I

*(Resolutsioonid, soovitused ja arvamused)*

ARVAMUSED

# EUROOPA ANDMEKAITSEINSPEKTOR

## Euroopa andmekaitseinspektori arvamus, mis käsitleb komisjoni teatist Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Raadiosagedustuvastus (RFID) Euroopas: sammud poliitilise raamistiku suunas", KOM(2007) 96

(2008/C 101/01)

EUROOPA ANDMEKAITSEINSPEKTOR,

võttes arvesse Euroopa Ühenduse asutamislepingut, eriti selle artiklit 286,

võttes arvesse Euroopa Liidu põhiõiguste hartat, eriti selle artiklit 8,

võttes arvesse Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta,

võttes arvesse Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris,

võttes arvesse Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrust (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta, eriti selle artiklit 41,

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

### I. **SISSEJUHATUS**

1. 15. märtsil 2007 võttis komisjon vastu teatise Raadiosagedustuvastus (RFID) Euroopas: sammud poliitilise raamistiku suunas ([1]) (edaspidi: „teatis"). Määruse (EÜ) nr 45/2001 artikli 41 kohaselt on Euroopa andmekaitseinspektori ülesanne ühenduse institutsioonide ja asutuste nõustamine kõikides isikuandmete töötlemisega seotud küsimustes. Euroopa andmekaitseinspektor (edaspidi andmekaitseinspektor) esitab käesoleva arvamuse, tuginedes nimetatud artiklile.

2. Käesolevat arvamust tuleb käsitada andmekaitseinspektori vastusena teatisele ning samuti RFID valdkonnas pärast teatise vastuvõtmist võetud muudele meetmetele. Nimetatud muud meetmed, mida võetakse arvesse käesolevas arvamuses:

— komisjoni 28. juuni 2007. aasta otsus raadiosagedustuvastuse eksperdirühma moodustamise kohta ([2]), mis tuleneb otseselt teatisest. Seda rühma kutsutakse ka RFID-sidusrühmaks. Vastavalt nimetatud otsuse artikli 4 lõike 4 punktile b osaleb andmekaitseinspektor rühma töös vaatlejana;

— nõukogu 22. märtsi 2007. aasta resolutsioon turvalise infoühiskonna strateegia kohta Euroopas ([3]);

— Euroopa Parlamendi algatatud projekt „Raadiosagedustuvastus ja tunnusandmete haldamine" ([4]);

([1]) KOM(2007) 96 (lõplik).
([2]) Otsus nr 467/2007/EÜ (ELT L 176, 6.7.2007, lk 25).
([3]) ELT C 68, 24.3.2007, lk 1.
([4]) Projekt „Raadiosagedustuvastus ja tunnusandmete haldamine — juhtumianalüüsid aruka keskkonna väljaarendamise eesliinil", mille tellis Euroopa Parlamendi teaduslike ja tehnoloogiliste võimaluste hindamise üksus (STOA) ja teostas Euroopa tehnoloogiahindamise rühm (ETAG): http://www.europarl.europa.eu/stoa/default_en.htm

— artikli 29 (andmekaitse) töörühma poolt 2007. aasta juunis vastu võetud arvamus nr 4/2007 isikuandmete mõiste määratluse kohta ([1]);

— komisjoni teatis Euroopa Parlamendile ja nõukogule andmekaitsedirektiivi parema rakendamise tööprogrammi järelmeetmete kohta ([2]) ning andmekaitseinspektori 25. juuli 2007. aasta arvamus selle teatise kohta ([3]);

— komisjoni ettepanek direktiivi kohta, millega muudetakse (muu hulgas) direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris ([4]).

3. Andmekaitseinspektor tervitab komisjoni teatist RFID kohta, kuna see käsitleb põhilisi RFID-tehnoloogia kasutamisega seotud küsimusi, võttes arvesse otsustavad eraelu puutumatuse ja andmekaitse küsimused. Nimetatud teatise koostamiseks on toimunud järjekindel ja hoolikas ettevalmistus. Teatisele on eelnenud komisjoni tellitud viis temaatilist seminari ja avalik Interneti-arutelu ([5]).

4. Andmekaitseinspektor on nõus seisukohaga, et RFID-süsteem võiks täita põhilist rolli tavaliselt „asjade Internetiks" nimetatava infoühiskonna arendamisel ja jagab täielikult teatise punktis 3.2 nimetatud kahtlusi, et RFID-süsteem võib ohustada eraelu puutumatust ja andmekaitseõigusi. Oma 2005. aasta aruandes nimetas andmekaitseinspektor selliseid uusi tehnoloogilisi arenguid nagu RFID, biomeetria, arukas keskkond ja tunnusandmete haldamise süsteemid, mis tõenäoliselt avaldavad andmekaitsele väga suurt mõju.

5. Vastavalt andmekaitseinspektori arvamusele ei ole RFID-tehnoloogiatega kohanemine ja nende laialdane vastuvõtmine saavutatav vaid nende atraktiivse mugavuse või pakutavate uute teenuste abil, vaid seda hõlbustavad ka hästikohandatud ja järjekindlad andmekaitsemeetmed.

6. Lühidalt: andmekaitseinspektori arvates on RFID täiesti uus tehnoloogiaarendus, mida komisjoni teatises nimetatakse õigustatult väravaks infoühiskonna uude arenguetappi.

7. Nimetatud arendusega seoses kerkivad esile eri valdkondi puudutavad küsimused, sealhulgas andmekaitse ja eraelu puutumatuse valdkonnas. Andmekaitseinspektori nimetatud arvamus piirdub nimetatud valdkonnaga.

## II. ARVAMUSE PÕHITEEMAD

8. Eelkõige keskendub arvamus nimetatud arengute võimalikele tagajärgedele andmekaitse ja eraelu puutumatuse valdkonnas. Nimetatud tagajärjed on praegu veel teadmata, kuna RFID-süsteemide areng ja nendega kohanemine on täies hoos ja ei ole teada, milleni need arengud viivad.

9. Sellest seisukohast lähtudes tegutseb andmekaitseinspektor järgmise skeemi järgi:

— esiteks on vaja selgitada RFID-süsteemide kasutuselevõtu tegelikke tagajärgi andmekaitsele ja eraelu puutumatusele;

— teiseks on vaja nimetatud tagajärgi täpsustada seoses andmekaitset ja eraelu puutumatust käsitleva kehtiva õigusliku raamistikuga;

— kolmandaks tegeleb andmekaitseinspektor küsimusega, kas nimetatud tagajärgedega tegelemiseks on vaja erieeskirju, et käsitleda RFID-tehnoloogia kasutamisel tekkivaid andmekaitseprobleeme. Nimetatud küsimus tõstatati juba andmekaitseinspektori arvamuses andmekaitsedirektiivi käsitleva teatise kohta ning seda täpsustatakse täiendavalt käesolevas arvamuses.

10. Nimetatud lähenemisviisi alusel soovib andmekaitseinspektor edendada RFID-süsteemide ja nende kasutuselevõtu arendamist nii, et see võtaks arvesse andmekaitse ja eraelu puutumatusega seotud õigustatud muresid.

## III. TAGAJÄRGEDE SELGITAMINE

### RFID-süsteemid ja kiibid

11. Kuigi nn arengud on täies hoos ja tulemused ei ole veel teada, on täitsa võimalik kirjeldada nende arengute selliseid põhilisi tunnuseid, mis on seotud andmekaitset puudutavate tagajärgedega.

