Radiotaajuustunnistusteknologiaan (RFID) liittyvät tietosuojaongelmat

Lapin yliopisto
Oikeustieteiden tiedekunta
Oikeusinformatiikan tutkielma
Tero Kankaanpää
Kevät 2006

I TIIVISTELMÄ

Lapin yliopisto, oikeustieteiden tiedekunta
Työn nimi: Radiotaajuustunnistusteknologiaan (RFID) liittyvät tietosuojaongelmat.
Tekijä: Kankaanpää, Tero
Opintokokonaisuus ja oppiaine: OTK
Työn laji: Oikeusinformatiikan oppiaineeseen kuuluva syventävien aineiden tutkielma
Sivumäärä: XIX + 89 s.
Vuosi: Kevät 2006

Tutkielmani käsittelee radiotaajuustunnistusteknologiaan liittyviä tietosuojaongelmia. RFID *(Radio Frequency Identification*) eli radiotaajuinen etätunnistus on menetelmä tiedon etälukuun käyttäen RFID-tunnisteita. RFID-teknologia tarjoaa lukuisia hyödyntämismahdollisuuksia liike-elämälle, yksityisille ihmisille ja julkisille palveluille. Kuten moniin muihinkin uusiin teknologioihin, myös RFID-teknologiaan, liittyy tiettyjä haittapuolia. Näistä haittapuolista ovat vahvimmin nousseet esiin tekniikkaan liittyvät yksityisyyden suoja- ja tietosuojakysymykset. Tutkimustehtävänäni oli selvittää, millaisia mahdollisia tietosuojaongelmia RFID-teknologian sovelluksiin sisältyy ja miten näiden ongelmien aktualisoituminen voidaan välttää. Lisäksi pyrin selvittämään, miten Euroopan unionin ja Suomen lainsäädäntöjä tulee soveltaa RFID-sovelluksiin.

Myös Euroopan unionissa on havahduttu kyseisiin haittapuoliin. Henkilötietodirektiivin (95/46/EC) artiklan 29 nojalla perustettu tietosuojatyöryhmä julkaisi keväällä 2005 työasiakirjan koskien RFID-tunnistukseen liittyviä tietosuojakysymyksiä. Työasiakirjassa mainitaan, että RFID-tekniikan potentiaalisia väärinkäyttäjiä ovat mm. yritykset ja valtiot. Tietosuojatyöryhmän mukaan RFID-teknologian herättämiä yksityisyyteen liittyviä kysymyksiä ovat esimerkiksi mahdollisuus kerätä salaa erilaisia tietoja yksityishenkilöistä, mahdollisuus seurata ihmisiä heidän liikkuessaan julkisilla paikoilla, mahdollisuus lukea tietoja asiakkaiden kantamista vaatteista, varusteista ja esimerkiksi lääkkeistä sekä kauppojen tarkennetut ostajaprofiilit. Tietosuojatyöryhmä asetti työasiakirjansa julkisesti kommentoitavaksi.

Tutkielmassa edetään radiotaajuustunnistuksen tekniikan sekä yksityisyyden suojan ja henkilötietojen suojan yleiskuvausten kautta radiotaajuustunnistukseen liittyviin erityisiin yksityisyydensuoja- ja tietosuojakysymyksiin. Näitä kysymyksiä lähestytään tietosuojatyöryhmän keväällä 2005 julkaiseman työasiakirjan ja siihen saatujen lausuntojen valossa. Tietosuojatyöryhmä ja monet lausunnonantajat olivat erimielisiä siitä, milloin RFID-järjestelmissä käsitellään henkilötietoja henkilötietodirektiivin valossa. Lisäksi erimielisyyttä aiheutti henkilötieto-käsitteen määrittely. Alan toimijat kritisoivat lisäksi tietosuojatyöryhmän luomia skenaarioita, joiden toteutuminen ei ainakaan vielä ole heidän mielestään teknisesti mahdollista.

Tutkielmassani päädyin siihen, että alan ollessa vielä erittäin nopeassa kehitysvaiheessa, on tärkeämpää antaa ohjeita alan toimijoille nykyisen tietosuojalainsäädännön soveltamisesta RFID-tekniikkaan kuin antaa vielä tässä vaiheessa erillislainsäätöä. Katson, että tietosuojatyöryhmän tulee kuitenkin seurata alan kehitystä aktiivisesti, antaa lisäohjeistusta sekä olla valmiina tarvittaessa käyttämään järeämpiä keinoja unionin kansalaisten yksityisyyden suojan takaamiseksi.

Asiasanat: henkilötieto, radiotaajuustunnistus, RFID, tietosuoja, yksityisyyden suoja

SISÄLLYS

LÄHTEET

Virallislähteet

Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja niiden tietojen vapaasta liikkuvuudesta *(henkilötietoasetus)*

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta *(henkilötieto- tai tietosuojadirektiivi)*

HE 49/1986 vp hallituksen esitys henkilörekisterilaiksi ja siihen liittyviksi laeiksi

HE 309/1993 vp hallituksen esitys perustuslakien perusoikeussäännösten muuttamisesta

HE 96/1998 vp hallituksen esitys henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi

HE 184/1999 vp hallituksen esitys yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi

HE 26/2001 vp hallituksen esitys laiksi henkilötietojen käsittelystä rangaistusten täytäntöönpanossa

KM 1992:3 perusoikeuskomitean mietintö

PeVL 4/1986 vp hallituksen esitys henkilörekisterilaiksi ja siihen liittyviksi laeiksi

PeVL 25/1998 vp hallituksen esitys henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi

PeVM 25/1994 perustuslakivaliokunnan mietintö n:o 25 hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta

SopS 7-8/1976 Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus *(108/1976, KP-sopimus)*

SopS 19/1990 Euroopan ihmisoikeussopimus. *(439/1990)*

Työasiakirja WP 105: Working document on data protection issues related to RFID technology (2005). Article 29 Data Protection Working Party. Saatavissa internetissä: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Viestintäviraston määräys (15V/2005 M) luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä. Saatavissa internetissä: http://www.ficora.fi/suomi/document/Viestintavirasto15V2005M.pdf

Kirjat ja artikkelit

Aarnio, Reijo (2003). *Mitä yksityisyys on?* Artikkeli julkaisussa *Tietosuoja 1/2003*, s. 10-13.

Blume, Peter (2001). *Introduction.* Teoksessa: Blume, Peter (toim.). *Nordic Data Protection Law.* Uppsala: Iustus.

Juels, Ari & Rivest, Ronald L & Szydlo Michael. *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy.*

Jyränki, Antero (2000). *Uusi perustuslakimme.* Turku: Iura Nova.

Järvinen, Petteri (2002). *Tietoturva & Yksityisyys.* Porvoo: Docendo Finland Oy.

Konstari, Timo (1992). *Henkilörekisterilaki. Säännökset ja käytäntö.* Helsinki: Lakimiesliiton kustannus.

Korhonen, Rauno (2003). *Perusrekisterit ja tietosuoja.* Helsinki: Edita.

Lehtonen, Lasse (2001). *Potilaan yksityisyyden suoja.* Vammala: Suomalainen Lakimiesyhdistys.

Länsineva, Pekka (1998). *Perusoikeudet – nyt.* Teoksessa Länsineva, Pekka – Viljanen, Veli-Pekka (toim.). *Perusoikeuspuheenvuoroja.* Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. Julkisoikeuden sarja A N:o 32. Turku: Turun yliopisto.

Nieminen, Liisa (1999). *Yksityiselämän ja perhe-elämän suoja perusoikeutena.* Teoksessa Nieminen, Liisa (toim.). *Perusoikeudet Suomessa.* Helsinki: Kauppakaari.

Nyyssölä, Mikko (2001). *Yksityisyyden suoja työsuhteessa.* Helsinki: WSOY.

Ojanen, Tuomas (2003). *Perusoikeudet ja ihmisoikeudet Suomessa.* Helsinki: Helsingin yliopiston oikeustieteellinen tiedekunta.

Ollila, Riitta (2001). *Freedom of Speech and Protection of Privacy in Convergence of Electronic Communications.* Rovaniemi: Lapin yliopisto.

Ollila, Riitta (2002). *Henkilötietojen vapaa liikkuvuus ja viestintä.* Teoksessa Kulla ym.: Viestintäoikeus. Vantaa: WSOY.

Pölönen, Pasi (1997). *Salaiset pakkokeinot.* Helsinki: Lakimiesliiton kustannus.

Pellonpää, Matti (2000). *Euroopan ihmisoikeussopimus.* Helsinki: Talentum.

Raatikainen, Ari (2002). *Yksityisyyden suoja työelämässä.* Helsinki: Edita.

Rautio, Ilkka (2002). *RL 38: Tieto- ja viestintärikokset.* Teoksessa Heinonen, Olavi – Koskinen, Pekka – Lappi-Seppälä, Tapio – Majanen ,Martti – Nuotio, Kimmo – Nuutila, Ari-Matti– Rautio, Ilkka: *Rikosoikeus*. Helsinki: WSOY.

Saraviita, Ilkka (2000). *Perustuslaki 2000.* Helsinki: Kauppakaari.

Saarenpää, Ahti (2002). *Yksityisyys, yksityiselämä, yksilön suoja – yksityisyyden käsitteellistä kuvausta.* Teoksessa Haavisto, Risto (toim.): *Professori Kyösti Holman juhlakirja* 11.6.2002, s. 313-337. Rovaniemi: Lapin yliopisto.

Saarenpää, Ahti (2005). *Henkilö- ja persoonallisuusoikeus.* Teoksessa Haavisto, Risto (toim.): *Oikeusjärjestys 2000.* Osa III. 3. täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 38. Rovaniemi: Lapin yliopisto. *(Saarenpää 2005a).*

Saarenpää, Ahti (2005). *Oikeusinformatiikka.* Teoksessa Haavisto, Risto (toim.): *Oikeusjärjestys 2000.* Osa I. 4. täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 38. Rovaniemi: Lapin yliopisto. *(Saarenpää 2005b).*

Viljanen, Veli-Pekka (1998). *Perusoikeudet ja rikoslainsäädäntö.* Teoksessa Länsineva, Pekka – Viljanen, Veli-Pekka (toim.): *Perusoikeuspuheenvuoroja.* Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. Julkisoikeuden sarja A N:o 32. Turku: Turun yliopisto.

Viljanen, Veli-Pekka (1999). *Perusoikeuksien soveltamisala.* Teoksessa Hallberg, Pekka – Karapuu, Heikki, Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka: *Perusoikeudet.* Juva: WSLT. *(Viljanen 1999a).*

Viljanen, Veli-Pekka (1999). *Yksittäiset perusoikeudet. Yksityiselämän suoja (PL 10 §).* Teoksessa Hallberg, Pekka – Karapuu, Heikki, Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka: *Perusoikeudet.* Helsinki : Werner Söderström Lakitieto Oy. *(Viljanen 1999b).*

Viljanen, Veli-Pekka (2001): *Perusoikeuksien rajoitusedellytykset.* Helsinki : Werner Söderström Lakitieto Oy.

Viljanen, Veli-Pekka (1996). *Perusoikeusuudistus ja kansainväliset ihmisoikeussopimukset.* Lakimies 5-6/1996 s. 797-798.

Wallin, Anna-Riitta – Nurmi, Pekka (1991). *Tietosuojalainsäädäntö.* Helsinki: Lakimiesliiton kustannus.

Wallin, Anna-Riitta (2001). *Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnustettuina perusoikeuksina.* Teoksessa Nieminen, Liisa (toim.): *Perusoikeudet EU:ssa*. Helsinki: Kauppakaari.

Warren Samuel D. - Brandeis Louis D.: *The Right to Privacy*. Harward Law Review. Vol. IV. December 1890. NO.5., 193-220.

Elektroniset lähteet

Electronic Frontier Finland ry:n kotisivut. http://www.effi.org/. Käyty 19.1.2006.

EPCglobalin kotisivu. http://www.epcglobalinc.org/. Käyty 11.12.2005.

EPCglobal European Working Group. Submission to the Article 29 Working Party in Response to its Working Document 10107/05 WP 105 of January 19, 2005 on Data Protection issues related to RFID Technology *(EPCglobalin lausunto).* Saatavissa internetissä: http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/consultations/rfid_en.htm. Käyty 15.2.2006.

Euroopan komissio (2000). Tietosuoja Euroopan unionissa. Vuoropuhelua kansalaisten ja yritysten kanssa. Luxemburg: Euroopan yhteisöjen virallisten julkaisujen toimisto. Saatavissa internetissä: http://www.eu.int/comm/justice_home/fsj/privacy/docs/guide/guide-finland_fi.pdf. Käyty 16.1.2006.

Euroopan unionin perusoikeuskirjan puheenjohtajiston selitykset, CHARTE 4473/00 CONVENT 49. http://www.europarl.eu.int/charter/pdf/04473_fi.pdf. Käyty 18.1.2006.

European Commission DG Internal Market – Art. 29 Data Protection Working Party Working Document on data protection issues related to RFID technology – WP 105. Response by ICC, EICTA, ICRT and JBCE to the public consultation *(ICC:n EICTA:n, ICRT:n ja JBCE:n lausunto).* Saatavissa internetissä: http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/consultations/rfid_en.htm. Käyty 21.2.2006.

Feldhofer, Martin & Dominikus, Sandra & Wolkerstorfer Johannes. *Strong Authentication for RFID Systems Using the AES Algorithm.* In the Proceedings of the Workshop on Cryptographic Harware and Embedded Systems. CHES August 11-13, 2004, Boston, USA, Lecture Notes in Computer Science (LNCS) Vol. 3156, Springer Verlag, 2004, ISBN 3-540-22666-4, s. 357-370. Saatavissa internetissä: http://www.iaik.tugraz.at/research/publications/2004/CHES2004_AES.htm

FIFAworldcup.com sivuilla oleva tiedote jalkapallon MM-kilpailujen tietosuojasäännöistä. http://fifaworldcup.yahoo.com/06/en/tickets/dpr.html. Käyty 22.4.2006.

Finn-id:n kotisivuilla oleva uutinen. http://www.finn-id.fi/uutisia/uutiset/fi_FI/Uutiset/. Käyty 9.12.2005.

Grant, Hazel (2005). RFID Consultation on WP 105 *(Hazel Grantin lausunto).* Saatavissa internetissä: http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/consultations/rfid_en.htm. Käyty 21.2.2006.

Kaleva. Oulussa tehtiin kännykästä bussilippu. Uutinen 13.12.2005. http://hightechforum.kaleva.fi/index.cfm?alue=10&id5=530323&OpenStory=1&msg=530323&lang=1&secure=0&scs=1. Käyty 10.1.2006.

Kaleva. RFID-teknologiakin saattaa olla virusaltis. Uutinen 16.3.2006. http://hightechforum.kaleva.fi/index.cfm?alue=10&Id1=556427&OpenStory=1&lang=1&scs=1. Käyty 16.3.2006.

Li, Zhekun & Gadh, Rajit &. Prabhu B.S (2004). *Applications of RFID technology and smart parts in manufacturing.* Proceedings of DETC'04: ASME 2004 Design Engineering Technical Conferences and Computers and Information in Engineering Conference September 28-October 2, 2004, Salt Lake City, Utah USA. Saatavissa internetissä: http://wireless.ucla.edu/gadh/pdf/04b.pdf. Käyty 15.1.2006.

Metro Future Storen kotisivu. www.future-store.org. Käyty 10.1.2006.

Network it-week. Uutinen standardeista http://www.networkitweek.co.uk/vnunet/news/2125069/european-standard-won-stop-rfid. Käyty 11.12.2005.

MobileCloakin kotisivut. http://www.mobilecloak.com/. Käyty 14.2.2006.

Muttilainen, Vesa (2006). Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistilastojen tietoja 1990-luvulta ja 2000-luvun alusta. Oikeuspoliittisen tutkimuslaitoksen julkaisuja 218. Saatavissa internetissä: http://www.om.fi/optula/35424.htm Käyty 10.4.2006.

Oikeuspoliittinen tutkimuslaitos (2003). Yleisissä alioikeuksissa rangaistukseen tuomitut rikoslajeittain 1999-2002. Liitetaulukko 6. Saatavissa internetissä: http://www.om.fi/optula/uploads/hd12ms.pdf.

Plichta, Greg (2004). Accommodating RFID Technology and Expectations of Privacy: An Examination and Proposed Guidelines. Electronic Privacy Information Center. Saatavissa internetissä: http://www.epic.org/privacy/rfid/rfidplichta.html. Käyty 15.1.2006.

Resolution on Radio-Frequence Identification, 25th Conference on Data Protection & Privacy Commissioners, Sydney 2003. Saatavissa internetissä: http://www.privacyconference2003.org/commissioners.asp. Käyty 13.2.2006.

RFID Journal. Can Tag Viruses Infect RFID Systems? Uutinen 15.3.2006. http://www.rfidjournal.com/article/articleprint/2201/-1/1/. Käyty 16.3.2006.

RFID Lab Finlandin kotisivu. RFID-tekniikan perusteet. http://www.rfidlab.fi. Käyty 9.12.2005.

RFID Lab Finlandin kotisivuilla oleva uutinen ”UPM Rafsec vauhdittaa UHF RFID-järjestelmien yleistymistä laskemalla uusien tunnistemallien hinnan 0.08 euroon”. http://www.rfidlab.fi/?1;2;300;300;181.html. Julkaistu 17.10.2005. Käyty 23.2.2006.

RFID Lab Finlandin kotisivuilla oleva uutinen ”Pfizer hyödyntää RFID-tekniikkaa tuotteidensa aitouden varmistamisessa”. http://www.rfidlab.fi/?1;2;300;300;213.html Julkaistu 26.1.2006. Käyty 9.2.2006.

RFID Lab Finlandin kotisivuilla oleva uutinen ”RFID-tekniikka tehostaa matkalaukkujen tunnistusta lentokentillä”. http://www.rfidlab.fi/?1;2;300;300;212.html. Julkaistu 26.1.2006. Käyty 9.2.2006.

RFID Lab Finlandin kotisivuilla oleva uutinen ”Gen2 RFID Lab Finlandin testauksessa”. http://www.rfidlab.fi/?1;2;300;300;212.html. Julkaistu 26.1.2006. Käyty 9.2.2006.

RFID-valmistaja Sysgenin kotisivu. http://www.sysgen.com/webdata/Solutions/What_is_RFID/. Käyty 23.2.2006.

Rinta-Runsala, Esa & Tallgren Markus (2004). RFID-tekniikan hyödyntäminen asiakkuudenhallinnassa. Espoo: VTT Tietotekniikka. Saatavissa internetissä: http://www.vtt.fi/tte/datamining/publications/rfid-raportti.pdf. Käyty 17.9.2005.

Saarenpää, Ahti. Näkökulmia yksilön suojasta. 55 teesiä tietosuojasta. Saatavissa internetissä: http://www.ulapland.fi/home/oiffi/julkaisut/teesit.htm. Käyty 20.2.2006.

Sovellusvalmistaja Buscom Oy:n kotisivulla oleva uutinen YTV:n rahastusjärjestelmän käyttöönotosta 20.9.2002. http://www.buscom.fi/suomi/uutiset/1kaupalykort.html. Käyty 14.12.2005.

Statement of the METRO Group in the context of the consultation process “Data Protection Issues Related to RFID Technology” initiated by the Article 29 Data Protection Working Party *(Metro Groupin lausunto)*. Saatavissa internetissä: http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/consultations/rfid_en.htm. Käyty 15.2.2006.

The Register -lehden kotisivulla oleva uutinen Japanin jenien RFID-tunnistuksesta. http://www.theregister.co.uk/2003/07/30/japan_yens_for_rfid_chips/. Käyty 10.1.2006

The Register -lehden kotisivulla oleva uutinen RFID-tunnisteiden käytöstä jalkapallon MM-kilpailuissa. http://www.theregister.co.uk/2005/04/04/world_cup_rfid/. Julkaistu 4.4.2005. Käyty 22.4.2006.

Tietosuojavaltuutetun toimisto (2002). Ota oppaaksi henkilötietolaki. Esite rekisterinpitäjille. Helsinki: Tietosuojavaltuutetun toimisto. Saatavissa internetissä: http://www.tietosuoja.fi/15939.htm. Käyty 23.1.2006.

Tunnistevalmistaja UPM Rafsec:n kotisivu. Lehdistötiedote 29.9.2005. http://www.rafsec.com. Käyty 10.12.2005

Työasiakirja WP 105:een saadut lausunnot ja tiivistelmä lausunnoista: http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/consultations/rfid_en.htm. Käyty 19.1.2006.

USA Today -lehden kotisivuilla oleva uutinen 8.8.2005 elektronisten passien käyttöönotosta Yhdysvalloissa. http://www.usatoday.com/tech/news/2005-08-08-electronic-passports_x.htm. Käyty 10.1.2006.

Valtiovarainministeriön internetsivuilla oleva tietoturvasanasto. http://www.vm.fi/tietoturvasanasto/sisallys.htm. Käyty 14.2.2006.

VeriChip -nimisen yhtiön kotisivu. http://www.verichipcorp.com/. Käyty 10.1.2006.

YTV:n kotisivut. Yleiset matkaehdot Helsingin seudun matkakortin käyttäjälle. http://www.ytv.fi/FIN/liikenne/matkustajan_opas/Matkakortti/Matkakortti/matkaehdot.htm. Käyty 5.4.2006.

Wikipedia. Vapaa tietosanakirja. http://fi.wikipedia.org/wiki/RFID. Käyty 9.12.2005

Luentoja ja haastatteluja

Hämäläinen, Vesa-Pekka (2005). RFID Lab Finlandin projektipäällikkö Vesa-Pekka Hämäläisen haastattelu RFID Lab Finlandin demohuoneessa Vantaalla 7.12.2005.

Kajava, Jorma (2005). Radiotaajuinen tunnistaminen – vanha kenttä mutta uudet haasteet. Esitelmä Tietoturvallisuus ja laki – Rovaniemen VI tietoturvapäivillä 9.11.2005.

Karhu, Juha (2005). Euroopan unionin perusoikeuskirja. Luento Lapin yliopistossa 21.9.2005 järjestetyssä EU:n perustuslakiseminaarissa.

Strömberg, Samuli (2005). UPM Rafsecin Samuli Strömbergin haastattelu yhtiön tiloissa Tampereella 7.12.2005.

Euroopan ihmisoikeustuomioistuimen ratkaisut

Asia 9248/81 Leander v. Sweden, julkaisusarja A 116

Asia 22009/93 Z. v. Finland, julkaisusarja 1997-I

Asia 27798/95 Amann v. Switzerland, julkaisusarja 2000-II

Asia 28341/95 Rotaru v. Romania, julkaisusarja 2000-V

LYHENTEET JA SANASTO

AES	Advanced Encryption Standard. Eräs pitkälle kehittynyt salausalgoritmi eli sarja ohjelmoitavia matemaattisia toimituksia, joita käyttäen tieto salakirjoitetaan tai salakirjoitettu tieto avataan.
Aktiivinen tunniste	Tunniste, jolla on oma virtalähde, jonka avulla se voi lähettää tietoja.
Blocker tag	Tunniste, joka lähettää yhtäjaksoisesti hälysignaalia ja estää siten lukijaa lukemasta mitään lähistöllä olevaa tunnistetta.
Deaktivaattori	RFID-tunnisteen toimimattomaksi tekevä laite (eng. tag disabler).
EASA	European Aviation Safety Agency. Toimii Euroopan unionin ilmailuviranomaisena.
EIOS	Euroopan neuvoston ihmisoikeussopimus (439/1990).
EIT	Euroopan ihmisoikeustuomioistuin.
EPC	Electronic Product Code eli sähköinen tuotekoodi. Koodi, joka identifioi yksittäisen tuotteen. EPC tallennetaan RFID-tunnisteeseen.
EPCglobal	Organisaatio, joka tukee sähköisten tuotekoodien (EPC) käyttöä ja johtaa niiden standardisointia. EAN Internationalin ja Uniform Code Councilin (UCC) yhteishanke.
ETSI	European Telecommunications Standards Institute. ETSI on Eurooppalainen telealan standardisointijärjestö.
Etätunniste	Ks. RFID-tunniste.
Faradayn häkki	Sähköä johtava häkki tai muu yhtenäinen kuori, jonka sisälle sähkömagneettinen säteily ei pääse. Eräs fyysinen keino suojata RFID-tunniste lukutapahtumilta.
Gen2	UHF Generation 2. Uuden sukupolven RFID-tunniste, joka toimii UHF-taajuusalueella.
HE	Hallituksen esitys.
Henkilötietoasetus	Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja niiden tietojen

	vapaasta liikkuvuudesta, joka täydentää henkilötietodirektiiviä.
Henkilötietodirektiivi	Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Epävirallisemmissa yhteyksissä henkilötietodirektiiviä kutsutaan myös tietosuojadirektiiviksi.
HenkRekL	Henkilörekisterilaki (471/1987).
HetiL	Henkilötietolaki (523/1999).
HF	High Frequency -taajuusalue, käytännössä 13,56 MHz .
IATA	International Air Transport Association eli kansainvälinen ilmakuljetusliitto.
ICAO	International Civil Aviation Organization eli kansainvälinen siviili-ilmailujärjestö. ICAO on Yhdistyneiden kansakuntien alainen yhteistyöjärjestö.
JulkL	Laki viranomaisten toiminnan julkisuudesta (621/1999) eli julkisuuslaki.
Kill-komento	Tunnetuin ja käytetyin ratkaisu estää RFID-tunnisteen myöhempi lukeminen. Kill-komento on lopullinen ja se tehdään erityisellä tunnisteen tietosisällön tuhoavalla laitteella.
KP-sopimus	Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (108/1976).
LF	Low Frequency -taajuusalue, alle 135 kHz.
Lukija	Laite, joka pystyy lukemaan tunnisteen tietosisällön. Lukija lähettää signaalin, jonka havaitessaan tunniste lähettää tietosisältönsä lukijalle.
Lukijatörmäys	Tilanne, jossa useampi lukija häiritsee toisiaan siten, että se vaikeuttaa tunnisteiden lukemista.
MAC	Message Authentication Code. ISO 8731-1 standardin mukaisesti symmetrisellä salauksella tuotettu varmiste.
Mikrotaajuusalue	Korkein taajuusalue, käytännössä 2,45 Ghz.
OECD	Organization for Economic Cooperation and Development. Taloudellisen yhteistyön ja kehityksen järjestö, jonka tehtävänä on harmonisoida ja kehittää jäsenmaiden yhteiskunnallista hyvinvointia.

Ohjelmistolukko	Eräs tapa tehdä RFID-tunniste toimimattomaksi tilapäisesti.
ONS	Object Name Service eli nimipalvelin. ONS:n tarkoituksena on EPC-järjestelmässä kertoa tuotteen tarkemmat tiedot sisältävän palvelimen IP-osoite.
Passiivinen tunniste	Tunniste, jolla ei ole omaa virtalähdettä. Passiivinen tunniste käyttää lukijan lähettämästä signaalista saamaansa virtaa lähettäessään tietojaan takaisin lukijalle.
PeL	Suomen Perustuslaki (731/1999).
PeVL	Perustuslakivaliokunnan lausunto.
PeVM	Perustuslakivaliokunnan mietintö.
Piktogrammi	Kuvamerkki tai kuvasymboli, jolla on erityinen sovittu merkitys. Piktogrammit ovat yksi tapa tiedottaa kuluttajaa RFID-tunnisteiden lukutapahtumasta.
RFID	Radio Frequency Identification. Tekniikka, jossa esineeseen kiinnitetty tunniste voidaan havaita, lukea ja/tai kirjoittaa sähkömagneettisten aaltojen välityksellä ilman lukijan ja tunnisteen välistä näköyhteyttä.
RFID-tunniste	Tunniste, joka kiinnitetään esineeseen ja joka voidaan havaita, lukea ja joissain tapauksissa myös kirjoittaa ilman näköyhteyttä lukijan ja tunnisteen välillä.
RL	Rikoslaki (39/1889).
RSA	Rivest-Shamir-Adelman algorithm. Eräs epäsymmetrinen salausalgoritmi, jossa avaimen pituudella ei ole ylärajaa.
Semi-passiivinen tunniste	Tunniste, jolla on oma virtalähde, mutta joka käyttää sitä ainoastaan lähettäessään tunnisteen tietoja lukijan pyynnöstä.
Taajuus	Tunniste ja lukija viestivät keskenään tietyllä taajuudella. Tunnisteen ominaisuudet riippuvat käytetystä viestintätaajuudesta.
Tag disabler	Ks. deaktivaattori.
Tagi	Ks. RFID-tunniste.
Tietosuojadirektiivi	Ks. henkilötietodirektiivi.
Tietosuojasopimus	Euroopan neuvoston yleissopimus nro 108 yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä.
Tunniste	Ks. RFID-tunniste.

Tunnistetörmäys	Tilanne, jossa useampi tunniste häiritsee toisiaan niin, ettei niiden tietoja pystystä lukemaan.
UCC	the Uniform Code Council.
UHF	Ultra High Frequency, taajuusalue 860-930 MHz.
UPC	Universal Product Code. Viivakoodi.
YTV	Pääkaupunkiseudun yhteistyövaltuuskunta.

1. Johdanto

RFID (*Radio Frequency Identification*) on yleisnimitys etätunnistusteknologialle, joka toimii radiotaajuuksilla. Kuten tästäkin tutkimuksesta jäljempänä käy ilmi, RFID-teknologian sovellusmahdollisuudet ovat varsin monipuoliset. Samalla kun teknologian tarjoamat hyödyt liike-elämälle, yksityisille ihmisille ja julkisille palveluille näyttävät selviltä ja sovellukset ovat vähitellen tulossa näkyväksi osaksi jokapäiväistä elämäämme, myös teknologiaan liittyviä haittapuolia ollaan vähitellen havaitsemassa.

Myös Euroopan unionissa teknologian haitat on jo havaittu. Henkilötietodirektiivin (95/46/EC) artiklan 29 nojalla perustettu tietosuojatyöryhmä julkaisi keväällä 2005 työasiakirjan koskien RFID-tunnistukseen liittyviä tietosuojakysymyksiä.[1] Tietosuojatyöryhmä kiinnitti huomionsa siihen, että tätä tekniikkaa voidaan käyttää myös siten, että se loukkaa ihmisoikeuksia ja erityisesti yksityisyyden suojaa. Tietosuojatyöryhmä asetti työasiakirjansa julkisesti kommentoitavaksi ja lausuntoja saatiin määräaikaan mennessä kaikkiaan 34.

Tämän tutkielman lähtökohtana on edellä mainittu työasiakirja ja siihen laaditut kommentit. Tutkimustehtävänäni on selvittää, millaisia mahdollisia tietosuojaongelmia RFID-teknologian sovelluksiin sisältyy ja miten näiden ongelmien aktualisoituminen voidaan välttää. Lisäksi pyrin selvittämään, miten Euroopan unionin ja Suomen tietosuojalainsäädäntöjä sovelletaan RFID-teknologiaan, ja onko RFID:ta koskevalle erillislainsäädännölle tarvetta.

[1] Työasiakirja WP 105

2. Yleiskatsaus radiotaajuustunnistuksen tekniikkaan

Tämän kappaleen tavoitteena on luoda välttämätön yleiskatsaus radiotaajuustunnistuksen tekniikkaan. Tässä kappaleessa luodaan perusteet tekniikkaan liittyvien tietosuojaongelmien käsittelylle. Tarkoituksena on kuitenkin pitää tekninen osuus mahdollisimman suppeana, koska kyseessä on oikeustieteellinen tutkielma.

Radiotaajuustunnistuksen historian voidaan nähdä juontavan juurensa 14 miljardin vuoden takaiseen alkuräjähdykseen. Nykytietämyksen mukaan elektromagneettinen energia, joka toimii RFID-teknologian perustana, syntyi alkuräjähdyksessä.[2] Ensimmäisiä tunnettuja RFID-sovelluksia olivat Britannian toisessa maailmansodassa käyttämät järjestelmät, joilla kyettiin erottelemaan saapuvat brittikoneet saksalaisista.[3] Harry Stockman ennusti tutkimuksessaan *"Communication by Means of Reflected Power"* vuonna 1948, että on tehtävä huomattavaa tutkimus- ja kehitystyötä, ennen kuin jäljellä olevat perustavanlaatuiset ongelmat *"heijastetun käyttöjännitteen"* kommunikaatiossa on ratkaistu, ja ennen kuin sovellusten vaatima perustekniikka on hallussa. Tämä veikin lopulta kolmekymmentä vuotta, ja siihen vaadittiin teknisiä harppauksia monilla muillakin aloilla.[4]

RFID on siis tekniikka radioaaltojen välityksellä tapahtuvaan tunnistamiseen. Tunnistukseen tarvitaan kaksi osapuolta: tunniste eli tagi ja lukijalaite. Tunnistustilanteessa lukija lähettää antenninsa kautta signaalin, jolla se pyytää lähellä olevia tunnisteita lähettämään tietonsa lukijalle. Tunniste vastaanottaa signaalin oman pienen antenninsa kautta. Tämän jälkeen tunniste hakee mikrosiruunsa tallennetut tiedot ja lähettää ne antenninsa avulla edelleen lukijalle. Lukija vastaanottaa tunnisteen lähettämät tiedot ja tunnistaa niiden perusteella, mistä tunnisteesta on kyse. Tunnistetietojen lisäksi tunnisteessa voi olla tallennettuna mitä tahansa muuta tietoa ja joidenkin tunnistetyyppien tapauksessa tuota tietoa voidaan tarvittaessa myös uudelleenkirjoittaa etänä.[5]

RFID-tunniste voi olla tunnistettavaan kohteeseen kiinnitettävä tarra, kortti, lappu, nappi, implantti, tms., joka sisältää antennin ja sirun, jossa tietoa säilytetään.

