I

(Päätöslauselmat, suositukset ja lausunnot)

LAUSUNNOT

EUROOPAN TIETOSUOJAVALTUUTETTU

Euroopan tietosuojavaltuutetun lausunto komission tiedonannosta Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle ”Radiotaajuustunnistus Euroopassa: Asteittain kohti alan yhteisiä periaatteita” (KOM(2007) 96)

(2008/C 101/01)

EUROOPAN TIETOSUOJAVALTUUTETTU, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen ja erityisesti sen 286 artiklan,

ottaa huomioon Euroopan unionin perusoikeuskirjan ja erityisesti sen 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,

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

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 ja erityisesti sen 41 artiklan,

ON ANTANUT SEURAAVAN LAUSUNNON:

I **JOHDANTO**

1. Komissio antoi 15. maaliskuuta 2007 tiedonannon ”Radiotaajuustunnistus Euroopassa: asteittain kohti alan yhteisiä periaatteita” ([1]) (jäljempänä ’tiedonanto’). Asetuksessa (EY) N:o 45/2001 olevan 41 artiklan mukaan Euroopan tietosuojavaltuutetun tehtävänä on antaa ohjeita yhteisöjen toimielimille ja elimille kaikista henkilötietojen käsittelyä koskevista seikoista. Euroopan tietosuojavaltuutettu esittää tämän lausunnon kyseisen artiklan nojalla.

2. Tämä lausunto on Euroopan tietosuojavaltuutetun kanta tiedonantoon sekä muihin radiotaajuustunnistuksen (RFID) alalla tiedonannon antamisen jälkeen toteutettuihin toimiin. Näihin muihin asiaankuuluviin toimiin, jotka on otettu huomioon tässä lausunnossa, sisältyvät:

— Radiotaajuustunnistuksen (RFID) asiantuntijaryhmän perustamisesta 28 päivänä kesäkuuta 2007 tehty komission päätös ([2]), joka on suora seuraus tiedonannosta. Tämä ryhmä tunnetaan myös nimellä RFID-työryhmä. Päätöksen 4 artiklan 4 kohdan b alakohdan mukaisesti Euroopan tietosuojavaltuutettu osallistuu ryhmän toimintaan tarkkailijana.

— Euroopan turvallisen tietoyhteiskunnan strategiasta 22 päivänä maaliskuuta 2007 annettu neuvoston päätöslauselma ([3]).

— Euroopan parlamentin käynnistämä hanke ”RFID and identity management” ([4]).

([1]) KOM(2007) 96 lopullinen.
([2]) Päätös N:o 467/2007/EY (EUVL L 176, 6.7.2007, s. 25).
([3]) EUVL C 68, 24.3.2007, s. 1.
([4]) Hanke ”RFID and identity management — Case studies from the frontline of the development towards ambient intelligence”, jonka on antanut tehtäväksi Euroopan parlamentin tieteellisten ja teknisten vaihtoehtojen arviointiyksikkö (STOA) ja jonka toteuttaa Euroopan teknologian arviointiryhmä ETAG (European Technology Assessment Group)
http://www.europarl.europa.eu/stoa/default_en.htm

— Henkilötietojen käsitteestä kesäkuussa 2007 annettu 29 artiklan mukaisen tietosuojatyöryhmän lausunto N:o 4/2007 ([1]).

— Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojadirektiivin tehokkaampaa täytäntöönpanoa koskevan työohjelman seurannasta ([2]) sekä Euroopan tietosuojavaltuutetun 25. heinäkuuta 2007 antama lausunto tästä tiedonannosta ([3]).

— Komission antama ehdotus direktiiviksi (muun muassa) henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY muuttamisesta ([4]).

3. Euroopan tietosuojavaltuutettu on tyytyväinen RFID:tä koskevaan komission tiedonantoon, koska siinä käsitellään tärkeimpiä RFID-teknologian käyttämiseen liittyviä kysymyksiä unohtamatta yksityisyyden suojaa ja tietosuojaa koskevia ratkaisevia kysymyksiä. Tämä tiedonanto perustuu johdonmukaiseen ja perusteelliseen valmisteluun. Tiedonantoa ovat edeltäneet viisi aihekohtaista asiantuntijaseminaaria sekä komission järjestämä julkinen Internet-kuuleminen ([5]).

4. Euroopan tietosuojavaltuutettu on samaa mieltä näkemyksestä, että RFID-järjestelmillä voi olla keskeinen rooli tietoyhteiskunnan kehitysvaiheessa, jota tavallisesti kutsutaan ”tavaroiden internetiksi” ja hän on myös täysin samaa mieltä tiedonannon 3.2 -kohdassa mainituista huolista siitä, että RFID-järjestelmät voivat olla uhka yksilön yksityisyyden suojalle ja tietosuojaoikeuksille. Euroopan tietosuojavaltuutettu totesikin vuotta 2005 koskevassa kertomuksessaan, että RFID yhdessä biometriikan, toimintaympäristöön sulautetun tietotekniikan ja henkilöllisyyden tunnistamisjärjestelmien kanssa on teknologiaa, jolla odotetaan olevan merkittävä vaikutus tietosuojaan.

5. Euroopan tietosuojavaltuutetun mielestä RFID-tekniikoiden yleistyminen ja niiden laaja hyväksyminen saavutetaan niiden houkuttelevalla käytettävyydellä tai niiden tarjoamilla uusilla palveluilla, ja yleistymistä ja hyväksymistä helpottavat hyvin suunniteltujen ja yhdenmukaisten tietosuojatakeiden tarjoamat edut.

6. Lyhyesti voidaan todeta, että Euroopan tietosuojavaltuutettu pitää RFID:tä perustavasti uutena teknisenä kehityksenä, joka perustellusti mainitaan komission tiedonannossa tienä tietoyhteiskunnan uuteen kehitysvaiheeseen.

7. Tämä kehitys herättää tärkeitä kysymyksiä eri aloilla, kuten tietosuojan ja yksityisyyden suojan alalla. Tässä Euroopan tietosuojavaltuutetun lausunnossa rajoitutaan käsittelemään tätä alaa.

II **LAUSUNNON AIHEPIIRI**

8. Tässä lausunnossa keskitytään erityisesti niihin mahdollisiin vaikutuksiin, joita tällä kehityksellä on tietosuojaan ja yksityisyyden suojaan. Näistä vaikutuksista ei ole tällä hetkellä varmuutta, mikä johtuu myös siitä, että RFID-järjestelmien kehitys ja niiden yleistyminen etenevät nopeasti ja ei ole lainkaan selvää, mihin tämä kehitys johtaa.

9. Näin ollen Euroopan tietosuojavaltuutettu on noudattanut seuraavaa lähestymistapaa:

— Ensinnäkin on tarpeen selvittää käytännön vaikutukset, joita RFID-järjestelmien käytöllä on tietosuojaan ja yksityisyyden suojaan.

— Toiseksi on tarpeen määrittää nämä vaikutukset tarkemmin tietosuojaa ja yksityisyyden suojaa koskevassa nykyisessä lainsäädännössä.

— Kolmanneksi Euroopan tietosuojavaltuutettu tarkastelee, edellyttävätkö nämä vaikutukset täsmällisempiä sääntöjä RFID-tekniikoiden käytön herättämien tietosuojakysymysten ratkaisemiseksi. Euroopan tietosuojavaltuutettu toi tämän asian esiin jo lausunnossaan tietosuojadirektiiviä koskevasta tiedonannosta, ja sitä käsitellään tarkemmin tässä lausunnossa.

10. Euroopan tietosuojavaltuutettu pyrkii tällä lähestymistavalla edistämään sitä, että RFID-järjestelmien kehityksessä ja niiden yleistymisessä otetaan huomioon perustellut tietosuojaan ja yksityisyyden suojaan liittyvät huolenaiheet.

III **VAIKUTUKSET**

RFID-järjestelmät ja -tunnisteet

11. Vaikka siis kehitys on vielä kesken ja tuloksista ei ole varmuutta, on aivan mahdollista kuvata tämän kehityksen tärkeimpiä piirteitä siltä osin, mitä vaikutuksia niillä on tietosuojaan.