([1]) Dokument WP 136, avaldatud töörühma veebisaidil.
([2]) Komisjoni 7. märtsi 2007. aasta teatis Euroopa Parlamendile ja nõukogule andmekaitsedirektiivi parema rakendamise tööprogrammi järelmeetmete kohta (KOM (2007) 87 (lõplik)).
([3]) ELT C 255, 27.10.2007, lk 1. Vt lisaks: „Arvamus andmekaitsedirektiivi käsitleva teatise kohta".
([4]) 13. novembri 2007. aasta Euroopa Parlamendi ja nõukogu direktiivi ettepanek, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris ning määrust (EÜ) nr 2006/2004 tarbijakaitsealase koostöö kohta (KOM(2007) 0698 (lõplik)). Direktiivile 2002/58/EÜ viidates kasutatakse edaspidi nimetust „eraelu puutumatuse direktiiv".
([5]) http://www.rfidconsultation.eu/

12. RFID-tehnoloogia andmekaitse ja eraelu puutumatuse võimalike aspektide hindamisel on väga oluline kaaluda mitte ainult RFID-kiipe vaid kogu RFID-infrastruktuuri: kiip, kiibilugeja, võrk, võrdlusandmebaas ja andmebaas, kus hoitakse kiibi/kiibilugeja poolt koos loodud andmeid. Nagu on rõhutatud teatise sissejuhatuses, pole RFID-seadmed pelgalt „elektroonilised märgised" ja seetõttu ei piirdu andmekaitse probleemid vaid kiipidega, vaid ulatuvad kogu RFID-infrastruktuuri kõikide osadeni. Iga nimetatud element saab vajadusel aidata kaasa Euroopa andmekaitse õigusliku raamistiku kohaldamisele. Neile sillutavad teed infoühiskonna arengu põhisuundumused, näiteks peaaegu piiramatu ribalaius, asukohast sõltumatud võrguühendused ja lõputu salvestusmaht.

**RFID-süsteemide ja kiipide mõju**

13. Olenemata eelmises lõigus rõhutatud laiaulatuslikuma lähenemisviisi vajadusest, on erinevatel põhjustel õigustatud keskendumine kõigepealt RFID kasutamisele tarbekaupade kiibistamisel, näiteks jaemüügisektoris. Ilmselt on ennustatav suurem kasutamine, mis viib laiema rakendamise poole. Vastupidiselt muude RFID-rakenduste kitsale või piiratud kasutamisele võib toodete tasandil kiibistamine saada massituru rakendusteks. Juba praegu on paljud tarbekaubad varustatud RFID-kiibiga. Sellega seonduvalt mõjutab selline kasutamine tohutut hulka isikuid, kelle isikuandmeid tõenäoliselt töödeldakse iga kord, kui nad omandavad RFID-kiipi sisaldava toote.

14. Erilist tähelepanu tuleks pöörata RFID-kiibistamisest tooteomanikele tulenevatele tagajärgedele. RFID-süsteemid võivad tekitada seose toote ja selle omaniku vahel. Kui selline seos on tekkinud, on võimalik omanikku jälgida ning liigitada ta tulevaste tehingute suhtes kas „väikese eelarvega" või „atraktiivseks sihtmärgiks"; liigne üks-ühele omistamine ([1]) võib soodustada teatud käitumise automaatset „karistamist" (ringlussevõtukohustus, jäätmed, jne). Inimeste suhtes ei tohiks kohaldada ebasoodsat automatiseeritud otsustusprotsessi. RFID-suutlikkuse tulemusena suureneb oht, et infoühiskond liigub selles suunas, et tehakse automatiseeritud otsustusi ja kuritarvitatakse tehnoloogiat inimkäitumise juhtimiseks.

15. RFID-kiibis salvestatud või sellega loodud andmed võivad olla andmekaitse direktiivi artiklis 2 määratletud isikuandmed. Näiteks reisimisel kasutataval kiipkaardil võivad olla tuvastamisandmed ning andmed omaniku hiljutiste reiside kohta. Kui vastutustundetu isik tahab kedagi jälgida, piisab kaardiomanike liikumisandmete teadasaamiseks kiibilugejate paigutamisest olulistesse kohtadesse, millega rikutakse nende eraelu ja isikuandmete puutumatust.

16. Samasugune oht eraelu puutumatusele võib tekkida isegi siis, kui RFID-kiibis salvestatud teave ei sisalda isikunime. RFID-kiibid sisaldavad tarbekaupadele lisatud kordumatuid identiteete: kui igal kiibil on kordumatu identiteet, võib sellist tuvastamist kasutada jälgimiseks. Näiteks kell, milles on ID-numbriga RFID-kiip, võib olla isegi tuvastamata kellakandja kordumatuks tunnuseks. Direktiivi kas kohaldatakse või ei kohaldata, sõltuvalt teabe kasutamise viisist ja sellest, kas see on seotud kellaga või isikuga. Direktiivi kohaldatakse näiteks juhul, kui kogutakse isikute asukohateavet, mida kasutatakse tõenäoliselt nende käitumise jälgimiseks, või näiteks erinevate hindade määramiseks, juurdepääsu piiramiseks või mittesoovitud reklaamiks.

17. Seoses sellega on vaja tagada, et RFID-rakendusi kasutatakse koos tehniliste meetmetega, mis on vajalikud soovimatu teabeavaldamise riski vähendamiseks. Sellised meetmed võivad hõlmata RFID-infrastruktuuri, eelkõige RFID-kiipide projekteerimisnõudeid, mis on kavandatud nimetatud tagajärgede vältimiseks. Näiteks on RFID-kiipe võimalik kasutada koos nende väljalülitamise võimalusega. Seda võimalust käsitletakse täiendavalt käesoleva arvamuse IV peatükis.

18. Toodete müügijärgse jälgimise võimalusega tekitavad RFID-süsteemid eraelu puutumatuse valdkonnas uusi probleeme. Selle mõju analüüsimisel tuleb arvesse võtta kahte asja: seda, kui personaalseks eset loetakse, ning eseme mobiilsust ([2]).

19. Ka eseme olelustsükkel võib täiendada nõutavat riskianalüüsi ja aidata kaasa eraelu puutumatuse võimalike ohtude kvantitatiivsele hindamisele. Juhul kui kiipi ei saa deaktiveerida, saab pika olelustsükliga toote lõpptarbija kohta koguda rohkem teavet ja koostada tema täpsema profiili. Teisest küljest tekitab lühikese olelustsükliga ese, näiteks joogipurk, oma tootmisest kuni ringlussevõtuni madalamat riski ja seetõttu nõuab see leebemaid meetmeid kui palju pikema olelustsükliga tooted.

([1]) Dr Sarah Spiekermann, Internetimajanduse Berliini Teadusuuringute Keskuse direktor, transatlantilise tarbijateemalise dialoogi poolt korraldatud seminar RFID ja asukohast sõltumatu andmetöötluse kohta, 13. märts 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.

**Eraelu puutumatuse ja andmekaitse küsimused RFID-süsteemi rakendamisel**

20. RFID-süsteemist eraelu puutumatusele ja andmekaitsele tulenevate tagajärgede paremaks mõistmiseks on võimalik eristada viit peamist eraelu puutumatuse ja turvalisusega seotud küsimust.

21. Esimene küsimus on isiku tuvastamine. Rohkem kui 60 aastat tagasi oli RFID-kiibi eesmärk tuvastada, kas läheneb sõber või vaenlane. Tänapäeval suudab RFID-süsteem lisaks objekti peamistele tunnustele tuvastada lõpuks ka isikut ja seetõttu peab seda tegema kooskõlas andmekaitsenõuetega.

22. Teine küsimus on vastutava(te) töötleja(te) tuvastamine. RFID-süsteemi korral võib andmekaitsedirektiivi artikli 2 punktis d määratletud vastutava töötleja tuvastamine olla raskem ja seetõttu nõuab see põhjalikumat uurimist. Kuid vastutava töötleja tuvastamine on kriitiline etapp kõikide nende asjaomaste osalejate vastutuse määratlemisel, kes peavad järgima andmekaitsealast õiguslikku raamistikku. Kiibi olelustsükli jooksul võib andmeid töötlev vastutav töötleja mitmeid kordi muutuda, kuna seoses kiibistatud objektiga võidakse osutada lisateenuseid.