[2] Plichta 2004
[3] Kajava 2005
[4] http://www.sysgen.com/webdata/Solutions/What_is_RFID/
[5] Rinta-Runsala & Tallgren 2004, s. 8

Normaalisti tunniste sisältää kiinteän sarjanumeron ja standardista riippuvan määrän vapaata kirjoitustilaa. Tunniste voidaan sisällyttää tuotteeseen jo valmistusvaiheessa tai kiinnittää tuotteeseen jälkikäteen. RFID-järjestelmien idea on yksinkertainen: kiinnitä RFID-tunniste haluttuun kohteeseen, lue ja kirjoita tietoa tunnisteeseen RFID-lukijalla, ja käytä tietoa hyväksesi taustajärjestelmän avulla.[6]

2.1. RFID-tunnisteiden tyypit ja ominaisuudet

Radiotaajuustunnisteet voidaan jakaa erilaisiin ryhmiin niiden fyysisten ja teknisten ominaisuuksien perusteella. Fyysisiä ominaisuuksia ovat mm. taajuus ja sen tuomat rajoitukset sekä tunnisteen koko. Teknisiä ominaisuuksia ovat mm. aktiivisuus/passiivisuus, luettavuus/kirjoitettavuus ja muistin koko. Jokainen näistä ominaisuuksista tuo omat piirteensä tunnisteiden käyttöön.[7] Seuraavaksi esittelen lyhyesti eri ominaisuuksien tuomia mahdollisuuksia ja rajoituksia.

2.1.1. Taajuus

Tunniste ja lukija viestivät siis keskenään radioaaltojen välityksellä. Tunniste ja lukija kykenevät olemaan yhteydessä toisiinsa ilman suoraa näköyhteyttä, koska radioaallot läpäisevät kiinteän aineen paremmin kuin näkyvä valo. Tämä on merkittävä ero verrattuna viivakoodeihin, jotka tunnetusti vaativat aina suoran näköyhteyden koodin ja lukijan välille.[8]

Tunniste ja lukija on suunniteltu keskustelemaan keskenään radioteitse juuri tietyllä taajuudella. Erilaisiin käyttötarkoituksiin valmistetaan eri taajuuksia käyttäviä tunnisteita. Maailmalla on käytössä neljä eri taajuusaluetta: 1) Low Frequency -taajuusalue (alle 135 kHz), 2) High Frequency -taajuusalue (käytännössä 13 MHz), 3) Ultra High Frequency -taajuusalue (860-930 MHz), sekä 4) mikroaaltotaajuusalue (käytännössä 2,45 Ghz). Kullakin näistä taajuusalueista on omat erityispiirteensä, jotka vaikuttavat mm. lukuetäisyyteen ja läpäisykykyyn. Eri taajuusalueiden erityispiirteet käyvät ilmi alla olevasta taulukosta (taulukko 1). Sekä tunnisteessa että lukijassa

[6] www.rfidlab.fi
[7] Rinta-Runsala & Tallgren 2004, s. 8
[8] Rinta-Runsala & Tallgren 2004, s. 8

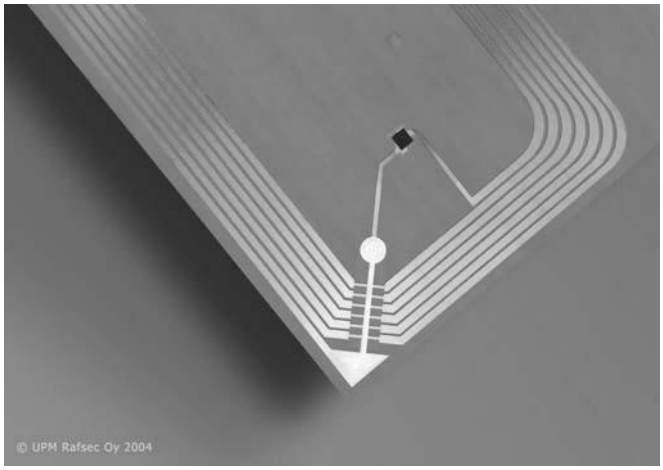
tarvittavan antennin koko riippuu käytetystä taajuudesta, ja tämä rajoittaa mahdollisuuksia pienentää sekä tunnisteen että lukijan fyysistä kokoa.[9]

Taulukko 1. Eri taajuudella toimivien RFID-tunnisteiden ominaisuuksia.

Taajuusalue	Lukuetäisyys	Käyttö	Mahdollisuudet	Rajoitteita
LF: Alle 135 khz.	Erittäin lyhyt.	Varkaudenestojärjes-telmät, kulunvalvonta, eläinten tunnistus.	Toimii metallin läheisyydessä.	Lukuetäisyys.
HF: 13,56 MHz.	Lyhyt, käytännössä parhaimmillaan 1,5 m.	Matkakortti-, kirjasto-, kulunvalvonta- ja teollisuuslogistiikka-sovellukset.	Laajasti käytetty tekniikka. Monenlaisia tunnisteita saatavissa.	Lyhyt lukuetäisyys. Tunnisteen pienentäminen rajoitettua. Ei toimi metallin lähellä.
UHF: 860-930 MHz.	Maksimissaan noin 5 metriä.	EPC koodien taajuus ja sitä kautta tulossa jakeluketjujen hallintaan. EPC mahdollistaa myös 13,56 MHz käytön.	Pitkä lukuetäisyys, kasvava kaupallinen käyttö.	Vaimenee vedessä tai vettä sisältävässä aineessa. Ei yhtä maailmanlaajuista standarditaajuutta.
Mikrotaajuus-alue: 2,45 GHz.	Maksimissaan noin 5 metriä.	Ajoneuvojen etätunnistus.	Erittäin pienikokoinen tunniste. Lukija esim. kännyköihin.	Vaimenee nopeasti vedessä tai vettä sisältävissä aineissa.

Eri taajuusalueilla lukutapahtumassa käytettävä fysikaalinen mekanismi on erilainen. LF- ja HF-tunnisteissa on nähtävissä yleensä kuparisia silmukoita, jotka muodostavat käämin ja toimivat tunnisteen "antennina". Lukijassa on vastaavanlainen silmukka. LF- ja HF-taajuusalueilla kyse on induktiivisesta kytkennästä, jossa tunniste reagoi lukijan luomaan magneettikenttään. UHF- ja mikrotaajuusalueilla taas on kysymys tekniikasta, jossa tunniste ja lukija kommunikoivat radioaaltoja lähettämällä. Lukija lähettää antenninsa kautta radioaaltoja ja tunnisteen antenni vastaanottaa aallot sekä heijastaa niitä takaisin sisältäen sirun tiedot. Kansantajuisesti LF- ja HF-tekniikan toimintaperiaatetta on verrattu muuntajaan ja UHF- sekä mikrotaajuustekniikan toimintaperiaatetta radioon.[10]

[9] Rinta-Runsala & Tallgren 2004, s. 8
[10] www.rfidlab.fi



Kuvassa UPM Raflatacin HF-tunniste.

Copyright UPM Raflatac RFID business.

Matalimmalla eli LF-taajuudella olevia tunnisteita käytetään mm. autoteollisuudessa autojen avaimissa varkaudenestoon. Harva tulee ajatelleeksi käyttävänsä RFID-tekniikkaa käynnistäessään varkaudenestojärjestelmällä varustettua autoa. Näissä järjestelmissä auton sytytysjärjestelmä tunnistaa avaimeen liitetyn tunnisteen ja sallii käynnistyksen vasta, kun tunniste on onnistuneesti tunnistettu.[11] LF-järjestelmiä ei enää juuri käytetä uusissa sovelluskohteissa. Vanhoista sovelluksista mainittakoon kulunvalvonta ja eläintunnistus.[12]

Tällä hetkellä yleisin Euroopassa käytetty RFID-tunnisteiden taajuus on HF-taajuuksista 13,56 MHz. Tällä taajuudella tunnisteen lukuetäisyys on melko lyhyt, parhaimmillaan reilun metrin luokkaa. Yleensä joudutaan kuitenkin tyytymään muutamien kymmenien senttimetrien lukuetäisyyteen. Lukuetäisyyttä voidaan kasvattaa jonkin verran kasvattamalla lukijan antennin kokoa.[13] Magneettikenttä loppuu kuitenkin noin 3,5 metrin etäisyydellä, mikä asettaa HF-taajuudella toimiville lukijoille teoreettisen maksimin.[14] Tunnisteen pienentäminen taas lyhentää lukuetäisyyttä, joten 13,56 MHz:n taajuudella toimivia tunnisteita ei voida merkittävästi nykyisestä pienentää.[15] Tämän taajuusalueen käyttö sisältää kuitenkin merkittäviä etuja verrattuna UHF-tekniikkaan. Ensinnäkin HF-tunniste toimii kohtalaisesti myös vettä sisältävien aineiden läheisyydessä. Toiseksi taajuusalue sietää hyvin häiriöitä teollisuusympäristöissä, ja kolmanneksi, lukualue on helposti rajattavissa halutun pituiseksi.[16]

[11] Rinta-Runsala & Tallgren 2004, s. 9
[12] www.rfidlab.fi
[13] Rinta-Runsala & Tallgren 2004, s. 9
[14] Hämäläinen 2005
[15] Rinta-Runsala & Tallgren 2004, s. 9
[16] www.rfidlab.fi

UHF-taajuusalueella toimivat järjestelmät ovat melko uusi keksintö. UHF-tekniikka on saavuttanut laajaa mielenkiintoa sen käyttökelpoisuudesta logistiikan sovelluksissa. Kyseistä tekniikkaa sovelletaan tunnetuissa toimitusketjuissa, joita mm. Wal-Mart, Tesco ja Metro Group ovat ottaneet käyttöön.[17] UHF-taajuusalueella tunnisteiden käyttökelpoisuutta parantaa pidempi lukuetäisyys.

Mikrotaajuusalueella kaikkein korkein ja yleisin käytössä oleva taajuus on 2,45 GHz. Tällä taajuudella signaalin vaimeneminen vettä sisältävässä aineessa on vielä nopeampaa kuin UHF-alueella ja rajoittaa näin ollen tunnisteen käyttöä enemmän. Käytännössä jo paksu kerros paperia vaimentaa signaalin lukukelvottomaksi. Tällä taajuusalueella tunniste on kuitenkin mahdollista tehdä erittäin pienikokoiseksi. Mikrotaajuusalueen käyttö on yleisintä Japanissa.[18] Mikroaaltojen tunnetuimpia sovelluksia on autojen automaattinen tunnistus tietullissa.[19]

2.1.1. Aktiivisuus ja passiivisuus

RFID-tunnisteet voidaan jakaa aktiivisiin, passiivisiin tai puoli-passiivisiin. Tämä jako tehdään tunnisteen viestintään ja laskentaan käyttämän energianlähteen mukaan. Passiiviset tunnisteet eivät sisällä omaa virtalähdettä. Laskenta ja viestintä on niissä mahdollista vain, kun lukija lähettää signaalia tunnisteeseen ja tunniste on lukuetäisyydellä.[20] Laitteen käyttöön vaadittava erittäin pieni sähkövirta induktoituu antenniin saapuvasta radiotaajuisesta skannauksesta, jonka avulla tunniste pystyy lähettämään vastauksen. Virta- ja hintavaatimuksista johtuen passiivisen RFID-tunnisteen vastaus on lyhyt, tyypillisesti pelkkä ID-numero. Koska passiiviset tunnisteet ovat halvempia valmistaa, suurin osa RFID-tunnisteista on passiivisia. Myös Suomessa on keskitytty lähes pelkästään passiivisiin tunnisteisiin.

Puoli-passiivinen eli semi-passiivinen RFID-tunniste sisältää virtalähteen, mutta sitä käytetään vain tietojen lähettämiseen lukijalle, kun ensin on vastaanotettu lukijan lähettämä signaali. Omalla virtalähteellä saavutetaan passiivista tunnistetta suurempi toimintasäde ja mahdollistetaan laajennettu toiminnallisuus, mukaan lukien tietojen säilyttäminen tunnisteen omassa muistissa. Muuten puoli-passiivinen tunniste toimii

[17] www.rfidlab.fi
[18] Rinta-Runsala & Tallgren 2004, s. 10
[19] www.rfidlab.fi
[20] Rinta-Runsala & Tallgren 2004, s. 10

kuten passiivinen tunniste. Puolipassiivisia tunnisteita käytetään esimerkiksi tietullin keräämiseen tarkoitetuissa autojen tuulilaseihin kiinnitettävissä tunnisteissa. Tunnisteen oma virtalähde mahdollistaa tietullin perimisen, vaikka auto liikkuu ja on useiden metrien etäisyydellä lukijasta.[21]

Aktiivisessa tunnisteessa omaa virtalähdettä käytetään myös tunnisteen laskennan virtalähteenä. Tärkeänä aktiivisen tunnisteen ominaisuutena on se, että niihin kirjoittaminen on mahdollista myös silloin, kun tunniste ei ole lukijan lukuetäisyydellä. Aktiivisissa tunnisteissa on yleensä selvästi suurempi muisti kuin passiivisissa tunnisteissa. Aktiivisiin tunnisteisiin voidaan liittää esimerkiksi lämpöanturi, jolloin tunniste voi mitata lämpötilaa ja lähettää keräämänsä tiedot eteenpäin saavutettuaan lukuetäisyyden. Tällä hetkellä pienimmät aktiiviset RFID-tunnisteet ovat suunnilleen kolikon kokoluokkaa, mutta ohuempia. Monilla aktiivisilla tunnisteilla lukuetäisyydet ovat kymmeniä metrejä ja virtalähteen ikä useita vuosia.[22]

2.1.2. Koko

Nyrkkisääntö on, että suurempi tunniste tuo suuremman lukuetäisyyden. Tunnisteen koon vaikutus lukuetäisyyteen riippuu kuitenkin myös käytetystä taajuudesta ja tunnisteiden sijoittelusta.[23] Oman virtalähteen puuttuminen tekee passiivisista tunnisteista varsin pieniä. Pienimmät passiiviset tunnisteet ovat alle puolen millimetrin levyisiä ja pituisia sekä ohuempia kuin paperiarkki. Suuremmat tarratunnisteet maksavat yleensä pieniä enemmän.[24] Sekä HF-tunnisteista, että UHF-tunnisteista löytyy monenkokoisia tarroja. Kirjaston kirjoissa yleisesti käytetyt HF-tunnistetarrat ovat noin kymmenen senttimetrin mittaisia ja siten helposti havaittavia, mutta UHF- ja mikrotaajuusalueella toimivat tunnisteet ovat vaikeasti ihmissilmän nähtävissä.

2.1.3. Tallennuskyky

Tunnisteiden muisti eli tallennuskapasiteetti vaihtelee kymmenistä biteistä pariin kilotavuun. Yksinkertaisimmat tunnisteet sisältävät vain yksikäsitteisen

[21] Rinta-Runsala & Tallgren 2004, s. 10-11
[22] Rinta-Runsala & Tallgren 2004, s. 11 ja http://fi.wikipedia.org/wiki/RFID
[23] Rinta-Runsala & Tallgren 2004, s. 11
[24] Rinta-Runsala & Tallgren 2004, s. 11

tunnistenumeron.[25] Lukumääräisesti suurin osa tunnisteista tulee todennäköisesti myös jatkossa sisältämään vain tunnistenumeron.

Osa tunnisteista on vain luettavia, osa kerran kirjoitettavia ja osa useasti kirjoitettavia. Edellä mainitut yksinkertaisimmat ja halvimmat tunnisteet ovat kerran kirjoitettavia, jolloin informaatio kirjoitetaan muistiin joko jo tehtaalla tai tunnistetta asetettaessa. Tuon jälkeen näitä tunnisteita voidaan pelkästään lukea.[26] Käytännössä tällä hetkellä tunnisteelle kirjoitetaan RFID-printterillä usein vain viivakoodi numeroina. Tällöin tunnistetarraan tulee sama tieto kolmena kappaleena: viivakoodi, viivakoodi näkyvinä numeroina sekä tunnisteelle tallennettu viivakoodinumero. Tulevaisuudessa on tarkoituksena, että tunnisteeseen kirjoitetaan sähköinen tuotekoodi (Electronic Product Code, EPC).[27] Uudelleenkirjoitettaviin tunnisteisiin voidaan kirjoittaa tietoa luku- ja kirjoituslaitteella myöhemminkin. Kirjoitusetäisyys on yleensä 0-50 % lukuetäisyyttä pienempi.[28]

Tärkeänä ominaisuutena tämän tutkimuksen kannalta on mainittava tunnisteelle määritelty erityinen ”kill-komento”, jolloin oikean salasanan antamalla tunniste inaktivoituu pysyvästi. Tällaisen komennon suorittanut tunniste ei enää vastaa lukijan signaaleihin, eikä sille voida enää kirjoittaa.[29]

2.1.4. Hinta

RFID-tunnisteen kappalehinnan merkittävin määräävä tekijä on kerralla tilattavien tunnisteiden määrä.[30] RFID-järjestelmäinvestointeja jarruttamassa kerrotaan usein olevan liian korkeat tunnistehinnat. Taloustieteilijät ovat laskeneet, että yksinkertaisimpien passiivisten tunnisteiden hinnat pitäisi saada n. 0,05 euroon, jotta RFID-tekniikasta tulisi kannattavaa ja laajasti käytettyä.[31] Hinnat ovatkin olleet viime vuosina vauhdikkaassa laskussa johtuen laajenevasta kysynnästä.

[25] Rinta-Runsala & Tallgren 2004, s. 11
[26] Rinta-Runsala & Tallgren 2004, s. 11
[27] Hämäläinen 2005
[28] Rinta-Runsala & Tallgren 2004, s. 11
[29] Rinta-Runsala & Tallgren 2004, s. 11
[30] Rinta-Runsala & Tallgren 2004, s. 12
[31] http://fi.wikipedia.org/wiki/RFID

Kotimainen tunnistevalmistaja UPM-Rafsec on syksyllä 2005 pudottanut halvimpien tunnisteidensa hinnat noin 0,08 euroon tunnisteelta yli 50 000 kappaleen tilauksissa.[32] Tätä kertaostomäärää voidaan pitää varsin pienenä, sillä hintoja listataan yleisesti yli miljoonan tunnisteen kertatilauksille.[33] Puoli-passiivisten ja aktiivisten tunnisteiden hinta on selvästi kalliimpi. Aktiivisten tunnisteiden hinnat voivat nousta jopa kymmeniin euroihin.[34]

2.2. Lukijat

Yleisesti ottaen lukijan on toimittava samalla taajuudella kuin luettava tunniste ja sen on oltava yhteensopiva tunnisteen kanssa. Monilla lukijoilla pystytään lukemaan saman taajuusalueen sisällä erilaisia tunnisteita. Sen sijaan sellaisia lukijoita, jotka lukisivat kaikkia tunnisteita kaikilla taajuusalueella, ei ole.

RFID-lukijalaite muodostuu antennista ja itse lukijasta. Varsinainen lukija vastaanottaa antennilta tulevat tiedot, varastoi niitä ja lähettää ne sen jälkeen kaapelin tai langattoman verkon välityksellä eteenpäin hyödynnettäväksi. Lukijat voivat olla joko kiinteitä tai liikuteltavia. Kiinteä lukija voidaan asentaa esimerkiksi ovelle tai kaupan hyllyyn. Liikuteltavia lukijoita ovat erilaiset kannettavat käsilukijat, jotka voivat olla yhteydessä tietojärjestelmiin langattomasti tai ne voivat päivittää tietonsa eräajotyyppisesti. Kannettavien lukijoiden lukuetäisyydet ovat kiinteisiin lukijoihin verrattuna lyhyitä ja niitä on saatavilla lähinnä vain HF-tunnisteille.

Lukijat ovat RFID-järjestelmän kallein osa. EPC-standardien mukaisen lukijan hinta on halvimmillaankin satoja euroja ja trukkien läpiajettavien porttilukijoiden hinnat ovat noin 10 000 eurossa.[35] Yksinkertaisimpien langallisten käsilukijoiden hinta on pudonnut noin 150 euroon, mutta useimmiten niissä on myös muita ominaisuuksia, kuten oma prosessori ja langaton wlan-tiedonsiirto, mitkä nostavat käsilukijan hinnan noin 2000 euroon.[36] RFID:n yleistyessä myös lukijoiden hinnat tulevat todennäköisesti laskemaan vauhdilla.

[32] www.rafsec.com
[33] http://www.rfidlab.fi/?1;2;300;300;181.html
[34] Rinta-Runsala & Tallgren 2004, s. 12
[35] Rinta-Runsala & Tallgren 2004, s. 13
[36] Hämäläinen 2005

2.3. Ominaisuuksien tarjoamat mahdollisuudet

Monesti RFID-teknologiaa on verrattu viivakoodiin (*Universal Product Code, UPC*) ja nähty teknologia viivakoodien potentiaalisena korvaajana. Tärkeimpänä erona viivakoodiin on, että radiotaajuinen tunnistus voi tapahtua ilman suoraa katsekontaktia tunnisteeseen. Lisäksi RFID-tunnisteen sisältöä voidaan muuttaa matkan varrella, kun taas viivakoodi on tulostuksen jälkeen muuttumaton. RFID-tunnisteet kestävät myös paremmin likaisia teollisuusolosuhteita kuin tavanomaiset viivakoodit. RFID-koodit ovat riittävän pitkiä, jotta jokaisella tunnisteella voi olla oma uniikki koodi, kun UPC-koodit ovat rajoittuneet yhteen koodiin tuotetta kohden. RFID-tekniikan etuna on myös se, että useita tunnisteita voidaan lukea lähes samaan aikaan.[37]

2.3.1. Tunnistaminen

RFID-tekniikka mahdollistaa tuotteen tunnistamisen ilman suoraa näköyhteyttä. Kuten edellä on todettu, tunnistuskentän laajuus riippuu käytettävien tunnisteiden ja lukijoiden tyypistä, mutta kentän laajuus voidaan määritellä sovelluskohtaisesti juuri tiettyyn tarpeeseen sopivaksi. Tunnistamisen kannalta tärkeä mahdollisuus on myös kyky yksilöidä tunnisteet ja tätä kautta yksittäiset tuotteet. Tunnisteiden avulla voidaan seurata, miten tietty tuote on kulkenut jakeluketjussa ja missä se on esimerkiksi valmistettu.[38]

2.3.2. Muisti

Tällä hetkellä tunniste sisältää vähintään saman tiedon kuin viivakoodikin.[39] Tulevaisuudessa on tarkoituksena, että sisältönä on vähintään yksilöivä koodi, kuten valmistajan sarjanumero tai EPC-koodi. Muistiin mahtuu kuitenkin runsaasti muutakin informaatiota, minkä vuoksi tekniikkaa kutsutaankin joskus saattomuistitekniikaksi. Tuo informaatio voi olla suoraan tuotteeseen liittyvää, kuten käsittelyohje, valmistusaika ja -paikka, tai informaatio voi olla linkki internetsivulle tai muuhun tietolähteeseen, josta kuluttaja voi hakea tuotetta koskevia lisätietoja.[40]

[37] Rinta-Runsala & Tallgren 2004, s. 13
[38] Rinta-Runsala & Tallgren 2004, s. 14
[39] Hämäläinen 2005
[40] Rinta-Runsala & Tallgren 2004, s. 14

Vähittäiskauppiaat haluavat tallentaa tunnisteelle tuotetta koskevia takuu- ja kuittitietoja, mikä helpottaisi myöhemmän mahdollisen takuuasian käsittelyä.

2.3.3. Yhdistäminen internetiin

Yksi RFID:n tarjoama mahdollisuus on sen linkittäminen internetiin ja tuotetietojen hakeminen sitä kautta. Itse tunnisteelle mahtuu kuitenkin edelleen rajattu määrä tietoa, mutta tietoverkkojen kautta sitä voidaan hakea rajattomasti. AutoID Center on visioinut tuotepakkausten ja yksittäisten tuotteiden merkitsemistä tunnisteilla ja tunnisteeseen liittyvän tuoteinformaation tallentamista internetiin.

Visiossa tuotteilla olisi sähköinen tuotekoodi, *Electronic Product Code (EPC)*, joka yksilöisi tunnisteet. Lukijan havaitessa tunnisteen se välittää tunnisteen EPC-numeron Savant-ohjelmistolle, joka toimii lukijan ja muiden tietojärjestelmien välissä. Tämän jälkeen Savant-ohjelmisto ottaa yhteyden nimipalvelimeen *(Object Name Service, ONS)*, joka kertoo tuotteen tarkemmat tiedot sisältävän palvelimen IP-osoitteen. Palvelin sisältää tunnistettua EPC-numeroa vastaavan tuotteen kuvauksen; esimerkiksi valmistusajan, koon, painon tai tiedon siitä, missä tuote on viimeksi havaittu. Järjestelmä on vielä kokeiluasteella.[41]

AutoID Centerin lopetettua toimintansa vuonna 2003, EPC:hen liittyvien standardien hallinnointia ja kehittämistä jatkaa *EPCglobal* -niminen[42] *EAN Internationalin* ja *the Uniform Code Councilin (UCC)* yhteishanke. EPCglobalin tavoitteena on luoda kansainvälinen standardi RFID:n ja UPC-koodin käytölle minkä tahansa tavaran tunnistamiseksi tuotantoketjussa – koskien kaikkia tuotantoaloja sekä maita.[43]

2.4. Haasteita

Yksityisyyden suojan lisäksi on olemassa muitakin RFID:n laajamittaiseen käyttöön liittyviä haasteita. Vaikka tämän tutkielma keskittyykin yksityisyyden suojaan liittyviin kysymyksiin, on tarpeen käydä lyhyesti läpi myös muita haasteita.

---

[41] Rinta-Runsala & Tallgren 2004, s. 15
[42] Rinta-Runsala & Tallgren 2004, s. 15
[43] http://www.epcglobalinc.org/

2.4.1. Standardit

RFID-tekniikan yleistymistä kansainvälisesti on pitkään hidastanut puute yhteisesti käytettävästä taajuusalueesta. Ongelmia on aiheuttanut erityisesti se, että UHF-taajuus on joissakin maissa osittain jo matkapuhelinten käytössä.[44] Esimerkiksi USA:ssa ja Kanadassa UHF-alueen RFID:t käyttävät 915 MHz taajuutta, kun taas eurooppalainen sallittu taajuusalue on 868-869 MHz ympärillä ja Japanissa on suunniteltu käytettäväksi 950-956 MHz taajuutta. Brittiläisen e.centre -standardisointitahon mukaan Euroopan ja USA:n standardien erot eivät kuitenkaan enää hidastaisi tekniikan käyttöönottoa.[45]

Suomessa taajuusalueiden käyttöä kontrolloi viestintävirasto, mikä asettaa omat vaatimuksensa ja rajoitteensa myös RFID-laitteistoille.[46] Viestintävirasto on hyväksynyt muutoksen UHF-taajuusalueen RFID-lukijoiden tehorajoituksiin[47] ja helmikuussa 2005 voimaan tulleen muutoksen jälkeen Suomessakin voidaan käyttää 2 W:n teholla toimivia UHF-lukijoita aikaisemman 0,5 W:n sijasta. Muutos mahdollisti sen, että lukuetäisyydessä päästiin USA:n tasolle.[48]

Standardisointiin liittyvät ongelmat näyttävät siten olevan ratkeamassa. Tämä on tärkeää varsinkin logistiikkaan liittyvissä sovelluksissa, joissa tullaan rakentamaan avoimia kuljetusketjuja, jolloin usean eri toimijan järjestelmien tulee pystyä lukemaan samoja tunnisteita. Kehitys UHF-standardien osalta jatkuu EPCglobalin aloitettua EPC Gen2 -protokollan määrittelyn, joka tulee olemaan ISO18000-6 standardin mukainen. Gen2 on Suomessa vasta RFID Labin testikäytössä, mutta testitulokset ovat lupaavia.

Maailmalla Gen2 on jo käytössä. Wal Martin tavarantoimittaja Texas Instruments on ensimmäisenä tavarantoimittajana ottanut käyttöön Gen2-tunnisteet osassa lähetyksiään. Vuoden 2006 alussa tosin vasta yksi Wal Martin jakelukeskuksista oli varustettu Gen2-lukijalla, mutta Wal Mart on parhaillaan asentamassa Gen2-lukijoita muihinkin jakelukeskuksiinsa.[49] Joka tapauksessa on toivottavaa, että lopulta päästäisiin yhteen

[44] Rinta-Runsala & Tallgren 2004, s. 10
[45] http://www.networkitweek.co.uk/vnunet/news/2125069/european-standard-won-stop-rfid
[46] www.rfidlab.fi
[47] Viestintäviraston määräys (15V/2005 M), liite s.12
[48] Rinta-Runsala & Tallgren 2004, s. 15
[49] http://www.rfidlab.fi/?1;2;300;300;211.html

globaaliin avoimeen standardiin. Standardien toisena tärkeänä tehtävänä on taata valmistajariippumattomuus.[50]

Rulla UPM Rafletacin Gen2 UHF-tunnistetarroja.

Copyright UPM Raflatac RFID business.

LF-taajuusalueella ei ole olemassa vapaita standardeja. Useimmat sovellukset, kuten kulunvalvontajärjestelmät, on toteutettu suljettuina järjestelminä.[51] LF-taajuusalue jäänee jatkossa vähemmälle käytölle, joten standardisointiin ei lienekään tarvetta.

HF-taajuusalueella 13,56 MHz:n taajuudella on olemassa sovittuja standardeja. Esimerkiksi standardi ISO14443 ei takaa valmistajariippumatonta tunnisteiden ja lukijoiden yhteensopivuutta, eikä siten tuo taajuusalueelle kaikkia standardien etuja. Käytännössä kuitenkin Philips Mifare -tekniikka on saavuttanut standardin aseman. Mifarea käytetään erilaisissa maksusovelluksissa ja sen lukuetäisyys on rajattu 3-4 senttimetriin.[52]

2.4.2. Tunnistintörmäys

Tunnistintörmäys on tilanne, jossa lukijan kentässä on useampi kuin yksi tunnistin. Lukija ei kykene erottamaan samaan aikaan tietojaan lähettäviä tunnisteita toisistaan. Vaikka on onnistuttu rakentamaan järjestelmiä, joissa tunnisteet lähettävät tietonsa hieman eri aikoihin, ongelmaa ei ole pystytty täysin poistamaan. Kun useita tunnistimia sisältävä lava kuljetetaan portista läpi, on vauhtia edelleen hidastettava, jotta kaikki tunnistimet ehditään varmasti lukea.[53] RFID Labin Gen2-testien tulokset ovat lupaavia tunnistintörmäyksen suhteen ja ongelma näyttää olevan ratkeamassa.[54]

---

[50] www.rfidlab.fi
[51] www.rfidlab.fi
[52] www.rfidlab.fi
[53] Rinta-Runsala & Tallgren 2004, s. 16
[54] http://www.rfidlab.fi/?1;2;300;300;211.html. Testeissä kuljetettiin UHF-portin läpi lavallinen Gen2-tunnisteilla varustettuja tuotteita ja portti tunnisti joka kerralla 100% tunnisteista. Gen2-standardin etuna

2.4.3. Lukijatörmäys

Lukijatörmäyksessä kaksi tai useampi lukija lukee saman tunnistimen tietoja. Ongelmalliseksi tilanne muodostuu, jos tunnistimen pitäisi olla vain jommankumman lukijan kentässä, esimerkiksi paikannussovelluksessa. Ongelmaa voidaan pyrkiä ratkaisemaan esimerkiksi lukijoiden sijaintia ja tehoa muuttamalla.[55]

2.4.4. Materiaalit

Metallit ja nesteet hankaloittavat tunnisteiden lukemista. Tunnistimen asettaminen metallipinnalle saattaa joillakin taajuuksilla estää lukemisen kokonaan.[56] Ratkaisuksi on Suomessa kehitetty muovinen lista, jolla tunniste kohotetaan parilla sentillä metallipinnasta. Listan yläosaan on valmiiksi upotettuna tunniste.[57]

UHF-taajuudella monissa sovelluksissa on muodostunut ongelmaksi se, että UHF-aallot vaimenevat nopeasti kulkiessaan vettä sisältävien kohteiden, kuten ihmisten läpi, mikä rajoittaa lukuetäisyyttä.[58] Käytännössä UHF-tunnisteen laittaminen käsien väliin estää lukemisen jo hyvinkin lyhyellä etäisyydellä. Jos pahvilaatikon kylkeen on liimattu tunnistetarra ja laatikko sisältää appelsiinimehupurkkeja, tunnistaminen saattaa myös estyä UHF-aaltojen absorboitumisen takia.

Tunnistetarran liimaaminen suoraan muovin pinnalle aiheuttaa sen, että taajuus, jolla tunniste heijastaa aallot takaisin, muuttuu. Tunniste pystytään kyllä lukemaan, mutta lukuetäisyys puolittuu.[59]

2.4.5. Salaus

Kuten jäljempänäkin käy ilmi, joissakin käyttötarkoituksissa on välttämätöntä, että vain valtuutetut lukijat voivat tehdä luku- ja kirjoitustapahtumia. Tätä varten tunnisteisiin on

---

on myös nopeus; koko lavan luku kesti vain sekunnin murto-osia. Yksittäisen tuotteen tasolla merkittyjä makaronipusseja tunnistettaessa lähes sadan kappaleen erät onnistuttiin myös lukemaan varmasti ja nopeasti.