([1]) Asiakirja WP 136, julkaistu työryhmän Internet-sivustolla.
([2]) Komission tiedonanto 7 päivältä maaliskuuta 2007 Euroopan parlamentille ja neuvostolle tietosuojadirektiivin tehokkaampaa täytäntöönpanoa koskevan työohjelman seurannasta, KOM(2007) 87 lopullinen.
([3]) EUVL C 255, 27.10.2007, s. 1. Jäljempänä: ’lausunto tietosuojadirektiiviä koskevasta tiedonannosta’.
([4]) Marraskuun 13 päivänä 2007 annettu ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12. heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ja kuluttajansuojaa koskevasta yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta, KOM(2007) 698 lopullinen. Direktiivistä 2002/58/EY käytetään nimitystä ”sähköisen viestinnän tietosuojadirektiivi”.
([5]) http://www.rfidconsultation.eu/

12. Arvioitaessa RFID-teknologian mahdollisia tietosuojaan ja yksityisyyden suojaan liittyviä näkökohtia on erittäin tärkeää ottaa RFID-tunnisteiden lisäksi huomioon myös yleinen RFID-infrastruktuuri: tunniste, lukulaite, verkko, viitetietokanta sekä tietokanta, johon tunnisteen ja lukulaitteen yhteistoiminnan tuottamat tiedot tallennetaan. Kuten tiedonannon johdannossa lyhyesti korostetaan, radiotaajuustunnisteet eivät ole pelkästään ”elektronisia tunnuksia”, joten tietosuojakysymykset eivät rajoitu pelkästään tunnisteisiin, vaan liittyvät koko RFID-infrastruktuurin kaikkiin osiin. Kukin näistä tekijöistä on siis merkittävä edistettäessä sitä, että eurooppalainen tietosuojalainsäädäntö pannaan täytäntöön tarvittaessa. Niiden kehitystä vauhdittavat kehittyvän tietoyhteiskunnan tärkeimmät suuntaukset, kuten lähes rajaton kaistanleveys, kaikkialle ulottuvat verkkoyhteydet ja ääretön tallennuskapasiteetti.

RFID-järjestelmien ja -tunnisteiden vaikutus

13. Vaikka tarvitaan laajempaa lähestymistapaa kuten edellisessä kohdassa korostettiin, useista syistä on perusteltua keskittyä ensin RFID:n käyttöön kuluttajatuotteiden merkitsemisessä tunnistein esimerkiksi vähittäiskaupassa. Ilmeinen syy on sen ennustettu lisääntyvä käyttö, mikä näyttää olevan johtamassa sen laajaan soveltamiseen. Toisin kuin muilla RFID-sovelluksilla, joiden käyttö on kapea-alaista tai rajoitettua, tuotteiden merkitsemisestä tunnistein voi tulla massamarkkinasovellus. Jo nyt monet kuluttajatuotteet on varustettu RFID-tunnisteella. Tähän liittyy se, että tällaisella käytöllä on vaikutus valtavaan määrään henkilöitä, joiden henkilötiedot todennäköisesti käsitellään joka kerta heidän hankkiessaan tuotteen, johon on sisällytetty RFID-tunniste.

14. Erityistä huomiota olisi kiinnitettävä niihin seurauksiin, joita RFID-merkinnöillä on tuotteiden omistajien kannalta. RFID-järjestelmät saattavat vääristää tuotteen ja sen omistajan välisen suhteen: omistaja voidaan skannata ja luokitella ”pienen budjetin” kuluttajaksi tai ”houkuttelevaksi kohteeksi” tulevaa kaupankäyntiä silmällä pitäen, ja liian pitkälle viety yksi yhteen -ajattelu ([1]) saattaa johtaa automaattiseen tietynlaisesta käyttäytymisestä ”rankaisemiseen” (kierrätysvelvollisuus, jätehuolto jne.). Kukaan ei saisi olla epäedullisten automaattisten päätösten kohteena. Tämä RFID:n ominaisuus lisää sen riskiä, että tietoyhteiskunnassa siirrytään tilanteeseen, jossa tehdään automaattisia päätöksiä ja teknologiaa käytetään väärin ihmisten käyttäytymisen säätelemiseksi.

15. RFID-tunnisteeseen tallennetut tai sen tuottamat tiedot voivat olla henkilötietoja sellaisina kuin ne määritellään tietosuojadirektiivin 2 artiklassa. Esimerkiksi matkustamisessa käytetyt älykortit voivat sisältää tunnistustietoja sekä tietoja haltijan äskettäisistä matkoista. Jos joku vilpillisessä mielessä toimiva haluaa seurata muita henkilöitä, hänen tarvitsee vain sijoittaa strategisille paikoille lukijoita, jotka tuottavat tietoja kortinhaltijoiden liikkumisesta, mikä loukkaa heidän oikeuttaan yksityisyyden ja henkilötietojen suojaan.

16. Yksityisyyden suojalle voi aiheutua vastaavia uhkia, vaikka RDIF-tunnisteeseen tallennetut tiedot eivät sisältäisikään henkilöiden nimiä. RFID-tunnisteet sisältävät kuluttajatuotteisiin kiinnitetyt yksilölliset tunnukset: jos kullakin RFID-tunnisteella on yksilöllinen tunnus, tällaista tunnistamista voidaan käyttää valvontatarkoituksiin. Jos joku esimerkiksi käyttää rannekelloa, jossa on tunnusnumeron sisältävä RFID-tunniste, se voi myös toimia kellon omistajan yksilöllisenä tunnisteena, vaikka hänen henkilöllisyytensä ei olisikaan tiedossa. Riippuen siitä, miten tietoja käytetään ja miten ne suhteutetaan kelloon tai omistajaan, direktiiviä sovellettaisiin tai oltaisiin soveltamatta. Sitä sovellettaisiin esimerkiksi, jos henkilöiden liikkumisesta tuotetaan tietoja, joita käytettäisiin todennäköisesti heidän käyttäytymisensä seurantaan, tai esimerkiksi hintojen eriyttämiseen, pääsyn epäämiseen tai ei-toivottuun julkisuudelle altistamiseen.

17. Tässä yhteydessä on tarpeen varmistaa, että RFID-sovelluksia käytettäessä toteutetaan tarvittavat teknologiset toimenpiteet, jotta minimoidaan tietojen ei-toivotun paljastumisen riski. Tällaisiin toimenpiteisiin voi sisältyä vaatimus suunnitella RFID-infrastruktuuri ja erityisesti RFID-tunnisteet siten, että tällainen seuraus vältetään. RFID-tunnisteiden käytön yhteydessä voidaan esimerkiksi antaa ”tappokäsky”, jolla tunnisteet deaktivoidaan. Tätä mahdollisuutta käsitellään tarkemmin tämän lausunnon IV luvussa.

18. Koska RFID-järjestelmät antavat mahdollisuuden tuotteiden jäljittämiseen myyntipaikan jälkeen, ne herättävät uusia kysymyksiä yksityisyyden suojaa koskevassa keskustelussa. Niiden vaikutuksen analysoimisessa onkin otettava huomioon kaksi seikkaa: se, miten henkilökohtaisena tuotetta pidetään, sekä tuotteen liikkuvuus ([2]).

19. Tuotteen elinkaaren huomioon ottaminen saattaa myös täydentää vaadittavaa riskianalyysia ja helpottaa yksityisyyden suojaa koskevien mahdollisten uhkien määrällistä arviointia. Koska tunnistetta ei kenties deaktivoida, pitkän elinkaaren omaava loppukäyttäjälle tarkoitettu tuote pystyy keräämään tuotteen omistajasta asiaankuuluvampaa tietoa ja muodostamaan hänestä täsmällisemmän profiilin. Toisaalta esimerkiksi virvoitusjuomatölkin lyhyt elinkaari valmistuksesta kierrätykseen saattaa aiheuttaa vähemmän riskejä ja näin ollen edellyttää kevyempiä toimenpiteitä kuin paljon pidemmän elinkaaren omaava tuote.

([1]) Tohtori Sarah Spiekermann, Internetin taloutta tutkivan Berliinissä toimivan tutkimuskeskuksen (Berlin Research Centre on Internet Economics) johtaja, transatlanttisen kuluttajavuoropuhelufoorumin (the Trans Atlantic Consumer Dialogue) järjestämä RFID:tä ja sulautettua tietotekniikkaa käsitellyt seminaari, 13. maaliskuuta 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman ja Norman G. Einspruch: Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volume 9, No 2/2007.

RFID-järjestelmän käyttöön liittyvät yksityisyyden suojaa ja tietosuojaa koskevat kysymykset

20. Jotta selvennettäisiin RFID-järjestelmien vaikutukset yksityisyyden suojaan ja tietosuojaan, on erotettava viisi perustavaa yksityisyyteen ja turvallisuuteen liittyvää kysymystä.

21. Ensimmäinen näistä kysymyksistä on rekisteröidyn tunnistaminen. Yli 60 vuotta sitten RFID-tunnisteen tarkoituksena oli omien ja vihollisten tunnistaminen. Tänä päivänä RFID-järjestelmät voivat paitsi tunnistaa kohteen yleiset ominaisuudet myös viime kädessä johtaa yksilön tunnistamiseen, joten niiden on tehtävä se tietosuojaa kunnioittaen.