23. Kolmas küsimus on era- ja avaliku sfääri traditsioonilise eristamise vähenemine. Kuigi era- ja avaliku sfääri erinevus pole ka varem olnud alati selge, on enamik inimesi nendevahelistest piiridest (ja hallidest tsoonidest) teadlik ning teevad teadlikke või intuitiivseid otsuseid vastavas olukorras tegutsemiseks. Vastavalt Hallile ([1]) on isiklik ruum tavaliselt vahemaa teiste isikuteni. Privaatsuse hoidmist võib pidada ka dünaamiliseks piiride reguleerimiseks ([2]). Seega pole üllatav, et kiibiga peetav raadioside ja selle nägemisulatusest väljapoole küündiv lugemisvõime tõstatab eraelu puudutavaid kahtlusi, hägustades traditsioonilisi piire ja nende piiride kontrolli. Tuntakse hirmu, et inimesed võivad osaliselt või täielikult kaotada kontrolli siiani kasu toonud kaugjuhtimise üle. Sellega seoses on RFID-süsteemide esimeste rakenduste lugemiskaugus olnud probleemiks nii RFID pooldajatele kui ka vastastele.

24. Neljas küsimus käsitleb RFID-kiipide mõõtmeid ja füüsikalisi omadusi. Kuna kiip peab olema põhimõtteliselt väike ja odav, on selles RFID-süsteemi osas rakendatavad turvameetmed piiratud. Kuid traatsidega võrreldes on raadiosidega seotud täiendavad riskid ja seetõttu on tarvis täiendavaid turvanõudeid.

25. Viies küsimus on andmetöötlusega seotud läbipaistvuse puudumine. RFID-süsteemid võivad tuua kaasa märkamatu andmete kogumise ja töötlemise, mida saab kasutada isiku profiili koostamiseks. Neid tagajärgi saab hästi kirjeldada, võrreldes RFID-süsteeme mobiiltelefoniga, ja seda võrdlust kasutatakse järjest rohkem. Ühest küljest on mobiiltelefon kasutanud ära tehnoloogiate aktsepteerimise väga kõrget taset, sõltumata selle võimalikust ohust rikkuda eraelu puutumatust. Võiks järeldada, et RFID aktsepteeritakse samamoodi. Teisest küljest on rõhutatud, et mobiiltelefon on nähtav ese, mis on lõppkasutaja kontrolli all, kuna seda saab välja lülitada. RFID puhul see ei kehti.

26. Kuigi eespool mainitud märkamatu andmete kogumine ja töötlemine võib olla seaduspärane, on samuti võimalik ja teatud tingimustel isegi täiesti tõenäoline, et toimub selliste andmete ebaseaduslik kogumine ja töötlemine.

27. Käesoleva peatüki selgitused õigustavad alljärgnevat järeldust. RFID-tehnoloogia laiaulatuslik kasutamine on täiesti uus nähtus ja sellel võib olla põhjalik mõju meie ühiskonnale ja põhiõiguste kaitsele meie ühiskonnas, näiteks eraelu puutumatusele ja andmekaitsele. RFID võib tuua kaasa kvalitatiivse muutuse.

## IV. TAGAJÄRGEDE MÄÄRATLEMINE

**Sissejuhatus**

28. Käesolev peatükk keskendub peamiselt mõjule, mida RFID avaldab põhiõiguste kaitsele meie ühiskonnas, näiteks eraelu puutumatusele ja andmekaitsele. Seda kirjeldatakse kahes osas, millest esimeses kirjeldatakse lühidalt, kuidas kehtivas õiguslikus raamistikus nimetatud põhiõigusi kaitstakse. Teises etapis kirjeldab andmekaitseinspektor kehtiva õigusliku raamistiku täieliku ärakasutamise võimalusi. Nimetatud püüe on esitatud andmekaitseinspektori arvamuses andmekaitsedirektiivi käsitleva teatise kohta sõnastuses „tuleb täielikult rakendada direktiivi praegused sätted".

29. Lähtekoht on järgmine: uued tehnoloogilised arengud, näiteks RFID-süsteemid, avaldavad olulist mõju nõudmistele kehtestada andmekaitse tõhus õiguslik raamistik. Lisaks võib üksikisiku isikuandmete tõhusa kaitsmise vajadus seada piiranguid nimetatud uute tehnoloogiate kasutamisele. Koostoime on seega kahepoolne: tehnoloogia mõjutab õigusakte ja õigusaktid mõjutavad tehnoloogiat ([3]).

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

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

([3]) Vaata Euroopa andmekaitseinspektori märtsis 2006. aastal tehtud märkusi (avaldatud Euroopa andmekaitseinspektori veebisaidil) komisjoni teatise kohta, mis käsitleb Euroopa andmebaaside koostalitlusvõimet.

**Põhiõiguste kaitse**

30. Eraelu puutumatuse ja andmekaitsega seotud põhiõiguste kaitse Euroopa Liidus on tagatud kõigepealt õigusraamistikuga, mis on vajalik seetõttu, et me käsitleme õigusi, mida on tunnustatud inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni artiklis 8 ning Euroopa Liidu põhiõiguste harta artiklites 7 ja 8. Asjaomane õigusraamistik andmekaitse ja RFID jaoks koosneb peamiselt andmekaitsedirektiivist 95/46/EÜ ja e-privaatsuse direktiivist 2002/58/EÜ ([1]).

31. RFID suhtes kohaldatakse direktiivis 95/46/EÜ sätestatud andmekaitse üldist õigusraamistikku, kuna RFID-süsteemide abil töödeldud andmed vastavad isikuandmete määratlusele. Kuigi teatud juhtudel töötlevad RFID-rakendused selgelt isikuandmeid ja kuuluvad kahtlemata andmekaitsedirektiivi reguleerimisalasse, on rakendusi, mille puhul andmekaitsedirektiivi kohaldatavus pole nii ilmne. Artikli 29 andmekaitse töörühma arvamus nr 4/2007 isikuandmete mõiste määratluse kohta aitab kaasa selgemale ja ühiselt tunnustatud arusaamale isikuandmete mõistest ning vähendab sellega ebakindlust ([2]).

32. E-privaatsuse direktiivi osas on olukord järgmine: Seni ei ole selge, kas nimetatud direktiivi kohaldatakse RFID-rakenduste suhtes. Komisjoni 13. novembri 2007. aasta ettepanek direktiivi muutmise kohta sisaldab seetõttu sätet, mille eesmärk on täpsustada, et direktiivi kohaldatakse teatud RFID-rakenduste suhtes. Kuid teised RFID-rakendused ei ole võib-olla hõlmatud, kuna nimetatud direktiivi kohaldatakse ainult isikuandmete sellise töötlemise suhtes, mis toimub seoses üldkasutatavate elektrooniliste sideteenuste osutamisega üldkasutatavates sidevõrkudes.

33. Isikuandmeid on võimalik täiendavalt kaitsta mitmete eneseregulatsiooni vahenditega (mitteseadusandlik raamistik). Mõlemas direktiivis soodustatakse aktiivselt nimetatud vahendite kasutamist, eriti andmekaitsedirektiivi artiklis 27, kus on sätestatud, et liikmesriigid ja komisjon toetavad tegevusjuhendite koostamist, mille eesmärk on aidata kaasa nimetatud direktiivi nõuetekohasele rakendamisele. Lisaks võivad eneseregulatsiooni vahendid aidata tõhusalt kaasa andmekaitsedirektiivi artiklis 17 ja e-privaatsuse direktiivi artiklis 14 nõutud turvameetmete rakendamisele.