[55] Rinta-Runsala & Tallgren 2004, s. 16
[56] Rinta-Runsala & Tallgren 2004, s. 16
[57] Hämäläinen 2005
[58] Rinta-Runsala & Tallgren 2004, s. 10
[59] Hämäläinen 2005

mahdollista lisätä salasanasuojaus. Toistaiseksi suojaustaso on kuitenkin ollut melko heikko verrattuna muun tietotekniikan käyttämiin suojauksiin.[60]

[60] Rinta-Runsala & Tallgren 2004, s. 17

3. RFID:n käyttömahdollisuudet eri toimialoilla

Tässä luvussa käydään läpi RFID:n hyödyntämistapoja eri toimialoilla. Tyhjentävää luetteloa käyttömahdollisuuksista ei varmasti kukaan pysty tällä hetkellä luomaan, sillä uusia toimintoja, joita tunnisteet voivat tarjota eri toimialoilla, havaitaan jatkuvasti lisää. Osa esiteltävistä sovelluksista on vielä testikäytössä, kun taas toiset ovat osana jokapäiväistä elämäämme – toisinaan ilman, että olemme niistä edes tietoisia.[61]

3.1. Liikenne

RFID-järjestelmät soveltuvat hyvin liikenteen sovelluksiin. Esimerkiksi sopivalla lukijoiden sijoittelulla tunnisteilla varustetut ajoneuvot voidaan jäljittää. Lisäksi monet julkisen liikenteen matkaliput perustuvat jo tällä hetkellä RFID-teknologiaan. Koko julkisen liikenteen kattava etäkortteihin perustuva rahastusjärjestelmä otettiin Euroopan pääkaupungeista ensimmäisenä käyttöön pääkaupunkiseudullamme vuonna 2002. Etäkortti luetaan liikennevälineeseen astuttaessa muutaman sentin etäisyydeltä lukulaitteesta. Päivittäin matkustustapahtumia kertyy noin 1,2 miljoonaa, kortteja tätä varten on yli miljoona ja kortinlukijoita 3000 laitetta sekä 100 käsilukijaa tarkastajilla.[62] Järjestelmä käyttää 13,56 MHz taajuutta.[63]

RFID:n tuominen kännyköihin mahdollistaa matkan maksamisen näyttämällä kännykkää etälukijalle. Käytännössä RFID-piiri rakennetaan kännykän kuoreen, jolloin kännykkä toimii kuten etäkortti. Oulun paikallisliikenteessä on tarkoitus tuoda järjestelmä yleiseen käyttöön keväällä 2006.[64]

3.2. Ilmailu

RFID-järjestelmät soveltuvat hyvin myös matkalaukkujen tunnistamiseen lentokentillä. Tunnisteet kiinnitetään matkalaukkuihin check-in -tiskillä. Lukijoiden järkevällä sijoittelulla laukkuja pystytään seuraamaan niiden liikkuessa lentokentältä toiselle sekä tietyn lentokentän alueella. Ensimmäisenä järjestelmää kokeili British Airways Heathrown lentokentällä. Kokeilusta saatujen positiivisten tulosten innoittamana

[61] Työasiakirja WP 105, s. 4
[62] Rinta-Runsala & Tallgren 2004, s. 23 ja www.buscom.fi/suomi/uutiset/1kaupalykort.html
[63] Hämäläinen 2005
[64] http://hightechforum.kaleva.fi/index.cfm?alue=10&id5=530323&OpenStory=1&msg=530323&lang=1&secure=0&scs=1

kansainvälinen ilmakuljetusliitto IATA *(International Air Transport Association)* suositteli aluksi HF-taajuusalueella toimivia tunnisteita matkatavaroiden sähköiseen tunnistamiseen. Nyt näyttää kuitenkin siltä, että UHF-taajuusalueen uusi standardi Gen2 on viemässä voiton matkatavaroiden tunnistuksessa. IATA:n jäseninä olevat lentoyhtiöt ovat hyväksyneet ehdotuksen käyttää Gen2-tunnisteita ja -lukijoita matkalaukkujen globaaleissa lentokuljetuksissa. RFID-tekniikan odotetaan vähentävän matkalaukkujen lähettämistä vääriin kohteisiin ja vähentävän tähän liittyviä kustannuksia sekä nopeuttavan lajittelua ja pakkaamista laukkukontteihin.[65]

Yksityisyyden suojan kannalta epäluuloja on herättänyt Euroopan unionin ilmailuviranomaisen EASA:n (*European Aviation Safety Agency*) aikomus sallia RFID:n käyttö tarkistuskorteissa (eng. *boarding card*). Etäluettavat tarkistuskortit mahdollistaisivat portilta myöhässä olevien matkustajien jäljittämisen ja helpottaisivat siten lentokenttävirkailijoiden toimintaa. [66]

3.3. Terveydenhoito

RFID-järjestelmiä käytetään lääketeollisuudessa paitsi helpottamaan lääkkeiden tunnistamista myös estämään lääkeväärennöksiä sekä estämään varkauksia kuljetuksen aikana. Lääkevalmistaja asentaa lääkepurkkiin tunnisteen ja apteekkari tarkistaa lukijalla, että purkki on peräisin oikealta valmistajalta. Lääketeollisuus onkin ensimmäisenä, vaateteollisuuden lisäksi, vienyt RFID-tunnistuksen yksittäisen tuotteen tasolle USA:ssa siten, että tunnisteen sisältävä tuote saattaa päätyä kuluttajalle saakka.[67] Yhdysvalloissa lääkevalmistaja Pfizer on alkanut käyttämään RFID-tekniikkaa varmistamaan markkinoimansa Viagran aitouden ja estämään väärennetyn Viagran myymisen. Lääkepurkkeihin on liimattu HF 13,56MHz RFID-tunniste, mikä rajoittaa lukuetäisyyden muutamiin sentteihin.[68]

Sairaaloissa RFID:n on nähty lisäävän potilasturvallisuutta. Mikäli leikkausinstrumentteihin asetettaisiin tunnisteet, niitä ei voitaisi enää unohtaa potilaan kehon sisään. Yksityisyyden suojan kannalta epäilyksiä on herättänyt RFID-tarrojen

[65] http://www.rfidlab.fi/?1;2;300;300;212.html. Hong Kongin lentokentällä on jo otettu käyttöön matkalaukkujen RFID-pohjainen tunnistusjärjestelmä. Tällä hetkellä kentällä käytetään RFID-tunnisteita viivakoodin rinnalla.
[66] http://www.rfidgazette.org/2005/10/index.html ja Työasiakirja WP 105, s. 4
[67] Työasiakirja WP 105, s. 4 ja Strömberg 2005
[68] http://www.rfidlab.fi/?1;2;300;300;213.html

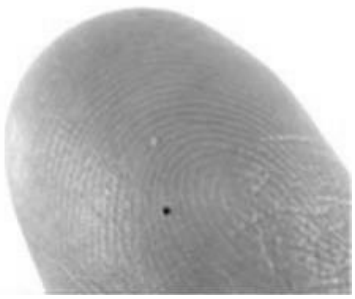
kiinnittäminen potilaisiin tarkoituksena varmistaa heidän henkilöllisyytensä, sijaintinsa sairaalassa sekä aiottu toimenpide. Toisaalta myös sairaalan henkilökunnalle voitaisiin antaa omat tunnisteet, jotta he olisivat nopeasti paikannettavissa hätätapauksessa.[69]

Yhdysvaltojen elintarvike- ja lääkevirasto FDA on antanut VeriChip -nimiselle yhtiölle luvan asentaa RFID-tunnisteita myös henkilöiden ihon alle.[70] Yhtiön mukaan ratkaisu on suunnattu niille, jotka haluavat potilastietojensa olevan helposti saatavilla silloin, kun potilas ei itse pysty puhumaan, hänellä on muistikatkoksia tai hän on tajuton. Tunnisteelle on kuitenkin tallennettu ainoastaan tunnistenumero, jonka avulla terveydenhuollon ammattihenkilö pääsee hätätapauksessa käsiksi henkilön potilastietoihin.[71]

3.4. Turvallisuus ja kulunvalvonta

Arvoesineiden kulunseurannassa RFID:n hyödyt on havaittu jo vuosia sitten. Edellä mainitun autojen varkaudenestojärjestelmien lisäksi tuttuja sovelluksia ovat mm. työpaikkojen kulunvalvontajärjestelmät ja kauppojen varkaudenestojärjestelmät.

RFID:n käyttömahdollisuuksia seteliväärennösten vaikeuttamiseen on tutkittu viime vuosien aikana. Japani on jo sijoittanut 10 000 jenin seteleihin tunnisteet, jotka sisältävät sarjanumeron sekä valmistusajan ja -paikan.[72] Jeneissä käytetty siru on ultrataajuusalueella toimiva Hitachin kehittämä ns. ”mu-chip”, joka on yksi maailman pienimmistä RFID-tunnisteista. Yksityisyyden suojan kannalta oleellista on, että tunnisteen maksimilukuetäisyys on vain noin 30 cm.[73] Myös Euroopan keskuspankki EKP harkitsee tunnisteiden sijoittamista euroihin, mutta lopullista päätöstä ei ole vielä tehty.[74]



Kaksi Hitachin mu-chip:ia sormen päällä.

Lähde: http://www.hitachi-eu.com/mu/products/mu_chip.htm

[69] Työasiakirja WP 105, s. 4
[70] Työasiakirja WP 105, s. 4
[71] http://www.verichipcorp.com/
[72] http://www.theregister.co.uk/2003/07/30/japan_yens_for_rfid_chips/
[73] Li (ym.) 2004. - Lähteen mukaan tunnisteen pinta-ala on 0,16 mm^2
[74] http://www.theregister.co.uk/2003/05/23/ec_moots_trackable_cyber_euro/

Valtiot haluavat sijoittaa RFID-tunnisteet passeihin väärennösten ehkäisemiseksi. Kansainvälisen siviili-ilmailujärjestön ICAO:n *(International Civil Aviation Organisation)* toimesta on valmisteltu jo vuonna 2003 tekniset vaatimukset, jotka on täytettävä passeissa, joissa halutaan käyttää RFID-tunnisteita.[75] Näin pystytään takaamaan se, että passit pystytään lukemaan maailmanlaajuisesti. Ensimmäisiä RFID-tunnisteen sisältäviä passeja aletaan myöntää kansalaisille Yhdysvalloissa kevään 2006 aikana, huolimatta yksityisyyden suojajärjestöjen vastustuksesta. Viranomaisten mukaan käyttöönotettava elektroninen passi vastaa hyvin asetettuihin tietosuojavaatimuksiin ja sitä on mahdoton väärentää.[76]

3.5. Vähittäiskauppa ja asiakkuuden hallinta

3.5.1. Jakeluketjujen seuranta

RFID-tekniikan laajamittaisimmat hyödyntämissuunnitelmat liittyvät jakeluketjujen seurantaan. Ensin tehtaalla pakkauslaatikko tai tuote varustetaan RFID-tunnisteella. Tehtaan lastausovella lukija tunnistaa kenttään tuodut laatikot tai tuotteet. Vastaavasti laatikot tai tuotteet tunnistettaisiin jakelukeskuksen ovella. Poikkeamat saapuneiden ja tilattujen tavaroiden välillä havaittaisiin heti. Lastattaessa jakelukeskuksesta vähittäiskauppaan menevää rekkaa, ovella on jälleen lukija, jonka avulla tunnistetaan lähtevät tuotteet ja päivitetään varastokirjanpito. Lopulta kaupan varaston ovella sijaitseva lukija päivittää kaupan varastokirjanpidon saapuneilla tuotteilla. Näin kauppa tietää tarkasti, mitä tuotteita sillä on varastossa ja miten tuoreita tavarat ovat.

Yhdysvaltalainen kauppaketju *Wal-Mart* oli aikanaan 1970-luvulla ensimmäisenä vaatimassa tavarantoimittajiltaan viivakoodien käyttöä. Vastaavasti *Wal-Mart* on 2000-luvulla vaatinut tavarantoimittajiltaan vuoden 2005 loppuun mennessä EPC-numeron sisältäviä RFID-tunnisteita kuormalavoihin ja laatikoihin. *Wal-Martin* tavoitteena on myöhemmin automatisoida logistiikkaketju raaka-aineiden toimituksesta siihen pisteeseen, kun asiakas työntää itse ostoksensa ulos kaupasta ja automaattinen lukilaite rekisteröi ja laskuttaa ostokset.[77] Epäilemättä tämä tavoite on vielä kaukana tulevaisuudessa ja saattaa olla, ettei se toteudu koskaan. Lähivuosien realistinen tavoite

[75] Työasiakirja WP 105, s. 5. Nämä vaatimukset on määritelty ICAO:n dokumentissa 9303.
[76] http://www.usatoday.com/tech/news/2005-08-08-electronic-passports_x.htm. Lähteen mukaan lukuetäisyys on saatu rajattua muutamiin senttimetreihin, lukutapahtumaa varten passi on avattava ja lisäksi harkitaan vielä tietojen salakirjoittamista.
[77] Rinta-Runsala & Tallgren 2004, s. 19 ja Kajava 2005.

on pyrkiä seuraamaan tuotteiden kuljetuslavoja, -laatikoita ja rullakkoja läpi logistiikkaketjun.[78]

Pisimmälle viedyssä visiossa itse tuotteissa olisi siis RFID-tunnisteet ja lukijoita ympäri kauppaa. Lukijat olisivat ns. älyhyllyjä, jotka tietäisivät reaaliaikaisesti, kuinka paljon tiettyä tuotetta on hyllyssä, ja ilmoittaisivat hyllyn täydennystarpeesta henkilökunnalle. Järjestelmä mahdollistaisi myös väärissä paikoissa olevien tuotteiden automaattisen havaitsemisen.[79] Metro Group on vuodesta 2003 kokeillut monia uusia teknologioitaan ”tulevaisuuden kaupassaan” Saksassa lähellä Duisburgia. Yksi kokeiltavista teknologioista on ollut RFID. Vaikka RFID:n käyttötavat Metron kaupassa ovat pääasiassa logistiikan- ja varastonhallinnassa, kaupasta löytyy myös muutamia älyhyllyjä, jotka seuraavat muutamien yksittäisten RFID-tunnisteella varustettujen tuotteiden riittävyyttä hyllyssä. Metro Groupin kaupassa RFID-tunnisteet toimivat myös varkaudenestona tavallisen varashälyttimen tapaan.[80]

3.5.2. Asiakkuudenhallinta

Kaupat haluavat saada tietoa asiakkaidensa kulutustottumuksista ja siitä, miten asiakkaan ostopäätös syntyy. Japanissa *Tokyo International Book 2003:ssa* esiteltiin RFID-tunnisteiden käyttöä kirjakaupan asiakkaiden käyttäytymisen tutkimiseen. Järjestelmä perustui kirjoihin asennettuihin tunnisteisiin ja hyllyihin asennettuihin lukijoihin. Näillä mahdollistettiin jälkikäteiset analyysit kirjojen selailuajasta, selailujen määrästä sekä hyllyjen läpikäyntijärjestyksestä ennen ostopäätöstä. Mikäli asiakas otti hyllystä suuren määrän kirjoja, henkilökuntaa varoitettiin mahdollisesta myymälävarkaudesta.[81] Asiakaspalveluun RFID saattaa tuoda myös uusia ulottuvuuksia. Mikäli asiakas on kiinnostunut tietystä tuotteesta, sitä koskevaa lisäinformaatiota voidaan tuoda kaupan videonäytöille. Lisäinformaatio voisi olla esimerkiksi muita varastosta löytyviä värivaihtoehtoja puvusta, puvun kanssa sopivia muita vaatteita saman valmistajan mallistosta tai videokuvaa puvusta muotinäytöksessä. Tällaisia järjestelmiä on ollut jo ainakin italialaisen design-vaatettaja *Pradan* käytössä New Yorkin myymälässä.[82]

[78] Rinta-Runsala & Tallgren 2004, s. 18
[79] Rinta-Runsala & Tallgren 2004, s. 19
[80] Rinta-Runsala & Tallgren 2004, s. 19 ja www.future-store.org
[81] Rinta-Runsala & Tallgren 2004, s. 25
[82] Rinta-Runsala & Tallgren 2004, s. 19 ja www.ideo.com/case_studies/prada.asp

4. Yksityisyys perusoikeutena

4.1. Yksityisyyden käsite

Oikeuskirjallisuudessa käsite *yksityisyyden suoja* nähdään yleensä juontavan juurensa kahden yhdysvaltalaislakimiehen, Samuel D. Warrenin ja Louis D. Brandeisin, tutkielmaan yksilön oikeudesta olla yksin tai omassa rauhassa – *"right to be let alone"*.[83] Warren ja Brandeis olivat omakohtaisten kokemuksiensa kautta saaneet tarpeekseen ns. keltaisen lehdistön kansalaisten yksityiselämään puuttumisesta julkisuudessa.[84] Heidän tutkimuksellaan oli ratkaiseva merkitys yksityisyysdoktriinin läpimurrossa länsimaisessa oikeuskirjallisuudessa, vaikkakin yksityisyyden vaatimus oli esitetty jo Ranskan vallankumouksen aikaan.[85] Saarenpää huomauttaa, että keskustelua oikeudellisesta yksityisyydestä on käyty jo paljon aikaisemmin.[86]

Yksityisyyden määrittelyssä on esitetty kansainvälisesti monenlaisia näkemyksiä. Yksityisyyden ja yksityiselämän käsitteitä on toisinaan käytetty toistensa synonyymeina, toisinaan yksityisyyden suoja on nähty yksityiselämän suojaa laajempana kokonaisuutena koostuen eri perusoikeuksista.[87] Tässä tutkielmassa käytän yksityisyyden ja yksityiselämän käsitteitä samassa merkityksessä. Kotimaisessa oikeuskirjallisuudessa yksityisyyttä ja yksityiselämää on kyllä tarkasteltu laajalti, mutta hyvin usein johtopäätöksenä on, että yksityisyyttä ei yleisenä käsitteenä voida määritellä.[88] Myöskään lainsäädännössämme ei yksityisyyttä ole määritelty, vaikkakin siitä puhutaan sekä henkilötietolakia edeltäneessä tietosuojan perussäädöksessämme henkilörekisterilaissa *(HenkRekL)* että nykyisessä henkilötietolaissa *(HetiL)*.[89] Hallituksen esitykseen henkilötietolaiksi sisällytettiin henkilötietolakia valmistelleen komitean näkemys siitä, että lain 1 §:stä ilmenee, että oikeus yksityisyyden suojaan muodostuu yksityiselämän suojan lisäksi muistakin henkilötietojen käsittelyssä

[83] Warrein & Brandeis 1890.
[84] Korhonen 2003, s. 79.
[85] Konstari 1992, s.10-11.
[86] Saarenpää 2002. Saarenpää viittaa Platonin, John Stuart Millin ja James Fitzjames Stephenin kirjoituksiin.
[87] Viljanen 1999, s. 336. Esimerkiksi henkilörekisterilakia koskevan hallituksen esityksen yksityiskohtaisissa perusteluissa (HE 49/86 s. 21) yksityisyyden suoja on ymmärretty yksityiselämän suojaa laajemmaksi kokonaisuudeksi. Perustelujen mukaan yksityisyyteen kuuluu lähtökohtaisesti oikeus tietää tai päättää itseään koskevien tietojen käytöstä, mikä merkitsee muun ohella sitä, ettei kukaan ole velvollinen kertomaan yksityiselämäänsä koskevia tietoja viranomaiselle, ellei tietojenantovelvollisuus perustu lakiin.
[88] Lehtonen 2001, s. 6
[89] Korhonen 2003, s.75

merkityksellisistä perusoikeuksista, jotka ovat itsemääräämisoikeuden ja sitä ilmentävän henkilökohtaisen vapauden lisäksi oikeus kunniaan.[90]

Saarenpää pitää yksityisyyttä muuttuvana suhdekäsitteenä. Oikeutta yksityisyyteen suojataan yhteiskunnan muuttuessa tarvittaessa erilaisin lainsäädännöllisin ratkaisuin.[91] Saarenpään mukaan yksityisyyden määrittely ei kuulukaan lainsäätäjän tehtäviin, sillä sen yksityiskohtainen määrittely yhdessä erityislaissa olisi omiaan lisäämään epätietoisuutta yksityisyyden roolista yhteiskunnassa.[92] Saarenpää toteaa, että riittävää onkin luonnehtia yksityisyys oikeudeksemme olla yksin suhteessa muihin yksilöihin, yhteisöihin ja yhteiskuntaan sekä oikeudeksemme päättää ensisijaisesti itse siitä, missä määrin, millä tavoin ja millä hinnalla paljastamme yksityisyyttämme muille. Tällainen yleinen luonnehdinta osoittaa Saarenpään mukaan, että yksityisyys ei merkitse vain suojaa muilta, vaan myös oikeutta päättää ja toimia – yksityisyydellä on siten aktiivinen ja passiivinen puolensa.[93] Myös Lehtonen on todennut, että vaikka yksityisyyden määrittelyä pidettäisiin mahdottomana tai tarpeettomana, tämä ei tarkoita sitä, ettei niillä erityisillä elämänalueilla, jotka kuuluvat yksityiselämän kovaan ytimeen, voitaisi kuvata sitä, mikä ainakin kuuluu yksityisyyteen.[94] Konstarin mukaan yksityisyydestä on sanottu jotakin olennaista, kun todetaan, että kysymys on ennen muuta yksilöä koskevien tietojen hankkimisen, tallentamisen, käytön ja luovutuksen rajoittamisesta.[95] Yksityisyyteen luetaan kuuluvaksi ainakin yksilöä läheisesti koskevat tiedot sekä yleensä oikeus oleskella määrätyllä alueella tarvitsematta sietää ulkopuolisen läheisyyttä, häirintää, katselua tai kuuntelua.[96] Yksityisyyden suojan sisältö ja merkitys ovat kuitenkin voimakkaasti aika-, arvostus- ja yhteiskuntasidonnaisia, joten senkin takia yksiselitteistä ja yleisesti hyväksyttävää määritelmää ei voida löytää.[97] Epäilemättä lainsäätäjän tarkoituksena onkin ollut jättää lainsoveltajalle eli tuomioistuimille runsaasti liikkumavaraa arvioidessaan sitä, milloin kyse on yksityisyydestä ja sen suojaa vaarantavasta menettelystä.[98]

[90] HE 96/1998 vp, yksityiskohtaiset perustelut.
[91] Saarenpää 2005b, s. 67.
[92] Saarenpää 2002, s. 319. Saarenpää toteaa lisäksi, että käsitteen määrittelyn vaikeus ei saisi kuitenkaan johtaa siihen, että emme pyrkisi luomaan kuvaa yksityisyydestä.
[93] Saarenpää 2005, s. 323
[94] Lehtonen 2001, s. 6
[95] Konstari 1992, s.12
[96] HE 184/1999 vp, yleisperustelut
[97] Wallin & Nurmi 1991, s. 5
[98] Konstari 1992, s.12

Jo tässä vaiheessa on huomattava, että käsitteenä yksityisyyden suoja on pidettävä erillään *tietosuojan* -käsitteestä, jota pidettiin jo HenkRekL:a säädettäessä käsitteellisesti laajasisältöisempänä kuin yksityisyyden suojan käsitettä.[99] Saarenpää pitää myös tietosuoja-käsitteen määrittelyä tarpeettomana, sillä siinäkin on kyse samalla kertaa sekä oikeudellisesta käsitteestä että oikeudellisesta instituutiosta, joka on aina suhteellinen.[100] Konstari määritteli tietosuojan henkilörekisterilain tavoitteista käsin siten, että siinä on kyse ”henkilötietolainsäädäntöön sisältyvien säännösten kokonaisuudesta, jonka tarkoituksena on henkilötietoja kerättäessä, tallennettaessa, luovutettaessa, arkistoitaessa ja hävitettäessä henkilön yksityisyyden sekä hänen etujensa ja oikeuksiensa suojeleminen, valtion turvallisuuden varmistaminen samoin kuin hyvän rekisteritavan toteuttaminen”.[101] Henkilötietolaissa ei enää mainita *hyvää rekisteritapaa*, vaan lain yhtenä tarkoituksena mainitaan *hyvän tietojenkäsittelytavan* kehittämisen ja noudattamisen edistäminen *(HetiL 1 §)*. Hallituksen esityksessä todetaan, että lain toiminnallisena tavoitteena on edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista henkilötietojen käsittelyssä ja toteuttaa siinä hyvään tietojenkäsittelytapaan perustuvaa yhtenäistä käytäntöä. Hyvä tietojenkäsittelytapa ilmentää paremmin henkilötietojen keskeistä sääntelyn kohdetta, henkilötietojen käsittelyä. Hallituksen esityksen mukaan hyvän tietojenkäsittelytavan kehittämiseen ja edistämiseen kuuluu muun ohella se, että henkilötietoja käsiteltäessä varmistetaan, että käsittelyn tekninen toteuttaminen on asianmukaista, ja että henkilötietoja käsittelevät perehdytetään henkilötietojen käsittelyyn sekä niihin säännöksiin ja velvoitteisiin, jotka on siinä otettava huomioon.[102] Henkilötietolain tarkoituksena ei myöskään mainita enää *valtion turvallisuuden varmistamista*. Tällä tavalla halutaan korostaa yksityisyyden suojaa lain keskeisenä tavoitteena.[103] Muilta osin Konstarin määritelmä tietosuojasta kuvaa mielestäni edelleen hyvin tietosuojan ydinsisältöä. Wallin toteaa, että tietosuojan tarkoituksena on tiedon referenssin yksityisyyden sekä etujen ja oikeuksien turvaaminen.[104]

[99] HE 49/1986 s. 3
[100] Saarenpää. Näkökulmia yksilön suojasta (kohta 7). Saarenpää toteaa, että ajatus tietosuojan tarkasta määrittelystä olisi kuin yritys keksiä ikiliikkuja.
[101] Konstari 1992, s.13
[102] HE 96/1998, yksityiskohtaiset perustelut. Hyvän tietojenkäsittelytavan turvaaminen koostuu kuitenkin käytännössä pitkälti samoista keinoista, joilla aikanaan pyrittiin hyvän rekisteritavan toteuttamiseen.
[103] HE 96/1998, yksityiskohtaiset perustelut. Valtion turvallisuus on sen sijaan muiden suojattavien etujen rinnalla otettu huomioon lakiehdotuksen yksittäisissä säännöksissä. Valtion turvallisuus ei sisälly myöskään henkilötietodirektiivin 1 artiklaan, jossa ilmaistaan direktiivin tavoitteet.
[104] Wallin 2001, s. 377

4.2. Yksityiselämän suoja perustuslaissa

Perustuslain 10 § 1 mom.:

> ***Yksityiselämän suoja.*** *Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.*

Perustuslain (PeL) 10 § vastaa sellaisenaan vuoden 1995 perusoikeusuudistuksen yhteydessä uudistettua hallitusmuodon 8 §:ää, kuitenkin siten, että siihen on lisätty pykäläotsakkeeksi *"Yksityiselämän suoja"*. Yksityiselämän suoja viittaa siten sekä laajemmassa merkityksessä 10 §:n turvaamien oikeuksien kokonaisuuteen että suppeassa merkityksessä 10 §:n 1 momentissa turvattuun erityiseen perusoikeuteen. Laajassa merkityksessä yksityiselämän suojaan kuuluu myös 2 momentin kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus. Yksityiselämän suoja on omaksuttu perustuslakiimme kansainvälisistä ihmisoikeussopimuksista: lähinnä *Euroopan neuvoston ihmisoikeussopimuksen (EIOS 439/1990)* 8 artiklasta ja *Kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen (KP-sopimus 108/1976)* 17 artiklasta. Perustuslaki ei kuitenkaan sisällä, kansainvälisistä ihmisoikeussopimuksista poiketen, mainintaa perhe-elämän suojasta. Perhe-elämä kuitenkin kuuluu säännöksen tarkoittaman yksityiselämän piiriin. Hallituksen esityksessä todetaan yksityiselämän piirin määrittämisen olevan vaikeaa. Esityksen mukaan yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä. Lisäksi siinä luetellaan esimerkinomaisesti yksityiselämän piiriin kuuluvaksi yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään ja ruumiistaan.[105]

Nieminen on kiinnittänyt huomionsa siihen, että yksityiselämän ja perhe-elämän suoja ovat jääneet sisällöltään jossain määrin epätäsmällisiksi. Käsitteiden tarkemman määrittelyn vaikeudesta johtuen ei ole kovin helppoa määritellä, milloin jonkun yksityiselämän suojaa on rikottu. Nieminen katsoo, että vastaisuudessa yksityiselämän suojan merkitys perus- ja ihmisoikeutena saattaa kasvaa huomattavastikin nykyiseen verrattuna.[106]

---

[105] HE 309/1993 vp, yksityiskohtaiset perustelut

[106] Nieminen 1999, s. 109. Nieminen viittaa teknisen kehityksen myötä syntyviin uusiin kontrollimuotoihin ja automaattisen tietojenkäsittelyn aikaansaamiin uudenlaisiin ongelmiin.

PeL 10 §:n 1 momentin loppuosa sisältää myös tietosuojaa koskevan ns. sääntelyvarauksen, jonka mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Tällaisia sääntelyvarauksia käytetään silloin, kun perusoikeus selvästi edellyttää tuekseen tavallista lainsäädäntöä, tai kun perusoikeutta on mahdoton kirjoittaa ehdottomaan ja riittävän kattavaan muotoon. Sääntelyvarauksen tehtävänä on osoittaa, että perusoikeuden täsmällinen sisältö määräytyy vasta perusoikeussäännöksen ja tavallisen lain muodostaman kokonaisuuden pohjalta.[107] PeL 10 § 1 momentin sääntelyvaraus asettaa lainsäätäjälle velvollisuuden antaa perusoikeutta täsmentävän säännöksen. Lainsäädännön tasolla varmistetaan siten viime kädessä yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä.[108] Säännös jättää sääntelyn yksityiskohdat lainsäätäjän harkintaan. Lainsäätäjän liikkumavaraa rajoittaa kuitenkin se, että henkilötietojen suoja osittain sisältyy samassa momentissa lähtökohtaisesti suojatun yksityiselämän piiriin.[109]

Keskeisin PeL:n 10 §:n 1 momentin sääntelyvarauksen sisältämää toimeksiantoa täyttävä laki on nykyisin 1.6.1999 voimaan tullut henkilötietolaki *(HetiL 523/1999)*, jota käsittelen tarkemmin jäljempänä (ks. luku 5).

4.3. Perusoikeuksien vaikutustapa

PeL:n 22 § sisältää yleisluontoisen perusoikeuksien turvaamisvelvoitteen: ”Julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen.”[110] Vaikka keinovalikoima on jätetty PeL:ssa avoimeksi, yleisesti katsotaan, että ensisijaisina keinoina tulevat kyseeseen lainsääntötoimenpiteet.[111] Rikoslainsäädäntö on perinteisesti ollut keino, jolla oikeusjärjestys on konkreettisimmin suojannut yksityiselämää.[112] Pykälä asettaa siten eduskuntalain säätäjälle toimintavelvoitteen; se sisältää ns. perustuslaillisen toimeksiannon.[113] Paitsi, että PeL 22 § velvoittaa lainsäätäjää, edellyttää se perusoikeuksien huomioon ottamista myös hallinnossa ja tuomioistuimessa. Vuoden 1995 perusoikeusuudistuksella pyrittiin nimenomaisesti

[107] Saraviita 2000, s. 11
[108] Saraviita 2000, s. 134-135
[109] PeVL 25/1998 vp
[110] Jyränki 2000, s. 286
[111] Nieminen 1999, s. 119
[112] Viljanen 1998, s. 296
[113] Jyränki 2000, s. 287

lisäämään perusoikeuksien suoraa sovellettavuutta tuomioistuimissa ja muissa viranomaisissa sekä parantamaan yksityisten ihmisten mahdollisuutta vedota oikeuksiensa tueksi välittömästi perusoikeussäännöksiin.[114]

Julkisen vallan turvaamisvelvoitetta voidaan pitää rinnasteisena *ns. perusoikeusmyönteisen laintulkinnan periaatteelle*.[115] Perusoikeusmyönteisellä laintulkinnalla tarkoitetaan sitä, että tuomioistuimen tulee valita perusteltavissa olevista lain tulkintavaihtoehdoista sellainen, joka parhaiten edistää perusoikeuksien toteutumista ja joka eliminoi perustuslain kanssa ristiriitaiseksi katsottavat vaihtoehdot.[116]

Vaikka klassisena lähtökohtana on, että perusoikeudet vaikuttavat ensi sijassa vertikaalisessa suunnassa eli yksityisten ihmisten ja julkisyhteisöjen välillä, perusoikeuksille konstruoidaan nykyisin myös horisontaalinen eli vaakatason vaikutus, millä tarkoitetaan perusoikeuksien vaikutusta yksityisten välisissä suhteissa.[117] Jo perusoikeuksien asema yhteiskunnan perusarvoina korostaa niiden merkitystä myös yksityisten välisissä suhteissa.[118] Horisontaalivaikutus voi olla välitöntä, jolloin yksilö voi vedota tuomioistuimessa suoraan perustuslain mukaisiin oikeuksiinsa ilman alemmanasteisen lainsäädännön välitystä. Välillisellä horisontaalivaikutuksella tarkoitetaan sitä, että tavallista lakia sovellettaessa on otettava huomioon perusoikeuksien olemassaolo, vaikka niihin ei voida vedota suoraan.[119] PeL:n 22 §:ssä julkiselle vallalle asetettu perusoikeuksien ja ihmisoikeuksien toteuttamisen edistämisvelvollisuus koskee siis myös niiden toteutumista yksityisten ihmisten keskinäisissä suhteissa. Apuna voidaan tuolloin käyttää mm. kriminalisointeja.[120]

PeL:n 10 §:ssä turvattujen oikeuksien osalta edellä todettu tarkoittaa sitä, että sen ohella että julkisen vallan tulee itse suojata ihmisten perhe- ja yksityiselämää julkisen vallan taholta tulevilta loukkauksilta ja huolehtia myös positiivisin toimenpitein oikeuden toteutumista, sen tulee huolehtia myös yksityiselämän suojaamisesta toisten yksilöiden

[114] HE 309/1993 vp, yleisperustelut
[115] Saraviita 2000, s. 179
[116] PeVM 25/1994, s. 7
[117] Jyränki 2000, s. 288
[118] Viljanen 1999a, s. 154
[119] Ojanen 2003, s. 49. Vallitsevana kantana on, että perusoikeuksien horisontaalivaikutus on ensisijaisesti luonteeltaan välillistä eli käytännössä perusoikeuksien vaikutus yksityisten oikeussuhteissa voi ilmetä perusoikeuksia täsmentävän tavallisen lainsäädännön välityksellä eli lähinnä niiden suojaamiseksi säädettyjen kriminalisointien kautta.
[120] Nieminen 1999, s. 119. Katso tarkemmin perusoikeusuudistusta koskeva HE 309/1993 vp. s. 75

loukkauksilta.[121] Yksityiselämä nauttii siten suojaa sekä vertikaalisuhteessa eli julkisyhteisön ja yksityisten välillä että horisontaalisesti eli yksityisten keskinäisissä suhteissa, mistä jälkimmäisellä on ilmeisesti tulevaisuudessa kasvava merkitys. Henkilön oikeutta yksityiselämään ei uhkaa niinkään julkisyhteisö, vaan pikemminkin toinen yksityinen toimija.[122]

4.4. Perusoikeuksien rajoittaminen ja yleiset rajoittamisen edellytykset

Perusoikeudet eivät yleisesti voi olla siten ehdottomia, ettei niitä saisi missään oloissa ja missään laajuudessa rajoittaa.[123] Henkilötietojen suoja on esimerkki alasta, jolla yksilön nauttiman suojan laajuus riippuu kulloisestakin asiayhteydestä. Perusoikeuksien muodostamassa kokonaisjärjestelmässä on ominaista, että siihen sisältyvät ainesosat ovat usein jännitteisessä suhteessa keskenään. Jännite liittyy usein siihen, että yhtäältä on kunnioitettava yksilöiden toimintavapautta ja samalla huolehdittava toisten ihmisten turvallisuudesta. Yhden yksilön oikeudet ja vapaudet on sovitettava yhteen toisten yksilöiden oikeuksien ja vapauksien sekä koko yhteisön etujen kanssa. Olennaista on hahmottaa, mitä perusoikeuksia tietyssä tilanteessa rajoitetaan, ja toisaalta mitä perusoikeuksia sillä mahdollisesti suojataan ja punnita niitä keskenään ratkaisuntekohetkellä vallitsevien käsitysten pohjalta.[124]

Perusoikeutta voidaan ensinnäkin rajoittaa kyseistä perusoikeutta koskevan erityisen rajoituslausekkeen nojalla.[125] Koska perustuslain 10 §:ään ei kuitenkaan sisälly tällaista yksityiselämän suojaa koskevaa erityistä rajoituslauseketta, on yksityiselämän suojaan puuttumisen sallittavuutta arvioitava seuraavaksi käsiteltävien perusoikeuksien yleisten rajoitusedellytysten valossa, jotka perustuslakivaliokunta muodosti vuoden 1994 mietinnössään.[126]

---

[121] Nieminen 1999, s. 119. Tämä tarkoittaa Niemisen mukaan myös perheenjäsenten keskinäisiä suhteita.
[122] Viljanen 1999b, s. 338
[123] Jyränki 2000, s. 291. Muutamat perusoikeussäännökset on kuitenkin kirjoitettu ehdottomaan ja täsmällisen kiellon muotoon, joka ilmaistaan yksiselitteisellä ”ei saa” -lausekkeella.
[124] Länsineva 1998, s. 113-114
[125] Jyränki 2000, s. 292-294. Näitä ovat: 1) ns. kvalifioidut lakivaraukset, joissa yhtäältä annetaan tavalliselle lain säätäjälle valtuus oikeuden rajoittamiseen (”voidaan lailla säätää rajoituksia”) ja toisaalta asetetaan rajoitusvaltuuden käyttämiselle lainsäätäjän harkintaa supistavia lisäkriteerejä; 2) sääntelyvaraukset, joilla perusoikeus kytketään läheisellä tavalla lailla toteutettavaan sääntelyyn; 3)lakiviittaukset, joka edellyttää lainsäätäjän säätävän kyseisestä oikeudesta ja jättää samalla sääntelyn yksityiskohdat lainsäätäjän harkintaan; 4) rajoituksettomat perusoikeudet, joista puuttuu kokonaan rajoituslauseke tai lakivaraus, mutta joiden tarkoituksena ei kuitenkaan ole ollut, että nämä oikeudet olisivat ehdottomia, täysin vailla rajoitusmahdollisuutta tai että niitä voitaisiin vapaasti tavallisella lainsäädännöllä rajoittaa.
[126] Viljanen 1999b, s. 338-339. PeVM 25/1994:ssa muotoiltiin yleiset rajoitusperusteet.

