyden suojaa ohjaavana periaatteena pannessaan täytäntöön politiikkaa, toimia ja aloitteita yksittäisillä TVT-aloilla, esimerkkeinä sähköinen terveydenhuolto, sähköiset hankinnat, sähköinen sosiaaliturva, sähköinen oppiminen jne. Monet näistä aloitteista ovat osa eurooppalaisen digitaalistrategian toimia.

50. Tämä tarkoittaa esimerkiksi sitä, että kansalaisten viranomaisasioinnin mahdollistavista aloitteista on kehitettävä tehokkaita ja nykyaikaisia suunnittelemalla ne ja käyttämällä niitä sisäänrakennetun yksityisyyden suojan periaatteen mukaisesti. Sama koskee komission politiikkaa ja toimia, joilla toteutetaan entistä nopeampi Internet, digitaalisia sisältöjä tai kannustetaan yleisesti kiinteää tai langatonta viestintää ja tiedonsiirtoa.

([1]) Eurooppa-neuvoston joulukuussa 2009 hyväksymä Tukholman ohjelma – avoin ja turvallinen Eurooppa kansalaisia varten.

([2]) Euroopan tietosuojavaltuutetun lausunto komission neuvostolle ja Euroopan parlamentille antamasta tiedonannosta ”Vapauden, turvallisuuden ja oikeuden alue kansalaisia varten”, annettu 10 päivänä heinäkuuta 2009, EUVL C 276, 17.11.2009, s. 8, kohta 60.

([3]) Katso 29 artiklan mukaisen tietosuojatyöryhmän lausunto 168 ”The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, annettu 1 päivänä joulukuuta 2009.

51. Edellä mainittu sisältää niin ikään alueet, joissa komissio on vastuussa laaja-alaisista tietojärjestelmistä, kuten Schengenin tietojärjestelmä SIS ja viisumitietojärjestelmä VIS, sekä tapaukset, joissa komission vastuu on rajoitettu järjestelmän yleisen infrastruktuuriin kehittämiseen ja ylläpitämiseen, esimerkkinä eurooppalainen rikosrekisteritietojärjestelmä ECRIS.

52. Sisäänrakennetun yksityisyyden suojan periaatteen yksityiskohtainen kehittäminen riippuu kulloisestakin alasta ja tilanteesta. Kun komission aloitteisiin liittyy esimerkiksi yksittäistä TVT-sektoria koskevia lainsäädäntöehdotuksia, monissa tapauksissa on aiheellista sisällyttää nimenomainen viittaus kyseisen TVT-sovelluksen tai -järjestelmän suunnittelussa noudatettavaan sisäänrakennetun yksityisyyden suojaan. Kun komissio suunnittelee alakohtaisia toimintasuunnitelmia, niissä on järjestelmällisesti varmistettava lainsäädännön soveltaminen ja taattava nimenomaisesti, että kyseisen TVT:n kehittämisessä huomioidaan sisäänrakennettu yksityisyyden suoja.

53. Tutkimuksen osalta seitsemättä puiteohjelmaa ja sitä seuraavia puiteohjelmia olisi käytettävä sellaisten hankkeiden tukemiseen, joissa on tarkoituksena määritellä standardeja, tieto- ja viestintätekniikkaa ja -arkkitehtuuria, joissa otetaan yksityisyys ja erityisesti sisäänrakennetun yksityisyyden suojan periaate entistä paremmin huomioon. Lisäksi sisäänrakennettu yksityisyyden suoja on otettava välttämättömäksi osaksi laajempia TVT-hankkeita, joissa on tarkoituksena yksilöiden henkilötietojen käsittely.

Erityistä huoltava aiheuttava alat

54. Eräissä tapauksissa voi olla tarpeen määritellä yksityiskohtaisia tai erityisiä sisäänrakennetun yksityisyyden suojan toimenpiteitä, jotka on sisällytettävä tietynlaiseen tietoja viestintätuotteeseen tai -tekniikkaan joko lainsäädäntöteitse tai muuten, koska kansalaisten yksityisyyden suoja tai tietosuoja on erityisesti alttiina riskille tai koska muut tekijät (alan vastustus sisäänrakennetun yksityisyyden suojan sisältävien tuotteiden tarjontaan, kuluttajakysyntä tms.) tätä edellyttävät.

55. Tietosuojavaltuutettu on yksilöinyt useita aloja (radiotaajuustunnistus, sosiaaliset verkkoyhteisöt ja selainsovellukset), jotka ansaitsevat tietosuojavaltuutetun mielestä jo tässä vaiheessa komission erityisen huomion ja edellä mainittuja konkreettisia toimenpiteitä. Näitä aloja käsitellään seuraavassa.

V. **RADIOTAAJUUSTUNNISTUS RFID**

56. RFID-tunnisteita voidaan liittää esineisiin, eläimiin ja ihmisiin. Niiden avulla voidaan kerätä ja tallentaa henkilötietoja kuten potilaskertomuksia, seurata ihmisten liikkumista tai profiloida heidän käyttäytymistään eri tarkoituksia varten. Tämä voi tapahtua ihmisten tietämättä ([1]).

57. Tehokkaat takuut tietosuojasta, yksityiseen suojasta ja kaikista asiaan liittyvistä eettisistä kysymyksistä ovat ratkaisevan tärkeitä ihmisten luottamukselle radiotaajuustunnistukseen ja esineiden Internetiin. Vain tällöin tekniikasta saadaan sen lukuisia taloudellisia ja yhteiskunnallisia hyötyjä.

V.1 **Sovellettavan tietosuojalainsäädännön aukot**

58. Tietosuojadirektiiviä ja sähköisen viestinnän tietosuojadirektiiviä sovelletaan RFID-sovellusten avulla tapahtuvaan tiedonkeruuseen ([2]). Direktiivit edellyttävät muun muassa, että RFID-sovellusten käytössä noudatetaan riittäviä yksityisyyden suojaavia toimenpiteitä ([3]).

59. Tässä lainsäädännössä ei kuitenkaan kattavasti vastata tämän tekniikan aiheuttamiin tietosuojan ja yksityisyyden suojan ongelmiin. Tämä johtuu siitä, etteivät direktiivit olet riittävän yksityiskohtaisia RFID-sovellusten yhteydessä

([1]) RFID on lyhenne sanoista Radio Frequency Identification eli radiotaajuustunnistus. Radiotaajuustunnistuksen tekniikan eli infrastruktuurin pääosat ovat *tunniste* (esim. mikrosiru), *lukulaite* sekä *sovellus*, joka on yhdistetty tunnisteisiin ja lukulaitteisiin väliohjelmiston avulla ja joka käsittelee tuotettuja tietoja. Tunniste on elektroninen piiri, joka tallentaa tietoja ja sisältää antennin, joka lähettää tietoja radioaaltojen avulla. Lukulaitteessa on antenni ja demodulaattori, joka muuntaa radiolinkiltä vastaanotetun analogisen tiedon digitaaliseksi tiedoksi. Sen jälkeen tiedot voidaan välittää verkkoja pitkin edelleen tietokantoihin ja palvelimiin käsiteltäväksi tietokoneen avulla.