22. Toinen näistä kysymyksistä on rekisterinpitäjän (-pitäjien) tunnistaminen. RFID-järjestelmien ollessa kyseessä rekisterinpitäjän, sellaisena kuin se määritellään tietosuojadirektiivin 2 artiklan d kohdassa, tunnistaminen saattaa olla vaikeampaa ja edellyttää näin ollen lähempää tarkastelua. Rekisterinpitäjän tunnistaminen on kuitenkin ratkaisevan tärkeä vaihe määritettäessä kaikkien niiden asiaankuuluvien toimijoiden vastuu, joiden on noudatettava tietosuojalainsäädäntöä. Tietoja käsittelevä rekisterinpitäjä voi tunnisteen elinkaaren aikana vaihtua useaan kertaan niiden lisäpalvelujen mukaan, joita voidaan tarjota tunnisteella varustetun tuotteen osalta.

23. Kolmas kysymys on yksityisen ja julkisen välillä perinteisesti tehdyn eron vähentynyt merkitys. Vaikka ero yksityisen ja julkisen välillä ei ole aina aiemminkaan ollut täysin selvä, useimmat ihmiset ovat tietoisia niiden välisestä rajasta (ja harmaasta vyöhykkeestä) ja tekevät tietoon perustuvia tai intuitiivisia päätöksiä siitä, miten toimia tilanteen mukaan. Hallin ([1]) mukaan yksityisyyden alue ilmenee tavallisesti fyysisenä etäisyytenä muista. Yksityisyyden hallintaa voidaan pitää myös dynaamisena rajojensäätelyprosessina ([2]). Näin ollen ei ole yllättävää, että tunnisteiden avulla tapahtuvan viestinnän langattomuus ja kyky lukea tietoja ilman näköyhteyttä hämärtävät nämä perinteiset rajat ja niiden hallinnan ja herättävät yksityisyyteen liittyviä huolia. On olemassa pelko siitä, että yksilö voi menettää tähän saakka nauttimansa etäisyydensäätelyn hallinnan osittain tai kokonaan. Näin ollen RFID-järjestelmien ensimmäisten toteutusten lukuetäisyys oli sekä niiden kannattajien että niiden vastustajien arvostelun kohteena.

24. Neljäs kysymys koskee RFID-tunnisteiden kokoa ja fyysisiä ominaisuuksia. Koska tunnisteen on oltava ennen kaikkea pieni ja hinnaltaan edullinen, ovat ne turvatoimet, joita voitaisiin käyttää RFID-järjestelmän tässä osassa, näin ollen rajoitetut. Kyseisen viestinnän langattomuus lisää kuitenkin myös riskejä verrattuna langalliseen viestintään, minkä vuoksi tarvitaan täydentäviä turvallisuusvaatimuksia.

25. Viides kysymys on avoimuuden puute tietojenkäsittelyssä. RFID-järjestelmät voivat johtaa sellaisten tietojen huomaamattomaan keräämiseen ja käsittelyyn, joita voidaan käyttää tietyn henkilön profilointiin. Tässä tehdään usein vertaus matkapuhelinviestintään, joka sai erittäin laajan teknologisen hyväksynnän huolimatta siihen liittyvistä mahdollisista yksityisyyden loukkaamisen riskeistä. Voitaisiin päätellä, että RFID tullaan hyväksymään samalla tavalla. Toisaalta on korostettava, että matkapuhelin on konkreettinen esine, jota loppukäyttäjä voi hallita, sillä se voidaan sulkea, toisin kuin RFID.

26. Vaikka edellä mainittu tietojen huomaamaton kerääminen ja käsittely saattaa olla laillista, on myös mahdollista ja useissa tilanteissa jopa hyvin todennäköistä, että tällaisia tietoja kerätään ja käsitellään laittomasti.

27. Tässä luvussa esitettyjen selvitysten perusteella voidaan tehdä johtopäätös, että RFID-teknologian laaja käyttö on perustavalla tavalla uusi ilmiö, jolla saattaa olla merkittävä vaikutus yhteiskuntaamme ja perusoikeuksien kuten yksityisyyden suojan ja tietosuojan varmistamiseen yhteiskunnassamme. RFID voi merkitä laadullista muutosta.

IV SEURAUKSET

Johdanto

28. Tässä luvussa keskitytään pääasiassa RFID:n vaikutuksiin yhteiskuntamme perusoikeuksien suojeluun, esimerkiksi yksityisyyden suojaan ja tietosuojan. Tämä esitetään kahdessa vaiheessa. Ensiksi annetaan lyhyt kuvaus siitä, miten näitä perusoikeuksia suojellaan nykyisessä lainsäädännössä. Toiseksi Euroopan tietosuojavaltuutettu kartoittaa mahdollisuudet hyödyntää nykyistä lainsäädäntöä täysipainoisesti. Tämä pyrkimys on tietosuojadirektiivistä annettua tiedonantoa koskevan lausunnon mukaan ”direktiivin nykyisten säännösten täytäntöönpano kaikilta osin.”

29. Lähtökohta on, että uuden teknologian kehitys, esimerkiksi RFID-järjestelmät, vaikuttaa selkeästi tehokasta tietosuojalainsäädäntöä koskeviin vaatimuksiin. Yksilön henkilötietojen tehokas suoja voi myös asettaa rajoituksia uuden teknologian käytölle. Vuorovaikutus on näin ollen kaksipuolista: uusi teknologia vaikuttaa lainsäädäntöön, joka vuorostaan vaikuttaa teknologiaan ([3]).

([1]) Hall, E.T.1966. The Hidden Dimension. (1. laitos). Garden City, N.Y: Doubleday.

([2]) Altman, I. 1975. The Environment and Social Behaviour, Brooks/Cole Monterrey.

([3]) Ks. Euroopan tietosuojavaltuutetun maaliskuussa 2006 esittämät huomautukset eurooppalaisia tietokantoja koskevasta komission tiedonannosta, julkaistu Euroopan tietosuojavaltuutetun Internet-sivustolla.

Perusoikeuksien suojelu

30. Yksityisyyttä ja tietosuojaa koskevien perusoikeuksien suojelu Euroopan unionissa on ensi sijassa taattu lainsäädännöllä, jolla toteutetaan oikeudet, jotka on tunnustettu ihmisoikeuksien ja perusvapauksien suojaamista koskevan Euroopan yleissopimuksen 8 artiklassa sekä Euroopan unionin perusoikeuskirjan 7 ja 8 artiklassa. Tietosuojaa ja RFID:tä koskeva lainsäädäntö käsittää pääasiassa tietosuojadirektiivin 95/46/EY sekä sähköisen viestinnän tietosuojadirektiivin 2002/58/EY ([1]).

31. Direktiivissä 95/46/EY annettua yleistä tietosuojalainsäädäntöä sovelletaan RFID:en siltä osin, kuin RFID-järjestelmissä käsitellyt tiedot kuuluvat henkilötietojen määritelmän piiriin. Vaikka tietyissä tapauksissa RFID-sovelluksissa selvästi käsitellään henkilötietoja ja ne epäilemättä kuuluvat tietosuojadirektiivin soveltamisalaan, on myös sovelluksia, joissa tietosuojadirektiivin sovellettavuus ei ole ehkä niin ilmeistä. 29 artiklan mukaisen tietosuojatyöryhmän lausunnossa nro 4/2007 henkilötietojen käsitteestä pyritään esittämään selkeämpi ja yleisesti hyväksytty tulkinta henkilötietojen käsitteestä ja siten vähentämään siihen liittyvää epävarmuutta ([2]).

32. Sähköisen viestinnän tietosuojadirektiivin osalta tilanne on seuraava: Tähän mennessä ei ole selvinnyt, sovelletaanko tätä direktiiviä RFID-sovelluksiin. Tämän vuoksi direktiivin muuttamista koskevaan 13. marraskuuta 2007 annettuun komission ehdotukseen on sisällytetty säännös, jolla pyritään täsmentämään, että direktiiviä todella sovelletaan tiettyihin RFID-sovelluksiin. Muut RFID-sovellukset eivät kuitenkaan välttämättä kuulu sen soveltamisalaan, koska direktiivi on rajoitettu henkilötietojen käsittelyyn yleisissä viestintäverkoissa yleisesti saatavilla olevissa sähköisen viestinnän palveluissa.