Ensinnäkin yksityiselämän suojan rajoitusten tulee perustua eduskunnan säätämään lakiin *(lailla säätämisen vaatimus)*. Tähän liittyy kielto delegoida yksityiselämän suojan rajoittamista koskevaa toimivaltaa lakia alemmalle säädöstasolle.[127] Toiseksi rajoitusten on oltava tarkkarajaisia ja riittävän täsmällisesti määriteltyjä. Rajoitusten olennaisen sisällön tulee ilmetä laista *(täsmällisyys- ja tarkkarajaisuusvaatimus)*. Kolmanneksi rajoitusten tulee olla hyväksyttäviä *(hyväksyttävyysvaatimus)*. Tällä tarkoitetaan sitä, että rajoittamisen tulee olla painavan yhteiskunnallisen tarpeen vaatima, eivätkä ne saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa.[128] Hyväksyttävyyden arvioinnissa on huomioitava Euroopan ihmisoikeussopimuksen vastaavanlaista oikeutta, tässä tapauksessa yksityiselämän- ja perhe-elämän suojaa, koskevat määräykset.[129]

Neljänneksi tavallisella lailla ei voida säätää yksityiselämän suojan *ytimeen* ulottuvaa rajoitusta. Vaatimuksen taustalla on, ettei perusoikeuteen voida puuttua niin laajalti, että se kovertaa perusoikeuden sisällön tyhjäksi.[130] Viidenneksi rajoitusten on oltava *suhteellisuusvaatimuksen* mukaisia eli niiden tulee olla välttämättömiä hyväksyttävänä tarkoituksen saavuttamiseksi. Toisin sanoen rajoitus ei saa mennä pidemmälle kuin on perusteltua ottaen huomioon rajoituksen taustalla olevan yhteiskunnallisen intressin painavuus suhteessa rajoitettavaan oikeushyvään. Lisäksi rajoitettaessa on huolehdittava *riittävistä oikeusturvajärjestelyistä*.[131]

Vaikka Suomessakin pidettiin aikaisemmin mahdollisena rajoittaa tietyn ihmisryhmän, kuten vankien ja muiden laitoksessa elävien, perusoikeuksia suoraan erityisen vallanalaisuussuhteen tai laitosvallan perusteella, nyttemmin tällaiset perusteet perusoikeusrajoituksille on kuitenkin torjuttu. Siten esimerkiksi vankien perusoikeuksien, kuten yksityiselämän suojan, rajoittaminen edellyttää lakia, jonka säätämisjärjestys riippuu rajoituksen sisällöstä ja asteesta. Jos rajoituksia vankien perusoikeuksiin nykyään tarvitaan, tulee niiden hyväksyttävyys arvioida tavanomaisten

[127] Jyränki 2000, s. 294. Peruste vaatimukselle eduskuntalain käyttämisestä on siinä, että kun käytetään vain eduskuntalakia, rajoitus ja sen perustuslainmukaisuus on eduskunnan välittömässä valvonnassa.
[128] Jyränki 2000, s. 294-295
[129] Viljanen 1999b, s. 339. PeL:n ja EIOS:n suhteesta katso tarkemmin 4.5.1. alla.
[130] Viljanen 2001, s. 229 Perusoikeusuudistuksen yhteydessä perusoikeuskomitea totesi mietinnössään (KM 1992:3, s.139) jäävän lainsäädäntökäytännössä tarkemmin ratkaistavaksi, mitä kuuluu kunkin perusoikeuden ehdottomaan ydinsisältöön. Lähtökohtana komiteamietinnön mukaan on, että syvälle käyvät, poikkeukselliset tai summaariset rajoitukset merkitsisivät puuttumista perusoikeuden olennaiseen sisältöön.
[131] Jyränki 2000, s. 295

rajoitusedellytysten mukaan. Erityisesti vapaudenmenetys merkitsee erittäin pitkälle menevää puuttumista henkilön oikeuksiin. Se ei kuitenkaan sellaisenaan muodosta perustetta rajoittaa henkilön muita perusoikeuksia. Jos tarve rajoittaa henkilökohtaisen vapauden ohella muita perusoikeuksia, kuten yksityiselämän suojaa, vapaudenmenetyksen aikana on olemassa, rajoitukset tulisi voida oikeuttaa erikseen kussakin tapauksessa ja kunkin oikeuden osalta.[132] Tämä on pidettävä mielessä myös tulevaisuudessa, mikäli vankien seurantaan halutaan käyttää RFID-tunnisteita. Säädettäessä lakia henkilötietojen käsittelystä rangaistusten täytäntöönpanossa eli ns. vankitietolakia päädyttiin käyttämään tavallista lainsäätämisjärjestystä. Hallituksen esityksessä todettiin, että PeL 10 §:n 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Hallitus katsoi esityksen olevan sopusoinnussa perustuslain kanssa.[133] Yleisten rajoitusperusteiden luettelon merkitys ei rajoitu yksinomaan lakiehdotuksen säätämisvaiheen normikontrollitilanteisiin, vaan sillä voidaan nähdä kasvavaa merkitystä myös lakien soveltamisvaiheessa.[134]

4.5. Eurooppalainen sääntely

Yksityiselämän ja henkilötietojen suojaa koskevia kansainvälisiä, ja ennen kaikkea eurooppalaisia, säännöksiä on nykyään runsaasti. Tietotekniikan nopea kehittyminen ja henkilötietojen käsittelyn automatisoituminen ovat lisänneet myös eurooppalaisen sääntelyn tarvetta. Osa normistosta on valtioita lainsäädäntötoimiin velvoittavaa, kun taas osa sääntelystä on ainoastaan suositusluontoista, jota voidaan käyttää apuna lainvalmistelussa sekä soveltamisohjeena lain ohella. Seuraavassa luodaan lyhyt katsaus yksityiselämän suojaa ja henkilötietojen suojaa koskevaan eurooppalaiseen sääntelyyn.

4.5.1. KP-sopimus ja Euroopan ihmisoikeussopimus

Ihmisoikeussopimukset ovat saaneet konkreettista tulkintasisältöä etupäässä sellaisissa asioissa, joissa ei Suomen lainsäädännöstä ole ollut samanlaista apua.[135] Oma

[132] HE 309/1993 vp, yksityiskohtaiset perustelut.
[133] HE 26/2001 vp, yksityiskohtaiset perustelut. Laissa henkilötietojen käsittelystä rangaistuksen täytäntöönpanossa (422/2002) on henkilötietolakiin nähden erityissäännökset henkilötietojen käsittelystä vapauteen kohdistuvien rangaistusten täytäntöönpanossa sekä tutkintavankeuden toimeenpanossa. Laki koskee henkilötietojen käsittelyä rikosseuraamusvirastossa ja kriminaalihuoltolaitoksessa sekä vankeinhoitolaitoksessa. Laki tuli voimaan 1.1.2003. Katso vankitietolaista tarkemmin: Korhonen 2003, s. 133.
[134] Viljanen 2001, s. 351
[135] Nieminen 1999, s. 120

merkityksensä kotimaisen yksityiselämän suojan taustalla on ollut KP-sopimuksen 17 artiklalla, joka kieltää laittomasti tai mielivaltaisesti puuttumasta kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon. Toisin kuin Euroopan ihmisoikeussopimuksessa, KP-sopimuksessa ei ole säädetty edellytyksistä, milloin yksityiselämän suojaan voidaan puuttua. Euroopan ihmisoikeussopimuksen konkreettinen valvontamenettely on tehnyt sen säännöksistä osittain pidemmälle meneviä kuin KP-sopimuksen. Sopimukset ovat sisällöllisesti lähellä toisiaan, mutta Euroopan ihmisoikeussopimus on seikkaperäisempi.[136] Tästä huolimatta KP-sopimuksen merkitystä ei kuitenkaan ole syytä aliarvioida.

Euroopan ihmisoikeussopimuksen 8 artiklan ensimmäinen kappale takaa jokaiselle oikeuden nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Artiklan 2 kappaleessa säädetään tilanteista, jolloin viranomaisilla on oikeus puuttua yksityiselämän suojaan. Viranomaiset saavat puuttua mainittuihin oikeuksiin vain, jos laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä tiettyjen artiklassa määrättyjen oikeuksien ja vapauksien turvaamiseksi. Artiklan 2 kappale sisältää tyhjentävän luettelon sopimuksen turvaamaan yksityiselämään puuttumiselle. Luettelossa mainitaan rajoitusperusteina kansallinen ja yleinen turvallisuus, maan taloudellinen hyvinvointi, epäjärjestyksen ja rikollisuuden estäminen, terveyden ja moraalin suojaaminen sekä muiden henkilöiden oikeuksien ja vapauksien turvaaminen.[137] Vaatimus rajoitusten välttämättömyydestä demokraattisessa yhteiskunnassa ilmentää edellä yleisenä rajoittamisen edellytyksenä mainittua suhteellisuusperiaatetta.

Perusoikeusuudistuksessa puollettiin ihmisoikeuksien ja perusoikeuksien tulkinnallista harmonisointia. Siten em. luettelolla on suuri merkitys arvioitaessa, onko jokin rajoitusperuste hyväksyttävä PeL:n yksityiselämän suojasäännöksen kannalta. Rajoitusperuste, joka ei esiinny luettelossa, ei kelpaa myöskään PeL:n turvaamaan yksityiselämän suojaan puuttumisen perusteeksi.[138] Koska yksityiselämän käsite omaksuttiin perusoikeusuudistuksen yhteydessä kotimaiseen perustuslakiin lähinnä

[136] Pölönen 1997, s. 19
[137] Viljanen 1999b, s. 339
[138] Viljanen 1999b, s. 339. Viljanen huomauttaa kuitenkin, että ihmisoikeussopimuksen hyväksyttävien rajoitusperusteiden luettelo on kirjoitettu niin väljäksi, ettei siitä voida päätellä kaikkien luettelossa esiintyvien rajoitusperusteiden olevan hyväksyttäviä myös perusoikeuden rajoitusperusteina. Esimerkiksi maan taloudellinen hyvinvointi on niin epämääräinen rajoitusperuste, ettei se sellaisenaan voi oikeuttaa ilman olennaisia täsmennyksiä yksityiselämän suojaan puuttumista Suomen PeL:n kannalta.

EIOS:n 8 artiklasta ja siihen liittyvästä oikeuskäytännöstä sekä KP-sopimuksen 17 artiklasta, voidaan katsoa, että PeL:n 10 §:n soveltamisessa voidaan nojautua vielä tavanomaista enemmän Euroopan ihmisoikeustuomioistuimen (EIT) tulkintakäytäntöön.[139] Nieminen huomauttaa kuitenkin, että on vaikea verrata keskenään sisällöllisesti EIOS:n 8 artiklaa ja toisaalta PeL:n 10 §:n vastaavia säännöksiä, sillä monet ihmisoikeussopimuksen mainitun artiklan tulkintaa koskevat tapaukset ovat ajalta ennen Suomen perusoikeusuudistuksen voimaantuloa.[140]

Myös EIT on pidättäytynyt antamasta yksityiselämän tarkkaa määritelmää. Sen mukaan tarkka määritteleminen ei ole mahdollista eikä tarpeellista. EIT on ratkaisuissaan kuitenkin korostanut yksityiselämän piiriin laajaa tulkintaa. EIT:n soveltamiskäytännön pohjalta voidaan tulkita perustuslain yksityiselämän suojan sisältävän ainakin henkilökohtaisen identiteetin suojan, moraalisen ja fyysisen koskemattomuuden suojan, vaatimuksen riittävän yksityisyyden turvaavista ulkonaisista olosuhteista, henkilötietojen suojan sekä vapauden päättää suhteistaan muihin ihmisiin.[141] Euroopan ihmisoikeussopimuksessa ei siis ole erityistä henkilötietojen suojaa koskevaa säännöstä. Euroopan ihmisoikeustuomioistuin on kuitenkin ratkaissut henkilötietojen käyttöön ja luovuttamiseen liittyviä asioita osana yksityiselämän suojaa.[142] Henkilörekisteröinnin ja henkilön yksityiselämää koskevien rekisteritietojen antamisen on katsottu merkitsevän puuttumista yksityiselämään.[143]

Vaikka aikaisemmin EIT:lla oli tapana painottaa vapaudenriistoon luonnostaan liittyviä rajoituksia vankien yksityiselämää koskevissa ratkaisuissaan, nyttemmin EIT on tunnustanut myös periaatteen vankien oikeudesta yksityiselämään, joten sovellettavien rajoitusten tulee olla perusteltavissa jollakin 8 artiklan 2 kappaleessa mainitulla syyllä. Vaikka vapausrangaistusta kärsivän kohdalla tällaisia perusteita on esitettävissä helpommin kuin monissa tilanteissa, kohtuuttoman pitkälle menevät rajoitukset voivat vanginkin kohdalla merkitä 8 artiklan loukkausta.[144] Siten myös

[139] Viljanen 1996, s. 797-798
[140] Nieminen 1999, s. 121. Niemisen mukaan vaikuttaa kuitenkin siltä, että Euroopan ihmisoikeussopimuksen 8 artikla on saanut enemmän itsenäistä sisältöä kuin PeL:n (ent. hallitusmuodon) vastaava säännös.
[141] Viljanen 1999b, s. 336-337
[142] Asiassa Z v. Suomi vuonna 1997 antamassaan tuomiossa EIT katsoi henkilötietojen suojan kuuluvan keskeisesti yksityiselämän suojaan.
[143] Pellonpää 2000, s. 452. Ks. esim. asia 9248/81 Leander v. Sweden, asia 28341/95 Rotaru v. Romania ja asia 27798/95 Amann v. Switzerland.
[144] Pellonpää 2000, s. 453-454. Ks. esim valitus 21132/93, päätös 1994 (kysymys vangin velvollisuudesta antaa virtsanäyte huumeidenkäytön kontrollia koskevassa tarkoituksessa).

ihmisoikeussopimuksen soveltamiskäytäntö on pidettävä mielessä, mikäli RFID-tunnisteita on tarkoitus asentaa vangeille.

4.5.2. OECD:n tietosuojasuositus ja Euroopan neuvoston tietosuojasopimus

OECD:n tietosuojasuositus vuodelta 1980[145] on yksityisyyden suojaa ja kansainvälistä henkilötietojen siirtoa koskeva lainsäädäntösuositus valtioille. Tietosuojasuositus sisältää henkilötietojen keräämistä ja laatua, rekisteröidyn tarkastusoikeutta, tietoturvaa ja kansainvälistä tiedonsiirtoa koskevia yleisperiaatteita.[146]

Euroopan neuvoston yleissopimus nro 108 yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä *(tietosuojasopimus)* koskee nimenomaisesti henkilötietojen keruuta ja rekisteröintiä. Tietosuojasopimuksen tulkintaa on edelleen selvennetty Euroopan neuvoston ministerikomitean antamilla suosituksilla.[147] Lehtonen pitää tietosuojasopimusta EIOS:n 8 artiklan ”standardina” henkilötietojen käsittelyn osalta.[148] Tietosuojasopimuksen tarkoituksena on turvata jokaiselle yksilölle sopimuspuolten alueella hänen oikeutensa ja perusvapautensa sekä erityisesti hänen oikeutensa yksityisyyteen henkilötietojen automaattisessa käsittelyssä. Sopimus ei sen sijaan sääntele tietojen luovuttamista. Tietosuojasopimuksella on katsottu olevan sitova asema kansainvälisessä oikeudessa. Suomen osalta tietosuojasopimus on ollut voimassa huhtikuusta 1992 lähtien (SopS 36/1992). Entinen henkilörekisterilaki ja nykyinen henkilötietolaki täyttävät sopimuksen vaatimukset.[149]

---

[145] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 23.8.1980.
[146] Lehtonen 2001, s.216-217. Tietosuojasuosituksessa esitetään kahdeksan erillistä tietosuojaperiaatetta, joista poikkeamisen tulisi olla mahdollisimman vähäistä.
[147] Annettuja suosituksia ovat: 1) Tutkimuksen ja tilastoinnin tietosuojaa koskeva suositus R(83) 10/23.9.1983; 2) Suoramarkkinointia koskeva suositus R(85) 20/25.10.1985; 3) Sosiaaliturvan tietosuojaa koskeva suositus R(86) 1/23.1.1986; 4) Poliisitoimen tietosuojaa koskeva suositus R (87) 15/17.9.1987; 5) Työelämän tietosuojaa koskeva suositus R(89) 2/18.1.1989; 6) Henkilötietojen suojaamisesta maksutapahtumissa annettu suositus R(90) 19/13.9.1990; 7) Viranomaisten henkilötietojen luovuttamista koskeva suositus R(91) 10/9.9.1991; 8)Teletoimintaa koskeva suositus R(95) 4/7.2.1995; 9) Lääketieteellisten tietojen suojaa koskeva suositus R(97) 5/13.2.1997; 10) Tietosuojaa henkilötietojen käsittelyssä tilastotarkoituksia varten koskeva suositus R(97) 18/30.9.1997.
[148] Lehtonen 2001, s. 210
[149] Korhonen 2003, s.93. Korhonen katsoo OECD:n tietosuojasuosituksen ja Euroopan neuvoston tietosuojasopimuksen olevan perusperiaatteiltaan varsin lähellä toisiaan.

4.5.3. EU:n perusoikeuskirja

Euroopan unionin perusoikeuskirja[150] hyväksyttiin joulukuussa 2000 Nizzan Eurooppa-neuvostossa. Alun perin perusoikeuskirjan katsottiin olevan lähinnä poliittinen julistus. Huolimatta siitä, että Ranska ja Hollanti äänestivät alkukesästä 2005 ”*ei*” EU:n perustuslaille, johon perusoikeuskirja olennaisena osana kuuluu, perusoikeuskirjalla nähdään tällä hetkellä olevan myös jonkinlaista juridista painoarvoa. Vaikka perusoikeuskirjan oikeudellinen merkitys on vielä jossain määrin avoin, perusoikeuskirjaan sisältyvistä periaatteista kirjoitetaan ja niihin viitataan oikeudellisissa kirjoituksissa.[151] Perusoikeusoikeuskirjan 7 artiklassa säädetään yksityis- ja perhe-elämän kunnioittamisesta. Perusoikeuskirjan 7 artiklalla on perusoikeuskirjan laatineen valmistelukunnan puheenjohtajiston antaman selvityksen mukaan sama merkitys ja kattavuus kuin EIOS:n 8 artiklalla.[152] Henkilötietojen suoja on perusoikeuskirjan mukaan erillinen perusoikeus, joka ei ole riippuvainen yksityiselämän suojasta. Tämä ilmentää hyvin perusoikeuksien dynaamisuutta.[153]

Henkilötietojen suojaa koskeekin erillinen perusoikeuskirjan 8 artikla, joka kuuluu seuraavasti:

Henkilötietojen suoja:

1. *Jokaisella on oikeus henkilötietojensa suojaan.*
2. *Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.*
3. *Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.*

Perusoikeuskirjassa henkilötietojen suojan voidaan nähdä jakaantuvan viiteen eri tekijään, joita ovat: 1) henkilötietojen käsittelyn asianmukaisuus, 2) käsittelyn perustuminen suostumukseen tai lakiin, 3) käyttötarkoituksen määrittelyvelvoite, 4) rekisteröidyn tarkastusoikeus ja oikeus virheen oikaisuun, 5) riippumattoman valvontaviranomaisen perustaminen.[154] Perusoikeuskirjan perusteluissa[155] viitataan henkilötietodirektiiviin. Siten on perusteltua lähteä siitä, että perusoikeuskirjan

[150] Euroopan unionin perusoikeusasiakirja 2000/C 364/01
[151] Korhonen 2003, s. 96. Professori Juha Karhu on luennoillaan (Karhu 2005) esittänyt, että perusoikeuskirjan oikeudellinen merkitys tulee nähdä ”enemmän tai vähemmän” -asiana riippuen perustuslain ratifioinnin onnistumisesta, eikä niinkään ”voimassa tai ei-voimassa” -asiana.
[152] CHARTE 4473/00 CONVENT 49, puheenjohtajiston selitykset. Tämän vuoksi tähän oikeuteen voidaan laillisesti tehdä ainoastaan ne rajoitukset, jotka on sallittu EIOS:n 8 artiklassa.
[153] Wallin 2001, s. 374
[154] Wallin 2001, s.374
[155] CHARTE 4473/00 CONVENT 49, puheenjohtajiston selitykset.

tarkoittama oikeus henkilötietojen suojaan kattaa saman alan kuin direktiivi.[156] Direktiivin sisältöä ja soveltamisalaa käsitellään tarkemmin jäljempänä.

4.5.4. Henkilötietodirektiivi ja henkilötietoasetus

Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta kutsutaan meillä *henkilötietodirektiiviksi* ja epävirallisemmissa yhteyksissä myös *tietosuojadirektiiviksi.* Direktiivin sisältöön vaikuttivat paljon sekä OECD:n tietosuojasuositus että varsinkin Euroopan neuvoston tietosuojasopimus.[157] Sekä direktiivi että tietosuojasopimus ovat EU:n jäsenvaltioita velvoittavia ja mahdollisessa ristiriitatilanteessa tulisi Blumen mukaan etusija antaa henkilötietodirektiivin säännöksille.[158]

Henkilötietodirektiivi annettiin silloisen Euroopan yhteisön perustamissopimuksen 100a artiklan nojalla ja se liittyy siten sisämarkkinoiden kehittämiseen.[159] Direktiivin tavoitteina on turvata yksilöiden perusoikeudet ja -vapaudet, erityisesti oikeus yksityisyyteen henkilötietojen käsittelyssä sekä henkilötietojen vapaa liikkuminen jäsenvaltioiden välillä *(1 artikla).* Jäsenvaltio ei saa estää henkilötietojen siirtämistä toiseen jäsenvaltioon yksityisyyden suojaan liittyvistä syistä. Jäsenvaltioiden on lisäksi huolehdittava siitä, että sen lainsäädäntöä sovelletaan direktiivin osoittamalla tavalla jäsenvaltiossa tapahtuvaan tai jäsenvaltioon muutoin liittyvään henkilötietojen käsittelyyn sekä valvottava henkilötietojen siirtoa kolmansiin maihin.[160]

Henkilötietodirektiivin soveltamisalaan kuuluvat sekä automaattinen että manuaalinen tietojenkäsittely (*3 artiklan 1 kohta*). Henkilötietodirektiiviä sovelletaan toimintoihin tai toimintojen kokonaisuuksiin, joita kohdistetaan henkilötietoihin, mitä kutsutaan tietojen ”käsittelyksi” (*2 artiklan b-kohta*). Tällaisia toimintoja ovat mm. henkilötietojen kerääminen, niiden säilyttäminen ja luovuttaminen.[161] Soveltamisalaan eivät kuulu sellaiset kysymykset, jotka ovat yhteisön oikeuden soveltamisalan ulkopuolella,[162] eikä

[156] Wallin 2001, s. 377
[157] Korhonen 2003, s. 94
[158] Blume 2001, s. 7
[159] Wallin 2001, s. 375
[160] Wallin 2001, s. 375
[161] Euroopan komissio 2000, s.4
[162] Korhonen 2003, s. 95. Yhteisöoikeuden soveltamisalan ulkopuolelle jäävät ulko- ja turvallisuuspolitiikkaan sekä oikeudelliseen yhteistyöhön, poliisi- ja pakolaisasioihin ja valtion turvallisuuteen liittyvä henkilötietojen käsittely.

sellainen henkilötietojen käsittely, jonka luonnollinen henkilö suorittaa henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa *(3 artiklan 2 kohta)*.[163]

Henkilötietodirektiivi muodostaa sääntelyjärjestelmän, joka määrittelee, millaisia vaatimuksia yksilön suojan toteuttamiseksi on asetettava kansallisessa lainsäädännössä. Direktiivi asettaa kuitenkin ainoastaan yleispuitteet kansalliselle lainsäädännölle. Korhosen mukaan kansallista lainsäädäntöä valmisteltaessa on aiheutunut vaikeuksia tulkita sitä, mitkä direktiivin säännökset ovat ehdottoman sitovia ja mitkä taas enemmän mukailtavissa kansallisella tasolla. Tämän vuoksi myöskään pohjoismaiset henkilötietosäädökset eivät ole täysin identtisiä sisällöltään.[164] Suomen lainsäädäntö on saatettu vastaamaan henkilötietodirektiivin vaatimuksia 1.6.1999 voimaan tulleella henkilötietolailla (HetiL 523/1999).

Euroopan yhteisöjen perustamissopimuksen 286 artiklan perusteella[165] on säädetty Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja niiden tietojen vapaasta liikkuvuudesta *(henkilötietoasetus)*, joka täydentää henkilötietodirektiiviä.[166] Henkilötietoasetuksen peruslähtökohdat ovat samat kuin henkilötietodirektiivissä.[167] Asetuksen sääntely on kuitenkin tietyiltä osin yksityiskohtaisempaa ja syvemmälle menevää kuin direktiivin.[168]

4.5.5. Tietosuojatyöryhmän työasiakirja RFID-tunnistukseen liittyvistä tietosuojakysymyksistä

Henkilötietodirektiivin 29 artiklan mukaisesti on perustettu *tietosuojatyöryhmä* (jälj. *työryhmä*). Tietosuojatyöryhmä on riippumaton neuvoa-antava asiantuntijaelin tietosuojaan liittyvissä kysymyksissä *(29 artiklan 1 kohta)*. Erityisesti se neuvoo komissiota yksilöiden oikeuksiin ja vapauksiin vaikuttavissa päätöksissä, jotka liittyvät

[163] Euroopan komissio 2000, s. 4. Esimerkiksi sähköisessä muodossa oleva henkilökohtainen päiväkirja tai perheenjäsenten ja ystävien tiedot sisältävä kortisto eivät kuulu soveltamisalaan.
[164] Korhonen 2003, s. 95
[165] Euroopan yhteisöjen perustamissopimuksen 286 artikla määrää, että yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annettuja yhteisön säädöksiä sovelletaan yhteisön toimielimiin ja elimiin.
[166] Korhonen 2003, s. 95
[167] Wallin 2001, s. 375-376. Suojeltavia ovat henkilötietoasetuksen mukaan henkilöt, joiden henkilötietoja yhteisöjen toimielimet käsittelevät. Asetusta sovelletaan henkilötietojen käsittelyyn, joka tapahtuu EU:n toimielimissä, elimissä ja laitoksissa yhteisön oikeuden soveltamisalaan kuuluvien toimien toteuttamiseksi.
[168] Korhonen 2003, s. 95

henkilötietojen käsittelyyn ja yksityisyyteen.[169] Työryhmä koostuu jäsenvaltioiden tietosuojaviranomaisten edustajista *(29 artiklan 2 kohta)*. Työryhmän tavoitteena on mm. tutkia ja esittää tietosuojadirektiivin soveltamiseen ja tulkintaan liittyviä kysymyksiä. Se antaa tietosuojaan liittyviä lausuntoja ja suosituksia komissiolle sekä julkaisee vuosittain toimintakertomuksen.[170]

Työryhmä julkaisi 19.1.2005 työasiakirjan koskien RFID-tunnistukseen liittyviä tietosuojakysymyksiä.[171] Työryhmä kiinnitti huomionsa siihen, että tätä tekniikkaa voidaan käyttää myös siten, että se loukkaa ihmisoikeuksia ja erityisesti yksityisyyden suojaa. Työasiakirjassa mainitaan, että RFID-tekniikan potentiaalisia väärinkäyttäjiä ovat mm. yritykset ja valtiot. Työryhmän mukaan teknologian herättämiä yksityisyyden suojaan liittyviä kysymyksiä ovat esimerkiksi mahdollisuus kerätä salaa erilaisia tietoja yksityishenkilöistä, mahdollisuus seurata ihmisiä heidän liikkuessaan julkisilla paikoilla, mahdollisuus lukea tietoja asiakkaiden kantamista tavaroista sekä kauppojen laatimat tarkennetut ostajaprofiilit. Tieto uudesta riskistä pakotti työryhmän tutkimaan RFID-teknologiaan liittyviä yksityisyyden suojan ja muiden perusoikeuksien loukkauksia. Työryhmä kertoi konsultoineensa työasiakirjaa varten eri intressitahoja; kuten teknologian valmistajia, käyttöönottajia ja yksityisyyden suojaan perehtyneitä asianajajia. Työryhmä kertoi työasiakirjalla olevan kaksi päätehtävää: ensinnäkin antaa neuvoja RFID-tekniikan käyttöönottajille henkilötietodirektiivin perusperiaatteiden soveltamisesta ja toiseksi antaa neuvoja RFID-teknologian valmistajille ja standardisointielimille heidän vastuustaan suunnitella sellaisia teknisiä ratkaisuja, jotka huomioivat yksityisyyden suojaan.[172]

Työryhmä korosti työasiakirjan olevan vasta ensiarvio tilanteesta kyseisellä alueella. Työryhmä lupasi jatkaa tilanteen seurantaa ja tekniikan kehittyessä antaa tarvittaessa lisäohjeistusta.[173] Tietosuojatyöryhmän menettelytapoihin kuuluu, että se kuulee eri intressitahoja työasiakirjoistaan. Niinpä se asetti työasiakirjansa julkisesti kommentoitavaksi. Julkinen lausuntokierros herätti laajaa mielenkiintoa, sillä

[169] http://www.effi.org/yksityisyys/rfid-11-3-2005.html
[170] http://www.tietosuoja.fi/14891.htm
[171] Työasiakirja WP 105
[172] Työasiakirja WP 105, s. 2-3
[173] Työasiakirja WP 105, s. 3

määräaikaan mennessä lausunto saatiin 34:ltä eri taholta.[174] Tietosuojatyöryhmän ja lausunnonantajien kannanottoja käsittelen tarkemmin jäljempänä.

[174] Lausunnoista kahdeksan oli yksityishenkilöitä, yksi kuluttajansuojajärjestöltä, yhdeksän yliopistoilta tai ajatushautomoilta (*”think tank”*) ja kuusitoista yrityksiltä tai kauppajärjestöiltä. Monet lausunnon antajat edustavat liikevaihdoltaan suuria yrityksiä. Tiivistelmä lausunnoista ja lausunnot ovat saatavissa osoitteessa:
http://www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/consultations/rfid_en.htm

5. Henkilötietojen suoja henkilötietolain mukaan

5.1. Henkilörekisterilaista henkilötietolakiin

Henkilötietojen käsittelyä koskevat yleiset säännökset sisältyivät ennen nykyisen henkilötietolain voimaantuloa *henkilörekisterilakiin*. Henkilörekisterilaki (*HenkRekL* 471/1987) oli ns. yleislaki, millä tarkoitetaan sitä, että sitä sovellettiin vain silloin, kun muissa laeissa tai asetuksissa ei ollut toisin säädetty.[175] Henkilörekisterilaki määritteli henkilötietojen keräämiseen, tallentamiseen, käyttöön ja luovuttamiseen liittyvät oikeudet ja velvollisuudet. HenkRekL:n takaaman suojan tarkoituksena oli tiedon kohteena olevan henkilön yksityisyyden sekä hänen etujensa ja oikeuksiensa turvaaminen. Laki valmisteltiin ottamalla huomioon Euroopan neuvoston tietosuojasopimus. Lailla pyrittiin rekisteritoimintojen yleisohjaukseen lakiin sisältyneiden yleisvelvoitteiden avulla. Niitä täydensivät säännökset rekisteröityjen oikeuksista sekä valvontaviranomaisen ohjaus- ja tarkastustoimintaa sekä seuraamuksia koskeva säädökset. Henkilörekisterilakia sovellettiin sekä viranomaisten että yksityisten pitämiin rekistereihin ja se kattoi sekä atk-pohjaiset että manuaaliset rekisterit.[176]

Henkilötietodirektiivi tuli implementoida EU:n jäsenvaltioiden kansallisiin tietosuojasäännöksiin kolmen vuoden kuluessa sen antamisesta eli 24.10.1998 mennessä. Vaikka Suomessa asetettiin jo lokakuun 1995 alussa henkilötietotoimikunta valmistelemaan asiaa, Suomi myöhästyi implementoinnissa monien muiden maiden tavoin.[177] Henkilötietolaki (HetiL 523/1999) annettiin 22.4.1999 ja se tuli voimaan 1.6.1999.