([2]) Sähköisen viestinnän tietosuojadirektiivin 3 artiklassa viitataan sähköiseen tunnistamiseen: "Tätä direktiiviä sovelletaan henkilötietojen käsittelyyn, joka liittyy yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa yhteisössä, mukaan luettuina tiedonkeruu- ja tunnistuslaitteita tukevat yleiset viestintäverkot." Säännöstä täydennetään muutosdirektiivin johdantokohdassa 56: "Teknologian kehitys mahdollistaa uusien tiedonkeruuja tunnistuslaitteisiin perustuvien sovellusten kehittämisen. Nämä laitteet voisivat olla radiotaajuuksia käyttäviä kontaktittomia laitteita. Esimerkiksi radiotaajuiset etätunnistuslaitteet (Radio Frequency Identification Devices, RFID) käyttävät radiotaajuuksia tietojen lukemiseen yksilöllisistä tunnisteista, minkä jälkeen tietoja voidaan siirtää olemassa olevissa viestintäverkoissa. Tällaisten teknologioiden laajamittainen käyttö voi tuoda huomattavia taloudellisia ja sosiaalisia hyötyjä ja edistää merkittävästi sisämarkkinoiden kehitystä, jos kansalaiset hyväksyvät niiden käytön. Tämän tavoitteen saavuttamiseksi on tarpeen varmistaa kaikkien yksilön perusoikeuksien turvaaminen, mukaan lukien oikeus yksityisyyteen ja tietosuojaan. Kun tällaiset laitteet on liitetty yleisesti saatavilla oleviin sähköisiin viestintäverkkoihin tai ne käyttävät sähköisiä viestintäpalveluja perusinfrastruktuurina, olisi sovellettava direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) asiaa koskevia säännöksiä, kuten turvallisuutta, liikenne- ja sijaintitietoja ja luottamuksellisuutta koskevia säännöksiä."

([3]) Esimerkiksi tietosuojadirektiivin 17 artiklassa säädetään velvoitteesta toteuttaa tarpeellisia teknisiä ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta tai luvattomalta luovuttamiselta.

käytettävien suojatoimenpiteiden tyypin suhteen. Olemassa olevia sääntöjä on täydennettävä uusilla säännöillä, jossa velvoitetaan käyttämään erityisiä suojakeinoja ja erityisesti RFID-tekniikkaan upotettavia pakollisia teknisiä ratkaisuja (sisäänrakennettua yksityisyyden suojaa). Tämä liittyy henkilötietojen tallentamiseen käytettäviin tunnisteisiin, joissa olisi oltava tuhoamiskomento, ja salauksen käyttöä tietyn tyyppisiä henkilötietoja sisältävissä tunnisteissa.

V.2 **Ensi vaiheen itsesääntely**

60. Maaliskuussa 2007 komissio hyväksy tiedonannon ([1]), jossa se muun muassa toteaa, että alalla saatetaan tarvita yksityiskohtaisia ohjeita RFID:n käytännön käyttöönotosta ja sellaisten suunnittelukriteereiden määrittelyä ja käyttöönottoa, joilla voidaan välttää yksityisyyden suojaan ja tietoturvaan kohdistuvia riskejä.

61. Näihin päämääriin päästäkseen komissio hyväksyi toukokuussa 2009 suosituksen yksityisyyden suojaa ja tietosuojaa koskevien periaatteiden toteuttamisesta radiotaajuustunnistusta käyttävissä sovelluksissa ([2]). Vähittäiskaupan radiotaajuustunnistussovelluksissa komissio edellyttää RFID-tunnisteiden deaktivointia myyntipisteessä, paitsi jos kuluttaja on antanut luvan tunnisteen käyttöön. Tätä sääntöä olisi sovellettava, jollei yksityisyyden suojaa tai tietosuojaa koskevassa vaikutusten arvioinnissa ole osoitettu, etteivät myyntipisteen jälkeen toimiviksi jäävät tunnisteet todennäköisesti muodosta uhkaa yksityisyyden tai henkilötietojen suojalle. Tällöinkin kansalaisilla olisi oltava maksuton keino tunnisteiden poistamiseen.

62. Tietosuojavaltuutettu yhtyy komission kantaan itsesäänte-lyn välineiden käytöstä. Kuten jäljempänä kuitenkin selvitetään, on mahdollista, ettei itsesääntelyllä saavuteta olettuja tuloksia. Tämän vuoksi tietosuojavaltuutettu kehottaa komissiota valmistautumaan vaihtoehtoisten toimenpiteiden hyväksymiseen.

V.3 **Huolta aiheuttavat alat ja mahdolliset lisätoimet itsesääntelyn epäonnistuessa**

63. Tietosuojavaltuutettu on huolissaan siitä, että RFID-sovelluksia vähittäiskaupan alalla operoivat organisaatiot voivat jättää huomiota vaihtoehdon, että RFID-tunnisteita seuraavat myös ei-toivotut ulkopuoliset tahot. Seuranta saattaa paljastaa tunnisteeseen (mahdollisesti) tallennettuja henkilötietoja mutta voi antaa ulkopuoliselle mahdollisuuden seurata tai tunnistaa henkilöitä ajan mittaan pelkästään henkilön mukana kulkevan yhden tai useamman tunnisteen sisältämän yksilöllisen tunnistetiedon perusteella ympäristössä, joka ei välttämättä kuulu lainkaan RFID-sovelluksen käyttöalaan. Tietosuojavaltuutettu on lisäksi huolissaan siitä, että RFID-sovellusoperaattorit voivat virheellisesti vedota tähän poikkeukseen ja jättää tunnisteen toimintaan myyntipisteen jälkeenkin.

64. Mikäli tällaista tapahtuu, voi olla liian myöhäistä lieventää henkilön tietosuojaan ja yksityisyyden suojaan liittyviä riskejä, sillä ne ovat jo voineet toteutua. Lisäksi itsesääntely voi heikentää kansallisten lainvalvontaviranomaisten asemaa niiden vaatiessa RFID-sovellusoperaattoreita käyttämään tiettyjä sisäänrakennetun yksityisyyden suojan toimenpiteitä.

65. Edellä sanotun perusteella tietosuojavaltuutettu kehottaa komissiota valmistautumaan esittämään sellaisia säädöksiä, joissa säännellään radiotaajuustunnistuksen keskeiset seikat sinä tapauksessa, että nykyisen lainsäädännön tehokas soveltaminen epäonnistuu. Komission arviota ei tule tarpeettomasti lykätä: lykkääminen voisi lisätä kansalaisten riskejä ja haitata myös elinkeinoelämää, koska oikeudellinen epävarmuus voi kasvaa liian suureksi ja syntyneiden ongelmien ratkaisu on todennäköisesti hankalampaa ja kalliimpaa.