**Olemasoleva raamistiku täielik rakendamine**

34. Arvamuses andmekaitsedirektiivi käsitleva teatise kohta loetletakse mitmeid olemasolevaid vahendeid direktiivi paremaks rakendamiseks. Enamik nimetatud arvamuse mittesiduvaid vahendeid on RFID suhtes asjakohased, näiteks tõlgendavad teatised või muud teatised, parimate tavade edendamine, eraelu puutumatuse märgiste kasutamine ja eraelu puutumatuse alaste auditite läbiviimine kolmandate isikute poolt. V osas arutatakse RFID käsitlevate konkreetsete eeskirjade võimalikku vastuvõtmist. Kuid olukorda on võimalik parandada ka praegu kehtivas õigusraamistikus.

**Eneseregulatsiooni vahendid**

35. Andmekaitseinspektor nõustub komisjoniga, et esimesel etapil on asjakohane jätta ruumi eneseregulatsiooniks, mis lubab sidusrühmadel luua kiiresti õigusnõuetele vastav keskkond ja sellega aidata kaasa turvalisema õigusliku keskkonna loomisele.

36. Komisjonilt, kes konsulteerib RFID-sidusrühmaga, oodatakse nimetatud eneseregulatsiooni stimuleerimist ja juhtimist. Sellega seoses tervitab andmekaitseinspektor teatises väljakuulutatud soovitust, mis peaks sisaldama üksikasjalikumaid juhiseid, et määrata kindlaks „põhimõtted, mida ametiasutused ja teised sidusrühmad peaksid kohaldama raadiosagedustuvastuse kasutamise suhtes”.

37. Teatises nähakse ette, et eneseregulatsioonist kujuneb välja käitumisjuhend või heade tavade eeskiri. Andmekaitseinspektor leiab, et sõltumata eneseregulatsiooni vormist peaks see:

— andma konkreetsete RFID-rakenduste tüüpide kohta konkreetseid ja praktilisi juhiseid ning aitama sellega parandada andmekaitse õigusraamistikule vastavust;

— käsitlema konkreetseid andmekaitsega seotud küsimusi ja probleeme, mis esinevad seoses üldiste RFID-rakendustega;

— aitama kaasa andmekaitsedirektiivi ühetaolisele ja ühtlustatud rakendamisele kogu ELis, eelkõige konkreetses valdkonnas, kus kogu ELis kasutatakse tõenäoliselt samatüübilisi RFID-rakendusi;

— seda peaks rakendama kõik asjaomased sidusrühmad. Nõuete mittetäitmisel peaksid olema negatiivsed (võimalusel rahalised) tagajärjed.

([1]) Käesoleva arvamuse punktis 59 arutletakse kolmanda direktiivi, Euroopa Parlamendi ja nõukogu 9. märtsi 1999. aasta direktiivi 1999/5/EÜ (raadioseadmete ja telekommunikatsioonivõrgu lõppseadmete ning nende nõuetekohasuse vastastikuse tunnustamise kohta (ELT L 91, 7.4.1999, lk 10)) asjakohasuse üle.

([2]) Vaata muu hulgas viiendas joonealuses märkuses osutatud arvamuse lk 10.

38. Andmekaitseinspektor tõstab esile ühte küsimust, mille suhtes eneseregulatsioon on eriti kasulik. Isikuandmeid töötlevate RFID-rakenduste suhtes on andmekaitsedirektiivis sätestatud vastutavale andmetöötlejale mitmed kohustused, eelkõige artiklis 17 (töötlemise turvalisus) ja artiklis 7 (isikuandmeid võib töödelda ainult piisava õigusliku aluse olemasolul). Nimetatud sätete kohaselt peab vastutav andmetöötleja ühelt poolt rakendama meetmeid andmete loata avalikustamise vastu. Teiselt poolt peab vastutav andmetöötleja tagama, et andmete töötlemine, näiteks vajaduse korral teabe avaldamine kiibilugejate kaudu, toimub vaid juhul, kui on saadud selle isiku, keda need andmed puudutavad, teadlik nõusolek.

39. Andmekaitsedirektiivi nimetatud sätteid võib tõlgendada nii, et RFID-rakendusi tuleb rakendada selliste tehniliste lahendustega, mis väldivad soovimatut avalikustamist või viivad selle miinimumini ning tagavad, et andmete töötlemine või ülekandmine toimub vaid isiku teadlikul nõusolekul ja vajaduse korral. Andmekaitseinspektori arvates on see kohustus (rakendada selliseid tehnilisi lahendusi, mis väldivad soovimatut avalikustamist või viivad selle miinimumini) ja selle siduvus RFID-rakenduste kasutajatele isegi tugevam ja selgem, kui see nõue on esitatud eespool nimetatud kavandatavas käitumisjuhendis või heade tavade eeskirjas. Seetõttu soovitab andmekaitseinspektor tungivalt lisada andmekaitsedirektiivi selline tõlgendus komisjoni teatisesse, rõhutades kehtivat kohustust rakendada RFID-rakendusi, millel on vajalikud tehnilised meetmed, mis väldivad soovimatut andmete kogumist või avalikustamist.

**Vajadus juhise järele**

40. Andmekaitseinspektor soovitab komisjonil tihedas koostöös RFID-eksperdirühmaga koostada üks või mitu dokumenti, milles esitatakse selge juhis kehtiva õigusraamistiku kohaldamiseks RFID-keskkonnas. Nimetatud juhis peaks ette nägema praktilise viisi andmekaitsedirektiivis ja e-privaatsuse direktiivis sätestatud põhimõtetest kinnipidamiseks. Üldiseks lähenemisviisiks juhise ja selle konkreetse sisu suhtes on andmekaitseinspektoril järgmised soovitused.

41. Juhis, mis sätestab RFID kasutamise põhimõtted, peaks olema piisavalt keskendunud ja rakendama valdkondlikku lähenemisviisi. Selge ja ühtse raamistiku tagamise eesmärki ei ole võimalik saavutada kõigile sobiva ühesuguse lahendusega. Selle asemel tuleb juhise kohaldamisala piirata täpselt määratletud valdkondlike RFID-rakendustega.

42. Lisaks peaks juhis soovitama praktilisi ja tõhusaid meetodeid selliste tehnoloogiate ja standardite väljatöötamiseks, mis võiksid aidata kaasa RFID-süsteemide vastavusele andmekaitse õigusraamistikuga ja millega kaasneb „eraelu kavandatud puutumatuse" tehnoloogia kasutamine.

43. Kehtiva õigusraamistiku kohaldamisel RFID-keskkonnas tuleb erilist tähelepanu pöörata andmekaitse põhimõtete kohaldamisele ja RFID-rakenduste vastutavate andmetöötlejate kohustustele. Eriti olulised on järgmised kohustused ja põhimõtted:

— õigus olla teavitatud, sh õigus teada, millal kogutakse kiibilugejatega andmeid, ja asjakohastel juhtudel sellest, et tooted on kiibistatud;

— nõusoleku olemasolu kui üks andmete töötlemise õiguslik alus. See tähendab, et juhul kui andmesubjekt ei ole kiibi aktiivseks jätmiseks nõusolekut andnud, tuleb RFID-kiibid müümise hetkel deaktiveerida ([1]). RFID-kiipide deaktiveerimise õigus täidab ülesannet tagada andmete turvalisus, st tagada, et RFID-kiipide abil töödeldud andmeid ei avaldata mittesoovitud kolmandatele isikutele;

— inimeste õigus nõuda, et nende suhtes ei tehtaks võimalike ebasoovitavate tagajärgedega otsuseid üksnes konkreetse isiku isikliku profiili automatiseeritud töötlemisele tuginedes.