Oikeuspoliittisen tutkimuslaitoksen uusimpien tutkimusten mukaan suomalaiset ovat entistä kiinnostuneempia henkilötietojensa asianmukaisesta käsittelystä. Suomessa

[175] Korhonen 2003, s. 114

[176] HE 49/1986 vp, yleisperustelut. Ks. myös Korhonen 2003, s. 114-115: Henkilörekisterilaki toteutti tietosuojan yleisiä perusperiaatteita: hyvän rekisteritavan periaatetta; tarpeettomat henkilörekisterit oli hävitettävä; henkilöllä oli oikeus tarkastaa itseään koskevat tiedot henkilörekisteristä sekä saada tietää rekisterin käyttötarkoitus, käyttötekniikka, rekisterin sisältämät tiedot ja tietojen luovutuskohteet; henkilöllä oli oikeus kieltää itseään koskevien tietojen luovuttaminen suoramainontaan, osoite- ja postipalveluun sekä markkinointi- ja mielipidetutkimukseen.

[177] Korhonen 2003, s. 94 ja s. 116-117. Vain Kreikka, Italia, Portugali ja Ruotsi implementoivat lain ajoissa. Sittemmin implementointi on toteutettu sekä kaikissa vanhoissa jäsenvaltiossa että uusissa jäsenvaltioissa (TK).

henkilötietojensa suojaa epäili vuonna 2003 kuitenkin edelleen hieman pienempi osa väestöstä kuin koko Euroopan unionin alueella.[178]

5.2. Soveltamisala ja henkilötietojen käsittelyä koskevat yleiset edellytykset

Henkilötietolakia sovelletaan henkilötietojen käsittelyyn. Laki koskee viranomaisten, yritysten, järjestöjen, muiden yhteisöjen ja yksityisten henkilöiden toimintaa. Soveltamisalan ulkopuolelle jää tietyin rajoituksin henkilötietojen käsittely toimituksellisia sekä taiteellisen ja kirjallisen ilmaisun tarkoituksia varten. Lakia ei sovelleta myöskään tavanomaiseen, yksinomaan henkilökohtaisessa tarkoituksessa tapahtuvaan henkilötietojen käsittelyyn. Tällaista käsittelyä on muun muassa tuttavapiirin osoitteiden ylläpito. Lakia sovelletaan sekä automaattiseen tietojenkäsittelyyn että manuaalisesti tapahtuvaan henkilötietojen käsittelyyn.[179]

Henkilötietolain 3 §:n 1-kohdan määritelmän mukaan *henkilötiedolla* tarkoitetaan kaikenlaisia luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. Henkilötiedon määritelmä laajentui hieman henkilörekisterilakiin verrattuna.[180]

Uutena yleiskäsitteenä henkilötietolaissa määritellään *henkilötietojen käsittely*. Sillä tarkoitetaan 3 §:n 2-kohdan mukaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista ja tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.[181] Siten henkilötietojen käsittely kattaa kaikki toimenpiteet,

---

[178] Muttilainen 2006, s. 74. Eurobarometri-kyselyn mukaan noin joka toinen 15 vuotta täyttänyt suomalainen ja kuusi kymmenestä EU:n asukkaasta oli huolissaan yksityisyydestään henkilötietojen käsittelyssä.

[179] Tietosuojavaltuutetun toimisto 2002, s. 2

[180] Henkilörekisterilaissa sillä tarkoitettiin luonnollista, yksityistä henkilöä koskevia tietoja. Lainkohdan maininta ominaisuuksia ja elinolosuhteita kuvaavista merkinnöistä sisältää hallituksen esityksen mukaan ajatuksen siitä, että henkilötietoja ovat jollekin alustalle talletetut tiedot. Käsitteen kannalta merkitystä ei ole sillä, millä keinoin tai mille alustalle tieto on tallennettu.

[181] Määritelmän selkeänä esikuvana on henkilötietodirektiivin 2 artiklan b-kohdan vastaavanlainen laaja määritelmä: ”henkilötietojen käsittelyllä (”käsittely”) tarkoitetaan kaikenlaisia sellaisia toimintoja tai toimintojen kokonaisuuksia, joita kohdistetaan henkilötietoihin joko automaattisen tietojenkäsittelyn avulla tai manuaalisesti, kuten tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen tai muuttaminen, tiedon haku, kysely, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville, yhteensovittaminen tai yhdistäminen sekä suojaaminen, poistaminen tai tuhoaminen.”

jotka kohdistuvat henkilötietoihin niiden keräämisestä aina luovuttamiseen tietojen kerääjän määräysvallan ulkopuolelle.[182]

Henkilötietolain kolmas merkittävä käsite on *henkilörekisteri.*[183] Sillä tarkoitetaan 3 §:n 3-kohdan mukaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla tai joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia. Hallituksen esityksessä on kuvattu tarkemmin tätä *ns. loogista rekisterikäsitettä*.[184]

Henkilötietojen käsittelyn yleiset edellytykset luetellaan henkilötietolain 8 §:ssä.[185] Pykälää voidaan pitää lain tärkeimpänä yksittäisenä pykälänä.[186] Tyhjentäväksi kirjoitetun 9-kohtaisen luettelon mukaan henkilötietoja saa käsitellä ainoastaan (HetiL 8 §:n 1 mom):

> *”1) rekisteröidyn yksiselitteisesti antamalla suostumuksella;*
>
> *2) rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;*
>
> *3) jos käsittely yksittäistapauksessa on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi;*
>
> *4) jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta;*

---

[182] Ollila 2002, s. 300

[183] Korhonen 2003, s.142

[184] HE 96/1998 vp. yksityiskohtaiset perustelut. Looginen rekisterikäsite merkitsee, että samaan henkilörekisteriin luetaan kuuluviksi kaikki ne tiedot, joita käytetään samassa käyttöyhteydessä riippumatta siitä, miten ja mihin ne on talletettu. Looginen rekisterikäsite merkitsee myös sitä, että tietojenkäsittelyssä syntyviä lyhytaikaisia tiedostoja ja tallenteiden eri sukupolvia ei pidetä eri henkilörekistereinä silloin, kun ne ovat rekisterinpitäjän hallussa ja niitä käytetään määriteltyihin henkilötietojen käsittelyn tarkoituksiin. Automaattisen tietojenkäsittelyn avulla toteutettava tekstinkäsittely, kuten päätöksen, muistion, luettelon, kirjeen tai muun vastaavan asiakirjan laatiminen, ei vielä sellaisenaan muodostaisi ehdotetussa laissa tarkoitettua henkilörekisteriä, vaikka siinä käsiteltäisiin henkilötietoja. Edellytykseksi asetetaan se, että tekstinkäsittelyllä yksinomaan tuotetaan asiakirja ilman, että asiakirjaa pysyvämmin säilytetään sähköisessä muodossa osana tietojenkäsittelyjärjestelmää.

[185] HE 96/1998 vp. yksityiskohtaiset perustelut. Pykälä perustuu henkilötietodirektiivin 7 artiklaan sisältyvään lainsäädäntötoimeksiantoon. Artiklassa määritellään jäsenvaltioita velvoittavalla tavalla tietojenkäsittelyn laillisuutta koskevat periaatteet.

[186] Korhonen 2003, s. 162

*5) jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan (*yhteysvaatimus*);*

6) jos kysymys on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista ja näitä tietoja käsitellään kyseisen yhteenliittymän sisällä;

7) jos käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai muita niihin verrattavia tehtäviä varten;

8) jos kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedoista ja näitä tietoja käsitellään rekisterinpitäjän tai tiedot saavan sivullisen oikeuksien ja etujen turvaamiseksi; tai

9) jos tietosuojalautakunta on antanut käsittelyyn 43 §:n 1 momentissa tarkoitetun luvan."

Henkilötietojen käsittely on siis sallittua vain silloin, kun jokin momentissa mainittu edellytys täyttyy. Käytännössä yleisin henkilötietojen käsittelyn edellytys on 1-kohdassa mainittu *rekisteröidyn yksiselitteisesti antama suostumus.*[187] Suostumuksella tarkoitetaan 3 §:n 7-kohdan mukaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Henkilötietojen käsittelyn tulee lähtökohtaisesti perustua rekisteröidyn suostumukseen, koska suostumukseen perustuvassa käsittelyssä toteutuu parhaiten henkilön tiedollinen itsemääräämisoikeus ja rekisterinpidon avoimuus. Hallituksen esityksen mukaan yksiselitteisen suostumuksen vaatimus ei täyty, jos esimerkiksi rekisteröidyltä pyydetään hänen sairaalaan saapuessaan yleinen suostumus hänen terveyttään tai hoitoaan koskevien tietojen luovuttamiseen. Tällaisessa tapauksessa rekisteröity ei suostumusta antaessaan ole vielä voinut tietää, millaisten tietojen luovuttamista suostumus koskee. Lisäksi hallituksen esityksessä todetaan, että suostumukselle asetettavat vaatimukset määräytyvät viimekädessä tapauskohtaisesti. Tällöin merkitystä on annettava muun muassa kerättävien tietojen laadulle. Jos suostumuksen olemassaolosta syntyisi kiistaa, todistustaakka suostumuksen olemassaolosta on rekisterinpitäjällä.[188] Katso suostumuksen ensisijaisuudesta tarkemmin kappaleessa 7.2.2.1.

[187] Suostumuksen vaatimus vastaa asiallisesti henkilörekisterilain aikaista sääntelyä ja henkilötietodirektiivin (95/46/EY) 7 artiklan a alakohtaa.
[188] HE 96/1998 vp. yksityiskohtaiset perustelut.

Arkaluonteisten henkilötietojen käsittely on lähtökohtaisesti henkilötietolain 11 §:n nojalla kielletty.[189] Kiellosta on kuitenkin poikkeuksia, jotka on lueteltu 12 §:ssä, ja jotka tekevät arkaluonteisten henkilötietojen käsittelystä sallittua.

On huomattava, että viranomaisten rekistereissä olevien tietojen julkisuuteen sovelletaan lakia viranomaisten toiminnan julkisuudesta *(621/1999 julkisuuslaki, JulkL).* Siten ulkopuolisen oikeus saada tietoa viranomaisen pitämistä rekistereistä ratkaistaan samalla tavalla kuin tietojen saaminen muistakin viranomaisen asiakirjoista. Henkilötietolain 8 §:n 4 momenttiin on otettu asiasta säännös, jonka mukaan oikeudesta saada tieto ja muusta henkilötietojen luovuttamisesta viranomaisen henkilörekisteristä on voimassa, mitä viranomaisten asiakirjojen julkisuudesta säädetään. Vaikka henkilötietojen luovutukseen viranomaisten henkilörekistereistä sovelletaankin tiettyjä julkisuuslain pykäliä, henkilötietolain yleisperiaatteet tulevat silti sovellettavaksi.[190] Saarenpää on todennut, että vaikka viranomaisten rekistereistä on koko joukko erityislakeja – kuten esimerkiksi julkisuuslaki – henkilötietolaki on myös niiden osalta yleensä ensisijainen laki. Henkilötietolaki syrjäytyisi vain, mikäli toisessa laissa sivuutettaisiin kaikki henkilötietolain säännökset. Toistaiseksi yhtään tällaista kattavasti henkilötietolain sivuuttavaa lakia ei ole säädetty.[191]

5.3. Henkilötietojen käsittelyn periaatteet

Henkilötietolain 2 luku sisältää tärkeitä henkilötietojen käsittelyn yleisperiaatteita, joilla lain tavoitetta[192], yksityisyyden suojaamisvaatimusta, käytännössä toteutetaan. Tässä luvussa tarkastellaan tärkeimpiä henkilötietolain mukaisia henkilötietojen käsittelyn yleisiä periaatteita: huolellisuusvelvoitetta, tarpeellisuusvaatimusta sekä suunnitteluvelvoitetta ja käyttötarkoitussidonnaisuutta. Lisäksi tässä luvussa käsitellään tietoturvallisuuden vaatimusta henkilötietojen käsittelyssä.

---

[189] Arkaluonteisina tietoina pidetään 11 §:n mukaan henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan: 1) rotua tai etnistä alkuperää; 2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista; 3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta; 4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia; 5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka 6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

[190] Ks. tarkemmin julkisuuslain soveltamisalasta ja tarkoituksesta Korhonen 2003, s. 140-144.

[191] Saarenpää 2005, s. 429

[192] Henkilötietolain 1 §:n mukaan lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

5.3.1. Huolellisuusvelvoite

Henkilötietolain 5 §:ssä asetetaan huolellisuusvelvoite rekisterinpitäjälle ja sille, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun. Pykälän mukaan näiden tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta.

Hallituksen esityksen mukaan pykälä ilmentää jo henkilörekisterilaissa omaksuttua rekisterinpidon itseohjautuvuuden ajatusta, mikä tarkoittaa, että rekisterinpitäjät pyrkivät oma-aloitteisesti huolehtimaan siitä, että henkilötietojen käsittely toteutetaan ottaen huomioon yksityisyyden suojaa turvaavat säännökset ja periaatteet.[193] Hallituksen esityksen mukaan *hyvään tietojenkäsittelytapaan* sisältyvät muun muassa yksityisyyttä tukevat menettelytavat henkilötietoja käsiteltäessä. Tämä tarkoittaa muun ohella sitä, että käsiteltävien tietojen suojaamisesta huolehditaan asianmukaisella tavalla. Lisäksi hallituksen esityksessä todettiin, että rekisterinpitäjän on otettava huomioon 1 §:n tarkoitussäännöksessä ilmaistut lain tavoitteet ja toimittava niitä edistävästi.[194]

Saarenpään mukaan huolellisuusvelvoitetta voidaan pitää normiteoreettisesti eräänlaisena *optimointikäskynä*. Henkilötietoja on käsiteltävä niin, että huolellinen henkilötietojen käsittelijä varoo avoimessa tulkintatilanteessa toimimasta yksityisyyttä loukkaavalla tavalla. Huolellisuusvelvoite ohjaa tarpeellisten tietojen määrää pohdittaessa ensisijaisesti minimoimaan käsiteltävien tietojen määrän.[195]

Pykälässä asetettua laillisuuden vaatimusta voidaan pitää epätavallisena edellytyksenä lainsäädännössämme. Lakihan velvoittaa jo olemassaololollaan toimimaan sen mukaisesti. Nyyssölä pitää sanonnan mahdollisena perusteena sitä, että henkilötietojen käsittelyä koskeva lainsäädäntö on oikeudenalana melko uutta.[196] Taustalla vaikuttaa varmasti myös henkilötietodirektiivin 6 artiklan 1-kohdan a-alakohta, jossa edellytetään

[193] HE 96/1998 vp. yksityiskohtaiset perustelut.
[194] HE 96/1998 vp. yksityiskohtaiset perustelut.
[195] Saarenpää 2005, s. 415
[196] Nyyssölä 2001, s.34

jäsenvaltioiden säätävän siitä, että henkilötietoja käsitellään asianmukaisesti ja laillisesti. Hallituksen esityksessä lausetta ei perusteltu lainkaan.

5.3.2. Tarpeellisuusvaatimus

Henkilötietolain 9 §:n 1 momentin mukaan käsiteltävien henkilötietojen tulee olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia.[197] Hallituksen esityksen mukaan henkilötietoja voidaan pitää käsittelyn tarkoituksen kannalta tarpeellisina silloin, kun ne ovat asianmukaisia ja olennaisia eivätkä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään. Vaatimus kohdistuu sekä rekisterinpidon tarpeellisuuteen yleensä että rekisterin käyttötarkoitukseen. Henkilörekisteriä saa pitää ja käyttää vain sellaisessa tarkoituksessa ja siten, että toiminta täyttää asiallisuuden ja yleisen mittapuun mukaan arvioituna myös hyväksyttävyyden kriteerit.[198] Saarenpää on todennut tarpeellisuusvaatimuksen olevan keskeinen mittapuu rekisterinpitäjän toiminnalle. Tarpeellisuusvaatimus liittyy läheisesti jäljempänä käsiteltävään suunnitteluvelvoitteeseen (ks. luku 5.3.3), sillä tietojärjestelmät ja niiden käyttö on suunniteltava *tarpeellisten tietojen* käsittelyä varten.[199]

Rekisterinpidon perusteena ei voi olla mikä tahansa syy, esimerkiksi yleinen mielenkiinto toisten ihmisten asioihin, vaan rekisterinpitäjän toiminnasta johtuva, yleisesti hyväksyttävä tarve käyttää toiminnassa henkilötietoja.[200] Tarpeellisuusvaatimus tähtää henkilötietojen rekisteröinnin minimointiin. Se edellyttää, että vältetään kaikkien sellaisten tietojen tallettamista, joita ei tavanomaisesti ja usein tarvita rekisterin käyttötarkoituksen mukaiseen toimintaan. Rekisterinpitäjällä ei siis välttämättä ole oikeutta tallettaa henkilörekisteriin kaikkea sitä tietoa, jota toimintaa varten on oikeutettu saamaan.[201] Konstari lähtee siitä, että riittävää ei ole pelkästään se, että tiedon tallentaminen rekisteriin on rekisterinpitäjän tehtävien ja toiminnan kannalta *hyödyllistä.* Toisaalta ei myöskään ole perusteltua lähteä niin ankarasta vaatimuksesta, että tiedon tallentaminen henkilörekisteriin on oltava rekisterinpitäjän tehtävien kannalta

[197] Henkilötietodirektiivin (95/46/EY) 6 artiklan 1 kohdan d-alakohdassa jäsenvaltiot velvoitetaan säätämään siitä, että henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä. Rekisterinpitäjän on artiklan 2 kohdan mukaan huolehdittava käsiteltävien tietojen tarpeellisuus- ja virheettömyysvaatimuksen noudattamisesta.
[198] HE 96/1998 vp. yleisperustelut ja yksityiskohtaiset perustelut
[199] Saarenpää 2005, s. 411
[200] Wallin & Nurmi 1991, s. 40
[201] Wallin & Nurmi 1991, s. 67.

katsoen *ehdottoman välttämätöntä.*[202] Myös Lehtonen lähtee siitä, että rekisterinpitäjän tulee pääsääntöisesti minimoida rekisteriin koottavat tiedot yksilöstä, eikä käyttötarkoituksen kannalta merkityksettömien tietojen kokoaminen ”varmuuden vuoksi” ole sallittua.[203] Tarpeellisuutta tuleekin arvioida ajan ja käyttötarkoituksen näkökulmasta suppeasti. Siten vain todellinen ajankohtainen tarve on hyväksyttävä tarve.[204]

5.3.3. Suunnitteluvelvollisuus ja käyttötarkoitussidonnaisuus

Henkilötietolain 6 §:n mukaan henkilötietojen käsittelyn tulee olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot säännönmukaisesti hankitaan ja mihin niitä säännönmukaisesti luovutetaan, on määriteltävä ennen henkilötietojen keräämistä tai muodostamista henkilörekisteriksi. Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään *(suunnitteluvelvoite eli suunnitelmallisuusvaatimus).* Keskeistä suunnitelmallisuusvaatimuksen toteuttamisen kannalta on, että viimeistään ennen tietojen tallentamista laaditaan asianmukainen rekisterikuvaus eli HetiL 10 §:n mukainen *rekisteriseloste.*[205] Suunnitteluvelvoitteen tarkoituksena on parantaa yleistä rekisteritoiminnan ennakoitavuutta, mikä puolestaan on olennainen elementti rakennettaessa yhtenäistä *hyvää rekisteritapaa.*[206] Saarenpään mukaan suunnitelmallisuuden vaatimus edellyttää sellaista ennen sallitun käsittelyn aloittamista tapahtuvaa suunnittelua, missä otetaan huomioon informaation hankintatavat, sen erilaiset käsittelytavat, käyttötarkoitukset, mahdolliset luovutukset sekä säilyttäminen, arkistointi ja tuhoaminen. Näin ollen suunnitelmallisuuden voidaankin sanoa ulottuvan tiedon koko elinkaareen.[207]

Kumotun henkilörekisterilain mukaan oli mahdollista määritellä myöhemmin uudelleen henkilörekisterin käyttötarkoitus sekä säännönmukaiset tietojensiirrot, jos se oli muuttuneiden olosuhteiden vuoksi tarpeen eikä näin määritelty käyttötarkoitus olennaisesti poikennut alkuperäisestä käyttötarkoituksesta. Vaikka henkilötietolaissa ei

[202] Konstari 1992, s. 147
[203] Lehtonen 2001, s. 237
[204] Saarenpää 2005, s. 411
[205] Lehtonen 2001, s. 236
[206] Wallin & Nurmi 1991, s. 43
[207] Saarenpää 2005, s. 412

ole vastaavaa säännöstä, henkilötietojen käsittelyn tarkoitus sekä säännönmukaiset tietojensiirrot voidaan hallituksen esityksen mukaan määritellä myöhemmin uudelleen, jos se on muuttuneiden olosuhteiden vuoksi tarpeen.[208]

Yksi keskeinen henkilötietojen käsittelyä koskeva periaate on *käyttötarkoitussidonnaisuus.* Käyttötarkoituksen keskeinen asema ilmenee jo perusoikeuskirjan 7 artiklasta, jonka mukaan henkilötietojen käsittelyn tulee tapahtua tiettyä tarkoitusta varten. Vaatimus merkitsee velvollisuutta määritellä etukäteen henkilörekisterin ja siihen talletettavien erilaisten tietojen käyttötarkoitus. Käyttötarkoituksen kautta ja avulla määritellään monet keskeiset henkilötietojen suojaan vaikuttavat tekijät, kuten käsiteltävien tietojen sisältö ja laatu, tietojen käyttö käsittelijän toiminnassa ja tietojen luotettavuus.[209] Henkilötietolaissa käyttötarkoitussidonnaisuutta ilmentää ennen kaikkea 7 §, jonka mukaan henkilötietoja saa käyttää tai muutoin käsitellä vain tavalla, joka ei ole yhteensopimaton 6 §:ssä tarkoitettujen käsittelyn tarkoitusten kanssa.[210] Myöhempää henkilötietojen käsittelyä historiallista tutkimusta taikka tieteellistä tai tilastotarkoitusta varten ei pidetä yhteensopimattomana alkuperäisten käsittelyn tarkoitusten kanssa.

Säännöksen tarkoituksena on kiinnittää rekisterinpitäjän huomio siihen, että henkilörekisteriä pidetään aina ja vain tiettyä tarkoitusta varten.[211] Henkilörekisterin käyttötarkoitus on määriteltävä siten, että siitä ilmenee, millaisten rekisterinpitäjän tehtävien hoitamiseksi kyseistä rekisteriä käytetään.[212] Käyttötarkoitussidonnaisuus koskee myös tietojen luovuttamista. Henkilötietoja ei saa luovuttaa käytettäväksi muuhun kuin rekisteröitäessä määriteltyihin tarkoituksiin, jollei käsittely perustu rekisteröidyn suostumukseen.[213]

---

[208] HE 96/1998 vp. yksityiskohtaiset perustelut. On huomattava, että henkilötietodirektiivin (95/46/EY) 6 artiklan 1 kohdan b alakohdan huomioon ottaen näin määritelty tarkoitus ei kuitenkaan saa olla yhteensopimaton henkilötietojen alkuperäisen käsittelyn tarkoituksen kanssa.
[209] Wallin 2001, s. 379
[210] Pykälä toteuttaa henkilötietodirektiivin (95/46/EY) 6 artiklan 1 kohdan b alakohdan vaatimusta, jossa velvoitetaan jäsenvaltiot säätämään siitä, että henkilötiedot kerätään tiettyjä määriteltyjä ja laillisia tarkoituksia varten, eikä niitä saa myöhemmin käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla.
[211] Lehtonen 2001, s. 237
[212] Wallin & Nurmi 1991, s. 43
[213] Wallin 2001, s. 380

5.3.4. Tietoturvallisuuden vaatimus

Henkilötietolain 32 §:n 1 momentin mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta. Pykälä ilmentää *tietoturvallisuuden* periaatetta, joka on luettava nykyään yhdeksi tietosuojan perusperiaatteista.

Pykälässä ei ole pyritty määrittämään täsmällisesti tietoturvan tasoa. Tietoturvallisuus on Saarenpään mukaan kuitenkin pyrittävä mitoittamaan suojatarpeen mukaan. Henkilötietolain 32 §:n 1 momentin valossa *oikeutta tietoturvaan* voidaan pitää yksilön oikeutena henkilötietojen käsittelyssä, joten vaadittava tietoturvallisuuden taso ei voi olla vaatimaton. Saarenpää toteaa kuitenkin, että tietojärjestelmien ylläpitäjät pyrkivät usein asettamaan taloudellisen tehokkuuden yksilön oikeuksien edelle, joten tietoturva on yksi henkilötietojen suojan riskialteimmista elementeistä.[214]

5.4. Rekisteröidyn oikeudet

Yksilön mahdollisuuksiin valvoa itseään koskevien tietojen käyttöä ja muuta käsittelyä vaikuttaa *tietojenkäsittelyn avoimuus.* Siksi rekisteröidyn oikeus saada tietoja on keskeisin itsemääräämisoikeuden ja henkilötietojen suojan toteutumisen edellytys. Oikeus saada tietoja toimii yhtenä vallan käyttöä tasaavana tekijänä, jonka avulla rekisteritoiminnot tehdään läpinäkyviksi ja annetaan siten mahdollisuus yksilölle käyttää muita valvontakeinojaan sekä mahdollista määräämisvaltaansa.[215]

Henkilötietojen käsittelyn avoimuus on pyritty varmistamaan henkilötietolain 6 luvusta ilmenevillä rekisteröidyn oikeuksilla, joita ovat *rekisterinpitäjän informointivelvollisuus tietojen käsittelystä, rekisteröidyn tarkastusoikeus* ja *rekisterinpitäjän tiedonantovelvollisuus.* On huomattava, että rekisteröidyn oikeudet eivät kuitenkaan

[214] Saarenpää 2005a, s. 405
[215] Wallin 2001, s. 383

anna täydellistä itsemääräämisoikeutta määrätä omien tietojen käytöstä. Yksityisyyden suojan voitaisiin arvioida olevan maksimissaan, jos henkilötietoja saisi käsitellä kaikissa tilanteissa vain rekisteröidyn suostumuksella. Perusoikeusnäkökulmasta tätä voitaisiin perustella tiedollisella itsemääräämisoikeudella. Näin laajalle rekisteröidyn määräämisvallalle omista tiedoistaan ei kuitenkaan ole sijaa muiden oikeuksien vuoksi.[216]

5.4.1. Informointivelvollisuus henkilötietojen käsittelystä

Vaikka jo ensimmäiset tietosuojalait tunsivat rekisteröidyn oikeuden saada tietoa rekistereistä ja niiden sisällöstä, tuolloinen ratkaisu pohjautui lähinnä *rekisteröidyn tarkastusoikeudelle* ja edellytti siten rekisteröidyn oma-aloitteisuutta. Henkilötietodirektiivin myötä on meilläkin nykyisin vallitsevana periaatteena rekisterinpitäjien *ilmoittamisvelvollisuus* eli *informointivelvollisuus.*[217]

Henkilötietolain 24 § sisältää säännökset rekisterinpitäjän velvollisuudesta huolehtia henkilötietoja kerätessään siitä, että rekisteröity voi saada tiedon henkilötietojen käsittelystä ja siitä, millä edellytyksillä rekisteröidyn informoimisesta tietojen käsittelystä voidaan poiketa. Rekisterinpitäjän informointivelvollisuuden avulla pyritään turvaamaan, että rekisteröity on tietoinen itseään koskevien henkilötietojen käsittelystä. Rekisteröidyn oikeus tietää henkilötietojensa käsittelystä parantaa hänen mahdollisuuksiaan toteuttaa oikeuksiaan henkilötietojen käsittelyssä sekä arvioida henkilötietojen käsittelyn laillisuutta ja asianmukaisuutta.[218]

Pykälän *1 momentissa* säädetään rekisterinpitäjälle velvollisuus huolehtia siitä, että rekisteröity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta, henkilötietojen käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan, samoin kuin ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi asianomaisessa henkilötietojen käsittelyssä. Tiedot on annettava henkilötietoja kerättäessä ja talletettaessa tai, jos tiedot hankitaan muualta kuin

[216] Wallin 2001, s. 380-381
[217] Saarenpää 2005, s. 416
[218] HE 96/1998 vp, yksityiskohtaiset perustelut.

rekisteröidyltä itseltään ja tietoja on tarkoitus luovuttaa, viimeistään silloin kun tietoja ensi kerran luovutetaan.[219]

Informointivelvollisuudesta voidaan poiketa *2 momentissa* mainituilla perusteilla. Ensinnäkin poikkeaminen on *1 kohdan* nojalla mahdollista, jos rekisteröity on jo saanut 1 momentissa tarkoitetut tiedot.[220] Toiseksi *2 kohdan* nojalla poikkeaminen olisi mahdollista, kun poikkeaminen on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi.[221] Kerättäessä tietoja muualta kuin rekisteröidyltä itseltään, informointivelvollisuudesta voidaan *3 kohdan* nojalla lisäksi poiketa myös, jos tietojen antaminen rekisteröidylle on mahdotonta tai vaatii kohtuutonta vaivaa taikka aiheuttaa rekisteröidylle tai tietojenkäsittelyn tarkoitukselle olennaista vahinkoa tai haittaa eikä talletettavia tietoja käytetä rekisteröityä koskevaan päätöksentekoon.[222] Saarenpään mukaan pelkkä byrokraattinen tarve hallinnon toimintojen tehostamiseksi ei kuitenkaan oikeuta sivuuttamaan rekisteröidyn oikeutta asianmukaiseen tietojenkäsittelystä informointiin.[223] Tietosuojavaltuutetun käytännössä on hyväksytty ajatus, että erittäin suurten henkilörekisterien osalta jokaisen rekisteröidyn informointi aiheuttaisi kohtuutonta vaivaa. Lehtosen mukaan informoinnin kohtuuttomuutta tulisi tietosuojadirektiivin tarkoitus ja yleinen suhteellisuusperiaate huomioon ottaen käyttää informointivelvollisuuden laiminlyönnin hyväksyttävyyden perusteena vain, jos tietojen merkitys henkilön yksityisyydelle on vähäinen, taikka jos yksityisyydelle merkittäviä

---

[219] Säännös pohjautuu henkilötietodirektiivin (95/46/EY) vaatimuksiin. Direktiivin 10 artikla edellyttää, että jäsenvaltiot säätävät rekisterinpitäjän velvollisuudesta antaa rekisteröidylle, jolta tietoja kerätään, artiklassa mainitut tiedot, jollei rekisteröidyllä jo ole niitä. Tietosuojadirektiivin 11 artiklan 1 kohta puolestaan edellyttää jäsenvaltioiden säätävän siitä, että kun tiedot kerätään muualta kuin rekisteröidyltä itseltään, rekisterinpitäjän on annettava rekisteröidylle artiklassa tarkoitetut tiedot silloin, kun tiedot rekisteröidään tai viimeistään silloin, kun niitä ensi kerran luovutetaan, jollei rekisteröidyllä jo ole niitä.

[220] HE 96/1998 vp, yksityiskohtaiset perustelut. Hallituksen esityksen mukaan rekisteröidyn voitaisiin katsoa saaneen säännöksessä tarkoitetut tiedot esimerkiksi silloin, kun henkilötietojen kerääminen liittyy sellaisen sopimuksen täytäntöönpanoon, jossa rekisteröity on osallisena.

[221] Henkilötietodirektiivin 13 artiklan 1 kohdan mukaan jäsenvaltiot voivat lainsäädännöllisin toimenpitein rajoittaa muun muassa 10 ja 11 artiklassa säädettyä rekisteröidyn tiedonsaantioikeutta, jos se on välttämätöntä artiklassa lueteltujen tarkoitusten varmistamiseksi. Tällaisia tarkoituksia ovat muun muassa valtion turvallisuus ja yleinen turvallisuus sekä rikosten ehkäiseminen ja selvittäminen ja valvontatehtävä, joka liittyy verotukseen tai muuhun julkiseen talouteen.

[222] Hallituksen esityksessä (HE 96/1998 vp, yksityiskohtaiset perustelut) todettiin, että tietojen antaminen rekisteröidylle voi olla mahdotonta tai vaatia kohtuutonta vaivaa esimerkiksi silloin, kun henkilötietoja käsitellään historiallista, tieteellistä tai tilastollista tarkoitusta varten. Lisäksi todettiin, että arvioitaessa sitä, onko rekisteröidyn informoiminen mahdotonta tai aiheuttaisiko se kohtuutonta vaivaa, voidaan ottaa huomioon muun muassa rekisteröityjen määrä ja käsiteltävien tietojen ikä.

[223] Saarenpää. Näkökulmia yksilön suojasta (kohta 25).

tietoja kertyy vain harvoissa tapauksissa, joiden tavoittaminen tai tunnistaminen on vaikeaa.[224]

Rekisteröityä ei tarvitse myöskään informoida lakisääteisistä rekistereistä.[225] Ottaen huomioon rekisteröidyn informointivelvollisuuden luonteen keskeisenä henkilötietodirektiivin rekisteröidyn oikeusturvakeinona, informointivelvollisuuden rajoittamiseen on syytä suhtautua hyvin pidättyvästi.[226] Informointivelvollisuudella on yksityisyyden suojan kannalta suuri merkitys. Rekisteröityjen on vaikea käyttää oikeuksiaan, mikäli he eivät ole niistä tietoisia.