66. Mahdollisesti ehdotettavien toimenpiteiden osaksi tietosuojavaltuutettu suosittelee niin sanottua *opt-in*-periaatetta, jonka mukaan kaikki myyntipisteen jälkeen kuluttajatuotteisiin jäävät RDIS-tunnisteet olisi oletusarvoisesti deaktivoitava. Komission ei välttämättä ole tarpeellista tai aiheellista tarkentaa käytettävää konkreettistaa tekniikkaa. Euroopan unionin lainsäädännössä on sitä vastoin säädettävä lainmukaisesti velvoitteesta pyytää suostumus, jolloin operaattoreilla on riittävä valinnanvapaus päättää vaatimuksen toteutustavasta.

V.4 **Muita pohdittavia seikkoja: esineiden Internetin hallintotapa**

67. RFID-tunnisteiden tuottama tieto – esimerkiksi tuotetieto – voidaan loppujen lopuksi yhdistää maailmanlaajuisen viestintäverkoston infrastruktuuriin. Tästä käytetään yleensä käsitettä ”esineiden Internet”. Tämä aiheuttaa tietosuojaa ja yksityisyyden suojaa koskevia kysymyksiä, koska todellisen maailman esineitä voidaan tunnistaa RFID-tunnisteiden avulla, joissa on tuotetietojen lisäksi mahdollisesti myös henkilötietoja.

68. Ratkaisematta on monia kysymyksiä esimerkiksi siitä, kuka hallinnoi tunnisteilla seurattujen esineiden tietojen tallennusta. Miten se järjestetään? Kenellä on pääsy tietoihin? kesäkuussa 2009 komissio hyväksyi tiedonannon esineiden Internetistä ([3]), jossa se tunnisti nimenomaisesti ilmiöön liittyvät mahdolliset tietosuoja- ja yksityisyydensuojaongelmat.

([1]) Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle – Radiotaajuustunnistus Euroopassa: asteittain kohti alan yhteisiä periaatteita, KOM(2007) 96 lopullinen, hyväksytty 15.3.2007.

([2]) Komission suositus, annettu 12.5.2009, yksityisyyden suojaa ja tietosuojaa koskevien periaatteiden toteuttamisesta radiotaajuustunnistusta käyttävissä sovelluksissa (K(2009) 3200 lopullinen).

([3]) Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Esineiden internet – Toimintasuunnitelma Euroopalle, KOM(2009) 278 lopullinen, 18.6.2009.

69. Tietosuojavaltuutettu haluaa ottaa esiin eräitä tiedonannossa mainittuja seikkoja, jotka ansaitsevat tietosuojavaltuutetun mielestä erityistä huomiota esineiden Internetin kehittyessä. Ensimmäinen seikka on hajautettu arkkitehtuuri, joka voi helpottaa vastuukysymyksien jakoa ja EU:n lainsäädännön valvottavuutta. Toisena seikkana on mainittava, että kansalaisten oikeutta seuraamattomuuteen on varjeltava mahdollisuuksien mukaan. Toisin sanoen kansalaisia saisi seurata RFID-tunnisteiden avulla ilman heidän suostumustaan vain erittäin harvalukuisissa tapauksissa. Suostumuksen on oltava sanatarkka. Tähän viitataan yleensä käsitteillä ”radiohiljaisuus” ja oikeus kytkeytyä irti verkosta. Viimeisenä on mainittava esineiden Internetin suunnittelu sisäänrakennetun yksityisyyden suojan periaatteen näkökulmasta. Tämä voisi esimerkiksi edellyttää, että konkreettisissa RFID-sovelluksissa on yhdysrakenteiset mekanismit, joilla hallinta luovutetaan käyttäjille ja joiden oletusasetuksena on yksityisyyden suojaaminen.

70. Tietosuojavaltuutettu edellyttää, että tietosuojavaltuutettua kuullaan, kun komissio toteuttaa tiedonannossa suunniteltuja toimia, erityisesti kun se laatii tiedonantoa yksityisyydensuojan ja luottamuksen merkityksestä kaikkialle ulottuvassa tietoyhteiskunnassa.

VI. **SOSIAALISET VERKKOYHTEISÖT JA OLETUSARVOISEN YKSITYISYYDEN SUOJAN TARVE**

71. Sosiaaliset verkkoyhteisöt ovat nyt suuressa suosiossa. Ne näyttävät ylittäneen sähköpostinkin suosiossa. Niiden avulla samanlaisista asioista ja/tai harrastuksista kiinnostuneet ihmiset pääsevät yhteyteen toistensa kanssa. Ihmiset voivat luoda itselleen verkkoprofiileja ja jakaa mediatiedostoja, kuten videoita, valokuvia, musiikkia sekä ammatillisia profiilejaan.

72. Nuoret ovat nopeasti omaksuneet sosiaalisten medioiden verkkokäytön, eikä suuntaus näytä laantumisen merkkejä. Internet-käyttäjien keski-ikä on alentunut Euroopassa viime vuosina: nyt 9–10-vuotiaat käyvät Internetissä useita kertoja viikossa, 12–14-vuotiaat käyvät siellä päivittäin ja usein 1–3 tunnin ajan.

VI.1 **Sosiaaliset verkkoyhteisöt ja niihin sovellettava tietosuojaa ja yksityisyydensuojaa koskeva lainsäädäntö**

73. Sosiaalisten verkkoyhteisöjen kehittymisen myötä käyttäjät ovat voineet ladata Internetiin tietoja itsestään ja muista. Tällöin Internetin käyttäjät toimivat 29 artiklan mukaisen tietosuojatyöryhmän mukaan [1] tietosuojadirektiivin 2 artiklan d alakohdan mukaisina rekisterinpitäjinä [2]. Useimmissa tapauksissa tietojenkäsittely kuuluu kuitenkin direktiivin 3 artiklan 2 kohdassa tarkoitettuun kotitaloutta koskevaan tietojenkäsittelyyn, johon direktiiviä ei sovelleta. Toisaalta sosiaalisten verkkoyhteisöjen palvelut katsotaan rekisterinpitäjiksi, koska ne tarjoavat keinot käyttäjätietojen käsittelyyn ja kaikki käyttäjän hallinnan peruspalvelut (esim. tilien rekisteröinti ja poisto).

74. Oikeudellisesti tämä tarkoittaa, että Internetin käyttäjät ja sosiaalisten verkkoyhteisöjen palvelut ovat yhdessä vastuussa henkilötietojen käsittelystä direktiivin 2 artiklan d kohdassa tarkoitettuina ”rekisterinpitäjinä”, tosin eri laajuudessa ja erilaisin velvoittein.

75. Vastaavasti käyttäjien tulisi tietää ja ymmärtää, että käsittelemällä omia ja muiden henkilötietoja he kuuluvat EU:n tietosuojalainsäädännön piiriin, jolloin heidän edellytetään muun muassa hankkivan nimenomainen lupa niiltä henkilöiltä, joiden tiedot Internetiin ladataan, ja antaa henkilöille oikeus korjata tai estää tiedot ym. Samalla tavoin sosiaalisten verkkoyhteisöjen tulee muun muassa panna täytäntöön tarpeelliset tekniset ja organisatoriset toimenpiteet luvattoman käsittelyn estämiseksi, kun otetaan huomioon tietojen käsittelyn ja luonteen aiheuttamat riskit. Tämä puolestaan merkitsee, että sosiaalisten verkkoyhteisöjen olisi varmistettava yksityisyyttä suojelevat oletusasetukset, myös sellaiset asetukset, jotka rajoittavat profiilin näkyvyyden ainoastaan käyttäjien omille, itse valitsemille yhteyshenkilöille. Asetuksissa tulisi niin ikään edellyttää käyttäjän myönteistä vastinetta, ennen kuin profiili annetaan ulkopuolisten käyttöön, eivätkä pääsyltään rajoitetut profiilit saa tulla näkyviin sisäisissä hakukoneissa.