33. Henkilötietojen suojaa voidaan täydentää erilaisilla (lainsäädäntöön kuulumattomilla) itsesääntelyvälineillä. Niiden käyttöä edistetään aktiivisesti molemmissa direktiiveissä, erityisesti tietosuojadirektiivin 27 artiklassa, jonka mukaan jäsenvaltioiden ja komission on edistettävä sellaisten käytännesääntöjen laatimista, joiden tarkoituksena on direktiivin moitteeton soveltaminen. Lisäksi itsesääntelyvälineillä voidaan tehokkaasti edistää tietosuojadirektiivin 17 artiklassa ja sähköisen viestinnän tietosuojadirektiivin 14 artiklassa mainittuja turvatoimia.

Nykyisen lainsäädännön täysi täytäntöönpano

34. Lausunnossa tietosuojadirektiiviä koskevasta tiedonannosta luetellaan muutamia välineitä, jotka ovat käytettävissä direktiivin täytäntöönpanon parantamiseksi. Useimmat lausunnossa esitetyistä ei-sitovista välineistä ovat merkityksellisiä RFID:n kannalta, esimerkiksi selittävät tiedonannot tai muut ilmoitukset, parhaiden käytäntöjen edistäminen, yksityisyyden suojaa koskevien tunnusten käyttö sekä yksityisyyden suojaa koskevat kolmansien osapuolten tarkastukset. Luvussa V käsitellään mahdollisuutta antaa RFID:tä koskevia erityissääntöjä. Tosin parannukset ovat mahdollisia myös nykyisen lainsäädännön puitteissa.

Itsesääntelyvälineet

35. Euroopan tietosuojavaltuutettu on yhtä mieltä komission kanssa siitä, että ensimmäisessä vaiheessa on asianmukaista antaa tilaa itsesääntelylle, jonka ansiosta sidosryhmät voivat nopeasti luoda oikeudelliset vaatimukset täyttävän toimintaympäristön edistäen näin turvallisemman oikeudellisen ympäristön luomista.

36. Komission odotetaan edistävän ja ohjaavan tätä itsesääntelyprosessia kuullen RFID- työryhmää. Tältä osin Euroopan tietosuojavaltuutettu suhtautuu myönteisesti tiedonannossa mainittuun suositukseen antaa erityisiä ohjeita ”periaatteista, joita viranomaisten ja muiden sidosryhmien olisi noudatettava RFID:n käytön osalta”.

37. Tiedonannon mukaan itsesääntely toteutettaisiin käytännesääntöjen tai parhaiden käytäntöjen muodossa. Euroopan tietosuojavaltuutetun mukaan riippumatta siitä, missä muodossa itsesääntely toteutetaan, sen pitäisi

— tarjota konkreettista ja käytännön ohjausta RFID-sovellusten erityistyypeistä ja siten edistää tietosuojalainsäädännön noudattamista,

— käsitellä erityisiä tietosuojakysymyksiä ja -ongelmia, jotka tulevat esiin yleisten RFID-sovellusten yhteydessä,

— edistää tietosuojadirektiivin yhtenäistä ja yhdenmukaista soveltamista koko EU:ssa juuri alalla, jolla todennäköisesti käytetään samantyyppisiä RFID-sovelluksia koko EU:ssa,

— olla kaikkien asiaankuuluvien sidosryhmien soveltama. Soveltamatta jättämisellä tulisi olla kielteisiä (mahdollisesti taloudellisia) seuraamuksia.

([1]) Tämän lausunnon kohdassa 59 käsitellään kolmannen direktiivin eli radio- ja telepäätelaitteista ja niiden vaatimustenmukaisuuden vastavuoroisesta tunnustamisesta 9 päivänä maaliskuuta 1999 annetun Euroopan parlamentin ja neuvoston direktiivin 1999/5/EY merkityksellisyyttä (EYVL L 91, 7.4.1999, s. 10).

([2]) Ks. muun muassa lausunnon s. 10, josta on lainaus alaviitteessä 5.

38. Euroopan tietosuojavaltuutettu tähdentää yhtä kysymystä, jossa itsesääntely olisi erityisen hyödyllistä. Niiden RFID-sovellusten osalta, joihin liittyy henkilötietojen käsittelyä, tietosuojadirektiivi asettaa rekisterinpitäjille useita velvoitteita, erityisesti 17 artiklan (käsittelyn turvallisuus) ja 7 artiklan (tietojenkäsittely tarpeen ainoastaan asianmukaisin oikeudellisin perustein) mukaisesti. Näiden säännösten nojalla rekisterinpitäjien on toteutettava toimenpiteitä tietojen luvattoman luovuttamisen estämiseksi. Rekisterinpitäjien on toisaalta varmistettava, että tietojen käsittely, esimerkiksi tietojen julkistaminen lukulaitteiden avulla, tapahtuu tarpeen mukaan ainoastaan sen yksilön, johon tiedot viittaavat, antamalla tietoisella suostumuksella.

39. Näiden tietosuojadirektiivin säännösten voidaan tulkita edellyttävän sitä, että RFID-sovelluksissa on tarvittavat tekniset ratkaisut, jotta riski tietojen ei-toivotusta luovuttamisesta estettäisiin tai saataisiin mahdollisimman pieneksi ja varmistettaisiin, että tietojen käsittely tai siirto tapahtuu tarpeen mukaan ainoastaan tietoisella suostumuksella. Euroopan tietosuojavaltuutetun mielestä kyseisen velvoitteen olemassaolo (eli tarvittavien teknisten ratkaisujen soveltaminen tietojen ei-toivotun luovuttamisen riskin estämiseksi tai saattamiseksi mahdollisimman pieneksi) ja sen RFID-sovellusten käyttäjiä sitova luonne olisi vielä voimakkaampi ja selkeämpi, jos vaatimus sisällytettäisiin edellä mainittuihin tuleviin käytännesääntöihin ja parhaisiin käytäntöihin. Tämän vuoksi Euroopan tietosuojavaltuutettu kehottaa painokkaasti, että komission suositukseen sisällytettäisiin kyseinen tulkinta tietosuojadirektiivistä, ja korostaa velvoitetta, jonka mukaan RFID-sovelluksissa olisi käytettävä tarvittavia teknisiä toimenpiteitä tietojen ei-toivotun hankkimisen tai luovuttamisen estämiseksi.

Ohjauksen tarve

40. Euroopan tietosuojavaltuutettu suosittelee, että komissio laatii tiiviissä yhteistyössä RFID-asiantuntijaryhmän kanssa yhden tai useamman asiakirjan, jossa annetaan selkeää ohjausta siitä, miten nykyistä lainsäädäntöä sovelletaan RFID-ympäristöön. Ohjauksessa olisi esitettävä, miten tietosuojadirektiivissä ja sähköisen viestinnän tietosuojadirektiivissä vahvistettuja periaatteita noudatetaan käytännössä. Euroopan tietosuojavaltuutettu esittää seuraavat ehdotukset ohjauksen yleisestä lähestymistavasta ja sen konkreettisesta sisällöstä.

41. Ohjauksen RFID:n käyttöön sovellettavista periaatteista tulisi olla riittävän kohdennettu ja noudatettava alakohtaista lähestymistapaa. Yleisluonteinen lähestymistapa ei riitä varmistamaan selkeitä ja yhdenmukaisia puitteita. Ohjauksen soveltamisala onkin rajoitettava tarkasti määriteltyihin RFID:n alakohtaisiin sovelluksiin.

42. Lisäksi suuntaviivoissa olisi ehdotettava käytännöllisiä ja tehokkaita menetelmiä tekniikoiden ja standardien kehittämiseksi. Näillä edistettäisiin sitä, että RFID-järjestelmissä noudatetaan tietosuojalainsäädäntöä, ja niihin sisältyisi ”sisäänrakennetun yksityisyyden suojan” teknologian käyttö.

43. Sovellettaessa nykyistä lainsäädäntöä RFID-ympäristöön on erityisesti kiinnitettävä huomiota RFID-sovellusten rekisterinpitäjiin sovellettavien tietosuojaperiaatteiden ja -velvoitteiden soveltamiseen. Seuraavat velvoitteet ja periaatteet ovat erityisen tärkeitä:

— Tiedonsaannin oikeutta koskeva periaate, mukaan lukien oikeus saada tietää, milloin tietoja haetaan lukulaitteilla, ja asiaankuuluvissa tapauksissa, että tuotteet on varustettu tunnisteilla.

— Suostumuksen käsite yhtenä tiedonkäsittelyn oikeudellisista perusteista. Tämä käsite toteutuu velvoitteessa deaktivoida RFID-tunnisteet myyntipisteessä, ellei rekisteröity ole antanut suostumustaan ([1]). Oikeus RFID-tunnisteiden deaktivointiin täyttää myös tietojen turvallisuuden varmistamisen vaatimuksen eli sillä varmistetaan, että RFID-tunnisteiden avulla käsiteltyjä tietoja ei luovuteta ei-toivotuille kolmansille osapuolille.