5.4.2. Rekisteröidyn tarkastusoikeus

Henkilötietolain 26 § sisältää säännökset *rekisteröidyn tarkastusoikeudesta*. Jokaisella on 1 momentin mukaan salassapitosäännösten estämättä oikeus tiedon etsimiseksi tarpeelliset seikat ilmoitettuaan saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on talletettu tai, ettei rekisterissä ole häntä koskevia tietoja. Rekisterinpitäjän on samalla ilmoitettava rekisteröidylle rekisterin säännönmukaiset tietolähteet sekä, mihin rekisterin tietoja käytetään ja säännönmukaisesti luovutetaan. Tarkastusoikeus on kuitenkin osittain ajallisesti rajoitettu oikeus. Tarkastusoikeutta voidaan käyttää maksutta vain kerran vuodessa. Sen sijaan maksullisen tarkastusoikeuden käytölle ei ole rajoituksia. Maksun tulee olla kohtuullinen eikä se saa ylittää tiedon antamisesta aiheutuvia välittömiä kustannuksia (3 mom.).

Rekisteröidyn tarkastusoikeus kuuluu säännönmukaisesti eri valtioiden tietosuojalaeissa omaksuttuihin periaatteisiin. Myös OECD:n tietosuojasuositus ja Euroopan neuvoston tietosuojasopimus sisältävät artiklan tarkastusoikeudesta. Tarkastusoikeus sisältyi jo henkilörekisterilakiin. Sitä koskevassa hallituksen esityksessä tarkastusoikeutta perusteltiin paitsi rekisteröidyn yksityiselämän suojan ja oikeusturvan, myös rekisteröityjen tietojen luotettavuuden varmistamisen sekä rekisterikäytännön kehittämisen kannalta. Tarkastusoikeus siis mahdollistaa sen, että tietojen paikkansapitävyys tulee tarkastetuksi. Tarkastusoikeuden olemassaolo ilmentää osaltaan myös rekisteritoimintaan kuuluvaa avoimuuden periaatetta, mikä on omiaan poistamaan

[224] Lehtonen 2001, s. 240
[225] HetiL 24 § 2 mom. 3-kohta.
[226] Lehtonen 2001, s. 240. Lehtonen katsookin, että henkilötietolain poikkeukset ovat tietyiltä osin direktiiviä laajempia ja ne voidaan katsoa direktiivin puutteelliseksi implementoinniksi, joka tulisi ottaa huomioon sovellettaessa HetiL:n säännöksiä sekä viranomaistoiminnassa että tuomioistuimissa.

rekisteritoimintaa kohtaan tunnettuja epäluuloja ja epäluottamusta sekä siten luomaan edellytykset tarkoituksenmukaisille ja hyvään rekisteritapaan perustuville rekisterikäytännöille.[227] Ongelmallista saattaa kuitenkin pykälän soveltamisen kannalta olla edelleen se, etteivät kansalaiset yleensä tiedä, mitä henkilörekistereitä heistä ylipäänsä on olemassa.[228] Saarenpää näkee rekisteröidyn tarkastusoikeuden osana oikeuttamme tulla arvioiduksi oikeassa valossa.[229]

Henkilötietolain 27 §:ssä säädetään tarkastusoikeuden rajoituksista. On huomattava, että rajoitusperusteet eivät rajaa joitakin henkilörekistereitä kokonaan tarkastusoikeuden ulkopuolelle, vaan rajoituksissa on kyse tietyn henkilötiedon antamatta jättämisestä.[230] Pykälän 1 momentissa säädetään neljästä eri tilanteesta, jolloin tarkastusoikeutta ei ole. Rajoitusten perusteena on lähinnä poikkeuksellisen suurten yleisten tai yksityisten etujen suojeleminen. Tärkeimpänä perusteena voidaan pitää tarkastusoikeuden kieltämistä, jos tiedon antaminen saattaisi vahingoittaa valtion turvallisuutta, puolustusta tai yleistä järjestystä taikka haitata rikosten ehkäisemistä tai selvittämistä. Säännös jättää rekisterinpitäjälle laajan harkintavallan. On muistettava, että pääsäännön mukaan rekisteröidyllä on laaja tarkastusoikeus, josta poikkeamisperusteen olemassaoloa harkittaessa on aiheellista pidättäytyä liian laajoilta tulkinnoilta.[231] Mikäli vain osa henkilörekisteriin tallennetuista tiedoista jää jonkun 1 momentissa mainitun tilanteen nojalla tarkastusoikeuden ulkopuolelle, rekisteröidyllä on tällöinkin oikeus saada tietää muut hänestä talletetut tiedot *(HetiL 27 § 2 mom.).*

Rekisteröidyn tarkastusoikeus kohdistuu niin yksityisten kuin viranomaistenkin pitämiin rekistereihin. Henkilötietolain mukainen tarkastusoikeus, joka liittyy pelkästään henkilön omiin tallennettuihin tietoihin, on pidettävä tiukasti erillään julkisuuslain mukaisesta asiakirjajulkisuudesta ja kaikkien tiedonsaantioikeuksista. Kuten edellä on todettu, julkisuuslakia sovelletaan tiedonsaantiin viranomaisten rekistereistä. Julkisuuslain 9 §:ssä on säädös jokaisen oikeudesta saada tieto viranomaisen asiakirjasta, joka on julkinen. Lisäksi JulkL 11 §:ssä säädetään asianosaisen tiedonsaantioikeudesta ja JulkL 12 §:ssä jokaisen oikeudesta saada tieto itseään koskevasta viranomaisen asiakirjasta.

[227] HE 49/1986, s. 35
[228] Konstari 1992, s. 196
[229] Saarenpää 2005, s. 423
[230] Raatikainen 2002, s.257.
[231] Raatikainen 2002, s. 257

5.4.3. Henkilötiedon korjaamisvelvollisuus

Henkilörekistereihin sisältyvät virheelliset, puutteelliset ja vanhentuneet tiedot muodostavat rekisteröidyn tietosuojan ja oikeusturvan kannalta vakavan uhan.[232] Henkilötietolain 29 §:ssä säädetään rekisterinpitäjän velvollisuuksista korjata henkilörekisterissä oleva virheellinen tieto ja estää tällaisen tiedon leviäminen.[233] Rekisterinpitäjän on ilman aiheetonta viivytystä oma-aloitteisesti tai rekisteröidyn vaatimuksesta oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Pykälän mukainen henkilötieto on korjattava riippumatta siitä, vaarantaako se rekisteröidyn yksityisyyden suojaa taikka hänen etujaan tai oikeuksiaan.[234] Rekisterinpitäjän on myös estettävä tällaisen tiedon leviäminen, jos tieto voi vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan *(HetiL 29 § 1 mom.)*. Henkilötiedon leviämistä koskeva lause on henkilötietolain korjaamisvelvollisuuteen tuoma uutuus. Henkilötiedon leviämistä ei kuitenkaan määritellä laissa eikä sen perusteluissa. Raatikaisen mukaan henkilötieto voi levitä esimerkiksi kun sitä käytetään, siirretään, luovutetaan tai yhdistetään. Leviäminen tarkoittaa yhtä hyvin rekisterinpitäjän organisaation sisällä kuin sen ulkopuolellekin tapahtuvaa leviämistä.[235] Virheellisyysarviota tehtäessä on otettava huomioon rekisterin käyttötarkoitus. Tieto on virheellinen, kun se ei vastaa tosiasiallisia oloja, tai kun se ei tuo asianmukaisesti informaatiota niistä olosuhteista, joita sillä halutaan kuvata.[236]

Jos rekisterinpitäjä ei hyväksy rekisteröidyn vaatimusta tiedon korjaamisesta, hänen on 2 momentin mukaan annettava asiasta kirjallinen todistus. Todistuksessa on mainittava myös ne syyt, joiden vuoksi vaatimusta ei ole hyväksytty. On huomattava, että todistusta ei tarvitse enää nykyään pyytää, vaan se on annettava aina kun korjausvaatimusta ei hyväksytä.[237] Pykälän 3 momentissa säädetään rekisterinpitäjän velvollisuudesta ilmoittaa tiedon korjaamisesta sille, jolle rekisterinpitäjä on luovuttanut

[232] Konstari 1992, s. 216
[233] HetiL 29 § vastaa sisällöltään henkilötietodirektiivin (95/46/EY) 12 artiklan b ja c alakohtia.
[234] HE 96/1998 vp, yksityiskohtaiset perustelut. Henkilörekisterilain mukaan rekisterinpitäjän oli oma-aloitteisesti oikaistava virhe vain silloin, kun oli ilmeistä, että virheellinen tieto saattoi vaarantaa rekisteröidyn yksityisyyden suojaa taikka hänen etujaan tai oikeuksiaan. Koska henkilötietodirektiivin 12 artiklan vuoksi ei enää ollut mahdollista vaatia em. edellytystä virheen oikaisemiselle, tieto on nykyään aina korjattava.
[235] Raatikainen 2002, s. 270
[236] Wallin & Nurmi 1991, s. 153
[237] HE 96/1998 vp, yksityiskohtaiset perustelut.

tai jolta rekisterinpitäjä on saanut virheellisen henkilötiedon.[238] Ilmoitusvelvollisuutta ei kuitenkaan ole, jos ilmoittaminen on mahdotonta tai vaatii kohtuutonta vaivaa.[239] Mahdoton tilanne on olemassa ainakin silloin, jos henkilötiedon luovuttanutta organisaatiota ei enää ole olemassa. Ilmoitusvelvollisuuden tarkoituksesta johtuen vähäisten vaikeuksien ei tule olla peruste jättää virheilmoitus tekemättä.[240]

Korjaamisvelvollisuutta täydentää henkilötietolain 34 §, joka sisältää vaatimuksen tarpeettoman henkilörekisterin hävittämisestä. Henkilörekisteri, joka ei ole enää rekisterinpitäjän toiminnan kannalta tarpeellinen, on hävitettävä, jollei siihen talletettuja tietoja ole erikseen säädetty tai määrätty säilytettäviksi tai jollei rekisteriä siirretä henkilötietolain mukaiseen arkistoon. Tarpeellisuus toiminnan kannalta ratkaisee siis hävitysajankohdan.[241] Rekisterinpitäjällä ei ole oikeutta säilyttää tarpeetonta rekisteriä siinä tarkoituksessa, että sillä joskus vastaisuudessa ehkä jälleen tulee olemaan käyttöarvoa.[242]

5.5. Valvonta ja seuraamukset

5.5.1. Tietosuojavaltuutettu ja tietosuojalautakunta

Yleisesti nähdään, että valvontainstituutioiden asema yksityisyyden suojan toteuttajana on viime aikoina korostunut entisestään.[243] Myös henkilötietodirektiivin 28 artikla edellyttää, että jäsenvaltiot nimeävät yhden tai useamman julkisen valvontaviranomaisen, jonka tehtävänä on itsenäisesti valvoa jäsenvaltioiden direktiivin mukaisesti toteuttamien toimenpiteiden soveltamista. Suomessa on kaksi erillistä oikeusministeriön yhteydessä toimivaa tietosuojaviranomaista: *tietosuojavaltuutettu* ja *tietosuojalautakunta.* Henkilötietolakia tarkempia määräyksiä niistä on annettu lisäksi *laissa tietosuojalautakunnasta ja tietosuojavaltuutetusta (389/1994, muutos 524/1999)* ja *asetuksessa tietosuojalautakunnasta ja tietosuojavaltuutetusta (477/1987, muutos*

[238] Henkilötietodirektiivin 12 artiklan c alakohdan mukaisesti rekisterin pitäjän on aina ilmoitettava virheen oikaisusta kaikille, joille tämä on virheellisen tiedon luovuttanut. Direktiivi ei siten edellytä ilmoituksen tekemistä tiedon antajalle. HetiL:ssa säilytettiin kuitenkin HenkRekL:iin sisältynyt velvollisuus ilmoittaa virheen oikaisusta myös sille, jolta virheellinen tieto on saatu.
[239] Kyseinen poikkeaminen ilmoitusvelvollisuudesta on mahdollinen direktiivin 12 artiklan c alakohdan nojalla
[240] Raatikainen 2002, s. 271
[241] Raatikainen 2002, s. 375
[242] Konstari 1992, s. 376
[243] Wallin 2001, s. 384. Riippumaton valvontaviranomainen mainitaan sekä EU:n perusoikeuskirjan 8 artiklan 3 kohdassa että perustamissopimuksen 286 artiklan 2 kohdassa henkilötietojen suojan olennaisena osana.

529/1999). Henkilötietolaki määrittää molempien viranomaisten tehtäväalueen erittäin laajaksi ja ne voivat käyttää toimivaltuuksiaan silloinkin, kun henkilötietojen käsittelyyn ei muutoin sovelleta Suomen henkilötietolakia.[244]

Tietosuojavaltuutettu valvoo henkilötietojen käsittelyä lain tavoitteiden toteuttamiseksi. Tietosuojavaltuutettu voi myös antaa rekisterinpitäjälle henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa *(HetiL 38 § 1 mom.)*. Ohjauksen ja neuvonnan nimenomaisella mainitsemisella halutaan korostaa sitä, että tietosuojavaltuutetun ensisijainen tehtävä on vaikuttaa ennakollisilla toimenpiteillä rekisterinpidon lainmukaisuuteen.[245] Toissijaisena tehtävänä on toimia valvontaviranomaisena, joka puuttuu lainvastaiseksi havaitsemaansa tietojenkäsittelyyn toimivaltuuksiensa puitteissa.[246] Tehtäviään hoitaessaan tietosuojavaltuutetun on otettava huomioon lain tarkoitus toteuttaa yksityiselämän suojaa sekä muita perusoikeuksia samoin kuin edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Tietosuojavaltuutetun tehtävänä ei ole toimia kenenkään asiamiehenä, vaan rekisteröidyn etujen lisäksi hänen on otettava huomioon myös rekisterinpitäjän ja sivullisen intressit.[247] Rekisteröidyn ja rekisterinpitäjän välinen suhde ei ole yleensä kovinkaan tasapainoinen. Niinpä tietosuojaviranomaisilla – ja erityisesti tietosuojavaltuutetulla – on tärkeä rooli, paitsi henkilötietojen yleisessä ohjauksessa, myös yksittäisten ihmisten palvelijana.[248]

Tietosuojavaltuutetun toimivaltaan ei kuulu antaa ennakkoon sitovia ratkaisuja missä tahansa asioissa. Ohjauksella lainmukaiseen toimintaan ei ole juridista sitovuutta. Mahdollista lain vastaista toimintaa arvioidaan tarvittaessa vasta jälkikäteen tietosuojavaltuutetun, poliisin, syyttäjän ja tuomioistuimen toimesta.[249] Henkilötietolain vastaista menettelyä koskevassa asiassa virallisella syyttäjällä ja tuomioistuimella on HetiL 41 § 2 momentin mukaan velvollisuus kuulla tietosuojavaltuutettua. Henkilötietolain 40 § sisältää tietosuojavaltuutetun käytettävissä olevat toimenpiteet. Ensinnäkin tietosuojavaltuutetun on 1 momentin mukaan edistettävä hyvää tietojenkäsittelytapaa sekä ohjein ja neuvoin pyrittävä siihen, ettei lainvastaista menettelyä jatketa tai uusita. Tarvittaessa hänen on saatettava asia tietosuojalautakunnan

[244] Raatikainen 2002, s. 401. Toimivaltuuksien käyttö voi tapahtua joko Suomen viranomaisten omasta aloitteesta tai toisen valtion valvontaviranomaisen pyynnöstä.
[245] HE 96/1998 vp, yksityiskohtaiset perustelut.
[246] Raatikainen 2002, s. 403
[247] HE 96/1998 vp, yksityiskohtaiset perustelut.
[248] Saarenpää 2005, s. 427
[249] Raatikainen 2002, s. 404

ratkaistavaksi tai ilmoitettava se syytteeseen panoa varten. Toiseksi tietosuojavaltuutettu käyttää 2 momentin mukaista itsenäistä ratkaisuoikeutta asiassa, jonka rekisteröity on saattanut 28 ja 29 §:n nojalla hänen käsiteltäväkseen. Kyseessä ovat henkilön *tarkastusoikeuden toteuttamista* ja *henkilötiedon korjaamista koskevat asiat.* Lisäksi tietosuojavaltuutetulla on 3 momentin mukaan mahdollisuus antaa tarkempia ohjeita siitä, miten henkilötiedot on suojattava henkilötietojen laittomalta käsittelyltä.

Kansalaisten vireille laittamien asioiden määrä tietosuojavaltuutetun toimistossa on kaksinkertaistunut kymmenessä vuodessa. Pääosa kansalaisten vireille laittamista asioista on yleisiä neuvonta-asioita, joissa valtuutetulta on kysytty esimerkiksi henkilötietojen käsittelyn yleisistä periaatteista, rekisterinpitäjän toiminnasta tai rekisteröidynoikeuksista. Muttilainen arvelee, että kansalaisilla on aikaisempaa paremmat tiedot henkilötietojensa suojasta ja sen puutteista. Tämän vuoksi tietosuoja-asioista saatetaan valittaa entistä herkemmin rekisterinpitäjälle ja toisinaan myös tietosuojavaltuutetulle. Asioiden vireille laittaminen on lisäksi helpottunut sähköpostin vuoksi. [250]

Henkilötietolain 38 § 2 momentin mukaan *tietosuojalautakunta* käsittelee henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä ja käyttää päätösvaltaa tietosuoja-asioissa siten kuin HetiL:ssa säädetään. Tietosuojalautakunnalla on lupatoimivaltaa ja määräystoimivaltaa. Lupatoimivaltaan kuuluu, että lautakunnalta on mahdollista saada lupa sekä ei-arkaluonteisten että arkaluonteisten henkilötietojen käsittelyyn.[251] Määräystoimivallalla tarkoitetaan tietosuojalautakunnan HetiL 44 §:n nojalla antamia määräyksiä, joilla voidaan mm. kieltää HetiL:n säännösten ja määräysten vastainen henkilötietojen käsittely, velvoittaa oikaisemaan lain vastainen teko tai laiminlyönti sekä määrätä rekisteritoiminta lopetettavaksi. Toisin kuin tietosuojavaltuutetun osalta, tietosuojalautakuntaan saapuneiden asioiden määrä on vähentynyt selvästi viime vuosina. Henkilötietolain aikana asioiden määrä on vajonnut alle kymmeneen tapaukseen vuodessa. Tämä kehitys johtuu varmasti osittain lautakunnan aikaisempaa suppeammasta lupatoimivallasta. Muttilainen asettaa kuitenkin kysymyksen, pitäisikö

[250] Muttilainen 2006, s. 75. Vuonna 2004 tietosuojavaltuutetun toimistossa tuli kirjallisesti vireille yhteensä noin 2 000 asiaa, joista 840 oli kansalaisten vireille laittamia asioita. Lisäksi toimistoon on tullut viime vuosina puhelimitse yhteensä noin 7 500 yhteydenottoa vuodessa kansalaisilta ja rekisterinpitäjiltä.
[251] Ks. tarkemmin HetiL 43 §. Saarenpää 2005 s. 428-429: Saarenpää katsoo, että henkilötietolain mukainen tietosuojalautakunnan lupatoimivalta on erittäin suppea verrattuna henkilörekisterilain aikaiseen lupatoimivaltaan, jolloin tietosuojalautakunnalla oli laaja toimivalta poikkeuslupien antamiseen.

tietosuojalautakunnalla olla nykyistä painavampi asema linjanvetäjänä periaatteellisesti tärkeissä tietosuoja-asioissa.[252]

Tietosuojavaltuutetun ja tietosuojalautakunnan päätöksiin voidaan hakea muutosta. Sekä tietosuojavaltuutetun tarkastusoikeuden käyttämistä tai henkilötiedon korjaamista koskevassa asiassa tekemään päätökseen että tietosuojalautakunnan lupa- tai määräystoimivaltansa nojalla tekemään päätökseen haetaan HetiL 45 § 1 momentin mukaan muutosta valittamalla noudattaen, mitä *hallintolainkäyttölaissa (586/1996)* säädetään. Lisäksi tietosuojavaltuutettu voi hakea muutosta tietosuojalautakunnan lupatoimivaltansa nojalla tekemään päätökseen. Muutetun hallintolainkäyttölain 12 §:n 2 momentin mukaan sellaisen viranomaisen päätöksestä, jonka toimialueena on koko maa, valitus tehdään siihen hallinto-oikeuteen, jonka tuomiopiirissä sijaitsee sen henkilön kotikunta tai sen yhteisön kotipaikka, johon päätös pääosin liittyy. Muutoksenhakijaa oikean forumin löytämisessä helpottaa se, että tietosuojaviranomaisen päätöksen valitusosoituksesta ilmenee toimivaltainen muutoksenhakutuomioistuin.[253]

5.5.2. Rangaistussäännökset ja vahingonkorvaus

Kuten edellä on käynyt ilmi, henkilötietojen käsittelyyn liittyy monia velvollisuuksia. Näiden velvoitteiden tehostamiseksi on määritelty joukko rangaistavia tekoja. Yhdessä vahingonkorvaussäännösten kanssa ne pyrkivät edistämään rekisterinpitäjän toimien lainmukaisuutta niiden käsitellessä rekisteröityjen henkilötietoja. Lainsäätäjä on meillä jaotellut lain vastaiset teot niiden vakavuuden perusteella. Lievimmät teot on sijoitettu henkilötietolain *henkilörekisteririkkomus* -normiin ja vakavammat *henkilörekisteririkoksena* rikoslakiin (RL).

On muistettava, että tilastoitu ja ilmitullut rikollisuus on vain osa rikollisuudesta. Piilorikollisuus on henkilörekisteririkoksen ja muiden RL 38 luvussa säädettyjen tekojen kohdalla todennäköisesti huomattavasti suurempi kuin vuosien 1999-2002 yleisessä alioikeudessa rangaistukseen tuomittujen tapausten tilastosta käy ilmi. Tilaston mukaan tuona aikana henkilörekisteririkoksesta tuomittiin rangaistus kahdessa

[252] Muttilainen 2006, s. 75
[253] Raatikainen 2002, s. 405

tapauksessa.[254] Uusimpien tilastojen mukaan käräjäoikeudet ratkaisivat vuonna 2004 seitsemän asiaa, joissa päärikokseksi epäiltiin henkilörekisteririkosta. Niistä yhdessä syyte hylättiin ja muut johtivat sakkorangaistukseen.[255] Henkilörekisteririkosasioiden määrä tuomioistuimissa näyttää siten lisääntyneen viime vuosina. Henkilörekisteririkkomuksia tulee poliisin tietoon vain muutamia vuodessa ja vuonna 2004 niiden määrä oli viisi kappaletta.[256]

5.5.2.1. Henkilörekisteririkos

Henkilötietolain 48 § 1 momentin mukaan rangaistus henkilörekisteririkoksesta säädetään RL 38 luvun 9 §:ssä. Rikoslain säännöksen mukaan henkilörekisteririkoksena rangaistavaa on muun muassa se, että *henkilötietoja käsitellään tahallisesti tai törkeästä huolimattomuudesta vastoin henkilötietolain käyttötarkoitussidonnaisuutta, käsittelyn yleisiä edellytyksiä tai henkilötietojen käsittelyn tarpeellisuutta* (1 kohta). Tunnusmerkistön täyttymisen edellytyksenä on, että *teko loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa rekisteröidylle muuta vahinkoa tai olennaista haittaa*. Henkilörekisteririkoksesta voidaan tuomita sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Henkilörekisteririkos on virallisen syytteen alainen rikos, joskin virallisen syyttäjän on ennen syytteen nostamista kuultava tietosuojavaltuutettua.[257]

Henkilörekisteririkos aiheutuu siis teosta, joka on HetiL:n vastainen. Säännös on erittäin laaja. Jo edellä selostetun 1 kohdan osalta on huomattava, että ”käsittely” tarkoittaa tässäkin yhteydessä kaikkia mahdollisia henkilötietoihin kohdistuvia toimenpiteitä. Siten esimerkiksi kaikkia lain vastaisesti tapahtuneita luovutuksia arvioidaan säännöksen perusteella.[258]

Henkilörekisteririkoksen tekijänä on yleensä rekisterinpitäjä tai tämän edustaja. Henkilörekisteririkoksen tekijää ei kuitenkaan ole rajoitettu rekisterinpitäjään tai hänen edustajaansa, vaan henkilörekisteririkokseen voi syyllistyä esimerkiksi rekisterinpitäjän

[254] Raatikainen 2002, s. 411. Oikeuspoliittisen tutkimuslaitoksen kyseinen tilasto: http://www.om.fi/optula/uploads/hd12ms.pdf
[255] Muttilainen 2006, s. 69
[256] Muttilainen 2006, s. 66
[257] Lehtonen 2001, s. 355
[258] Raatikainen 2002, s. 413-414

palveluksessa olevat sekä toimeksisaaja ja toimeksisaajan palveluksessa olevat henkilöt.[259]

> **KKO 1998:85 (ään.)** Korkeimman oikeuden enemmistö on ratkaisussaan katsonut, että henkilötietojen luovuttaminen vastoin rekisteröidyn suostumusta muuhun käyttötarkoitukseen kuin siihen, mihin henkilötiedot on rekisteröity, on tyypillisesti yksityisyyden suojan perustavoitteiden vastaista. Yhtiö X oli luovuttanut omistamansa lakkautetun sanomalehden tilaajarekisterin tiedot yhtiöiden Z ja Y käyttöön suoramarkkinointia varten. KKO katsoi X:n edustajien syyllistyneen henkilörekisteririkokseen. Sen sijaan Z ja Y yhtiöiden edustajia vastaan ajetut syytteet hylättiin, koska ei voitu katsoa, että Z ja Y olisivat tienneet, ettei X:lla ollut rekisteröityjen suostumusta luovutukseen tai etteivät rekisteröidyt ilmeisesti tienneet luovutuksesta. Z:n ja Y:n edustajien syyksi ei siten voitu lukea teon edellyttämää tahallisuutta tai törkeää huolimattomuutta.
>
> Vähemmistöön jääneet jäsenet katsoivat, että luovuttamisesta aiheutuva haitta – mainospostin ja muun markkinoinnin kohteeksi joutuminen – oli yleensä vähäinen. Heidän mielestään valtakunnallisen sanomalehden tilaajatiedoissa voidaan nähdä yksityisyyden kannalta suojattavia arvoja, mutta kun rangaistusvastuun piiriin oli tarkoitettu saattaa vain selvät ja vakavat lain rikkomukset, oli ilmeistä, huomioon ottaen myös yksityisyyden käsitteen epämääräisyys ja laillisuusperiaatteen asettamat vaatimukset, ettei tapauksessa ollut kysymys henkilörekisteririkoksena rangaistavasta yksityisyyden loukkauksesta.

5.5.2.2. Henkilörekisteririkkomus

Henkilörekisteririkkomuksesta on säädetty henkilötietolain 48 § 2 momentissa. Henkilörekisteririkkomukseen voi syyllistyä esimerkiksi *henkilö, joka tahallaan tai törkeästä huolimattomuudesta HetiL:n vastaisesti laiminlyö noudattaa, mitä henkilötietojen käsittelyn tarkoitusten määrittelystä, rekisteriselosteen laatimisesta, tietojen käsittelystä, informoimisesta, henkilörekisterissä olevan tiedon korjaamisesta, rekisteröidyn kielto-oikeudesta tai ilmoituksen tekemisestä tietosuojavaltuutetulle säädetään tai rikkoo henkilötietojen suojaamisesta ja henkilörekisterin hävittämisestä annettuja säännöksiä ja määräyksiä*. Henkilötietorikkomuksen täyttymisen lisäedellytyksenä on, että *teko vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan*. Tämä lisäedellytys on tietysti omiaan nostamaan rangaistusseuraamukseen tuomitsemisen kynnystä, joten merkitykseltään vähäisiksi jäävät laiminlyönnit tuskin voivat johtaa rangaistusseuraamukseen. Henkilörekisteririkkomuksesta voidaan tuomita vain sakkoon.

[259] Rautio 2002

5.5.2.3.Vahingonkorvausvelvollisuus

Henkilötietolain 47 §:n mukaan rekisterinpitäjä on velvollinen korvaamaan sen taloudellisen tai muun vahingon, joka on aiheutunut rekisteröidylle tai muulle henkilölle henkilötietolain vastaisesta henkilötietojen käsittelystä.[260] Hallituksen esityksen mukaan vastuu kattaa myös henkilölle laittomasta käsittelystä aiheutuneen kärsimyksen.[261] Kärsimystä henkilölle saattaa aiheuttaa tilanne, jossa hän kokee itseään kohdellun lainvastaisen menettelyn perusteella hänen ihmisarvoaan halventavalla tai loukkaavalla tavalla. Vahingonkorvausvelvollisuus voi seurata millaisesta henkilötietojen lainvastaisesta käsittelystä tahansa. Vahingonkorvausvastuu on *tuottamuksesta riippumatonta* eli ns. *ankaraa vastuuta,* joten lainvastaista tekoa ei tarvitse lainkaan arvioida teon tahallisuuden tai huolimattomuuden asteen perusteella. Raatikaisen mukaan jyrkkä kanta on helpommin ymmärrettävissä, jos ajattelee ylipäätään rekisteröityjen tosiasiallista mahdollisuutta vaikuttaa henkilötietojensa käsittelyyn.[262]

Henkilötietolakiin perustuvan vahingonkorvausjärjestelmän ongelma on se, että rekisteröidyn velvollisuutena on näyttää toteen, että hänelle on syntynyt vahinkoa rekisterinpitäjän lainvastaisesta menettelystä.[263] Tämä voi olla käytännössä hankalaa. Konstarin mukaan kyseinen todistustaakkasääntö vähentää vahingonkorvaussäännöksen käytännön merkitystä huomattavasti.[264] Vahingonkorvauskannetta ajetaan käräjäoikeudessa.

[260] Pykälän taustalla on henkilötietodirektiivin 23 artikla, joka velvoittaa jäsenvaltiot säätämään rekisteröidyn tai muun henkilön oikeudesta saada rekisterinpitäjältä korvaus henkilötietojen tämän lain vastaisesta käsittelystä aiheutuneesta vahingosta.
[261] HE 96/1998 vp, yksityiskohtaiset perustelut.
[262] Raatikainen 2002, s. 417-418. Esimerkiksi virheellisen henkilötiedon käyttämisestä tai luovuttamisesta aiheutunut taloudellinen vahinko on korvattava. Samoin on korvattava vahinko, joka syntyy siitä, että henkilötiedon tallettaminen, käyttö, suojaaminen, luovutus tai ilmaiseminen on ollut lainvastaista.
[263] HE 49/1986 vp, yksityiskohtaiset perustelut.
[264] Konstari 1992, s. 380

6. RFID-tekniikan mahdollistamat tietosuojan ja yksityisyyden suojan loukkaukset

Tässä tutkimuksessa on edellä (ks. 3. luku) esitelty joitakin RFID:n hyödyntämistapoja eri toimialoilla. Vaikka osaan esitellyistä käyttömahdollisuuksista ei liitykään minkäänlaisia tietosuoja- tai yksityisyydensuojakysymyksiä, osassa ne ovat selvästi havaittavissa. Tässä luvussa esitellään tietosuojatyöryhmän luomia skenaarioita, joihin RFID-teknologian yksityisyydensuojakysymykset saattavat tulevaisuudessa liittyä.