76. Valitettavasti lainsäädännön vaatimusten ja todellisen noudattamisen välillä on aukko. Vaikka oikeudellisesti Internetin käyttäjät katsotaan rekisterinpitäjiksi, jolloin EU:n tietosuojaa ja yksityisyydensuojaa koskeva lainsäädäntö velvoittaa heitä, todellisuudessa he ovat usein tietämättömiä tästä asemastaan. Yleisesti he eivät ymmärrä, että he käsittelevät henkilötietoja ja että näiden tietojen julkaisemiseen liittyy yksityisyydensuojaa ja tietosuojaa koskevia riskejä. Erityisesti nuoret asettavat julkisesti näkyviin sisältöä arvioimatta riittävästi sen seurauksia heille itselleen ja muille, esimerkiksi silloin kun henkilöt myöhemmin hakevat oppilaitoksiin tai työpaikkoihin.

[1] Katso 29 artiklan mukaisen tietosuojatyöryhmän lausunto 163, 5/2009 internetin sosiaalisista verkkoyhteisöistä, annettu 12 päivänä kesäkuuta 2009.

[2] ”Rekisterinpitäjällä” tarkoitetaan luonnollista tai oikeushenkilöä, julkista viranomaista, virastoa tai muuta toimielintä, joka, yksin tai yhdessä toisten kanssa, määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot; jos käsittelyn tarkoitus ja keinot määritellään kansallisilla tai yhteisön laeilla tai asetuksilla, rekisterinpitäjä tai erityiset perusteet rekisterinpitäjän nimeämiseksi voidaan vahvistaa kansallisten tai yhteisön säännösten mukaisesti.

77. Toisaalta sosiaalisten verkkoyhteisöjen palveluntarjoajien oletusasetukset perustuvat siihen, että käyttäjän on erikseen kiellettävä tietojen näyttö, mikä helpottaa henkilötietojen luovuttamista. Osassa palveluista profiilit ovat julkisten hakukoneiden käytössä oletusarvoisesti. Tässä yhteydessä on pohdittava, ovatko henkilöt tosiasiassa suostuneet tietojen luovuttamiseen ja ovatko sosiaaliset verkkoyhteisöt noudattaneet direktiivin 17 artiklaa (ks. yllä), jossa niiltä edellytetään tarpeellisia teknisiä ja organisatorisia keinoja luvattoman käsittelyn estämiseksi.

VI.2 **Sosiaalisten verkkoyhteisöjen aiheuttamat riskit ja ehdotukset niihin puuttumiseksi**

78. Edellä mainittu lisää henkilön yksityisyydensuojaan ja tietosuojaan kohdistuvaa riskiä. Internetin käyttäjät ja ne, joiden tietoja verkkoon on ladattu, latistuvat yksityisyyden ja tietosuojan törkeille loukkauksille.

79. Tätä taustaa vasten komission olisi pohdittava, mitä tilanteen korjaamiseksi olisi tehtävä ja voitaisiin tehdä. Tässä lausunnossa ei anneta kattavaa vastausta tähän kysymykseen vaan tuodaan esiin muutamia ehdotuksia harkittaviksi.

Panostaminen Internet-käyttäjien koulutukseen

80. Ensimmäinen ehdotus koskee panostamista käyttäjäkoulutukseen. Tältä osin EU:n toimielinten ja kansallisten viranomaisten olisi panostettava koulutukseen ja tiedottamiseen sosiaalisten verkkoyhteisösivustojen aiheuttamista uhista. Esimerkiksi tietoyhteiskunnan pääosastolla on ollut käynnissä Turvallisempi Internet -ohjelma, jonka tarkoituksena on voimauttaa lapsia ja nuoria ja suojella heitä esimerkiksi tiedotuskampanjoiden avulla ([1]). EU:n toimielimet käynnistivät hiljattain kampanjansa ”Ajattele ennen kuin >klik<”, jolla tiedotetaan niistä vaaroista, joita henkilötietojen jakaminen muille aiheuttaa.

81. Tietosuojavaltuutettu kannustaa komissiota jatkamaan tällaisen toiminnan tukemista. Sosiaalisten verkkoyhteisöpalvelujen tarjoajien tulisi itse toimia aktiivisesti, sillä niillä on oikeudellinen ja sosiaalinen vastuu käyttäjien kouluttamisesta palveluiden käyttöön turvallisesti ja yksityisyyttä suojellen.

82. Kuten edellä on kuvattu, tietojen asettaminen luettavaksi sosiaalisiin verkkoyhteisöihin voi oletusarvoisesti tapahtua monilla eri tavoilla. Tiedot voivat näkyä esimerkiksi suurelle yleisölle, myös hakukoneille, jotka voivat indeksoida sen ja esittää suoria linkkejä tietoihin. Toisaalta tiedot voidaan rajata vain ”valikoiduille ystäville” tai pitää täysin yksityisinä. Luonnollisesti profiilien lupakäytäntö ja käsitteet vaihtelevat sivustoittain.

83. Kuten yllä on todettu, vain harvat sosiaalisten verkkoyhteisöjen käyttäjät kuitenkin tietävät, kuinka heidän lataamiensa tietojen käyttöä rajoitetaan, saati kuinka heidän yksityisyytensä oletusasetuksia muutetaan. Yksityisyysasetuksia ei yleensä muuteta, koska käyttäjät eivät ole selvillä niiden muuttamatta jättämisen vaikutuksista tai eivät osaa muuttaa niitä. Siksi yksityisyysasetusten muuttaminen ei yleensä tarkoita, että henkilöt olisivat tehneet tietoon perustuvan päätöksen tietojen jakamisen hyväksymisestä. Tätä taustaa vasten on erityisen tärkeää, että ulkopuoliset, kuten hakukoneet, eivät muodosta linkkejä henkilökohtaisiin profiileihin sillä perusteella, että käyttäjät ovat oletusarvoisesti suostuneet tähän (koska he eivät ole muuttaneet yksityisyysasetuksiaan) ja antaneet tiedot käyttöön rajoituksetta.

84. Vaikka käyttäjäkoulutuksella voidaan helpottaa tilannetta, muutos ei tapahdu itsestään. Kuten 29 artiklan mukainen tietosuojaryhmä suosittelee sosiaalisista verkkoyhteisöistä antamassaan lausunnossa, sosiaalisten verkkoyhteisöpalvelujen tarjoajien tulisi tarjota yksityisyyttä suojaavat, maksuttomat oletusarvoiset yksityisyysasetukset. Näin käyttäjät olisivat tietoisempia toimistaan ja he pystyisivät valitsemaan järkevämmin, haluavatko he jakaa tietojaan ja keiden kanssa.