— Oikeus olla joutumatta sellaisten kielteisten päätösten kohteeksi, jotka perustuvat yksinomaan määritellyn henkilöprofiilin automaattiseen käsittelyyn.

44. Siltä osin kuin on kyse oikeudesta tiedonsaantiin, ohjauksella olisi varmistettava, että yksilöille toimitetaan tietoja heidän henkilötietojensa käsittelystä. Ennen kaikkea heidän olisi saatava varoitus muun muassa i) lukulaitteiden käytöstä ja aktivoitujen RFID-tunnisteiden käytöstä tuotteissa tai niiden pakkauksissa, ii) tämän seurauksista tiedonkeruun kannalta ja iii) kerättyjen tietojen käyttötarkoituksesta.

45. Logojen käyttö saattaa olla sopiva tiedotuskeino. Logoja voidaan käyttää varoituksena lukulaitteiden ja RFID-tunnisteiden käytöstä silloin, kun niiden oletetaan pysyvän aktiivisina. Logojen käyttö ei kuitenkaan yksin riitä varmistamaan tietojen oikeaa käsittelyä, joka edellyttää, että rekisteröidyille annetaan tietoja selkeästi ja ymmärrettävästi. Logojen käyttöä olisi pidettävä toimenpiteenä, joka täydentää tarkempien tietojen antamista.

([1]) Ks. tarkemmin tämän lausunnon kohdat 46–50.

Keskeinen osallistumista koskeva periaate

46. Kaikissa asiaankuuluvissa RFID-sovellusten ratkaisuissa olisi noudatettava osallistumista koskevaa periaatetta ja pantava se ennakkoehtona täytäntöön myyntipisteessä. RFID-tunnisteiden käyttö edelleen tiedonvälitykseen myyntipisteen jälkeen olisi laitonta, ellei rekisterinpitäjällä ole asianmukaisia oikeudellisia perusteita. Asianmukaisia oikeudellisia perusteita ovat yleensä ainoastaan a) rekisteröidyn suostumus tai b) se, että tiedon luovuttaminen on tarpeen palvelun suorittamiseksi kyseisen yksilön nimenomaisen ja vapaan pyynnön pohjalta ([1]). Molempia oikeudellisia perusteita voidaan tällöin luonnehtia ”osallistumiseksi”.

47. Osallistumista koskevan periaatteen mukaisesti tunnisteet olisi deaktivoitava myyntipisteessä, jollei tunnisteella varustetun tuotteen ostaja halua jättää sitä aktiiviseksi. Käyttämällä oikeutta jättää tuote aktivoiduksi henkilö suostuu omien tietojensa jatkokäsittelyyn, esimerkiksi tiedonsiirtoon lukulaitteelle hänen käydessään seuraavan kerran rekisterinpitäjän luona.

48. RFID-sovellusten yhä suuremman monimuotoisuuden hallitsemiseksi ja uusien innovatiivisten liiketoimintamallien kehityksen helpottamiseksi Euroopan tietosuojavaltuutettu korostaa joustavan lähestymistavan tärkeyttä. Joustavuutta on sovellettava osallistumista koskevan periaatteen täytäntöönpanemisessa.

49. Osallistumista koskevaa periaatetta voidaan soveltaa monella eri tavalla. Tunnisteen poistamisen vaihtoehtona voisi esimerkiksi olla sen käytön esto, myös väliaikaisesti, tai sen lukitseminen tiettyä käyttäjää varten ankanpoikamalliksi (resurrecting duckling model) ([2]) kutsutun suojauskäytännön mukaisesti. Elinkaareltaan lyhyen tunnisteen osoite, joka viittaa tietokannassa säilytettyyn tietoon, voitaisiin myös poistaa viitetietokannasta tunnisteen avulla kerättyjen lisätietojen myöhemmän käsittelyn välttämiseksi.

50. Todettakoon lopuksi, että vaikka Euroopan tietosuojavaltuutettu pitää osallistumista koskevan periaatteen soveltamista myyntipisteessä oikeudellisena velvoitteena, joka sisältyy jo useimpien tilanteiden osalta tietosuojadirektiiviin, on hyviä syitä täsmentää tämä velvoite itsesääntelyvälineissä, myös sen varmistamiseksi, että periaate pannaan täytäntöön mahdollisimman asianmukaisesti. Erityistä täytäntöönpanoa tarvitaan joka tapauksessa tietosuojadirektiivin soveltamisalan ulkopuolelle jäävien RFID-sovellusten osalta.

([1]) Muutamissa RFID-sovelluksissa voidaan mahdollisesti käyttää muita perusteita, esimerkiksi 7 f artiklaa (rekisterinpitäjän oikeutetut edut, jotka edellyttävät riittäviä suojatakeita).

([2]) Tämän Frank Stajanon ja Ross Andersonin (Cambridgen yliopisto) kehittämän mallin nimi johtuu siitä, ”että ankanpoikanen olettaa ensimmäisen sen näkemän liikkuvan olennon olevan sen emo”.

Sisäänrakennetun yksityisyyden suojan tarve

51. Yksityisyyden suojaan ja tietosuojaan kohdistuvien uhkien minimoimiseksi komission tiedonannossa (kohta 3.2, sivu 6) esitetään suunnittelukriteerien määrittelyä ja käyttöönottoa jo varhaisessa vaiheessa. Euroopan tietosuojavaltuutettu on tyytyväinen tähän lähestymistapaan. Määritelmien ja suunnittelukriteerien eli ”parhaan käytettävissä olevan tekniikan” (BAT) käyttöönotolla edistetään tehokkaasti tietosuojaa koskevaa sääntelyä ja turvallisuusvaatimusten huomioon ottamista. Teknologisten ja organisatoristen kriteerien säännöllisesti tarkistetulla määrittelyllä lujitetaan yksityisyyttä ja turvallisuutta koskevien vaatimusten symbioottista mallia, jota Euroopan unioni parhaillaan kehittää.

52. Yksityisyyttä ja turvallisuutta koskevan BAT:n oikea määrittely RFID-järjestelmien osalta on myös ratkaisevaa sellaisen luotettavan toimintaympäristön luomiseksi, joka tukee niiden laajaa hyväksymistä loppukäyttäjien keskuudessa, samoin kuin eurooppalaisen teollisuuden kilpailukyvyn kannalta.

53. RFID-järjestelmiin liittyvän BAT:n valintaprosessia olisi tuettava yksityisyyttä ja turvallisuutta koskevilla vaikutusten arvioinneilla, joihin on vielä panostettava lisää. Euroopan tietosuojavaltuutettu katsoo, että Euroopan verkko- ja tietoturvavirasto (ENISA) voi yhdessä Euroopan komission yhteisten tutkimuskeskusten ja asiaankuuluvien teollisuuden sidosryhmien kanssa edistää tällaisten parhaiden käytäntöjen määrittelyä ja niihin liittyvien menetelmien kehittämistä. Käynnistämällä RFID:n teknisiä suuntaviivoja koskevan hankkeen Saksan liittovaltion tietosuojatoimisto (BSI) antoi hiljattain havainnollisen esimerkin ([3]) BAT:stä, jota tulisi nyt kehittää Euroopan tasolla.

54. Standardeilla voi myös olla ratkaiseva merkitys sisäänrakennetun yksityisyyden suojan periaatteen varhaisen käyttöönoton kannalta. Komission olisi näin ollen edistettävä yksityisyyden suojaa ja tietosuojaa koskevien takeiden käyttöönottoa kansainvälisten RFID-standardien kehittämisessä. 29 artiklan mukainen tietosuojatyöryhmä toi selvästi esiin RFID:tä koskevassa valmisteluasiakirjassaan ([4]), miten standardeilla voidaan edistää yksityisyyttä tukevaa RFID-järjestelmien kehitystä.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Valmisteluasiakirja (WP 105) RFID-teknologiaan liittyvistä tietosuojakysymyksistä, 19. tammikuuta 2005.

55. Euroopan tietosuojavaltuutettu on myös tyytyväinen komission kantaan, joka koskee RFID-teknologioiden tutkimusta ja kehittämistä sekä tarvetta minimoida yksityisyyden suojaan kohdistuvat riskit. Sisäänrakennetun yksityisyyden suojan periaate tulisi ottaa käyttöön teknologioiden kehittämisen varhaisimmassa vaiheessa, jotta näiden yhteensopivuus tietosuojalainsäädännön kanssa voidaan taata paremmin. Kuten Euroopan tietosuojavaltuutetun vuosikertomuksessa 2006 lyhyesti mainittiin, hän osallistuu tähän antamalla tapauskohtaisesti seitsemänteen puiteohjelmaan (2007–2013) kuuluviin hankkeisiin liittyviä lausuntoja ja neuvoja.