44. Seoses õigusega olla informeeritud tuleks juhises sätestada, et inimesi tuleb teavitada nende isikuandmete töötlemisest. Eelkõige tuleks neid hoiatada i) kiibilugejate olemasolust ja aktiivsete RFID-kiipide olemasolust toodetel või nende pakendil; ii) sellise olemasolu mõjust teabe kogumisele, ja iii) kogutud teabe kavandatud kasutamise eesmärkidest.

45. Sobivaks teavitamismeetmeks võib olla logode kasutamine. Logosid võib kasutada kiibilugejate ja eeldatavalt aktiivseks jäävate RFID-kiipide olemasolust hoiatamiseks. Kuid ainuüksi logode kasutamisest ei piisa andmete õiglase töötlemise tagamiseks; see nõuab andmesubjekti teavitamist selgel ja arusaadaval viisil. Logode kasutamine peaks olema üksikasjalikuma teavitamise lisameede.

([1]) Vaata üksikasju käesoleva arvamuse punktides 46–50.

**Keskne mõte: osalemispõhimõte**

46. Kõikide asjaomaste RFID-rakenduste puhul peaks lahendused eeldusena tunnustama ja rakendama osalemispõhimõtet müümise hetkel. Kui vastutaval andmetöötlejal puudub vastav õiguslik alus, on müügijärgne RFID-kiipide jätkuv teabeedastamine ebaseaduslik. Vastav õiguslik alus oleks vaid a) andmesubjekti nõusolek või b) kui selline avaldamine on nimetatud isikule vajalik teenuse osutamiseks, konkreetse ja tasuta taotluse esitamiseks ([1]). Mõlemad õiguslikud alused oleks seega osalemiseks sobivad.

47. Osalemispõhimõtte kohaselt tuleks kiibid müügihetkel deaktiveerida, kui toote ostja ei soovi, et lisatud kiip jääks aktiivseks. Kui kasutatakse aktiivseks jätmise õigust, palutakse isiku nõusolekut tema andmete edasiseks töötlemise eesmärgil, näiteks tema järgmise külastuse andmete edastamiseks kiibilugejalt vastutavale andmetöötlejale.

48. Et tulla toime RFID-rakenduste kasvava mitmekesisusega ning hõlbustada uuenduslike ärimudelite väljatöötamist, rõhutab andmekaitseinspektor paindliku lähenemisviisi tähtsust. Osalemispõhimõtte rakendamine peab olema paindlik.

49. Osalemispõhimõtte rakendamise võimalusi on mitmeid. Kiibi eemaldamise alternatiiviks võiks olla näiteks kiibi blokeerimine, ajutine mittetoimivaks muutmine või julgeolekupoliitika mudeli kohaselt, mida kutsutakse „pardipoja mudeliks" ([2]), kiibi konkreetsele kasutajale lukustamine. Lühikese olelustsükliga kiibi puhul võiks andmebaasi teabele viitava kiibi aadressi võrdlusandmebaasist kustutada, et vältida kiibi poolt kogutavate lisaandmete edasist töötlemist.

50. Kokkuvõtteks, kuigi andmekaitseinspektor väidab, et osalemispõhimõte on müügihetkel seaduslik nõue, mis kehtib enamikul juhtudel juba andmekaitsedirektiivi alusel, on siinkohal sobiv põhjus seda kohustust eneseregulatsiooni vahendites täpsustada, samuti oleks see vajalik selle põhimõtte rakendamise tagamiseks kõige sobivamal viisil. Igal juhul on konkreetne rakendamine vajalik nende RFID-rakenduste puhul, mis ei kuulu andmekaitsedirektiivi reguleerimisalasse.

([1]) Mõne RFID-rakenduse puhul võib olla võimalik tugineda muudele alustele, näiteks artikkel 7f (vastutava andmetöötleja õigustatud huvid, nõuetekohaste tagatiste olemasolul).

([2]) Selle mudeli loojad Frank Stajano ja Ross Anderson Cambridge Ülikoolist said nime valikul inspiratsiooni sellest „kuidas kooruv hanetibu eeldab, et esimene liikuv objekt, mida ta näeb, on tema ema".

**„Eraelu kavandatud puutumatuse" vajadus**

51. Eraelu puutumatuse ja andmekaitse ohtude vähendamiseks kiidetakse komisjoni teatise punktis 3.2 (lk 6) heaks eelprojekteerimiskriteeriumide väljatöötamise ja vastuvõtmise idee. Andmekaitseinspektor tervitab sellist lähenemisviisi. Spetsifikaatide ja projekteerimiskriteeriumide (mida nimetatakse ka parimaks võimalikuks tehnikaks) vastuvõtmine aitab tõhusalt kaasa andmekaitsealasele regulatsioonile ja turvanõuetele. Tehnoloogiliste ja organisatsiooniliste kriteeriumide kindlaksmääramine tugevdab nende sagedase läbivaatamise korral seda eraelu puutumatuse ja turvanõuete sümbiootilist mudelit, mida Euroopa Liit välja arendab.

52. Eraelu puutumatuse ja turvalisuse parim võimalik tehnika on RFID-süsteemide puhul määrav nii usaldusväärse keskkonna loomiseks, mis parandab nende laialdast vastuvõtmist lõppkasutajate poolt, kui ka Euroopa tööstuse konkurentsivõime aspektist.

53. Parima võimaliku tehnika valimisele RFID-süsteemide puhul peaksid kaasa aitama eraelu puutumatuse ja turvalisuse alased mõjuhinnangud, mille tegemiseks on vaja veelgi rohkem jõupingutusi. Andmekaitseinspektor leiab, et Euroopa Võrgu- ja Infoturbeamet (ENISA) koos Euroopa Komisjoni Teadusuuringute Ühiskeskuse ja sellega ühinenud tööstusvaldkonna asjaomaste sidusrühmadega saab kaasa aidata nimetatud parima võimaliku tehnika leidmisele ja sellise metoodika väljaarendamisele. Hiljuti käivitatud projektiga „RFID tehnilised juhised" esitas Saksamaa Föderaalne Teabeturbeamet (BSI) illustreeriva näite ([3]) parima võimaliku tehnika kohta, mida tuleks nüüd Euroopa tasemel edasi arendada.

54. Standardid võivad täita otsustavat rolli eraelu kavandatud puutumatuse põhimõtte kiirel kasutuselevõtul. Komisjon peaks seetõttu aitama kaasa eraelu puutumatuse ja andmekaitse kaitsemeetmete kasutuselevõtule rahvusvaheliste RFID-standardite väljatöötamisel. Artikli 29 töörühm tõstis oma RFID käsitlevas töödokumendis ([4]) selgelt esile, et standardid võivad aidata kaasa eraelu puutumatust toetavate RFID-süsteemide väljatöötamisele.

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

([4]) Töödokument (WP 105) RFID-tehnoloogiaga seotud andmekaitseküsimuste kohta, 19. jaanuar 2005.

55. Lisaks sellele tervitab andmekaitseinspektor komisjoni võetud seisukohta, mis käsitleb RFID-tehnoloogiate valdkonna teadusuuringuid ja arendustegevust ning vajadust vältida eraelu puutumatusega seotud ohte. Eraelu kavandatud puutumatuse põhimõtet tuleb rakendada alates tehnoloogiate väljaarendamise kõige varasemast etapist, kuna see aitab paremini kaasa nende vastavusele andmekaitse õigusraamistikuga. Andmekaitseinspektor, nagu ta lühidalt mainis oma 2006. aasta aruandes, osaleb selles töös, andes üksikjuhtumite puhul seitsmenda raamprogrammi (2007–2013) projektide kohta arvamusi ja nõuandeid.