Itsesääntelyn tehtävä

85. Komissio on tehnyt 20 sosiaalisten yhteisöpalvelujen tarjoajan kanssa sopimuksen, joka tunnetaan nimellä turvallisen sosiaalisen verkostoitumisen periaatteet ([2]). Sopimuksen tarkoituksena on parantaa alaikäisten käyttäjien turvallisuutta heidän käyttäessään sosiaalisten verkkoyhteisöjen sivustoja Euroopassa. Periaatteisiin sisältyy monia vaatimuksia, jotka perustuvat yllä kuvattuun tietosuojalainsäädännön soveltamiseen. Niitä ovat muun muassa vaatimus, jonka mukaan käyttäjät voivat työkalujen ja tekniikan avulla varmistaa, että he itse päättävät henkilötietojensa käytöstä ja levittämisestä. Niihin sisältyy myös yksityisyyden turvaaminen oletusasetuksissa.

86. Tammikuun 2010 alussa komissio julkisti tuloksia periaatteiden noudattamista koskevassa raportissa ([3]). Tietosuojavaltuutettu on huolissaan siitä, että jonkinlaisesta

([1]) Tietoja ohjelmasta on luettavissa osoitteesta http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Periaatteet ovat luettavissa osoitteesta http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Raportti turvallisen sosiaalisen verkostoitumisen periaatteiden toteuttamisen arvioinnista on luettavissa osoitteesta http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

edistymisestä huolimatta paljon on vielä tehtävää. Raportista käy esimerkiksi ilmi, että sivustoilla käytettävissä olevien turvallisuustoimenpiteitä ja työkaluja koskevassa viestinnässä on ongelmia. Raportissa todetaan myös, että alle puolet sopimuksen allekirjoittajista rajoittaa alaikäisten profiilit näkymään ainoastaan heidän ystävilleen.

Ehdotonta yksityisyyttä oletusasetuksilla

87. Tätä taustaa vasten on pohdittava keskeistä kysymystä siitä, tarvitaanko täydentäviä poliittisia toimenpiteitä, joilla varmistetaan, että sosiaaliset verkkoyhteisöt varustavat palvelunsa oletusarvoisesti yksityisyyden suojaavilla asetuksilla. Asian otti esiin edellinen tietoyhteiskunta-asioista vastannut komission jäsen Viviane Reding, joka viittasi mahdolliseen lainsäädännön tarpeeseen ([1]). Myös Euroopan talous- ja sosiaalikomitea on samoilla linjoilla todetessaan, että itsesääntelyn ohella vähimmäissuojaa koskevista normeista olisi säädettävä lainsäädännössä ([2]).

88. Kuten edellä todetaan, sosiaalisten verkkoyhteisöjen palveluntarjoajien velvoite saattaa voimaan oletusarvoisesti yksityisyyden suojaavat asetukset voidaan johtaa välillisesti tietosuojadirektiivin 17 artiklasta ([3]), jossa velvoitetaan rekisterinpitäjät toteuttamaan asianmukaiset tekniset ja organisaatiotoimenpiteet (”sekä käsittelyn suunnittelu- että toteuttamisvaiheessa”) henkilötietojen suojaamiseksi laittomalta käsittelyltä ottaen huomioon asianmukainen turvallisuuden taso suhteessa käsittelyn riskeihin ja suojattavien tietojen luonteeseen.

89. Tämä artikla on kuitenkin aivan liian yleinen ja eriyttämätön myös tältä osin. Siinä ei todeta selvästi, mitä asianmukaisilla teknisillä ja organisaatiotoimenpiteillä tarkoitetaan sosiaalisten verkkoyhteisöjen yhteydessä. Nykyisessä tilanneessa vallitsee näin ollen oikeudellinen epävarmuus, mikä aiheuttaa ongelmia niin sääntelijöille kuin kansalaisillekin, joiden yksityisyyttä ja henkilötietoja ei ole täysin suojattu.

90. Edellä sanotun perusteella tietosuojavaltuutettu kehottaa komissiota valmistelemaan lainsäädäntöä, johon sisältyy vähimmäisvaatimuksena yleisesti kattava velvollisuus varmistaa yksityisyys pakollisten asetusten avulla sekä tarkkoja vaatimuksia:

a) asetusten avulla on rajoitettava käyttäjäprofiilien näkyminen ainoastaan käyttäjän omille, itse valitsemille yhteyshenkilöille; asetuksissa olisi niin ikään edellytettävä käyttäjän suostumusta ennen minkään profiilin asettamista ulkopuolisten luettavaksi;

b) luettavuudeltaan rajoitetut profiilit eivät saa olla sisäisten eivätkä ulkoisen hakupalvelujen löydettävissä.

91. Sen lisäksi, että yksityisyyttä on suojattava oletusasetusten avulla, on selvitettävä myös, ovatko täydentävät, erityiset tietosuoja- ja muut toimenpiteet aiheellisia (esimerkiksi lastensuojelun perusteella). Samalla on pohdittava laajempaa kysymystä siitä, onko tällaisille palveluille luotava erityiset puitteet, joissa säädeltäisiin yksityisyyden suojaamisvelvoitteen ohella muitakin seikkoja. Tietosuojavaltuutettu pyytää komissiota ottamaan tämän asian huomioon.

VII. **YKSITYISYYDEN SUOJAAVAT SELAIMEN OLETUSASETUKSET TAKAAVAT TIETOON PERUSTUVAN SUOSTUMUKSEN ILMOITUSTEN VASTAANOTTOON**

92. Verkkomainosten tarjoajat seuraavat evästeiden ja muiden keinojen avulla yksittäisten käyttäjien toimintaa heidän liikkuessaan Internetissä. Näin luetteloidaan heitä kiinnostavia aiheita ja rakennetaan profiileja. Näiden tietojen perusteella heille lähetetään tämän jälkeen kohdistettuja ilmoituksia ([4]).

VII.1 **Muut haasteet ja riskit nykyisen tietosuoja- ja yksityisyyslainsäädännön puitteissa**

93. Tähän tietojenkäsittelyyn sovelletaan tietosuojadirektiiviä (henkilötietojen osalta) ja sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa. Kyseisessä kohdassa nimenomaisesti edellytetään, että käyttäjälle annetaan tiedot ja oikeus reagoida joko suostumalla evästeiden tai muiden vastaavien keinojen tallentamiseen omalle tietokoneelleen tai muuhun laitteeseen tai kieltäytymällä tästä ([5]).

94. Tähän mennessä verkkomainonnan tarjoajat ovat tiedottaneet evästeistä käyttäjille ja tarjonneet näille mahdollisuuden hyväksyä tai torjua evästeet selainten asetusten ja

([1]) Tietoyhteiskunnasta ja tiedotusvälineistä vastaava Euroopan komission jäsen Viviane Reding: Ajattele ennen kuin >klik<. How to make social networking sites safer for children and teenagers? Safer Internet Day, Strasburg, 9 päivänä helmikuuta 2010.