V TARVITAANKO ERITYISIÄ LAINSÄÄDÄNNÖLLISIÄ TOIMENPITEITÄ?

56. Itsesääntely ei välttämättä riitä nykyisen tietosuojaa ja yksityisyyttä koskevan lainsäädännön täyden täytäntöönpanon varmistamiseksi. Vaikka itsesääntely täyttää edellä mainitut vaatimukset, sen soveltaminen on vapaaehtoista ja sen noudattamatta jättämisestä ei voi aina tehokkaasti langettaa seuraamuksia. Lisäksi saatetaan kuitenkin tarvita sitovia lainsäädännöllisiä toimenpiteitä yksityisyyttä ja tietosuojaa koskevien oikeuksien suojan varmistamiseksi. Tämä on erityisen tarpeellista, jos itsesääntelyä koskevan lähestymistavan toteuttaminen epäonnistuu.

57. Keskeistä on määritellä tarvittavat säädökset sen varmistamiseksi, että RFID-sovelluksissa tosiasiallisesti käytetään tarvittavia teknisiä ratkaisuja tietosuojaa ja yksityisyyttä uhkaavien riskien ehkäisemiseksi tai minimoimiseksi ja että vastuulliset rekisterinpitäjät toteuttavat nykyisen lainsäädännön mukaisten velvoitteidensa noudattamiseksi tarvittavat toimenpiteet. Tästä aiheutuu seuraavia lisäkysymyksiä:

— Tarvitaanko erityisiä sääntöjä?

— Jos tarvitaan, voidaanko ne hyväksyä nykyisen lainsäädännön puitteissa, esimerkiksi nykyisiä komiteamenettelyitä noudattaen?

— Vai tarvitaanko uutta säädöstä sen varmistamiseksi, että tosiasiallisesti käytetään sisäänrakennettua yksityisyyttä suojaavaa teknologiaa hyödyntäviä RFID-sovelluksia.

58. Tässä luvussa käsitellään mahdollisuuksia toteuttaa sitovia lainsäädännöllisiä toimenpiteitä nykyisen lainsäädännön puitteissa, kun taas luvussa VI käsitellään erillisenä aiheena uuden säädöksen tarvetta.

59. Ensinnäkin olisi kiinnitettävä erityistä huomiota direktiivin 95/46/EY 17 artiklaan, direktiivin 2002/58/EY 14 artiklan 3 kohtaan sekä direktiivin 1999/5/EY 3 artiklan 3 kohdan c alakohtaan. 14 artiklan 3 kohta sallii jäsenvaltioiden toteuttaa toimenpiteitä sen varmistamiseksi, että päätelaitteet rakennetaan tavalla, joka on sopusoinnussa käyttäjien direktiivin 1999/5/EY mukaisen oikeuden kanssa, joka koskee heidän henkilötietojensa käytön suojelua ja valvontaa ([1]). Direktiivin 1999/5/EY 3 artiklan 3 kohdan c alakohdan mukaan komissio voi — komiteamenettelyä noudattaen — päättää, että tiettyihin laiteluokkiin kuuluvien laitteistojen tai tiettyjen laitteistotyyppien on oltava siten rakennettuja, että niihin sisältyy turvalaitteita, jotka takaavat käyttäjän ja tilaajan henkilötietojen ja yksityisyyden suojan. Direktiivin 1999/5/EY 3 artiklan 3 kohdan c alakohtaa ei ole tähän mennessä vielä sovellettu.

60. Nämä säännökset antavat lainsäätäjälle — niin kansallisella kuin yhteisönkin tasolla — vallan säätää, että yksityisyyttä ja tietosuojaa koskevat takeet on sisällytettävä RFID-järjestelmien valmistamiseen; kyseessä on ”sisäänrakennetun yksityisyyden suojan” soveltaminen ([2]). Myös BAT:ien käyttöä edellytetään.

61. Tehdäkseen sisäänrakennetun yksityisyyden suojan pakolliseksi Euroopan tietosuojavaltuutettu suosittaa, että komissio käyttäisi direktiivin 1999/5/EY 3 artiklan 3 kohdan c alakohdan mukaista järjestelyä ja kuulisi asiasta RFID-asiantuntijaryhmää.

62. Toiseksi on mahdollista itse direktiivejä muuttamalla täsmentää, miten nykyistä lainsäädäntöä on sovellettava RFID:hen. Kuten jo mainittiin, komissio on juuri esittänyt sähköisen viestinnän tietosuojadirektiivin tarkistamista koskevan ehdotuksen, jossa on tätä mahdollisuutta koskeva uusi säännös. Euroopan tietosuojavaltuutettu on tyytyväinen tähän ensimmäiseen vahvistukseen direktiivin soveltamisesta RFID-sovelluksiin. Euroopan tietosuojavaltuutettu käsittelee sähköisen viestinnän tietosuojadirektiivin ja RFID:n väliseen suhteeseen liittyviä kysymyksiä tarkistusehdotusta koskevassa lausunnossaan, joka annetaan vuoden 2008 alussa.

63. Koska komissio ei aio lähitulevaisuudessa muuttaa tietosuojadirektiiviä ([3]), mahdollisuudet täsmentää nykyisen lainsäädännön soveltamista radiotaajuustunnistukseen ovat rajalliset.

VI TARVITAANKO RFID:TÄ KOSKEVAA ERITYISLAINSÄÄDÄNTÖÄ?

Komission suunnitelmat

64. Komission tiedonannossa ([4]) painotetaan turvallisuuden ja sisäänrakennetun yksityisyyden suojan merkitystä. Siinä vaaditaan myös kaikkien sidosryhmien osallistumista.

([1]) Sekä lisäksi standardoinnista tietotekniikassa ja televiestinnässä 22 päivänä joulukuuta 1986 tehdyn neuvoston päätöksen 87/95/ETY mukaisesti (EYVL L 36, 7.2.1987, s. 31).
([2]) Ks. luku IV.
([3]) Euroopan tietosuojavaltuutettu kannattaa tätä lähestymistapaa, ks. kohta 64.
([4]) Ks. tiedonannon 4.1 kohta.

Komission työskentelyn päätuloksena on tarkoitus antaa ”suositus periaatteista, joita viranomaisten ja muiden sidosryhmien olisi noudatettava RFID:n käytön osalta”. Suositus hyväksytään todennäköisesti keväällä 2008. Tiedonannossa mainitut lainsäädännölliset tavoitteet ovat kaksivaiheiset. Komissio:

— tarkastelee sähköisen viestinnän tietosuojadirektiivin tulevan tarkistusehdotuksen asiaankuuluvia RFID:tä koskevia säännöksiä. Kuten edellä todettiin, komissio esitti marraskuussa 2007 sähköisen viestinnän tietosuojadirektiivin tarkistamista, jolla vahvistettaisiin direktiivin soveltaminen RFID-sovelluksiin ([1]) mutta ei laajennettaisi sen soveltamisalaa yksityisiin verkkoihin,

— arvioi, tarvitaanko tietosuojan ja yksityisyyden suojan varmistamiseksi muita lainsäädäntötoimia.

65. Tämän perusteella voidaan olettaa, että komissio ei ainakaan lähiaikoina aio esittää uutta erityislainsäädäntöä tietosuojan ja yksityisyyden suojan varmistamiseksi RFID-alalla.

Lainsäätäjää koskevat tekijät

66. Euroopan tietosuojavaltuutettu luetteli tietosuojadirektiiviä koskevasta tiedonannosta antamassaan lausunnossa joitakin henkilötietojen käsittelyyn liittyvien lainsäädäntötoimien suuntaviivoja, jotka voidaan tiivistää seuraavasti:

— Ensiksi tulisi noudattaa tietosuojaa koskevia pääperiaatteita: ”Uusia periaatteita ei tarvita mutta sen sijaan tarvitaan selvästi muita hallinnollisia järjestelyjä, jotka ovat toisaalta tehokkaita ja asianmukaisia verkottuneessa yhteiskunnassa ja joista toisaalta aiheutuu mahdollisimman vähän hallintokuluja” ([2]).

— Toiseksi säädösehdotuksia olisi annettava vain, jos niiden tarve ja oikeasuhteisuus on riittävällä tavalla osoitettu. Tästä syystä tietosuojaa koskevaa yleistä lainsäädäntöä ei ole syytä muuttaa lyhyellä aikavälillä.

— Kolmanneksi yhteiskunnan muutokset voivat johtaa erityissäädösten antamiseen, jotta tietosuojadirektiivin periaatteet voidaan mukauttaa RFID:n kaltaiseen erityisteknologiaan. On selvää, että tarpeellisuus ja oikeasuhteisuus on otettava huomioon myös tässä yhteydessä.