## V. **KAS ON VAJA KONKREETSEID SEADUSANDLIKKE MEETMEID?**

56. Eneseregulatsioon ei pruugi olla piisav vahend andmekaitse nõuete ja eraelu puutumatuse olemasoleva raamistiku täielikuks rakendamiseks. Isegi, kui eneseregulatsioon vastab eespool mainitud nõuetele, on selle rakendamine vabatahtlik ja nõuete mittetäitmine ei too alati kaasa tegelikku karistust. Lisaks on võib-olla vaja siiski siduvaid õigusakte, et tagada üksikisikute õigus eraelu puutumatusele ja andmekaitsele. Seda on veelgi rohkem vaja juhul, kui eneseregulatsioonile tuginev lähenemine ei tööta.

57. Põhiküsimuseks on selliste vajalike õigusaktide kindlaksmääramine, mis tagavad RFID-rakenduste tegeliku kasutuselevõtu selliste vajalike tehniliste lahendustega, mis väldivad andmekaitsega ja eraelu puutumatusega seotud ohte või viivad need miinimumini, ning et vastutavad töötlejad võtavad oma kohustuste täitmiseks vajalikud meetmed kooskõlas kehtiva õigusliku raamistikuga. See tõstatab mõned lisaküsimused:

— kas on vaja konkreetseid eeskirju?

— kui on, kas siis saab neid eeskirju vastu võtta kooskõlas kehtiva õigusliku raamistikuga, näiteks kasutades kehtivat komiteemenetlust?

— või on vaja uut õigusakti, et tagada selliste RFID-rakenduste kasutuselevõtt, mis sisaldab eraelu puutumatust soodustavaid tehnoloogiaid?

58. Käesolev peatükk käsitleb võimalusi kehtestada siduvaid õigusakte vastavalt kehtivale õiguslikule raamistikule, VI peatükis käsitletakse uue õigusakti vajadust, kuna see on eraldiseisev küsimus.

59. Esiteks tuleks erilist tähelepanu pöörata direktiivi 95/46/EÜ artiklile 17, direktiivi 2002/58/EÜ artikli 14 lõikele 3 ja direktiivi 1999/5/EÜ artikli 3 lõike 3 punktile c. Artikli 14 lõige 3 lubab liikmesriikidel vastu võtta meetmed, et tagada lõppseadmete konstrueerimine kooskõlas kasutajate õigusega kaitsta oma isikuandmeid ja kontrollida nende kasutamist vastavalt direktiivile 1999/5/EÜ ([1]). Direktiivi 1999/5/EÜ artikli 3 lõike 3 punktis c on sätestatud, et komisjon võib komiteemenetlusega otsustada, et teatavatesse seadmeklassidesse kuuluvad seadmed või konkreetset tüüpi seadmed peavad olema valmistatud sel viisil, et need sisaldavad turvaseadmeid, et tagada kasutajate ja abonentide isikuandmete ja eraelu puutumatuse kaitse. Direktiivi 1999/5/EÜ artikli 3 lõike 3 punkti c pole seni kasutatud.

60. Need sätted annavad seadusandjale nii siseriiklikul kui ka ELi tasandil õiguse nõuda, et RFID-süsteemide valmistamisel tuleb neile lisada eraelu puutumatuse ja andmekaitse kaitsemeetmed, mis on tuntud, kui „eraelu kavandatud puutumatuse" kontseptsioon ([2]). Selles kutsutakse ka üles kasutama parimat võimalikku tehnikat.

61. Selleks et teha „eraelu kavandatud puutumatuse" kontseptsiooni kasutamine kohustuslikuks, soovitab andmekaitseinspektor komisjonil kasutada direktiivi 1999/5/EÜ artikli 3 lõike 3 punkti c mehhanismi, konsulteerides RFID eksperdirühmaga.

62. Teiseks on direktiivide muutmisega võimalik täpsustada RFID käsitleva kehtiva õigusliku raamistiku kohaldamist. Komisjon on just esitanud e-privaatsuse direktiivi muutmise ettepaneku, mis sisaldab selles osas ühte uut sätet. Andmekaitseinspektor tervitab seda esimest kinnitust direktiivi kohaldamise kohta RFID-rakenduste suhtes. Oma 2008. aasta alguses nimetatud muudatusettepaneku kohta antavas arvamuses tegeleb andmekaitseinspektor eriküsimustega, mis on tõstatatud e-privaatsuse direktiivi ja RFID vahelise seose tõttu.

63. Võttes arvesse, et komisjon ei näe ette andmekaitsedirektiivi muutmist lähitulevikus ([3]), on võimalused täpsustada RFID suhtes kehtiva õigusraamistiku kohaldamist piiratud.

## VI. **KAS RFID JAOKS ON VAJA SPETSIIFILIST ÕIGUSLIKKU RAAMISTIKKU?**

### Komisjoni kavatsused

64. Teatises ([4]) rõhutatakse turvalisuse ja eraelu kavandatud puutumatuse tähtsust. See nõuab ka kõigi sidusrühmade kaasamist. Komisjoni tegevuse peamine tulemus on „soovitus määrata kindlaks põhimõtted, mida ametiasutused

([1]) Ja kooskõlas ja nõukogu 22. detsembri 1986. aasta otsusele 87/95/EMÜ standardimise kohta infotehnoloogia ja telekommunikatsiooni valdkonnas (EÜT L 36, 7.2.1987, lk 31).
([2]) Vt IV peatükk.
([3]) Andmekaitseinspektor toetab seda lähenemisviisi, vt punkt 64.
([4]) Vaata teatise punkt 4.1.

ja teised sidusrühmad peaksid kohaldama RFIDi kasutamise suhtes". Nimetatud soovitus võetakse tõenäoliselt vastu 2008. aasta kevadel. Teatises mainitud seadusandlikud eesmärgid on kaheastmelised. Komisjon:

— kaalub asjaomaseid RFID käsitlevaid sätteid peatselt esitatavas e-privaatsuse direktiivi muutmise ettepanekus. Nagu eespool mainitud, esitas komisjon sellise e-privaatsuse direktiivi muutmise ettepaneku 2007. aasta novembris, kinnitades, et direktiivi saab kohaldada RFID-rakenduste suhtes ([1]), aga ta ei teinud ettepanekut laiendada elektroonilise eraelu puutumatuse direktiivi reguleerimisala eravõrkudele;

— hindab vajadust edasiste õigusaktide järele, et tagada andmekaitse ja eraelu puutumatus.

65. Selle poliitika kohaselt on ennustatav, et vähemalt lähiajal komisjon ei kavanda uusi konkreetseid õigusakte andmekaitse ja eraelu puutumatuse tagamiseks RFID valdkonnas.

**Seadusandja parameetrid**

66. Oma arvamuses andmekaitsedirektiivi käsitleva teatise kohta esitas andmekaitseinspektor mõned isikuandmete töötlemisega seotud seadusandlike tegevuste kirjeldused, mis on kokkuvõtlikult järgmised:

— esiteks tuleks kinni pidada andmekaitse põhimõtetest: „Puudub vajadus uute põhimõtete kehtestamiseks, kuid esineb selge vajadus teist laadi halduskorralduste järele, mis on ühelt poolt tõhusad ja võrgustikuna toimiva ühiskonna seisukohalt asjakohased ning mis teiselt poolt viivad halduskulud miinimumini." ([2]);

— teiseks, õigusaktiettepanekuid tuleks esitada üksnes juhul, kui nende vajadus ja proportsionaalsus on piisavalt tõendatud. Sellel eesmärgil ei tohiks andmekaitse üldist õigusraamistikku lühiajalises perspektiivis muuta;

— Kolmandaks, ühiskonnas toimuvad mitmesugused arengud võivad viia spetsiifiliste õigusraamistike tekkimiseni, et kohandada andmekaitsedirektiivi põhimõtteid spetsiifiliste tehnoloogiate, näiteks RFID tõttu tekkinud probleemidega. Selge, et sellega seoses tuleb tegutseda vastavalt vajadusele ja proportsionaalsuse põhimõttele.