([2]) Euroopan talous- ja sosiaalikomitean lausunto aiheesta Verkkoyhteisösivustojen vaikutus kansalaisiin/kuluttajiin, annettu 4 päivänä marraskuuta 2009.

([3]) Asiaa on selvitetty myös tämän asiakirjan kohdassa 33.

([4]) Seurantaevästeet ovat ainutlaatuisen tunnisteen sisältäviä pieniä tekstitiedostoja. Verkkomainonnan tarjoajat (sekä Internet-sivustojen operaattorit tai julkaisijat) tallentavat evästeitä tyypillisesti sivustossa kävijän kiintolevylle, varsinkin Internet-käyttäjien selaimen yhteyteen, kun käyttäjät vierailevat ensimmäistä kertaa verkostoon kuuluvilla ilmoituksia sisältävillä sivustoilla. Evästeiden avulla verkkomainonnan tarjoaja tunnistaa sivustoon palaavan vanhan kävijän tai käynnin samaan verkkoon kuuluvalla sivustolla. Toistuvien käyntien perusteella verkkomainonnan tarjoaja pystyy muodostamaan profiilin kävijästä.

([5]) Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa muutettiin hiljattain niin, että käyttäjää suojataan entistä paremmin käyttäjän viestinnän sieppaamiselta esimerkiksi käyttäjän tietokoneelle tai muuhun laitteeseen tallennettujen vakoiluohjelmistojen tai evästeiden avulla. Uudessa direktiivissä käyttäjille olisi annettava paremmat tiedot ja helpommat keinot valvoa sitä, tallennetaanko evästeitä heidän päätelaitteisiinsa.

yksityisyysperiaatteiden avulla. Ne ovat selittäneet julkaisijoiden yksityisyysperiaatteissa, miten evästeiden vastaanottamisen voi estää kokonaan tai hyväksyä niitä tapauskohtaisesti. Tällä tavoin ne ovat pyrkineet täyttämään velvollisuutensa tarjota käyttäjille oikeus kieltäytyä evästeistä.

95. Vaikka tämä menetelmä voisi teoriassa tarjota todellisen mahdollisuuden tietoon perustuvaan valintaan (selaimen kautta), todellisuus on kovin erilainen. Yleensä käyttäjiltä puuttuvat perustiedot kaikesta tiedonkeräyksestä, erityisesti ulkopuolisten toimesta, tietojen arvosta, niiden käytöstä, teknologian toiminnasta ja siitä, miten ja missä tästä kieltäydytään. Työvaiheet, joiden avulla käyttäjien on kieltäydyttävä, ovat paitsi monimutkaisia myös pitkällisiä (käyttäjän on ensin asetettava selain hyväksymään evästeet ja tämän jälkeen valittava kieltäytymisvaihtoehto).

96. Tämän seurauksena hyvin harvat käyttävät kieltäytymismahdollisuutta. Syynä ei ole se, että he olisivat tehneet tietoon perustuvan päätöksen hyväksyä verkkokäyttäytymiseen perustuvaa mainontaa, vaan pikemminkin se, etteivät he ole tajunneet, että kieltäytymisen tekemättä jättäminen on johtanut käytännössä tilanteen hyväksymiseen.

97. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädetään oikeudellisesti tarkastellen tehollisesta oikeudellisesta suojasta. Käytännössä Internet-käyttäjät joutuvat kuitenkin myöntymään siihen, että heitä seurataan ja heille lähetetään käyttäytymiseen perustuvia ilmoituksia, vaikka monet – elleivät useimmat – ovat täysin tietämättömiä tällaisesta seurannasta.

98. 29 artiklan mukainen tietosuojaryhmä valmistelee lausuntoa, jonka tarkoituksena on selventää käyttäytymiseen perustuvien ilmoitusten käyttöä koskevia oikeudellisia vaatimuksia. Tämä onkin aiheellista. Tulkinta ei kuitenkaan sellaisenaan riitä ratkaisemaan tilannetta, vaan Euroopan unionin voi olla tarpeen käydä täydentäviin toimiin.

VII.2 **Täydentävät toimet, erityisesti yksityisyyden suojaamiseksi oletusasetuksin**

99. Kuten edellä todetaan, verkkoselaimet yleensä mahdollistavat jonkinlaisen valvonnan, joka kohdistuu tietynlaisiin evästeisiin. Nykyisin useimpien verkkoselainten oletusasetuksissa hyväksytään kaikki evästeet. Tosiin sanoen selaimet on oletusarvoisesti asetettu hyväksymään kaikki evästeet näiden tarkoituksesta riippumatta. Vain silloin, kun käyttäjä muuttaa selainsovelluksensa asetuksia siten, että hän kieltäytyy evästeistä, hänen koneelleen ei tallenneta evästeitä. Harvat näin kuitenkin tekevät, kuten edellä todetaan. Selainsovelluksen ensimmäisen asennuksen tai päivityksen yhteydessä ei myöskään ole yksityisyyteen liittyvää opastettua toimintoa.

100. Edellä kuvattua ongelmaa voitaisiin helpottaa määrittämällä selaimiin oletusarvoisesti yksityisyyden suojaavat asetukset. Toisin sanoen selaimissa olisi asetuksena ”torju ulkopuolisten evästeet”. Tämän tehostamiseksi ja täydentämiseksi selainten tulisi ohjata käyttäjät ohjattuun yksityisyydensuojaustoimintoon, kun selain asennetaan tai sitä päivitetään. Evästetyypeistä ja eräiden evästeiden hyödyllisyydestä olisi hyvä tarjota eriytetympää ja selvempää tietoa. Käyttäjille, jotka haluavat, että heitä seurataan ilmoitusten lähettämistä varten, ilmoitetaan asiasta asianmukaisesti, ja heidän olisi muutettava selainasetuksiaan. Näin heidän mahdollisuutensa valvoa henkilötietojaan ja yksityisyyttään kasvaisivat. Tämä olisi tietosuojavaltuutetun näkemyksen mukaan tehokas keino kunnioittaa ja suojella käyttäjien valintaa [1].

101. Kun toisaalta otetaan huomioon ongelman laajuus eli niiden Internet-käyttäjien määrä, joita parhaillaan seurataan näennäisen suostumuksen perusteella, ja kyseessä olevan taloudellisen edun mittakaava, täydentävän suojan tarve näyttää entistä kiireellisemmältä. Sisäänrakennetun yksityisyyden suojan periaatteen sisällyttäminen verkkoselainsovelluksiin olisi huomattava parannus kansalaisten mahdollisuuksiin hallita mainostarkoituksessa noudatettavia tiedonkeräyskäytäntöjä.

102. Näistä syistä tietosuojavaltuutettu kehottaa komissiota harkitsemaan lainsäädäntötoimenpiteitä, joissa edellytetään yksityisyyden suojaamista selainten oletusasetusten avulla ja merkityksellisen tiedon tarjoamista.