67. Seuraavaksi on hyödyllistä esittää lainsäätäjään RFID:n alalla kohdistuvat odotukset:

— Lainsäädännön tulee olla joustavaa ja jättää tilaa innovoinnille ja teknologian kehittymiselle. Tämän lähtökohdan tulisi johtaa teknologisesti riittävään neutraaliin lainsäädäntöön.

— Toiseksi lainsäädännön on taattava oikeusvarmuus. Tämän lähtökohdan tulisi johtaa riittävän erikoistuneeseen lainsäädäntöön. Sidosryhmien on tiedettävä tarkkaan, miten niiden toimintaa säännellään.

— Kolmanneksi lainsäädännön on suojeltava tehokkaasti kaikkia kyseessä olevia oikeutettuja etuja. Tämä edellyttää kaikissa tapauksissa lainsäädännön täytäntöönpanoa ja vastuiden selkeää määrittelyä: mikä taho vastaa mistäkin toiminnasta ([3])? Nämä vaatimukset ovat sitäkin tärkeämpiä kun kyse on yksityisyyden suojasta ja tietosuojasta, jotka on tunnustettu ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä yleissopimuksessa sekä Euroopan unionin perusoikeuskirjassa.

Euroopan tietosuojavaltuutetun näkemys

68. Euroopan tietosuojavaltuutetun mielestä on selvää, että kaikkien teknologisten kehitysaskeleiden ei tule johtaa EU:n lainsäätäjän toimiin. Teknologia voi kehittyä nopeasti, kun taas lainsäädännön hyväksyminen ja voimaantulo vie enemmän aikaa, kuten sen tuleekin tehdä. Lainsäädännön tulisi olla kaikkien kyseessä olevien etujen tasapainottamisen lopputulos. Kun säädösvälineeksi valitaan direktiivi, tarvitaan vielä enemmän aikaa, sillä direktiivit on saatettava täysimääräisesti osaksi jäsenvaltioiden oikeusjärjestelmiä.

69. RFID ei kuitenkaan ole vain teknologinen uutuus, mitä on korostettu tässä lausunnossa useassa eri kohdassa. Tiedonannossa RFID:hen viitataan tienä tietoyhteiskunnan uuteen kehitysvaiheeseen, jota usein kutsutaan ”tavaroiden internetiksi”, ja RFID-tunnisteet ovat älykkäiden ympäristöjen keskeisiä osatekijöitä. Tällaiset ympäristöt ovat myös tärkeitä vaiheita niin sanotun valvontayhteiskunnan ([4]) kehityksessä. Näin ollen on perusteltua toteuttaa lainsäädäntötoimia RFID:n alalla. RFID voi merkitä laadullista muutosta.

([1]) Ks. direktiiviin 2002/58/EY ehdotettu uusi 3 artikla.
([2]) Lausunto tietosuojadirektiiviä koskevasta tiedonannosta, kohta 24.
([3]) Tietosuojatermein ilmaistuna tämä edellyttää rekisterinpitäjän tunnistamista.
([4]) Tämä viesti toistettiin Euroopan tietosuojaviranomaisten Lontoossa 2. marraskuuta 2006 pitämässä puheenvuorossa, joka on saatavissa Internet-osoitteessa: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Tällä perusteella Euroopan tietosuojavaltuutettu suosittaa, että harkitaan yhteisön säädöksen antamista RFID:n käyttöön liittyvien päänäkökohtien sääntelemiseksi asiaankuuluvilla aloilla, mikäli nykyisen lainsäädännön asianmukainen täytäntöönpano ei johda riittävään lopputulokseen. Tämän lainsäädännön tultua voimaan se on katsottava erityissäännöstöksi (*lex specialis*) yleiseen tietosuojalainsäädäntöön nähden.

71. Tällaisen säädöksen antamiseen liittyvät seuraavat edut:

— Siinä voitaisiin määritellä itsesääntelyjärjestelyjen keskeiset tekijät.

— Sen antaminen voisi osoittautua tehokkaaksi kannusteeksi sille, että sidosryhmät perustaisivat asianmukaisen suojan tarjoavat itsesääntelyjärjestelyt.

72. Käytännössä komissiota voitaisiin pyytää laatimaan kuulemisasiakirja erityislainsäädännön hyvistä ja huonoista puolista sekä tällaisen lainsäädännön pääsisällöstä. Sidosryhmiä voitaisiin tietenkin pyytää antamaan omat lausuntonsa. Myös 29 artiklan mukainen tietosuojatyöryhmä voisi osallistua kuulemiseen.

Mahdolliset menettelytavat

73. Voitaisiin laatia erityissäännöstö, johon kuuluisi yhdistelmä nykyistä säännöstöä täsmentäviä ja täydentäviä erilaisia sääntelyvälineitä. Tämän erityissäännöstön olisi perustuttava tietosuojan vakiintuneisiin periaatteisiin, ja siinä olisi keskityttävä vastuunjakoon ja valvontajärjestelyjen tehokkuuteen.

74. Yksi erityinen syy tällaiselle mahdolliselle erityissäännöstölle liittyy siihen, että kaikkiin RFID-sovelluksiin ei liity henkilötietojen käsittelyä. Jos siis tiettyihin RFID-sovelluksiin ei liity henkilötietojen käsittelyä, niillä osapuolilla, jotka osallistuvat RFID-tuotteiden valmistamiseen ja myyntiin, ei ole oikeudellista velvoitetta toteuttaa teknisiä toimenpiteitä, joilla estetään salakuuntelu tai lukulaitteiden käyttö ilmoittamatta siitä etukäteen asianmukaisesti. Kuten on osoitettu, tällaisiinkin RFID-sovelluksiin liittyy kuitenkin yksityisyyden suojaa koskevia riskejä, jotka johtuvat mahdollisesta yksittäisten henkilöiden tarkkailusta ja edellyttävät tästä syystä samanlaisia yksityisyyden suojaa koskevia turvatoimia. Tällainen riski voi liittyä esimerkiksi siihen, että yksittäiset kulutustavarat varustetaan tunnistein ennen myyntipistettä. RFID-sovellukset, joihin ei liity henkilötietojen käsittelyä, voivat siis kuitenkin vaarantaa yksityisyyden suojan, koska niiden avulla voidaan toteuttaa piilotarkkailua ja käyttää näin saatuja tietoja tarkoituksiin, jotka eivät ole hyväksyttyjä.

75. Tietosuojavaltuutettu katsoo, että tällaisen epäsuotuisan tilanteen syntyminen olisi vältettävä. Koska nykyisen lainsäädännön pohjalta — ainakin niiden RFID-sovellusten osalta, joihin ei liity henkilötietojen käsittelyä — ei ole mahdollista estää tällaista yksityisyyden suojan vaarantumista ja ottaen huomioon vapaaehtoisuuteen perustuvien ratkaisujen puutteet, vaikuttaa tarpeelliselta käyttää pakollisia lainsäädäntötoimia tyydyttävän tuloksen varmistamiseksi.

76. Tällaisilla toimilla olisi

— vahvistettava osallistumista koskevan periaatteen soveltaminen myyntipisteessä täsmällisenä ja väistämättömänä oikeudellisena velvoitteena myös niiden RFID-sovellusten osalta, jotka eivät kuulu tietosuojadirektiivin soveltamisalaan ([1]),

— varmistettava, että RFID-sovellusten käyttöönottoon liittyy pakollinen vaatimus asianmukaisista teknisistä ominaisuuksista tai sisäänrakennetusta yksityisyyden suojasta.

VII **HALLINNOINTI**

77. Vaikka RFID-järjestelmien ”lähtökohtaisesti rajat ylittävää” ulottuvuutta käsitellään tiedonannossa vain sisämarkkinoiden kannalta, Euroopan tietosuojavaltuutettu katsoo, että tätä ulottuvuutta on tarkasteltava laajemmasta kansainvälisestä näkökulmasta. Kaupoissa RFID-järjestelmät ovat jo ”rajat ylittäviä”, koska tunnisteen toiminta ei välttämättä lakkaa myyntipisteessä. Koko RFID-järjestelmän tasolla näistä teknologioista tulee ”rajat ylittäviä” myös silloin, kun henkilötietoja saatetaan siirtää kolmanteen maahan tilanteessa, jossa RFID-järjestelmään kuuluvan, tunnisteella merkityn tavaran tuottajan toimipaikka on Euroopan unionin ulkopuolella ([2]).