Vaikkakin yksityiset kuluttajansuojajärjestöt, yliopistot ja ajatushautomot suhtautuivat tietosuojatyöryhmän työasiakirjaan positiivisesti, työryhmän luomat skenaariot saivat myös tylyn vastaanoton joiltain alan toimijoilta. Muun muassa Metro Group totesi lausunnossaan, että tässä luvussa kuvattavat skenaariot edustavat epärealistisia tilanteita.[265] EPCglobal oli samoilla linjoilla todeten lisäksi, että vaikka skenaariot ovat käyttökelpoisia herättämään huomion yksityisyydensuojakysymyksiin, ne eivät kuitenkaan anna aihetta välittömiin lainsäädännön muutoksiin.[266]

6.1. Tekniikan käyttö henkilötietoihin yhdistettävissä olevien tietojen keräämiseen

RFID-tekniikan kautta voidaan kerätä tietoja, jotka ovat suoraan tai epäsuorasti yhdistettävissä yksilön henkilötietoihin. Ensinnäkin voimme pohtia tilannetta, jossa tuotteeseen kiinnitetyn RFID-tunnisteen numero yhdistetään tuotteen ostaneen henkilön asiakasrekisteritietoihin. Tietosuojatyöryhmä käytti tässä kohdassa esimerkkinä elektroniikkaliikettä, joka voisi kiinnittää yksilöivän numeron sisältävät tunnisteet tuotteisiinsa ja tämän jälkeen systemaattisesti yhdistää numerot asiakkaiden nimiin, jotka myyjä saisi tietoonsa luottokorttiasiakkailta maksutapahtuman yhteydessä. Tieto ostosta siirtyisi tämän jälkeen liikkeen asiakastietokantaan. Liike voisi perustella menettelyään esimerkiksi takuujärjestelmän toimivuuden varmistamisella.[267]

Toisena esimerkkinä tietosuojatyöryhmä mainitsi tilanteen, jossa kauppaketju sijoittaa tunnisteen kanta-asiakaskortteihinsa. Kanta-asiakaskortit sisältäisivät asiakkaan

[265] Metro Groupin lausunto s. 8
[266] EPCglobalin lausunto, s. 12
[267] Työasiakirja WP 105, s. 5

henkilötiedot. Järjestelmä mahdollistaisi sen, että kauppaketju saisi tallennettua arvokasta tietoa asiakkaan kulutustottumuksista joka kerta, kun asiakas vierailisi kaupassa. Kerättävä tieto voisi olla esimerkiksi tietyllä kaupan osastolla vietetty aika tai niiden kertojen lukumäärä, kun asiakas on käynyt kaupassa ostamatta sieltä mitään.[268]

Molemmissa yllä kerrotuissa esimerkeissä yksityisyyden suoja nousee epäilemättä esiin, koska RFID-tekniikan avulla kerätyt tiedot ovat yhdistettävissä asiakkaan henkilötietoihin. Kanta-asiakaskortit ovat jo aikaisemmin mahdollistaneet asiakkaiden kulutustottumustietojen keräämisen ja asiakasprofiloinnin. RFID-tekniikka tuo tietosuojatyöryhmän mukaan lisää mahdollisuuksia täsmämarkkinointiin, mikäli asiakkaat pystytään tunnistamaan jo sisääntuloporteilla ja heidän käyttäytymistään kaupassa pystytään tarkkailemaan. Huomionarvoista on tietosuojatyöryhmän mukaan se, että mikäli RFID-teknologia otetaan laajamittaiseen käyttöön, käsiteltävän tiedon määrä kasvaa merkittävästi, mikä saattaa antaa aihetta huoleen. [269]

Metro Groupin mukaan RFID-teknologia ei itsessään tuo kanta-asiakasjärjestelmien luonteeseen tai toimintaan mitään uutta. Yhtiö korosti, että riippumatta siitä kerätäänkö tiedot viivakoodien vai RFID-tunnisteiden avulla, asiakastietoja kerätään tai käsitellään vain, jos asiakas antaa siihen etukäteisen kirjallisen suostumuksensa. Lisäksi Metro Group totesi, ettei sillä ole mitään aikomusta lisätä kanta-asiakaskortteihinsa RFID-tunnisteita.[270] Myös EPCglobal oli sitä mieltä, että jo tällä hetkellä on olemassa potentiaalisia henkilötietojen keräämiskeinoja, joita voitaisiin käyttää profilointiin ilman asiakkaan suostumusta. Niitä ei kuitenkaan ole käytetty EPCglobalin mukaan juuri siksi, että kaupat haluavat kunnioittaa tietosuojalainsäädäntöä.[271]

6.2. Henkilötietojen tallentaminen RFID-tunnisteelle

Edelliseen kappaleen esimerkkitilanteisiin verrattuna kokonaan toisentyyppinen tilanne yksityisyyden suojan kannalta syntyy, mikäli henkilötietoja tallennetaan itse RFID-tunnisteelle. Tämä saattaisi tulla kysymykseen esimerkiksi matkakorteissa. Julkista liikennettä harjoittava yritys voisi ottaa käyttöön etäluettavan rahastusjärjestelmän, jossa kuukausikortille olisi tallennettuna asiakkaan nimi ja yhteystiedot. Tämä mahdollistaisi

[268] Työasiakirja WP 105, s. 5-6
[269] Työasiakirja WP 105, s. 6
[270] Metro Groupin lausunto, s. 10
[271] EPCglobalin lausunto, s. 9-10

sen, että yritys tietäisi koko ajan, missä tietty tunnistettu asiakas liikkuu julkista liikennettä käyttäessään. Tämä loukkaisi ilmiselvästi henkilön yksityisyyttä. Koska kuka tahansa pystyy lukemaan tunnisteita käytössään olevalla RFID-lukijalla, myös muut osapuolet pystyisivät salaa hankkimaan itselleen vastaavia tietoja matkustajista. Tietosuojatyöryhmän mukaan on huomionarvoista, että RFID-järjestelmät ovat hyvin herkkiä hyökkäyksille. Mahdolliset hyökkääjät voisivat suorittaa etälukutapahtumia täysin huomaamatta.[272] Edellä on kerrottu (ks. luku 3.1) Suomen pääkaupunkiseudulla käyttöönotetusta rahastusjärjestelmästä. Kyseisen järjestelmän asiakastietojen päivitys- ja tarkistusoikeuksia on matkakortin palvelupisteiden toimihenkilöillä, joilla on salassapitovelvollisuus. Näillä henkilöillä on vain asiakkaan pyynnöstä oikeus selailla keskusjärjestelmästä käsiteltävänä olevan asiakkaan kortille tallentuneita kauden ja arvon lataustapahtumia sekä viimeisimpiä arvon käyttötapahtumia. Asiakkaan henkilötietoja on tallennettuna ainakin ns. haltijakohtaiselle matkakortille. Asiakas voi pyytää tiedot matkakortin tietosisällöstä ja viimeisimmistä arvon käyttötapahtumista matkakortin palvelupisteestä. Henkilökohtaisen kortin osalta matkustajan tulee tuolloin esittää matkakortti ja todistaa henkilöllisyytensä. Haltijakohtaisen kortin tiedot annetaan kortin haltijalle, jos korttiin ei ole tallennettu henkilötietoja. Jos haltijakohtaiseen matkakorttiin on tallennettu henkilötiedot, tietoja pyytävän on todistettava henkilöllisyytensä.[273] Kuten edellä on todettu (ks. luku 3.1.), YTV:n järjestelmä toimii 13,56 MHz:n taajuusalueella, mikä rajoittaa kortin lukuetäisyyden muutamiin senttimetreihin. Näin ollen ulkopuolisten suorittamat lukutapahtumat käyvät käytännössä mahdottomiksi. Yleisesti näyttää siltä, että YTV:n matkakorttijärjestelmässä on huolehdittu asiakkaan tietosuojasta ja järjestelmä pohjautuu asiakkaan suostumukseen henkilötietojen käsittelylle.

Keväällä 2006 joukko eurooppalaisia tietoturva-alan tutkijoita julkaisi tutkimuksen, jossa he varoittivat, että RFID saattaa tulevaisuudessa kärsiä viruksista. Tutkijat halusivat herättää RFID-valmistajat huomaamaan teknologian haavoittuvuuden tartuttamalla RFID-tunnisteelle viruksen. Tällä tavalla teknologia saattaisi tutkijoiden mukaan olla hakkereiden hyödynnettävissä ja virus saattaisi levitä järjestelmään.[274] Tutkijoiden huolet kyseenalaistettiin kuitenkin eräiden RFID-asiantuntijoiden toimesta välittömästi. Ensinnäkin asiantuntijat olivat sitä mieltä, että kyseisten EPC-tunnisteiden muistin pienuus estää hyökkäykset. Toiseksi EPCglobalin verkko on asiantuntijoiden

[272] Työasiakirja WP 105, s. 6
[273] http://www.ytv.fi/FIN/liikenne/matkustajan_opas/Matkakortti/Matkakortti/matkaehdot.htm
[274] http://hightechforum.kaleva.fi/index.cfm?alue=10&Id1=556427&OpenStory=1&lang=1&scs=1

mielestä hyvin suojattu hyökkäyksiltä. Vaikka virushyökkäykset olisivatkin teoriassa mahdollisia, hyvällä ohjelmistojen suunnittelulla pystytään asiantuntijoiden mukaan varmistamaan, että haavoittuvuuksia on erittäin vaikea löytää RFID-järjestelmästä.[275]

Mikäli henkilötietoja tallennetaan älykorttiin, passiin tai matkakorttiin sisältyvälle RFID-tunnisteelle, tullaan näissä järjestelmissä käytännössä käyttämään vahvoja tietoturvaratkaisuja, jotka suojaavat henkilön yksityisyyttä korttia tai passia käytettäessä. Kauppajärjestöt esittivät kritiikkiä tietosuojatyöryhmän ratkaisusta lähestyä tällaisia sovelluksia RFID:n käyttöön liittyvinä yksityisyydensuojakysymyksinä. Kauppajärjestöjen mukaan tällaisiin sovelluksiin liittyvät yksityisyydensuojakysymykset eivät liity RFID-teknologian käyttöön sinänsä. Kauppajärjestöt huomauttivat, että kyseisiin sovelluksiin liittyy yksityisyydensuojaongelmia huolimatta järjestelmän käyttämästä teknologiasta.[276] Erikseen on mielestäni arvioitava vielä sitä, millä tavalla RFID-passeja saatetaan tulevaisuudessa hyödyntää yksityisellä sektorilla, ja millaisia yksityisyydensuojakysymyksiä yksityisen sektorin käyttöön liittyy.

Kesän 2006 jalkapallon MM-kilpailujen sisäänpääsyliput on varustettu RFID-tunnisteilla, jotka luetaan sisäänpääsyporteilla. Järjestelmällä pyritään estämään väärennyksiä ja ns. mustan pörssin kauppaa sekä parantamaan katsojien turvallisuutta. Kisaturistien yksityisyyden suojan kannalta on tärkeää, että tunnisteelle ei tallenneta henkilötietoja. Järjestelmällä pystytään estämään saman lipun käyttö kahteen kertaan, sillä tunnisteelle tallentuu tieto sisäänpääsystä.[277]

6.3. RFID:n käyttö muuhun henkilöiden seurantaan ja profilointiin

Kolmantena tilanteena voidaan erottaa tilanne, jossa RFID-tekniikkaa käytetään siten, että yksilöiden seuranta ja henkilötietojen käsittely ovat mahdollisia. Tähän ryhmään

---

[275] http://www.rfidjournal.com/article/articleprint/2201/-1/1/

[276] ICC:n, EICTA:n, ICRT ja JBCE:n lausunto, s. 8-9

[277] http://fifaworldcup.yahoo.com/06/en/tickets/dpr.html. RFID-tunnisteita ei ole aikaisemmin käytetty pääsylipuissa tällaisessa mittakaavassa. RFID-tunnisteita käytetään turnauksen kaikissa pääsylipuissa, jolloin 3,2 miljoonan lipun tunnisteiden hinnaksi (á 10 snt) muodostuu noin 320.000 euroa. Tunnisteet valmistanut Philips uskoo, että tunnisteiden käyttäminen pääsylipuissa tulee yleistymään MM-kilpailujen jälkeen ja tunnisteiden hinnat tulevat laskemaan entisestään. (http://www.theregister.co.uk/2005/04/04/world_cup_rfid/)

kuuluu hyvin erilaisia mahdollisia seurantatapoja, jotka kaikki rikkovat henkilön yksityisyyden suojaa.[278]

EPCglobal huomautti, että jo pelkästään heidän lisenssisopimuksensa rajoittaa EPC:n käyttöä *ihmisten tunnistuksessa ja seurannassa*. Lisenssisopimus sallii tunnistuksen ja seurannan ainoastaan potilaiden ja sotilaiden osalta.[279]

6.3.1. Asiakkaille jaettujen välineiden käyttö profilointiin

Ensimmäisenä esimerkkinä tietosuojatyöryhmä käytti elintarvikekauppaa, joka saattaisi jakaa asiakkailleen RFID-tunnisteen sisältäviä poletteja, jotka mahdollistavat ostoskärryjen käytön, ja joita asiakkaat käyttäisivät joka kerta, kun he käyvät kyseisessä kaupassa. Tunniste voitaisiin käsitykseni mukaan upottaa nykyisen kaltaisiin ”kanta-asiakasavaimenperiin” asiakkaan huomaamatta. Kauppa voisi käyttää RFID-tunnisteen numeroa asiakkaan tunnisteena ja luoda jokaisesta järjestelmään kuuluvasta asiakkaasta oman tiedoston tietojärjestelmäänsä. Tämän jälkeen kauppa voisi mm. seurata, mitä tuotteita tietty asiakas ostaa ja miltä kaupan osastolta hän ostoksensa tekee. Näitä tietoja kauppa voisi käyttää tehdäkseen päätelmiä mm. asiakkaan tuloista, terveydentilasta ja ostoskäyttäytymisestä. Tehtyjen päätelmien perusteella voitaisiin jälleen toteuttaa täsmämarkkinointia tai jopa hinnoitella tuotteita erihintaisiksi eri asiakkaille. Koska järjestelmä tunnistaisi asiakkaan joka kerta hänen astuessaan kauppaan, markkinointia voitaisiin suunnata järjestelmään tallennettujen kulutustottumuksien mukaan. Järjestelmän keräämät tiedot saattaisivat jopa vaikuttaa siihen, millä tavalla asiakasta kohdellaan ja palvellaan. Tietosuojatyöryhmän mukaan myös kolmannet osapuolet saattaisivat päästä käsiksi kyseisiin tietoihin.

Alan toimijoista Metro Group korosti, ettei sillä ole minkäänlaisia suunnitelmia luoda profiileita asiakkaidensa liikkumisesta RFID:n avulla. Metro Groupilla ei ole myöskään minkäänlaisia suunnitelmia varustaa ostoskärryjä tunnisteilla. Metro Group pitikin huolta ihmisten seurannasta vähittäiskaupan sektorilla täysin aiheettomana. Sen mukaan seurannan asettamat tekniset ja taloudelliset vaatimukset ovat suhteettomia ja tekevät seurannasta käyttökelvottoman ja epärealistisen skenaarion.[280] Myös EPCglobal oli samoilla linjoilla Metro Groupin kanssa. Yhtiön mukaan olettamat siitä, että EPC-

[278] Työasiakirja WP 105, s. 6
[279] EPCglobalin lausunto, s. 9
[280] Metro Groupin lausunto, s. 8

numero yhdistettäisiin tietokannassa oleviin tietoihin ja profilointitekniikoita hyödynnettäisiin laajamittaisesti, eivät vastaa käytännön todellisuutta.[281]

6.3.2. Profilointi asiakkaan kantamien tuotteiden kautta

Toinen tietosuojatyöryhmän käyttämä esimerkki on varmasti vielä tällä hetkellä täysin hypoteettinen, mutta se ansaitsee tulla mainituksi havainnollistaakseen tekniikan tarjoamia mahdollisuuksia yksityisyyden suojan kannalta. Esimerkissä henkilö Z menee kauppaan C kantaen laukussaan tunnisteet sisältäviä tuotteita, jotka hän on ostanut kaupoista A ja B. Kauppa C lukee laukun sisääntuloportilla ja saa tuloksena haltuunsa joitakin numeroita. Kauppa C tallentaa kyseiset numerot järjestelmäänsä. Seuraavana päivänä henkilö Z palaa takaisin kauppaan ja hänet luetaan jälleen sisääntuloportilla. Tietty tuote Y, joka oli havaittu edellisenä päivänä, luetaan myös tänään. Kauppa C voi tehdä johtopäätöksen, että kyseinen henkilö kantaa tuotetta Y yleensä mukanaan. Niinpä kauppa C luo tiedoston, jonka ”avaimena” toimii tuotteen Y numero. Tuote Y voi olla esimerkiksi rannekello. Tämän jälkeen kaupan järjestelmä havaitsee henkilön Z myöhemmät käynnit kaupassa, edellyttäen, että hän käyttää rannekelloaan. Järjestelmä mahdollistaa sen, että kauppa voi luoda henkilön Z profiilin ja tietosuojatyöryhmän mukaan siten valvoa, mitä hänellä on kauppakassissaan seuraavilla ostoskerroillaan. On huomattava, että vaikka kauppa C ei koskaan saisi tietää henkilön Z nimeä, kauppa käsittelee tapauksessa henkilötietoja ja tietosuojalainsäädäntö tulee siten sovellettavaksi.[282]

Alan toimijoista Metro Group piti tätäkin skenaariota täysin epärealistisena. Metro Groupin mukaan heidän järjestelmällään ei voida tallentaa tai analysoida tuotekoodeja, jotka eivät kuulu heidän järjestelmäänsä. Kolmannelle osapuolelle heidän tunnisteidensa lähettämä tieto olisi ainoastaan pitkä numerosarja, jolla ei heidän mukaansa olisi mitään käyttöä.[283]

6.3.3. Sirulle tallennettu tieto paljastaa esineen luonteen

Viimeisenä esimerkkinä tietosuojatyöryhmä mainitsi, että tunnisteisiin tallennettu tieto saattaa joissakin esineissä olla sellaista, että tieto paljastaa esineen luonteen. Ihmisten

[281] EPCglobalin lausunto, s. 9
[282] Työasiakirja WP 105, s. 7
[283] Metro Groupin lausunto s. 8

mukanaan kantamat tuotteet ovat henkilökohtaisia ja sisältävät tietoa, joka joutuessaan kolmannelle osapuolelle saattaa loukata esineen omistajan yksityisyyden suojaa. Tietosuojatyöryhmän mukaan kuka tahansa saattaisi lukijallaan tunnistaa esimerkiksi seteleitä, kirjoja, lääkkeitä tai arvokkaita esineitä, joita ohikulkija kantaa mukanaan.[284]

Metro Group piti uhkaa siitä, että kolmas osapuoli vakoilisi yksittäistä kuluttajaa, täysin liioiteltuna. Korkeintaan luettavissa on tuotenumero, joka paljastaisi tuotetta koskevaa tietoa ainoastaan, mikäli numero kyetään yhdistämään tuotetietokantaan. Kyseiseen tietokantaan taas sisäänpääsyvaltuudet on ainoastaan henkilökunnalla.[285] Metro Groupin mukaan tekniset ja taloudelliset syyt tekevät tunnisteiden lähettämien tietomassojen lukemisen ja käsittelyn vähittäiskaupalle mahdottomaksi. Heidän mukaansa asiantuntijat ovat arvioineet, että Metro Groupin suuruinen yritys joutuisi käsittelemään yhdeksän teratavun verran tietoa sekunnissa, mikäli koko liiketoiminta ryhtyisi käyttämään RFID-tekniikkaa.[286]

EPCglobal totesi, ettei mikään edellä mainituista skenaarioista ole tällä hetkellä realistinen, eivätkä ne heidän mukaansa todennäköisesti toteudu myöskään tulevaisuudessa. Yhtiön mukaan kaupoilla ei ole varaa vaarantaa mainettaan asiakkaidensa keskuudessa ottamalla riskin siitä, että tieto salaisesta profiloinnista tulee asiakkaiden tietoon. Vaikka joku kauppa olisikin valmis ottamaan kyseisen riskin, hanke kaatuisi todennäköisesti siihen, että järjestelmän kautta saavutettavat kaupalliset hyödyt olisivat kuitenkin mitättömän pieniä verrattuna järjestelmän aiheuttamiin kustannuksiin. Yhtiö huomautti myös tekniikkaan edelleen liittyvistä haasteista, kuten tunnistintörmäyksestä, lukijatörmäyksestä ja erilaisista standardeista, jotka tekevät skenaarioiden mukaisen tiedonkeruun epätodennäköiseksi.[287]

[284] Työasiakirja WP 105, s. 7
[285] Metro Groupin lausunto s. 9
[286] Metro Groupin lausunto s. 9. Määrä vastaa noin 13 000 CD-ROM -levyn tallennuskapasiteettia.
[287] EPCglobalin lausunto, s. 10-11

7. Tietosuojalainsäädännön soveltaminen RFID-teknologian avulla kerättyyn tietoon

7.1. Ohjeita henkilötietodirektiivin soveltamiseen kerättäessä ja käsiteltäessä RFID-teknologian avulla kerättyä tietoa

Tietosuojatyöryhmän edellä kerrotut esimerkit osoittavat, että monet tietosuoja- ja yksityisyydensuojakysymykset, joita RFID-tekniikan käyttöön liittyy, johtuvat salaisesta seurannasta, jota toteuttaa henkilö tai yritys, jolla ei ole valtuutusta lukea kyseisten tunnisteiden tietoja. Niinpä tietosuojatyöryhmä antoi ohjeita, miten henkilötietodirektiiviä tulee soveltaa kyseisissä henkilötietojen käsittelytilanteissa.[288]

Henkilötietodirektiiviä sovelletaan kaikkeen henkilötietojen käsittelyyn. Henkilötietodirektiivin 2 artiklan a-kohdan määritelmän mukaan henkilötiedoilla tarkoitetaan *kaikenlaista tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevia tietoja.* Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa, erityisesti henkilönumeron taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella *(2 artiklan a-kohta).* Pohdittaessa, sovelletaanko henkilötietodirektiiviä kerättäessä tietoa RFID-tekniikan avulla, tulee siten tarkastella erikseen jokaista RFID-sovellusta. Erityisesti on tarkasteltava sitä, johtaako tietyn RFID-sovelluksen käyttö direktiivin mukaiseen henkilötietojen käsittelyyn.[289]

Tietosuojatyöryhmän mukaan arvioitaessa sitä, onko tietyn RFID-sovelluksen avulla toteutettava henkilötietojen kerääminen henkilötietodirektiivin alaista, on ensinnäkin määriteltävä, *missä laajuudessa käsiteltävät tiedot ovat yhteydessä yksilöön*, ja toiseksi, *koskevatko kyseiset tiedot yksilöä, joka on tunnistettu tai tunnistettavissa.* Tiedot ovat yhteydessä yksilöön, jos ne viittaavat yksilön henkilöllisyyteen, tuntomerkkeihin tai käyttäytymiseen, taikka jos kyseisiä tietoja käytetään yksilöä koskevassa päätöksenteossa tai arvioinnissa.[290] Arvioitaessa sitä, koskevatko kyseiset tiedot tunnistettavissa olevaa yksilöä, otettava huomioon henkilötietodirektiivin johdanto-osan

[288] Työasiakirja WP 105, s. 7
[289] Työasiakirja WP 105, s. 8
[290] Työasiakirja WP 105, s. 8

26-kohta, jonka mukaan *”sen määrittämiseksi, onko henkilö tunnistettavissa, olisi otettava huomioon kaikki kohtuullisesti toteutettavissa olevat keinot, joita joko rekisterinpitäjä tai joku muu voi kyseisen henkilön tunnistamiseksi käyttää.”*

Vaikkakin yllä mainittujen esimerkkien valossa on selvää, että kaikki RFID-tekniikan avulla tapahtuva tietojen keruu ei kuulu direktiivin soveltamisalaan, on yhtä lailla selvää, että monissa tapauksissa käsitellään henkilötietoja ja direktiivi tulee siten sovellettavaksi. Näin ollen niiden, jotka harkitsevat RFID-teknologian avulla kerättyjen tietojen käyttöä, on etukäteen arvioitava, onko tieto luettavissa *henkilötiedoksi* direktiivin valossa. Jos RFID-tekniikan avulla kerätty tieto ei sisällä henkilötietoa eikä se ole yhdistettävissä henkilötietoon, direktiivi ei tule sovellettavaksi.[291] Kauppajärjestöt pitivät tärkeänä, että pystymme erottamaan henkilötietoja käsittelevät sovellukset muista sovelluksista ja tiedämme siten, milloin henkilötietodirektiivi tulee sovellettavaksi.[292]

Kaikissa kolmessa tietosuojaryhmän skenaariossa, jotka on kuvattu tämän tutkimuksen 6. luvussa, henkilötietodirektiivi tulisi sovellettavaksi. Ensimmäisessä tapauksessa (6.1. luku) direktiivi tulisi sovellettavaksi, koska RFID-tekniikan avulla kerätty yksilöivä tieto on suoraan yhdistettynä luottokortille tai kanta-asiakaskortille tallennettuihin henkilötietoihin. Toisessa skenaariossa (6.2. luku) henkilötietodirektiivi soveltuu, mikäli henkilötietoja, esimerkiksi henkilön nimi upotetaan tunnisteeseen. Vaikkakaan viimeisissä esimerkeissä (6.3. luku) henkilöt, joiden liikkeitä ja tekemisiä seurattiin RFID-teknologian avulla, eivät ole *tunnistettuja*, he ovat tietosuojatyöryhmän mukaan *tunnistettavissa* ja direktiivi tulee siten sovellettavaksi.[293]

Joidenkin lausunnonantajien keskuudessa vallitsi erilainen käsitys henkilötieto-käsitteen määrittelystä. Metro Groupin mukaan missään tietosuojatyöryhmän esimerkissä ei ole mahdollista tunnistaa asiakkaiden nimiä tai muita henkilöön liittyvää tietoa. Asiakkaat pysyvät heidän mukaansa anonyymeina henkilötietodirektiivin määritelmän valossa. Metro Groupin mukaan skenaarioiden kaikenlainen muu tulkinta johtaisi *henkilötiedon* ja *muun tiedon* välisen kuilun selvään kapenemiseen lisäten oikeudellista epävarmuutta

[291] Työasiakirja WP 105, s. 8
[292] ICC:n, EICTA:n, ICRT:n ja JBCE:n lausunto, s. 8. Esimerkiksi laajassa käytössä autojen avaimissa sekä eläinten tunnistuksessa olevat RFID-tunnisteet ovat sellaisia, joissa henkilötietoja ei käsitellä. Tiedot eivät myöskään ole yhdistettävissä tunnistettavissa olevaan henkilöön ja direktiivi ei tule siten sovellettavaksi.
[293] Työasiakirja WP 105, s. 8

kaikkien osapuolten keskuudessa. Metro Groupin lausunnon mukaan yhtiön haaveena ei ole vakoilla asiakkaitaan tekniikan avulla, eikä yhtiö pidä vakoilua millään tavalla tarpeellisena. Kaikki vähittäiskaupan RFID-toiminnot nojaavat suuressa määrin asiakkaiden suostumukseen ja luottamuksen ylläpitoon. Yhtiön mukaan vähittäiskauppa ei tule missään nimessä vaarantamaan kauppiaan ja asiakkaan välistä luottamusta rikkomalla tietosuojalainsäädäntöä.[294]

EPCglobal korosti, ettei tavarakohtainen tunnistaminen itsessään ole minkäänlainen uhka yksityisyydelle. EPC-numero saattaa muodostua henkilötiedoksi vasta, jos se yhdistetään henkilötietoihin tai tietoihin, joista yksilö on perustellusti mahdollista tunnistaa.[295]

Kauppajärjestöt muistuttivat lausunnossaan, että ottaen huomioon RFID-tekniikan nykyisen käytön, käyttöönoton kustannukset ja odotettavissa olevan markkinoiden kasvun seuraavien viiden vuoden aikana, suuri enemmistö RFID:n käytöstä tulee olemaan henkilötietodirektiivin soveltamisalan ulkopuolella. Kauppajärjestöt viittaavat RFID-tunnisteiden pääasialliseen käyttöön jakeluketjuissa konttien, kuormauslavojen ja laatikoiden tunnistuksessa. Heidän mukaansa yksittäisten kaupassa myytävien tuotteiden tunnistus on vielä ainakin viiden vuoden päässä tulevaisuudessa, joten useimmat kuluttajat eivät tule törmäämään RFID-teknologiaan vähittäiskauppaympäristössä vielä muutamaan vuoteen.[296]

7.2. Ohjeita henkilötietodirektiivin velvoitteiden täyttämiseksi

RFID-teknologian avulla kerättyjen tietojen käsittelijät eli rekisterinpitäjät ovat velvollisia noudattamaan henkilötietodirektiivin asettamia velvoitteita. Tämän alaluvun tarkoituksena on antaa joitakin yleisohjeita, jotka saattavat auttaa rekisterinpitäjiä heidän käsitellessään henkilötietoja. Kuten myöhemmin 8. luvussa tarkemmin kuvaillaan, RFID-teknologian valmistajilla on suuri vastuu siitä, että tekniikka ottaa huomioon yksityisyyden suojan. Tämä auttaa paitsi rekisterinpitäjiä noudattamaan heidän henkilötietodirektiivin mukaisia velvollisuuksiaan myös rekisteröityjä käyttämään heidän oikeuksiaan.[297]

---

[294] Metro Groupin lausunto s. 9
[295] EPCglobalin lausunto, s. 9
[296] ICC:n, EICTA:n, ICRT:n ja JBCE:n lausunto, s. 8
[297] Työasiakirja WP 105, s. 9

Tietosuojatyöryhmä painotti, että RFID-teknologian – kuten kaikkien muidenkin teknologioiden – käytössä on huomioitava henkilötietodirektiivin johdanto-osan 2-kohta, jonka mukaan *"tietojenkäsittelyjärjestelmät on tehty palvelemaan ihmistä; järjestelmiä käytettäessä on kunnioitettava yksilöiden perusoikeuksia ja -vapauksia heidän kansalaisuudestaan tai asuinpaikastaan riippumatta, erityisesti oikeutta yksityisyyteen, ja osallistuttava taloudelliseen ja sosiaaliseen kehitykseen, kaupan kehittämiseen sekä yksilöiden hyvinvoinnin lisäämiseen"*. Tietosuojatyöryhmä totesi, että RFID-sovelluksia hyödyntävien rekisterinpitäjien on huomioitava useita tietosuojaperiaatteita, joita seuraavassa tarkastellaan.[298]

7.2.1. Tietojen laatua koskevat periaatteet

7.2.1.1.Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuuden periaatetta on käsitelty edellä (5.3.3. luku) henkilötietolain mukaisten henkilötietojen käsittelyä koskevien periaatteiden yhteydessä. Henkilötietolain mukainen käyttötarkoitussidonnaisuuden periaate pohjautuu henkilötietodirektiivin 6 artiklan 1-kohdan b-alakohtaan, joka velvoittaa jäsenvaltiot säätämään siitä, että henkilötiedot kerätään tiettyjä määriteltyjä ja laillisia tarkoituksia varten, eikä niitä saa myöhemmin käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Käyttötarkoitussidonnaisuuden osalta viittaan siten edellä (ks. luku 5.3.3.) henkilötietolain yhteydessä lausuttuun.

7.2.1.2.Tarpeellisuusvaatimus

Myös tarpeellisuusvaatimusta *(eng. the data quality principle)* on edellä käsitelty (5.3.2. luku) henkilötietolain valossa. Henkilötietolain mukainen tarpeellisuusvaatimus pohjautuu henkilötietodirektiivin 6 artiklan 1-kohdan c-alakohtaan, joka velvoittaa jäsenvaltiot säätämään siitä, että henkilötiedot ovat asianmukaisia, olennaisia eivätkä liian laajoja siihen tarkoitukseen, johon ne on kerätty, ja jossa niitä myöhemmin säilytetään. Näin ollen mitään tarpeetonta tietoa ei kerätä. Jos tarpeettomia tietoja on kuitenkin kerätty, ne on hävitettävä. Lisäksi saman artiklan d-alakohdan mukaan

[298] Työasiakirja WP 105, s. 9

jäsenvaltioiden on säädettävä siitä, että henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä.

7.2.1.3.Tietojen säilytystä koskeva periaate

Tietojen säilytystä koskeva periaate pohjautuu henkilötietodirektiivin 6 artiklan 1-kohdan e-alakohdan vaatimukseen, että henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan sen ajan, kun on tarpeen niiden tarkoitusten toteuttamista varten, joita varten tiedot kerättiin, tai joissa niitä myöhemmin käsitellään.

7.2.2. Oikeutusperuste henkilötietojen käsittelylle

Henkilötietojen käsittelyä koskevia yleisiä edellytyksiä on käsitelty edellä henkilötietolain 8 §:n valossa (ks. 5.2. luku). Henkilötietolain 8 § perustuu henkilötietodirektiivin 7 artiklan lainsäädäntötoimeksiantoon. Henkilötietoja voidaan käsitellä ainoastaan, jos käsittely on oikeutettua jonkun 7 artiklan alakohdan nojalla.[299]

Useimmissa tapauksissa, joissa RFID-teknologiaa käytetään henkilötietojen keräämiseen, *rekisteröidyn yksiselitteisesti antama suostumus* on ainoa henkilötietojen käsittelyn oikeutusperuste. Esimerkiksi jos kauppaketju haluaa sijoittaa tunnisteet kanta-asiakaskortteihin, sen täytyy kanta-asiakaskorttia myönnettäessä joko sopia asiasta asiakkaan kanssa kanta-asiakassopimuksessa tai pyytää asiakkaalta erillinen suostumus hankittujen henkilötietojen ja RFID-tekniikan avulla kerättyjen tietojen yhdistämiseen. Tietosuojatyöryhmän mukaan suostumus ei kuitenkaan aina ole tarkoituksenmukainen oikeutusperuste henkilötietojen käsittelylle. Työryhmä käytti esimerkkinä tilannetta, jossa sairaala käyttää RFID-tunnisteita leikkausinstrumenteissa vähentääkseen riskiä, että instrumentteja jää potilaan sisään leikkauksen päätyttyä. Työryhmän mukaan tässä tilanteessa ei tarvita potilaan suostumusta, koska *tietojenkäsittely on tarpeen potilaan*

[299] Henkilötietodirektiivin 7 artiklan mukaiset tietojenkäsittelyn laillisuutta koskevat edellytykset vastaavat pitkälti henkilötietolain 8 §:n edellytyksiä. Direktiivin 7 artiklan mukaan jäsenvaltioiden on säädettävä siitä, että henkilötietoja voidaan käsitellä ainoastaan: a) jos rekisteröity on yksiselitteisesti antanut suostumuksensa, tai b) jos käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osallisena, tai sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä, tai c) jos käsittely on tarpeen rekisterinpitäjän laillisen velvoitteen noudattamiseksi, tai d) jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi, tai e) jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai sivulliselle, jolle tiedot luovutetaan, tai f) jos käsittely on tarpeen rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseksi, paitsi milloin tämän intressin syrjäyttävät rekisteröidyn 1 artiklan 1 kohdan perusteella suojaa tarvitsevat intressit tai perusoikeudet ja -vapaudet.

elintärkeän edun suojaamiseksi, mikä on yksi 7 artiklan mukainen oikeutusperuste.[300] Tietosuojatyöryhmän esimerkki vaikuttaa tässä kohtaa kaukaa haetulta. Mikäli RFID-tunnisteita tullaan jatkossa käyttämään leikkausinstrumenteissa, niihin tullaan todennäköisesti tallentamaan ainoastaan yksilöivä numerosarja, eikä mitään henkilötietodirektiivin tarkoittamia henkilötietoja. Mielestäni direktiivi ei tule tällöin edes sovellettavaksi, eikä oikeutusperustetta näin ollen tarvitse hakea.