VIII. **MUUT KANSALAISTEN YKSITYISYYDENSUOJAAN JA TIETOSUOJAAN TÄHTÄÄVÄT PERIAATTEET**

103. Vaikka sisäänrakennetun yksityisyyden suojan periaate tarjoaa hyvät mahdollisuudet kohentaa kansalaisten henkilötietojen ja yksityisyyden suojaa, tarvitaan sitä täydentäviä periaatteita, jotka on määriteltävä ja toteuttava laeissa. Näin varmistetaan kuluttajien luottamus tieto- ja viestintätekniikkaan. Tätä taustaa vasten tietosuojavaltuutettu ottaa esiin vastuuvelvollisuuden periaatteen ja eri toimialoilla velvoittavasti sovellettavan tietoturvaloukkauksen käsitteen.

VIII.1 **Vastuuvelvollisuusperiaatteella varmistetaan sisäänrakennetun yksityisyyden suojan periaatteen noudattaminen**

104. 29 artiklan mukaisen tietosuojatyöryhmän asiakirjassa ”Future of Privacy” [2] suositellaan vastuuvelvollisuuden periaatteen sisällyttämistä tietosuojadirektiiviin. Tämä eräissä

[1] Toisaalta tietosuojavaltuutettu myöntää, ettei tämä ratkaisisi koko ongelmaa, koska selaimen avulla ei voida valvoa kaikkia evästeitä, esimerkkinä niin sanotut flash-evästeet. Tämän takia selainten kehittäjien olisi sisällytettävä flash-evästeiden hallinta oletusarvoisesti uusiin selainversioihin.

[2] Katso 29 artiklan mukaisen tietosuojatyöryhmän lausunto 168 ”The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data”, annettu 1 päivänä joulukuuta 2009.

monikansallisissa tietosuojavälineissä ([1]) tunnustettu periaate edellyttää, että organisaatiot ottavat käyttöön prosessit, joilla ne osoittavat noudattavansa nykyisiä lakeja, ja kehittävät menetelmät, joilla arvioidaan lainsäädännön ja muiden velvoittavien välineiden noudattamista ja osoitetaan se.

105. Tietosuojavaltuutettu tukee täysin 29 artiklan mukaisen tietosuojatyöryhmän suositusta. Tietosuojavaltuutettu pitää tätä periaatetta erittäin tärkeänä tietosuojaperiaatteiden ja -velvoitteiden tehokkaan soveltamisen vahvistajana. Vastuuvelvollisuus velvoittaa rekisterinpitäjät osoittamaan, että ne ovat toteuttaneet sovellettavan tietosuojalainsäädännön edellyttämän järjestelyn. Tämä on omiaan edistämään sisäänrakennetun yksityisyyden suojan tehokasta käyttöönottoa tieto- ja viestintätekniikoiden alalla erityisen sopivana keinona osoittaa vastuuvelvollisuuden toteutuminen.

106. Vastuuvelvollisuuden mittaamiseksi ja osoittamiseksi rekisterinpitäjät voivat käyttää sisäisiä menettelyjä ja ulkoisia tahoja, jotka suorittavat auditointeja tai muunlaisia tarkistuksia ja todentamisia, joiden perusteella voidaan myöntää laatumerkintöjä tai palkintoja. Tässä yhteydessä tietosuojavaltuutettu kehottaa komissiota harkitsemaan, voitaisiinko yleisen vastuuvelvollisuusperiaatteen ohella lainsäädännössä edellyttää tiettyjä vastuuvelvollisuustoimia, esimerkiksi yksityisyydensuojan ja tietosuojan vaikutusten arviointeja, ja missä olosuhteissa tämä olisi mahdollista.

VIII.2 **Tietoturvaloukkaus: lainsäädännön täydentäminen**

107. Sähköisen viestinnän tietosuojadirektiiviin viime vuonna tehdyissä muutoksissa direktiiviin sisällytettiin vaatimus, jonka mukaan tietoturvaloukkauksista on ilmoitettava niiden kohteena oleville henkilöille sekä asianomaisille viranomaisille. Tietoturvaloukkaukseksi määritellään väljästi kaikki loukkaukset, jotka johtavat palvelun yhteydessä siirrettyjen, tallennettujen tai muulla tavoin käsiteltyjen henkilötietojen tuhoutumiseen, häviämiseen, luovutukseen tms. Ilmoitus asianmukaiselle henkilölle on pakollinen, jos tietoturvaloukkaus todennäköisesti vaikuttaa haitallisesti hänen tietosuojaansa tai yksityisyyteensä. Näin voi käydä silloin, kun loukkaus voi johtaa väärän henkilöllisyyden käyttöön, huomattavan vakavaa nöyryytystä tai maineen vahingoittumista. Kaikista tietoturvaloukkauksista on ilmoitettava toimivaltaisille viranomaisille riippumatta siitä, onko henkiöille aiheutunut riskiä vai ei.

Tietoturvaloukkausta koskevien velvoitteiden soveltaminen eri aloilla

108. Valitettavasti tämä velvoite koskee ainoastaan yleisesti saatavilla olevan sähköisen viestintäpalvelun tarjoajia, kuten puhelinyhtiöitä, Internet-liittymän tarjoajia, nettisähköpostin tarjoajia jne. Tietosuojavaltuutettu kehottaa komissiota esittämään ehdotuksia tietoturvaloukkauksen soveltamisesta eri aloille. Sääntelyn sisällön osalta tietosuojavaltuutettu katsoo, että sähköisen viestinnän tietosuojadirektiivissä omaksutuissa tietoturvaloukkauksen sääntelypuitteissa on saatu aikaan asianmukainen tasapaino yksilön oikeuksien, myös henkilötietojen ja yksityisyyden suojaa koskevien oikeuksien, ja sovellusalaan kuuluville oikeushenkilöille asetettujen velvoitteiden välillä. Toisaalta näissä puitteissa on voimaa, koska niiden perustana olevissa merkityksellisissä valvontasäännöksissä annetaan viranomaisille riittävät tutkimus- ja seuraamustenmääräämisvaltuudet niiltä osin kuin säännöksiä ei noudateta.

109. Näin ollen tietosuojavaltuutettu kehottaa komissiota hyväksymään lainsäädäntöehdotuksen, jossa tätä sääntelyä sovelletaan eri aloille, tarvittaessa asianmukaisin mukautuksin. Näin varmistettaisiin, ett samoja normeja ja menettelyjä sovelletaan kaikilla eri aloilla.

Sähköisen viestinnän tietosuojadirektiiviin sisältyvän lainsäädännön täydentäminen komiteamenettelyn avulla

110. Tarkistetussa sähköisen viestinnän tietosuojadirektiivissä annetaan komissiolle valtuudet hyväksyä teknisiä täytäntöönpanotoimenpiteitä eli tietoturvaloukkauksia koskevia yksityiskohtaisia toimenpiteitä komiteamenettelyä käyttäen ([2]). Tämä valtuutus on perusteltu, jotta tietoturvaloukkausten sääntely pannaan täytäntöön ja sitä sovelletaan yhdenmukaisesti. Johdonmukaisella täytäntöönpanolla varmistetaan osaltaan, että kaikilla yhteisön kansalaisilla on yhtä korkea suojelun taso ja ettei soveltamisalaan kuuluviin oikeushenkilöihin kohdistu erilaisista ilmoitusvaatimuksista johtuvaa taakkaa.