67. Järgmiseks etapiks on kasulik määratleda ootused, millele seadusandja peab RFID valdkonnas vastama:

— õigusaktid peavad olema paindlikud ning jätma ruumi innovatsioonile ja tehnoloogia arengule. See peaks andma meile tehnoloogia suhtes piisavalt neutraalsed õigusaktid;

— teiseks peaks õigusaktid andma õiguskindluse. See peaks andma meile piisavalt spetsiifilised õigusaktid. Sidusrühmad peavad täpselt teadma, kuidas nende käitumist reguleeritakse;

— kolmandaks, peavad õigusaktid kaitsma tõhusalt kõiki õigustatud huvisid. See nõuab igal juhul õigusaktide jõustamist ja selget määratlemist: missugune osapool vastutab millise käitumise eest ([3])? Nimetatud nõuded on veelgi olulisemad, kui kaalul on eraelu puutumatus ja andmekaitse, üksikisikute põhiõigused inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni ja Euroopa Liidu põhiõiguste harta kohaselt.

**Andmekaitseinspektori arvamus**

68. Andmekaitseinspektorile on selge, et Euroopa seadusandja ei peaks reageerima kõikidele tehnoloogilistele arengutele. Tehnoloogilised arengud võivad toimuda kiiresti, kuid õigusakti vastuvõtmine ja jõustumine võtab aega, ja peakski võtma. Õigusakt peaks olema kõikide kaalul olevate huvide tasakaalustamise tulemus. Kui õigusaktiks valitakse direktiiv, on vaja isegi veel rohkem aega, kuna direktiivid tuleb täielikult rakendada liikmesriikide õigussüsteemides.

69. Kuid RFID ei ole lihtsalt üks järjekordne tehnoloogiaarendus, nagu käesolevas arvamuses on juba mitmel korral rõhutatud. Teatises nimetatakse RFID lausa väravaks infoühiskonna uude arenguetappi, mida sageli nimetatakse „asjade Internetiks", ja RFID-kiibid on tehisintellektikeskkondade põhielemendid. Nimetatud keskkonnad on olulised astmed nn järelevalveühiskonna arendamisel ([4]). Seda silmas pidades on RFID valdkonnas õigusakti vastuvõtmine õigustatud. RFID võib tuua kaasa kvalitatiivse muutuse.

([1]) Vt direktiivi 2002/58/EÜ kavandatud uut artiklit 3.
([2]) Arvamus andmekaitsedirektiivi käsitleva teatise kohta, punkt 24.
([3]) Lisada andmekaitset käsitlevasse terminoloogiasse; see hõlmab „vastutava andmetöötleja" määratlust.
([4]) Seda sõnumit korrati Euroopa andmekaitseasutuste avalduses, mis võeti vastu Londonis 2. novembril 2006 ja on kättesaadav andmekaitseinspektori veebisaidil: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Sellest seisukohast lähtudes andmekaitseinspektor soovitab, juhul kui kehtiva õigusliku raamistiku nõuetekohane rakendamine ebaõnnestub, kaaluda ühenduse sellise õigusakti (ettepaneku) vastuvõtmist, millega reguleeritakse RFID kasutamise põhilisi küsimusi asjaomastes valdkondades. Sellist õigusakti tuleb pärast selle jõustumist pidada *lex specialis*'eks võrreldes üldise andmekaitsealase raamistikuga.

71. Sellise õigusakti vastuvõtmisel võivad olla järgmised eelised:

— õigusakt võiks sätestada eneseregulatsioonimehhanismidele põhiparameetrid;

— õigusakti vastuvõtmise perspektiiv võib olla sidusrühmadele ajendiks korralikku kaitset pakkuvate eneseregulatsioonimehhanismide loomiseks.

72. Veelgi praktilisemalt, komisjonilt võiks paluda eriõigusakti poolt- ja vastuargumente ning sellise õigusakti põhielemente käsitleva nõuandedokumendi ettevalmistamist. Loomulikult tuleks paluda sidusrühmade panust sellesse nõuandedokumenti. Samuti tuleks kaasata artikli 29 töörühm.

**Võimalik kord**

73. Seadusandja sekkumine peaks andma sektori eripära arvesse võtva õigusraamistiku, mis koosneb reguleerimisvahenditest, mis täpsustavad ja täiendavad kehtivat õigusraamistikku. See sektori eripära arvesse võttev õigusraamistik peaks tuginema andmekaitse tuntud põhimõtetel ja keskenduma vastutuse jagunemisele ja kontrollimehhanismi tõhususele.

74. Sektori eripära arvesse võtvat õigusakti on vaja selleks, et kõikide RFID-rakendustega ei kaasne isikuandmete töötlemine. Teisisõnu, kui RFID-rakendustega ei kaasne isikuandmete töötlemine, ei ole RFID kasutavate toodete tootmise ja müügiga seotud osapooled õiguslikult kohustatud rakendama tehnoloogilisi meetmeid, mis väldiksid pealtkuulamist või kiibilugejate ülesseadmist ilma inimesi asjakohaselt teavitamata. Nagu näidatud, on ka selliste RFID-rakenduste juures olemas ohud eraelu puutumatusele seoses inimeste võimaliku jälgimisega, mis nõuavad samasuguseid kaitsemeetmeid eraelu puutumatuse tagamiseks. Täpsemalt, selline olukord võib tekkida tarbekaupade müügieelse kiibistamisega. Kokkuvõtteks võivad RFID-rakendused, mis ei töötle isikuandmeid, siiski ohustada üksikisikute eraelu puutumatust, kuna need võimaldavad varjatud jälgimist ja andmete kasutamist lubamatutel eesmärkidel.

75. Andmekaitseinspektor leiab, et sellist ebasoovitavat tulemust tuleb vältida. Kuna kehtivad õigusaktid osaliselt — vähemalt nende RFID-rakenduste osas, mis ei töötle isikuandmeid — ei suuda võidelda eraelu puutumatusele tuleneva ohuga, ja võttes arvesse mittesiduvate õigusaktide puudusi, on rahuldavate tulemuste saamiseks vaja arvatavasti kasutada siduvaid õigusakte.

76. Sellised meetmed peaks igal juhul:

— sätestama osalemispõhimõtte müügihetkel, mis on täpne ja vaieldamatu õiguslik kohustus, samuti nende RFID-rakenduste suhtes, mis ei kuulu andmekaitsedirektiivi reguleerimisalasse ([1]);

— tagama, et RFID-rakenduste juures oleks kohustuslik rakendada asjakohaseid tehnilisi lahendusi või „eraelu kavandatud puutumatuse" kontseptsiooni.

## VII. **HALDAMINE**

77. Kuigi RFID-süsteemidele olemuslikku piiriülest mõõdet vaadeldakse teatises vaid siseturu ulatuses, leiab andmekaitseinspektor, et seda mõõdet tuleks käsitleda laiemal rahvusvahelisel tasandil. Poes on RFID-süsteemid juba piiriülesed, kuna kiipi ei pruugita müügihetkel välja deaktiveerida. Üleüldise RFID-süsteemi tasemel muutuvad need tehnoloogiad piiriüleseks, sest isikuandmete edastamine kolmandasse riiki võib toimuda siis, kui RFID-süsteemi kuuluva kiibistatud toote tootja asub väljaspool Euroopa Liitu ([2]).