78. Pidemmästä perspektiivistä RFID-tunnistetietokantojen hallinnointi on myös ratkaisevaa eurooppalaisen tietosuojalainsäädännön asianmukaiselle täytäntöönpanolle. Euroopan tietosuojavaltuutettu pitää tärkeänä, että asia saadaan ratkaistua pian, koska kyseisen lainsäädännön heikentäminen entisestään ei ole hyväksyttävissä.

79. Tietosuojavaltuutettu pitää RFID-järjestelmien hallinnointikysymystä merkittävänä haasteena, joka edellyttää huomattavaa panostusta. On löydettävä oikea neuvottelufoorumi sekä asianmukaisin hallinnollinen infrastruktuuri sen varmistamiseksi, että tietosuojaan liittyviä oikeuksia kunnioitetaan asianmukaisesti näissä kansainvälisissä yhteyksissä.

([1]) Luvussa IV todettiin, että osallistumista koskevan periaatteen soveltaminen myyntipisteessä on oikeudellinen velvoite, joka sisältyy jo tietosuojadirektiiviin.

([2]) Henkilötietojen siirtoon liittyviä velvoitteita käsitellään tietosuojadirektiivin 25 ja 26 artiklassa.

80. Tämän perusteella Euroopan tietosuojavaltuutettu pyytää komissiota esittämään hallinnointia koskevat näkemyksensä, mahdollisesti yhteistyössä RFID-sidosryhmän kanssa.

VIII **PÄÄTELMÄT**

81. Euroopan tietosuojavaltuutettu on tyytyväinen RFID:tä koskevaan komission tiedonantoon, koska siinä käsitellään tärkeimpiä RFID-teknologian käyttämiseen liittyviä kysymyksiä unohtamatta yksityisyyden suojaan ja tietosuojaan liittyviä ratkaisevia kysymyksiä. Tietosuojavaltuutettu yhtyy näkemykseen, jonka mukaan RFID-järjestelmillä voisi olla keskeinen merkitys tietoyhteiskunnan uudessa kehitysvaiheessa, jota usein kutsutaan ”tavaroiden internetiksi”.

Seurausten selvittäminen

82. RFID-teknologian laaja käyttö on perustavan uusi ilmiö, jolla saattaa olla merkittävä vaikutus yhteiskuntaamme ja perusoikeuksien, kuten yksityisyyden suojan ja tietosuojan, varmistamiseen yhteiskunnassamme. RFID voi merkitä laadullista muutosta.

83. Tässä yhteydessä voidaan yksilöidä viisi yksityisyyteen ja turvallisuuteen liittyvää peruskysymystä:

— tietokantaan rekisteröidyn tunnistaminen,

— rekisterinpitäjän/rekisterinpitäjien tunnistaminen,

— yksityisen ja julkisen välillä perinteisesti tehdyn eron merkityksen väheneminen,

— RFID-tunnisteiden koosta ja fyysisistä ominaisuuksista aiheutuvat seuraukset,

— avoimuuden puute tietojenkäsittelyssä.

Seurausten täsmentäminen

84. Direktiivin 95/46/EY mukaista yleistä tietosuojalainsäädäntöä sovelletaan RFID-teknologiaan siltä osin, kuin RFID-järjestelmissä käsitellyt tiedot kuuluvat henkilötietojen määritelmän piiriin.

85. Sähköisen viestinnän tietosuojadirektiivin osalta: direktiivin muuttamisesta 13. marraskuuta 2007 annettuun komission ehdotukseen sisältyy säännös, jolla pyritään täsmentämään, että direktiiviä todellakin sovelletaan tiettyihin RFID-sovelluksiin. Tietyt muut RFID-sovellukset eivät kuitenkaan välttämättä kuulu sen soveltamisalaan, koska direktiivi on rajattu koskemaan henkilötietojen käsittelyä yleisissä viestintäverkoissa yleisesti saatavilla olevissa sähköisen viestinnän palveluissa.

86. Henkilötietojen suojaa voidaan täydentää erilaisilla itsesääntelyvälineillä. On asianmukaista säilyttää tällainen itsesääntelymahdollisuus sillä edellytyksellä, että

— sen avulla tarjotaan konkreettista käytännön ohjeistusta tietyntyyppisiä RFID-sovelluksia varten,

— sen avulla käsitellään erityisiä tietosuojakysymyksiä ja -ongelmia, jotka tulevat esiin yleisten RFID-sovellusten yhteydessä,

— se tukee osaltaan tietosuojadirektiivin soveltamista yhtenäisesti ja yhdenmukaistetusti koko EU:ssa,

— sitä soveltavat kaikki asiaankuuluvat sidosryhmät.

87. Euroopan tietosuojavaltuutettu suosittaa, että komissio laatisi tiiviissä yhteistyössä RFID-asiantuntijaryhmän kanssa yhden tai useamman asiakirjan, joissa annettaisiin selkeät ohjeet nykyisen lainsäädännön soveltamisesta RFID-ympäristöön.

88. Ohjeiden, joissa vahvistetaan RFID:n käyttöön sovellettavat periaatteet, tulisi olla riittävän kohdennetut ja niissä olisi noudatettava alakohtaista lähestymistapaa. Ohjeissa olisi ehdotettava käytännöllisiä ja tehokkaita menetelmiä tekniikoiden ja standardien kehittämiseksi. Näillä edistettäisiin sitä, että RFID-järjestelmissä noudatetaan tietosuojalainsäädäntöä, ja niihin sisältyisi sisäänrakennetun yksityisyyden suojan mahdollistavan teknologian käyttö.

89. Euroopan tietosuojavaltuutettu on tyytyväinen komission tiedonannon lähestymistapaan, jolla vahvistetaan periaate suunnittelukriteereiden määrittelystä ja käyttöönotosta varhaisessa vaiheessa.

90. Vaikka tietosuojavaltuutettu katsoo, että osallistumista koskevan periaatteen soveltaminen myyntipisteessä on oikeudellinen velvoite, joka sisältyy jo tietosuojadirektiiviin useimmissa tilanteissa, tämä velvoite olisi määriteltävä erikseen itsesääntelyvälineiden yhteydessä.

Tarvitaanko erityisiä toimenpiteitä?

91. Sisäänrakennetun yksityisyyden suojan periaatteen asettamiseksi pakolliseksi Euroopan tietosuojavaltuutettu suosittaa, että komissio soveltaisi direktiivin 1999/5/EY 3 artiklan 3 kohdan c alakohdan mukaista järjestelyä ja kuulisi asiasta RFID-asiantuntijaryhmää.

92. Tietosuojavaltuutettu suosittaa, että harkitaan yhteisön säädöksen antamista RFID:n käyttöön liittyvien päänäkökohtien sääntelemiseksi asiaankuuluvilla aloilla, mikäli nykyisen lainsäädännön asianmukainen täytäntöönpano ei johtaisi riittävään lopputulokseen. Tämän lainsäädännön tultua voimaan se katsottaisiin erityissäännöstöksi (*lex specialis*) yleiseen tietosuojalainsäädäntöön nähden. Sinä pitäisi myös käsitellä yksityisyyden suojaan ja tietosuojaan liittyviä ongelmia, jotka koskevat tiettyjä RFID-sovelluksia, joihin ei liity henkilötietojen käsittelyä, kuten yksittäisten kulutustavaroiden merkitsemiseen tunnistein ennen myyntipistettä.

93. Komission olisi syytä laatia tausta-asiakirja erityislainsäädännön eduista ja haitoista sekä tällaisen lainsäädännön pääsisällöstä.

94. Voitaisiin laatia erityissäännöstö, johon kuuluisi yhdistelmä nykyistä säännöstöä täsmentäviä ja täydentäviä sääntelyvälineitä. Tällaisilla toimilla olisi:

— vahvistettava osallistumista koskevan periaatteen soveltaminen myyntipisteessä täsmällisenä ja väistämättömänä oikeudellisena velvoitteena myös niiden RFID-sovellusten osalta, jotka eivät kuulu tietosuojadirektiivin soveltamisalaan ([1]),

— varmistettava, että RFID-sovellusten käyttöönottoon liittyy pakollinen vaatimus asianmukaisista teknisistä ominaisuuksista tai sisäänrakennetusta yksityisyyden suojasta.

Hallinnointi

95. Euroopan tietosuojavaltuutettu pyytää komissiota esittämään hallinnointia koskevat näkemyksensä, mahdollisesti yhteistyössä RFID-sidosryhmän kanssa.

Tehty Brysselissä 20. joulukuuta 2007.

Peter HUSTINX

Euroopan tietosuojavaltuutettu

([1]) Luvussa IV todettiin, että osallistumista koskevan periaatteen soveltaminen myyntipisteessä on oikeudellinen velvoite, joka sisältyy jo tietosuojadirektiiviin.