111. Sähköisen viestinnän tietosuojadirektiivi hyväksyttiin marraskuussa 2009. Teknisten täytäntöönpanotoimenpiteiden hyväksymisen lykkäämiseen ei näyttäisi olevan syytä. Tietosuojavaltuutettu on järjestänyt kaksi seminaaria, joiden tarkoituksena oli jakaa ja kerätä kokemuksia tietoturvaloukkausten ilmoituksista. Tietosuojavaltuutettu kertoo mielellään tässä yhteydessä saaduista tuloksista ja odottaa työskentelyä komission ja muiden sidosryhmien kanssa yleisen tietoturvaloukkauksen sääntelyn viimeistelemiseksi.

112. Tietosuojavaltuutettu kehottaa komissiota ryhtymään tarpeellisiin toimiin pikaisesti. Ennen teknisten täytäntöönpanotoimenpiteiden hyväksymistä komission on käynnistettävä laaja kuuleminen, jonka yhteydessä on kuultava myös Euroopan verkko- ja tietoturvavirastoa (ENISA) ja 29 artiklan mukaista tietosuojatyöryhmää. Lisäksi kuulemiseen on sisällytettävä muut ”merkittävät sidosryhmät”, jotta saadaan tietoa erityisesti parhaista käytettävissä olevista teknisistä ja taloudellisista täytäntöönpanokeinoista.

([1]) OECD:n vuoden 1980 suositukset ohjeiksi, jotka koskevat yksityisyyden suojaamista ja henkilötietojen liikkumista rajojen yli, sekä Madridin kansalaisyhteiskuntajulistus maailmanlaajuisesta yksityisyyttä suojelevasta järjestelmästä 3 päivänä marraskuuta 2009.

([2]) Komiteamenettelyssä hyväksytään teknisiä täytäntöönpanotoimenpiteitä komission puheenjohdolla kokoontuvassa jäsenvaltioiden edustajien komiteassa. Sähköisen viestinnän tietosuojadirektiivin yhteydessä sovelletaan niin sanottua valvonnan käsittävää sääntelymenettelyä noudattaen. Tämä tarkoittaa, että Euroopan parlamentti ja neuvosto voivat vastustaa komission ehdottamia toimenpiteitä. Katso lisätietoja osoitteesta http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **PÄÄTELMÄT**

113. Luottamus – tai pikemminkin sen puute – on todettu keskeiseksi vaikuttajaksi tieto- ja viestintätekniikan yleistymisessä ja onnistuneessa käyttöönotossa. Jolleivät kansalaiset luota tieto- ja viestintätekniikkaan, ne eivät todennäköisesti onnistu tehtävässään. Luottamus tieto- ja viestintätekniikkaan riippuu monista tekijöistä. Sillä, etteivät nämä tekniikat heikennä kansalaisten perusoikeutta yksityisyyteen ja henkilötietojen suojaamiseen, on ratkaiseva merkitys.

114. Tietoyhteiskunnassa täysin perusteltujen tietosuojan ja yksityisyyden suojan periaatteisiin perustuvan lainsäädännön vahvistamiseksi edelleen tietosuojavaltuutettu ehdottaa, että komissio sisällyttää sisäänrakennetun yksityisyyden suojan lainsäädännön ja poliittisen päätöksenteon eri tasoille.

115. Tietosuojavaltuutettu ehdottaa komissiolle seuraavaa neljää toimintalinjaa:

a) Sen olisi sisällytettävä sisäänrakennettua yksityisyyden suojaa koskeva yleinen säännös tietosuojaa koskevaan lainsäädäntöön. Säännöksen tulisi olla tekniikan kannalta neutraali, ja noudattamisen tulisi olla pakollista eri vaiheissa;

b) Tätä yleistä säännöstä olisi tarkennettava erityissäännöksissä, kun eri aloille ehdotetaan erityisiä oikeudellisia välineitä. Erityiset säännökset voitaisiin jo nyt sisällyttää säädöksiin tietosuojadirektiivin 17 artiklan (ja muun olemassa olevan lainsäädännön) nojalla;

c) Sisäänrakennettu yksityisyyden suoja olisi otettava eurooppalaiseen digitaalistrategiaan ohjaavaksi periaatteeksi;

d) Sisäänrakennettu yksityisyyden suoja olisi sisällytettävä periaatteena muihin EU:n aloitteisiin (kuin lainsäädännöllisiin aloitteisiin).

116. Kolmella erikseen nimetyllä tieto- ja viestintätekniikan alalla tietosuojavaltuutettu suosittelee, että komissio arvioi tarvetta antaa ehdotuksia sisäänrakennetun yksityisyyden suojan periaatteen täytäntöönpanosta erityisin keinoin:

a) Radiotaajuustunnistuksen yhteydessä olisi ehdotettava lainsäädäntötoimenpiteitä, joilla säädellään radiotaajuustunnistuksen käyttöön liittyviä keskeisiä kysymyksiä, mikäli nykyisen lainsäädännön täytäntöönpano itsevalvonnan avulla epäonnistuu. Erityisesti olisi tarjottava myyntipisteessä mahdollista kieltäytymisvaihtoehtoa, jonka mukaan kaikki kuluttajatuotteisiin liitetyt radiotaajuustunnisteet deaktivoidaan oletusarvoisesti myyntipisteessä.

b) Sosiaalisten verkkoyhteisöjen osalta olisi valmisteltava lainsäädäntöä, johon sisältyisi vähimmäisvaatimuksena yleisesti kattava velvollisuus varmistaa yksityisyys pakollisten asetusten avulla sekä yksityiskohtaisempia vaatimuksia käyttäjäprofiilien näkymisen rajoittamisesta yksinomaan käyttäjien omille, itse valitsemille yhteyshenkilöille ja näkyvyydeltään rajoitettujen profiilien suojaaminen näkymiseltä sisäisissä tai ulkoisissa hakupalveluissa;

c) Kohdennetun mainonnan osalta olisi harkittava lainsäädäntöä, jonka mukaan selainasetuksilla estettäisiin oletusarvoisesti ulkopuolisten tahojen evästeet ja käynnistettäisiin käyttäjien ohjattu yksityisyydensuojaustoiminto selainta ensimmäisen kerran asennettaessa tai päivitettäessä.

117. Lopuksi tietosuojavaltuutettu ehdottaa, että komissio:

a) harkitsee vastuuvelvollisuusperiaatteen täytäntöönpanoa nykyisessä tietosuojadirektiivissä ja

b) kehittää sääntö- ja menettelykokonaisuuden, jolla pannaan täytäntöön sähköisen viestinnän tietosuojadirektiiviin sisältyvät, tietoturvaloukkauksen ilmoittamista koskevat säännökset ja laajennetaan sääntöjen soveltaminen kattamaan yleisesti kaikki rekisterinpitäjät.

Tehty Brysselissä 18 päivänä maaliskuuta 2010.

Peter HUSTINX

Euroopan tietosuojavaltuutettu