78. Pikemas perspektiivis on oodata, et Euroopa andmekaitse õigusliku raamistiku jõustamise kriitiliseks valdkonnaks saab RFID-identiteedi võrdlusandmebaaside haldamine. Andmekaitseinspektor nõuab tungivalt lahenduse leidmist, kuna nimetatud raamistiku edasine nõrgestamine pole vastuvõetav.

79. Andmekaitseinspektor leiab, et RFID haldamise küsimus on suur probleem, mis nõuab märkimisväärseid investeeringuid. Tuleb leida sobiv läbirääkimisfoorum ja kõige parem haldusinfrastruktuur, et tagada andmekaitseõiguste nõuetekohane austamine nimetatud rahvusvahelises keskkonnas.

([1]) IV peatükis väidetakse, et „teabe soovimise" põhimõte müügihetkel on juba kehtiv õiguslik kohustus vastavalt andmekaitsedirektiivile.

([2]) Isikuandmete edastamisega seotud kohustusi käsitletakse andmekaitsedirektiivi artiklites 25 ja 26.

80. Sellega seoses kutsub andmekaitseinspektor komisjoni üles esitama oma vaated haldamise küsimuses, võimaluse korral konsulteerides RFID-sidusrühmaga.

## VIII. **JÄRELDUS**

81. Andmekaitseinspektor tervitab komisjoni teatist RFID kohta, kuna see käsitleb põhilisi RFID-tehnoloogia kasutamisega seotud küsimusi, võttes arvesse otsustavad eraelu puutumatuse ja andmekaitse küsimused. Ta on nõus seisukohaga, et RFID-süsteem võiks täita põhilist rolli tavaliselt „asjade Internetiks" nimetatava infoühiskonna arendamisel.

### Tagajärgede selgitamine

82. RFID-tehnoloogia laiaulatuslik kasutamine on täiesti uus nähtus ja sellel võib olla põhjalik mõju meie ühiskonnale ja põhiõiguste kaitsele meie ühiskonnas, näiteks eraelu puutumatusele ja andmekaitsele. RFID võib tuua kaasa kvalitatiivse muutuse.

83. Võimalik on eristada viit peamist eraelu puutumatuse ja turvalisuse küsimust:

— isiku tuvastamine;

— vastutava(te) andmetöötleja(te) tuvastamine;

— era- ja avaliku sfääri traditsioonilise eristamise vähenemine;

— RFID-kiipide mõõtmete ja füüsikaliste omaduste mõju;

— andmetöötlusega seotud läbipaistvuse puudumine.

### Tagajärgede määratlemine/tuvastamine

84. Direktiivis 95/46/EÜ sätestatud andmekaitse üldist õigusraamistikku kohaldatakse RFIDi suhtes, kuna RFID-süsteemide abil töödeldud andmed vastavad isikuandmete määratlusele.

85. E-privaatsuse direktiivi suhtes: komisjoni 13. novembri 2007. aasta ettepanek direktiivi muutmise kohta sisaldab sätet, mille eesmärk on täpsustada, et direktiivi kohaldatakse teatud RFID-rakenduste suhtes. Kuid mõned muud RFID-rakendused ei ole võib-olla hõlmatud, kuna nimetatud direktiivi kohaldatakse ainult isikuandmete sellise töötlemise suhtes, mis toimub seoses üldkasutatavate elektrooniliste sideteenuste osutamisega üldkasutatavates sidevõrkudes.

86. Isikuandmeid on võimalik täiendavalt kaitsta mitmete eneseregulatsiooni vahenditega. Asjakohane on jätta ruumi eneseregulatsiooniks, tingimusel et see:

— annab konkreetseid ja praktilisi juhiseid konkreetsete RFID-rakenduste tüüpide kohta;

— käsitleb konkreetseid andmekaitsega seotud küsimusi ja probleeme, mis esinevad seoses üldiste RFID-rakendustega;

— aitab kaasa andmekaitsedirektiivi ühetaolisele ja ühtlustatud rakendamisele kogu ELis;

— ja seda rakendavad kõik asjaomased sidusrühmad.

87. Andmekaitseinspektor soovitab komisjonil tihedas koostöös RFID eksperdirühmaga koostada üks või mitu dokumenti, milles esitatakse selge juhis kehtiva õigusraamistiku kohaldamiseks RFID-keskkonnas.

88. Juhis, mis sätestab RFID kasutamise põhimõtted, peaks olema piisavalt keskendunud ja rakendama valdkondlikku lähenemisviisi. Juhis peaks soovitama praktilisi ja tõhusaid meetodeid selliste tehnoloogiate ja standardite väljatöötamiseks, mis võiksid aidata kaasa RFID-süsteemide vastavusele andmekaitse õigusraamistikuga ja millega kaasneb „eraelu kavandatud puutumatuse" tehnoloogia kasutamine.

89. Andmekaitseinspektor tervitab komisjoni teatises võetud lähenemisviisi kiita heaks eelprojekteerimiskriteeriumide kindlaksmääramise ja kinnitamise idee.

90. Kuigi andmekaitseinspektor leiab, et osalemispõhimõte müügihetkel on enamikul juhtudel juba kehtiv õiguslik kohustus vastavalt andmekaitsedirektiivile, tuleks seda kohustust eneseregulatsiooni vahendites täpsustada.

### Kas on vaja konkreetseid meetmeid?

91. Selleks et teha „kavandatud puutumatuse" kontseptsiooni kasutamine kohustuslikuks, soovitab andmekaitseinspektor komisjonil rakendada direktiivi 1999/5/EÜ artikli 3 lõike 3 punkti c mehhanismi, konsulteerides RFID eksperdirühmaga.

92. Juhul kui kehtiva õigusliku raamistiku nõuetekohane rakendamine ei anna piisavaid tulemusi, soovitab andmekaitseinspektor kaaluda ühenduse sellise õigusakti (ettepaneku) vastuvõtmist, millega reguleeritakse RFID kasutamise põhilisi küsimusi asjaomastes valdkondades. Sellist õigusakti tuleb pärast selle jõustumist pidada *lex specialis*'eks võrreldes üldise andmekaitsealase raamistikuga. Nimetatud õigusakt peaks käsitlema eraelu puutumatuse ja andmekaitse probleeme, mis tekivad seoses mõnede RFID-rakendustega, näiteks kaupade müügieelse kiibistamisega, mis ei pruugi tingimata sisaldada isikuandmete töötlemist.

93. Komisjon võiks valmistada ette nõuandedokumendi, mis käsitleb eriõigusakti poolt- ja vastuargumente ning sellise õigusakti põhielemente.

94. Seadusandja peaks looma sektori eripära arvesse võtva õigusraamistiku, mis koosneb reguleerimisvahenditest, mis täpsustavad ja täiendavad kehtivaid õigusakte. Meetmed peaks igal juhul:

— sätestama osalemispõhimõtte rakendamise müügihetkel täpse ja vaieldamatu õigusliku kohustusena ka nende RFID-rakenduste suhtes, mis ei kuulu andmekaitsedirektiivi reguleerimisalasse ([1]);

— tagama, et RFID-rakenduste juures oleks kohustuslik rakendada asjakohaseid tehnilisi lahendusi või „eraelu kavandatud puutumatuse" kontseptsiooni.

**Haldamine**

95. Andmekaitseinspektor kutsub komisjoni üles esitama oma vaated haldamise küsimuses, võimaluse korral konsulteerides RFID-sidusrühmaga.

Brüssel, 20. detsember 2007

Peter HUSTINX

*Euroopa andmekaitseinspektor*

([1]) IV peatükis väidetakse, et „teabe soovimise" põhimõte müügihetkel on juba kehtiv õiguslik kohustus vastavalt andmekaitsedirektiivile.