7.2.2.1. Suostumuksen ensisijaisuus

Suostumusta on edellä käsitelty henkilötietolain 8 §:n valossa (ks. 5.2. luku). Suostumuksen ensisijaisuus henkilötietojen käsittelyn edellytyksenä on nimenomaisesti julkilausuttuna myös henkilötietodirektiivissä. Suostumukselle asetetaan henkilötietodirektiivin 2 artiklan h-kohdan[301] ja 7 artiklan a-kohdan valossa tiettyjä vaatimuksia. Ensinnäkin suostumuksen on oltava *vapaaehtoisesti annettu*. Tällä tarkoitetaan sitä, että suostumuksen hankkimiseen ei saa liittyä harhaanjohtamista tai pakottamista. Toiseksi, suostumuksen on oltava *nimenomainen.* Toisin sanoen sen on viitattava tiettyyn tarkoitukseen. Kolmanneksi, suostumuksen on *osoitettava yksilön todellista tahtoa*. Neljänneksi, suostumuksen täytyy olla *julkilausuttu.* Lisäksi suostumuksen on oltava vielä *yksiselitteinen*, mikä tarkoittaa sitä, että ”suostumusta”, jolla voidaan nähdä useampia kuin yksi merkitys, ei ole pidettävä suostumuksena.[302] Saarenpään mukaan suostumusta on arvioitava nimenomaan rekisteröidyn näkökulmasta.[303]

7.2.3. Tiedottamisvelvollisuus

Tiedottamis- eli informointivelvollisuutta (ks. luku 5.4.1.) on edellä käsitelty henkilötietolain valossa. Henkilötietodirektiivin 10 artiklan mukaisesti rekisterinpitäjän on toimitettava rekisteröidylle vähintään seuraavat tiedot: rekisterinpitäjän henkilöllisyys, tietojenkäsittelyn tarkoitukset sekä lisätietoina mm. tietojen vastaanottajat ja tieto siitä, onko rekisteröidyllä oikeus saada itseään koskevia tietoja ja

[300] Työasiakirja WP 105, s. 10
[301] Henkilötietodirektiivin 2 artiklan h-kohdan mukaan ”rekisteröidyn suostumuksella” tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.
[302] Työasiakirja WP 105, s. 10
[303] Saarenpää. Näkökulmia yksilön suojasta (kohta 22).

oikeus niiden oikaisuun.[304] Edellä (ks. luku 6.) on esitetty skenaarioita, joissa vähittäiskauppa voisi käyttää RFID-järjestelmää siten, että kauppa käsittelisi henkilötietoja. Tällaisen vähittäiskaupan osalta tiedottamisvelvoite tarkoittaisi sitä, että kaupan on tiedotettava rekisteröidylle ainakin: 1) RFID-tunnisteiden olemassaolosta tuotteissa tai pakkauksissa, 2) RFID-tunnisteiden olemassaolon seurauksista tietojen keräämisen kannalta,[305] 3) tarkoituksista, joihin tietoja on tarkoitus käyttää[306] sekä 4) rekisterinpitäjän henkilöllisyydestä.[307]

Lisäksi riippuen RFID-järjestelmän käyttötarkoituksesta rekisterinpitäjä saattaa joutua tiedottamaan asiakkaita muun muassa siitä, miten tunniste voidaan tehdä toimimattomaksi tai poistaa tuotteesta sekä siitä, miten asiakas voi toteuttaa tietojen tarkastusoikeuttaan. Nämä tiedot ovat tarpeen ainakin yhdistettäessä RFID:n avulla kerättyjä tietoja henkilötietoihin edellä kuvattujen (ks. luku 6.1.) skenaarioiden mukaisesti.[308]

Tietosuojatyöryhmä huomautti lisäksi, että henkilötietodirektiivin 6 artiklan a-alakohta vaatii, että henkilötietoja käsitellään asianmukaisesti ja laillisesti. Tietosuojatyöryhmä piti tärkeänä, että tiedottamisvelvollisuutta toteutettaessa rekisteröity ymmärtää helposti RFID-sovelluksen vaikutukset.[309]

EPCglobal on julkaissut ohjeet EPC-teknologian kuluttajakäytöstä. Niissä todetaan muun muassa, että kuluttajille annetaan selkeä ilmoitus EPC:n olemassaolosta tuotteissa tai niiden pakkauksessa käyttäen EPC-logoa. Kuluttajille annetaan myös mahdollisuus hankkia lisätietoja EPC:stä ja sovelluksista. EPC-tunnisteita kuluttajatasolla käyttävät yritykset tulevat toimimaan tiiviissä yhteistyössä tiedottaakseen kuluttajia EPC-logosta ja samalla auttaakseen kuluttajia ymmärtämään tekniikkaa ja sen tarjoamia hyötyjä.[310]

---

[304] Tiedot tietojen vastaanottajista, tieto kysymyksiin vastaamisen pakollisuudesta tai vapaaehtoisuudesta sekä tarkastus- ja oikaisuoikeudesta täytyy toimittaa siltä osin, kun nämä lisätiedot ovat tarpeen ottaen huomioon erityiset olosuhteet, joissa tiedot kerätään, rekisteröidyn kannalta asianmukaisen tietojenkäsittelyn takaamiseksi.
[305] Tällä tarkoitetaan erityisesti sitä, että rekisterinpitäjän täytyy tiedottaa asiakkaille selvästi, että järjestelmä mahdollistaa sen, että tunnisteet lähettävät tietoa ilman asiakkaan aktiivisia toimia.
[306] Tämä sisältää mm. tieto siitä, millaisten henkilötietojen kanssa RFID:n avulla kerätty tieto on tarkoitus yhdistää sekä tieto siitä, voidaanko kyseisiä tietoja luovuttaa kolmannelle osapuolelle.
[307] Työasiakirja WP 105, s. 10-11
[308] Työasiakirja WP 105, s. 11
[309] Työasiakirja WP 105, s. 11
[310] EPCglobalin lausunto, s. 24

Tietosuojatyöryhmä käsitteli tiedottamisvelvollisuutta lähinnä tuotteiden alkuperäismyynnin valossa. Eräs lausunnonantaja huomautti, että tiedottamisvelvollisuudesta on yhtä lailla huolehdittava myös jälleenmyyntitilanteissa.[311]

7.2.4. Tiedonsaantioikeus

Myös rekisteröidyn tarkastusoikeutta ja henkilötiedon korjaamisvelvollisuutta, joista henkilötietodirektiivi käyttää yhteisnimeä ”tiedonsaantioikeus”, on edellä käsitelty henkilötietolain valossa (ks. luku 5.4.2). Henkilötietodirektiivin 12 artikla antaa rekisteröidylle mahdollisuuden tarkastaa tietojensa virheettömyyden ja ajantasaisuuden. Nämä oikeudet koskevat täysin myös henkilötietoja, jotka on kerätty RFID-teknologian avulla.

Esimerkiksi skenaariossa, jossa kauppaketju (ks. luku 6.1.) sijoitti tunnisteet kanta-asiakaskortteihinsa, tiedonsaantioikeus koskee kaikkia tietoja, jotka ovat yhdistettävissä henkilöön. Toisin sanoen tiedonsaantioikeus koskee mm. tietoa siitä, kuinka monta kertaa asiakas on käynyt kaupassa ja mitä hän on ostanut.[312]

7.2.5. Tietoturvaa koskevat vaatimukset

Saarenpään mukaan *oikeus tietoturvaan* on koko uuden verkkoyhteiskunnan informaatio-infrastruktuurin toimivuuden perusedellytys. Hänen mukaansa oikeus tietoturvaan on yksi informaatio-oikeuden keskeisistä periaatteista ja siten osa informaatio-oikeuden yleisiä oppeja. Tietoverkkojen ja informaation varaan demokraattinen yhteiskunta ja sen oikeusvaltio voidaan rakentaa vain, jos asianmukaisen tietoturvan avulla voidaan taata infrastruktuurin ja sen käytön toimivuus.[313]

Henkilötietodirektiivin 17 artiklan 1-kohta määrää, että rekisterinpitäjien on toteutettava tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta, vahingossa tapahtuvalta hävittämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai tietojen antamiselta, erityisesti jos

[311] Hazel Grantin lausunto, s. 1
[312] Työasiakirja WP 105, s. 11
[313] Saarenpää 2005b, s. 65-66

käsittely muodostuu tietojen siirtämisestä verkossa, sekä kaikelta muulta laittomalta käsittelyltä. Kyseiset tietoturvaa koskevat toimenpiteet voivat siis olla teknisiä tai organisatorisia. Käsittelen tietoturvaa koskevia vaatimuksia RFID:n kannalta tarkemmin jäljempänä 8.5. luvussa.

8. Tietosuojaperiaatteiden asettamat vaatimukset alan toimijoille

Edellisessä kappaleessa käsiteltyjen tietosuojaperiaatteiden noudattaminen on ensiarvoisen tärkeää niille, jotka ottavat käyttöön RFID-sovelluksia. Tietosuojatyöryhmän mukaan alan teknologia saattaa olla hyvin tärkeässä asemassa varmistamassa, että tietosuojaperiaatteiden noudattaminen toteutuu käsiteltäessä RFID-teknologian avulla kerättyjä henkilötietoja. Esimerkiksi tunnisteiden, lukijoiden ja sovellusten suunnittelulla saattaa olla suuri vaikutus siihen, että henkilötietojen kerääminen ja käyttö pystytään minimoimaan sekä siihen, että kaikki laittomat tietojenkäsittelyn muodot pystytään estämään tekemällä luvaton henkilötietoihin käsiksi pääsy teknisesti mahdottomaksi.[314]

Tietosuojatyöryhmä korosti työasiakirjassaan sekä RFID-sovellusten käyttöönottajien, RFID-teknologian valmistajien että standardisointielimien vastuuta. Samalla kun RFID-sovellusten käyttöönottajat ovat viime kädessä vastuussa tietyn sovelluksen avulla kerätyistä henkilötiedoista, RFID-teknologian valmistajat ja standardisointielimet ovat vastuussa siitä, että käyttöönottajilla on saatavilla tietosuoja- ja yksityisyydensuojavaatimukset huomioonottavaa teknologiaa. Etenkin standardien täytyy olla tällaisia, jotta henkilötietoja RFID-tekniikan avulla käsittelevillä rekisterinpitäjillä on tarpeelliset välineet henkilötietodirektiivin vaatimusten toteuttamiseksi. Tämän vuoksi tietosuojatyöryhmä kehotti tunniste-, lukija- ja sovellusvalmistajia sekä standardisointielimiä huomioimaan tässä luvussa esitettävät suositukset.[315]

8.1. Standardisoinnin ja yhteentoimivuuden vaikutukset tietosuojaperiaatteiden toteuttamisessa

Yleensä kaikkien uusien teknologioiden kohdalla standardisointiprosessi muodostuu yhteentoimivuuden pääveturiksi, mikä on tärkeää uuden teknologian menestyksekkään käyttöönoton kannalta. Standardisointi voi myös helpottaa tietosuoja- ja yksityisyyden suojavaatimusten omaksumista.

[314] Työasiakirja WP 105, s. 12
[315] Työasiakirja WP 105, s. 12

Kaikki RFID-järjestelmän osatekijät ovat tai tulevat olemaan standardien alaisia. Kuten edellä on mainittu standardisointielimet ja muut ryhmät ovat jo tehneet paljon työtä RFID-toimialalla. On huomioitava, että RFID-standardisoinnilla on vaikutusta useilla eri markkina-alueilla, mikä tulee näkymään etenkin tavaroiden kaupassa.[316]

Tietosuojatyöryhmä muistutti, että tunnisteiden lukuetäisyys on kasvanut ETSI:n *(European Telecommunications Standards Institute)* hyväksyttyä uudet UHF-taajuusalueen tehorajoitukset lukijoille. Tietosuojatyöryhmän mukaan lukijan toimintaetäisyydellä ja teholla saattaa olla merkitystä siihen, miten tietty RFID-järjestelmä vaikuttaa yksityisyyden suojaan.[317]

RFID-järjestelmien *yhteentoimivuus* (laitteistot, ohjelmistot ja tuotettu data) on standardisointiprosessin looginen seuraus. Liike-elämän kannalta yhteentoimivuus on pelkästään positiivinen asia. Yhteentoimivuus takaa sen, ettei vähittäiskauppiaan tarvitse hankkia useita erilaisia lukijoita tunnistaakseen eri valmistajien tunnisteita. Tietosuojan näkökulmasta yhteentoimivuus on kuin kaksiteräinen miekka. Yhteentoimivuus saattaa nimittäin parantaa tarkasteltavien tietojen teknistä laatua ja vaikuttaa siten osaltaan siihen, että henkilötietodirektiivin vaatimusta[318] siitä, että *henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä*, noudatetaan. Toisaalta yhteentoimivuudella saattaa olla myös negatiivisia sivuvaikutuksia tietosuojan kannalta, ellei aiheellisiin toimenpiteisiin ryhdytä. Esimerkiksi edellä mainittua käyttötarkoitussidonnaisuuden periaatetta (ks. luku 7.2.2.1) saattaa olla vaikeampi soveltaa ja valvoa. Lisäksi käyttöoikeuksien hallinta yksityisyyden suhteen saattaa tulla ongelmalliseksi, kun useammat tahot pääsevät muokkaamaan tietoja.[319]

EPCglobalin mielestä yhteentoimivuus parantaa itsestään jakeluketjujen turvallisuutta. Yhtiön mukaan yhteentoimiva järjestelmä mahdollistaa mm. laittomaan kauppaan puuttumisen aikaisessa vaiheessa sekä paremman tuotteiden aitouden tunnistamisen. Maailmanlaajuisiin standardeihin perustuva verkosto, joka nojaa järjestelmien yhteentoimivuuteen, parantaa EPCglobalin mukaan ruoan ja lääkkeiden jakeluketjujen turvallisuutta sekä mahdollistaa väärennösten havaitsemisen tehokkaammin. Lisäksi

[316] Työasiakirja WP 105, s. 12
[317] Työasiakirja WP 105, s. 13
[318] Ks. 6 artiklan 1 kohdan d-alakohta.
[319] Työasiakirja WP 105, s. 13

tällaisessa verkostossa vastatoimet mahdollisiin turvallisuusuhkiin ovat helpommin ja nopeammin toteutettavissa.[320]

8.2. RFID:n olemassaolosta tiedottamisen, näkyvyyden ja aktivointi-ilmaisun asettamat vaatimukset

Edellä (ks. luku 7.2.3.) on todettu, että RFID-tekniikan käyttöönottajien on tiedotettava rekisteröityjä, paitsi henkilötietojen käsittelyn tarkoituksesta, myös RFID-tunnisteiden olemassaolosta tuotteissa. Tietosuojatyöryhmä halusi kuitenkin korostaa tiedottamiselle ja näkyvyydelle asetettavia lisävaatimuksia.

Ensinnäkin henkilöä on tiedotettava myös aktivoituneista RFID-lukijoista. Tätä varten tarvitaan maailmanlaajuisesti standardisoituja piktogrammeja[321] sekä muita tiedotuskeinoja. Tällaisen tiedon tarjoaminen on välttämätöntä, jotta tekniikan avulla tapahtuva luvaton tai salainen henkilötietojen kerääminen pystytään estämään. Henkilöä on siten tiedotettava esimerkiksi, jos kauppa tai sairaala on aktivoinut lukijoita.[322]

Toiseksi, jotta salainen henkilötietojen kerääminen voidaan välttää, vaaditaan myös henkilön vaatteissaan ja muissa esineissään kantamien RFID-tunnisteiden olemassaolon havaittavuutta. Tämä vaatimus johtuu RFID-tunnisteiden pienestä koosta, mikä saattaa tehdä niistä käytännössä näkymättömiä. Tämän vaatimuksen täyttämiseen on monia keinoja. Tieto tunnisteista voidaan tietosuojatyöryhmän mukaan antaa paitsi vakioilmoituksilla myös teknisesti.[323]

Kolmanneksi, RFID:n käytöstä ilmoittaminen ei kuitenkaan tietosuojatyöryhmän mukaan käytännössä pelkästään riitä, vaan RFID-tunnisteiden *aktivoitavuus* tai *reaaliaikainen aktivointi* ovat myös sellaisia tietoja, jotka on annettava henkilötietodirektiivin tarkoittamille rekisteröidyille. Siten yksinkertaiset tekniset ratkaisut, jotka mahdollistavat aktivoinnin tai aktivoitavuuden tilan näkyvän osoittamisen, ovat tietosuojatyöryhmän mukaan myös välttämättömiä.[324]

---

[320] EPCglobalin lausunto, s. 14
[321] Piktogrammi on kuvamerkki tai kuvasymboli, jolla on erityinen sovittu merkitys.
[322] Työasiakirja WP 105, s. 14
[323] Työasiakirja WP 105, s. 14
[324] Työasiakirja WP 105, s. 14

Tietosuojatyöryhmä painotti, että tässä vaiheessa vaaditaan kaikilta osapuolilta lisää tutkimus- ja kehitystyötä kolmen edellä mainitun tiedotuskysymyksen parissa.[325]

8.3. Käyttö-, oikaisu- ja tuhoamisoikeuden asettamat vaatimukset

RFID-teknologian rakennustavalla voidaan taata käyttö-, oikaisu- ja tuhoamisoikeuden tehokas toteutuminen. Kyseisiä oikeuksia on arvioitava henkilötietodirektiivin 12 artiklan takaaman tiedonsaantioikeuden valossa.

RFID-teknologian luonteeseen kuuluu, että RFID-tunnisteen sisältöön käsiksi pääseminen eli *sisällön tarkasteleminen* vaatii tunnisteen käytännön (HF tai UHF) mukaisen RFID-lukijan ja näytön. Olennaista tekniikassa on kuitenkin se, että suurimmassa osassa sovelluksia tunniste sisältää ainoastaan *yksilöivän tunnistenumeron*, jonka merkitys avautuu ainoastaan eheän tietojärjestelmäympäristön kautta. Tietosuojatyöryhmän käsityksen mukaan vain harvat RFID-tunnisteet itsessään sisältävät sellaista merkityksellistä tietoa, joka tekisi ulkopuolisten tietoihin käsiksi pääsystä ongelman. Tällaista tietoa voisi olla esimerkiksi tuotteen kuvaileminen tai rekisterinpitäjän henkilöllisyys tunnisteelle kirjoitettuna.[326]

Toisin kuin RFID-tunnisteen sisällön tarkasteleminen, tunnisteelle kirjoitettujen tietojen *muokkaaminen* tai *korjaaminen* vaatii paitsi tunnisteen käytännön mukaisen lukijan myös vuorovaikutteisen tietojärjestelmän. Tietojärjestelmä mahdollistaa sekä sisällön lukemisen että muokkaamisen valvomisen. Yhtenä mahdollisuutena on väläytetty sitä, että tunnisteeseen lisätään ominaisuus, joka mahdollistaisi tunnisteelle kirjoitettujen tietojen poispyyhkimisen tai tunnisteen sarjanumeron sekoittamisen, mutta jättäisi kuitenkin tavararyhmän tyypin kuvauksen kokonaan tai osittain käytettäväksi.[327]

Onko henkilölle tarjottava mahdollisuus tunnisteen toimimattomaksi tekevän laitteen eli *deaktivaattorin (eng. tag disabler)* käyttöön, jotta henkilö pystyy estämään henkilötietojensa käsittelyn tunnisteen tullessa myöhemmin lukuetäisyydelle lukijasta? Vastaus kysymykseen riippuu muun muassa siitä, millä oikeutusperusteella henkilötietoja on alettu käsittelemään. Kyseisten laitteiden käyttömahdollisuuden tarjoaminen ei ole tietosuojatyöryhmän mukaan perusteltua ainakaan passeihin

[325] Työasiakirja WP 105, s. 14
[326] Työasiakirja WP 105, s. 14-15
[327] Työasiakirja WP 105, s. 15

upotettujen RFID-tunnisteiden kohdalla. Sen sijaan tietosuojanäkökulmasta katsottuna on tietosuojatyöryhmän mukaan tarpeellista, että tuhoamismahdollisuus tarjotaan silloin, kun RFID-tunnisteita käytetään kulutustavaroissa.[328] Näin tietosuojatyöryhmä ottaa asiaan samansuuntaisen kannan kuin Sydneyn konferenssi 2003, jonka päätöslauselman mukaan ”aina kun RFID-tunnisteita on yksilön hallussa, heillä pitäisi olla mahdollisuus poistaa tiedot, tehdä tunniste toimimattomaksi tai tuhota tunniste”.[329] Käytännössä RFID-tunnisteita kulutustavaroissa käyttävät yritykset ovat myös tarjonneet mahdollisuuden tunnisteen tuhoamiseen. Tietosuojatyöryhmälle toimittamassaan lausunnossa Metro Group kertoi, että se tarjoaa deaktivointimahdollisuuden asiakkailleen ennen kaupasta poistumista, vaikka tietosuojalainsäädäntö ei heidän mukaansa sitä vaadi.[330] EPCglobalin mukaan deaktivointimahdollisuuden tarjoaminen ei tulisi olla pakollista. EPCglobalin mielestä kuluttajia tulisi informoida myös siitä, mitä RFID-teknologian tarjoamia hyötyjä he menettävät, mikäli he tekevät tunnisteen toimimattomaksi.[331]

Viime vuosien aikana on ehdotettu erilaisia ratkaisuja, joilla tunnisteen myöhempi lukeminen voidaan estää. Tunnetuin ja käytetyin ratkaisu on erityinen ”kill-komento”. Pysyvä deaktivoiminen voidaan tehdä tuhoamalla tunniste erityisellä tietosisällön tuhoavalla laitteella tai poistamalla tunniste tuotteesta. Deaktivoituminen voi olla myös tilapäistä, mikäli käytetään ns. ohjelmistolukkoa (*eng. software lock*). ”Kill-komennon” suurin ongelma on siinä, että kaikki RFID:n tarjoamat hyödyt kaupan ulkopuolella menetetään. Niinpä on alettu etsiä myös muita vaihtoehtoja.[332]

Eräänlaisena muunnelmana ”kill-komennosta” voidaan nähdä menetelmä, jossa RFID-tunnisteelle tallennettujen tietojen päälle kirjoitetaan pelkkiä *nollia*. Etu tässä on se, että tunniste pysyy yhä aktiivisena, mutta lähettää lukijalle ainoastaan nollia merkityksellisen tiedon tai yksilöivän numerosarjan sijaan. Huomionarvoista on kuitenkin se, että tunniste vastaa edelleen komentoihin ja antaa tiedon, että kyseinen henkilö kuljettaa mukanaan tunnisteella varustettua esinettä. Tietosuojatyöryhmän mukaan niin kauan kun RFID-tunnisteet, jotka lähettävät lukijalla pelkkiä nollia, eivät ole kovin yleisiä, pelkkä tieto tällaisen tunnisteen olemassaolosta on arvokasta tietoa.

[328] Työasiakirja WP 105, s. 15
[329] Resolution on Radio-Frequence Identification, 25th Conference on Data Protection & Privacy Commissioners, Sydney 2003.
[330] Metro Groupin lausunto, s. 10
[331] EPCglobalin lausunto, s. 12
[332] Työasiakirja WP 105, s. 15

Ensinnäkin se kertoo, että kyseinen henkilö on ostanut jotakin kaupasta, joka käyttää tunnisteita tuotteissaan. Asiantunteva kauppa voi tehdä tiettyjä päätelmiä asiakkaasta. Toiseksi se kertoo, että kyseinen henkilö saattaa kantaa todennäköisesti mukanaan arvokasta tavaraa, koska RFID-tunnisteiden käytön alkuvaiheessa tunnisteita tullaan todennäköisesti käyttämään lähinnä arvotavaroissa. Niinpä tietosuojatyöryhmän mukaan pelkkä RFID-tunnisteen olemassaolo tulee auttamaan varkaita etsimään varastamisen arvoista tavaraa matkatavaroiden säilytyslokeroista tai parkkihalleista muutaman ensimmäisen vuoden aikana.[333] Tietosuojatyöryhmän ajatukset ovat mielestäni tässä kohtaa täysin epärealistisia. Tunniste ei ole tietojeni mukaan luettavissa auton pellin lävitse, eikä myöskään matkatavaroiden säilytyslokeroista.[334] Periaatteessa optimaalisissa olosuhteissa saattaisi olla mahdollista lukea tunnisteita asuntojen ikkunoiden lävitse. Vaikka tuloksena olisi pelkkiä numerosarjoja, usean osuman saaminen tietystä asunnosta saattaisi rohkaista varasta murtautumaan kyseiseen asuntoon viereisen asunnon sijasta, mikäli viereisestä asunnosta ei ollut luettavissa yhtään tunnistetta. Kieltämättä tämäkin skenaario vaikuttaa kaukaa haetulta.

Täysin toisen tyyppinen tapa myöhempien lukutapahtumien estämiseksi on *tunnisteen fyysinen suojaaminen*. RFID-tunniste voidaan suojata lukemiselta sulkemalla se ns. *Faradayn häkkiin*. Henkilö voi käyttää esimerkiksi suojattua lompakkoa, jotta tunnisteella varustettuja seteleitä ei voida tunnistaa. Mikäli seteleitä ryhdytään varustamaan RFID-tunnisteilla, on todennäköistä, että foliosuojatuista kukkaroista tulee valtava myyntimenestys.[335] Passien kansissa on tarkoitus käyttää ohutta alumiinilevyä, joka riittää suojaamaan RFID-tunnisteen tietosisällön, ellei passin kansia avata. Tunnisteen fyysinen suojaaminen ei ole kuitenkaan järkevä ratkaisu kaikissa RFID-sovelluksissa. Ihmiset tuskin haluavat pukea päälleen alumiinisuojia suojatakseen vaatteissaan olevat RFID-tunnisteet lukutapahtumilta. Tunnisteen fyysinen suojaaminen vaikuttaakin kaiken kaikkiaan aiheuttavan kohtuutonta vaivaa yksittäiselle ihmiselle, joka kuitenkin viime kädessä on vastuussa siitä, haluaako hän tunnisteen lähettävän tietoja vai ei.[336]

Tietosuojatyöryhmä korosti, että RFID-tekniikan standardisointielimien, valmistajien ja käyttöönottajien tulisi huomioida kehitystyötä tehdessään, että riippumatta siitä,

[333] Työasiakirja WP 105, s. 15-16
[334] Hämäläinen 2005
[335] Ainakin yksi yritys tarjoaa jo nyt Faradayn häkki -tekniikkaan perustuvia kukkaroita: http://www.mobilecloak.com/
[336] Työasiakirja WP 105, s. 16

millainen tunnisteen toimimattomaksi tekevä ratkaisu valitaan, yksilölle ei saa aiheutua minkäänlaista ”rangaistusta” siitä, että hän päättää tehdä tunnisteen toimimattomaksi. Myös tässä kappaleessa esiin tuoduilta osin tietosuojatyöryhmä korosti lisätutkimuksen olevan vielä tarpeen, kehottaen kaikkia osapuolia jatkamaan tutkimus- ja kehitystyötä.[337]

8.4. Oikeutusperusteet käsittelylle

Vaatimus siitä, että henkilölle on tarjottava mahdollisuus tehdä tunniste toimimattomaksi, on johdettavissa 12 artiklan lisäksi myös muista henkilötietodirektiivin artikloista.[338] Silloin, kun rekisteröidyn 7 artiklan a-kohdan mukaisesti yksiselitteisesti antama *suostumus* on ainoa henkilötietojen käsittelyn oikeutusperuste, yksilöllä on kuitenkin aina *mahdollisuus peruuttaa suostumuksensa* henkilötietojen käsittelyyn. Mikäli keinoa, jolla tunniste on poistettavissa, ei tarjota, yksilöä estetään nauttimasta oikeuksistaan.[339]

Silloin, kun RFID-tunnisteelle upotetut henkilötiedot on kerätty *muulla oikeutusperusteella kuin suostumuksella,* ei ole aina välttämätöntä tarjota tunnisteen toimimattomaksi tekemisen mahdollisuutta. Esimerkiksi henkilötietojen käyttäminen työpaikkojen avainkorttien tunnisteissa ei tietosuojatyöryhmän mukaan vaadi tunnisteen poistamismahdollisuutta, mikäli tietojenkäsittely perustuu työsuhteeseen. Sellaisissa sovelluksissa, joissa yksilöllä on oikeus peruuttaa suostumuksensa ja siten tehdä tunniste toimimattomaksi, sekä RFID-tekniikan valmistajien että käyttöönottajien tulisi varmistaa, että tunnisteen poistaminen on käytännössä *helposti toteutettavissa.*[340]

8.5. Tietoturvallisuus

Henkilötietodirektiivin 17 artiklan mukaisesti rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi, mikäli RFID-tunnisteelle on tallennettu henkilötietoja. Näillä toimenpiteillä on tarkoitus estää

[337] Työasiakirja WP 105, s. 16
[338] Henkilötietodirektiivin 14 artiklan a-kohdan mukaan ”jäsenvaltioiden on turvattava rekisteröidylle oikeus ainakin 7 artiklan e ja f alakohdassa tarkoitetuissa tapauksissa *millä hetkellä tahansa* vastustaa itseään koskevien tietojen käsittelyä tilanteeseensa liittyvien huomattavan tärkeiden ja perusteltujen syiden vuoksi, paitsi milloin kansallisessa lainsäädännössä toisin säädetään. Jos vastustus on perusteltua, rekisterinpitäjä ei enää saa käsitellä kyseisiä tietoja.”
[339] Työasiakirja WP 105, s. 16
[340] Työasiakirja WP 105, s. 16

luvaton tietojenkäsittely. Ellei *tietoturvatoimenpiteistä* huolehdita, kuka tahansa saattaa sopivalla lukijalla saada käsikseen henkilötietoja. Tietoturvatoimenpiteet ovat välttämättömiä myös henkilötietodirektiivin 6 artiklan 1 kohdan d-alakohdan[341] *täsmällisyysvaatimuksen* valossa. Asianmukaisilla tietoturvatoimenpiteillä pystytään estämään luvaton tietojen muuttaminen ja siten varmistamaan tunnisteelle tallennettujen *tietojen täsmällisyys*.[342]

Tarpeelliset teknisten toimenpiteet riippuvat tiedon luonteesta. Useimmissa tapauksissa tunnisteet saattavat vaatia tietojen *salakirjoitusta* eli *enkryptointia* sekä lukilaitteen tunnistusta, ettei kolmas osapuoli pysty lukemaan henkilötietoja. Mikäli RFID-tarroille kirjoitetaan esimerkiksi tieto potilaan henkilöllisyydestä, vastaavasta lääkäristä tai suoritettavasta toimenpiteestä, on selvää, että sairaalan velvollisuutena on varmistaa, että kyseiset tiedot eivät ole kolmannen osapuolen lukijoiden luettavissa. Niinpä alan toimijoiden on kehitettävä teknisiä ratkaisuja, kuten salakirjoitustekniikoita, estämään henkilötietojen ulkopuolinen lukeminen.[343] Metro Group ilmoitti lausunnossaan pyrkivänsä vapaaehtoisesti jatkuvasti parantamaan salakirjoitusmenetelmiään, vaikkakaan he eivät ilmoituksensa mukaan käsittele henkilötietoja direktiivin valossa.[344]

Kaikkein yleisimpänä ja turvallisimpana ratkaisuna tietosuojatyöryhmä piti *standardisoitujen tunnistuskäytäntöjen* (esimerkiksi ISO/IEC 9798) käyttämistä. Ne ovat jo yleisessä käytössä tietoverkoissa sekä älykorteilla.[345] Menemättä tässä tarkemmin kyseisten käytäntöjen teknisiin yksityiskohtiin totean kuitenkin, että käytännöt jakautuvat *symmetrisiin* ja *epäsymmetrisiin*. *Symmetrisissä tunnistuskäytännöissä* (esimerkiksi MAC) viestin salaus ja avaaminen tehdään samalla avaimella, jonka on näin ollen oltava sekä lähettäjän että vastaanottajan tiedossa, kun taas *epäsymmetrisissä tunnistuskäytännöissä* (esimerkiksi RSA) viestin salakirjoitus tapahtuu eri avaimella kuin sen avaaminen.[346]

---

[341] Henkilötietodirektiivin 6 artiklan 1-kohdan d-alakohdan mukaan jäsenvaltioiden on säädettävä siitä, että henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä; on tehtävä kaikki mahdollinen sen varmistamiseksi, että niihin tarkoituksiin nähden virheelliset tai puutteelliset tiedot, joita varten tiedot kerättiin tai joissa niitä myöhemmin käsitellään, poistetaan tai oikaistaan.
[342] Työasiakirja WP 105, s. 17
[343] Työasiakirja WP 105, s. 17
[344] Metro Groupin lausunto, s. 10
[345] Työasiakirja WP 105, s. 17
[346] http://www.vm.fi/tietoturvasanasto/sisallys.htm

Jotkut salakirjoitustekniikoihin perustuvat tunnistusmenetelmät ovat jo käytössä autojen radiotaajuustunnistukseen perustuvissa käynnistyksenestolaitteissa sekä kulunvalvontajärjestelmissä, mutta ne käyttävät usein *sovelluskohtaisia käytäntöjä*, koska ne ovat usein helpompia ja halvempia toteuttaa kuin standardit käytännöt. Tietoturvallisuuden parantamiseksi pitäisi kuitenkin tietosuojatyöryhmän mukaan käyttää standardeja käytäntöjä, jotta mm. arkaluonteiset tiedot pystytään suojaamaan. Näiden käytäntöjen hyöty on siinä, että ne ovat jo yleisessä käytössä ja niitä on laajasti testattu. Tällä tavalla ne ovat tulleet yleisesti hyväksytyiksi ja ne on todettu turvallisiksi.[347]

Tällä hetkellä on jo olemassa tutkittua tietoa siitä, että symmetriset salausalgoritmit, kuten AES *(Advanced Encryption Standard)* ovat käyttökelpoisia RFID-tunnisteille.[348] Symmetristen tunnistuskäytäntöjen ongelmana on kuitenkin se, että avaimen muodostaminen ja hallinnointi on vaativaa. Asymmetrisissä käytännöissä sen sijaan ei ole tätä ongelmaa, mutta ne ovat kalliimpia kuin symmetriset menetelmät.[349]

EPCglobal kertoi tietoturvallisuuden parantuvan Gen2-tunnisteiden myötä. Niissä käytetään Q-algoritmia, jolloin tunnistetta luettaessa lukija ei näytä tunnisteen varsinaista yksilöivää numeroa, vaan täysin merkityksettömän numerosarjan. Tämä vähentää merkittävästi salakuuntelumahdollisuuksia, sillä lukijan kyselysignaali on merkittävästi voimakkaampi kuin tunnisteen vastaussignaali. Voidaankin sanoa, että Gen2-tunnisteiden myötä lukijat ”huutavat” ja tunnisteet vain ”kuiskaavat”. Toisena tietoturvallisuutta parantavana keksintönä EPCglobal mainitsi 32-bittisellä salasanalla suojatun *kirjoituslukon*, jonka käyttöönotto varmistaisi sen, ettei tunnisteella olevien tietojen päälle voida kirjoittaa.[350]

[347] Työasiakirja WP 105, s. 17
[348] Feldhofer ym. 2004
[349] Työasiakirja WP 105, s. 17
[350] EPCglobalin lausunto, 14

9. Yhteenveto

Tässä tutkielmassa on edetty radiotaajuustunnistuksen tekniikan sekä yksityisyyden suojan ja henkilötietojen suojan yleiskuvausten kautta radiotaajuustunnistukseen liittyviin erityisiin yksityisyydensuoja- ja tietosuojakysymyksiin. Näitä kysymyksiä on lähestytty henkilötietodirektiivin (95/46/EC) 29 artiklan nojalla perustetun tietosuojatyöryhmän keväällä 2005 julkaiseman työasiakirjan ja siihen saatujen lausuntojen valossa.

Suurin osa tietosuojatyöryhmän työasiakirjaan lausuntonsa antaneista yrityksistä sekä kauppajärjestöistä, lukuun ottamatta tietoturvayrityksiä, oli sitä mieltä, että olemassa oleva henkilötietodirektiivi kattaa RFID:n käyttöönotosta johtuvat yksityisyydensuoja- ja tietosuojakysymykset. He uskovat itsesääntelyn täydentävän henkilötietodirektiiviä. Vastaavasti, suurin osa yliopistoista, ajatushautomoista ja yksityisistä henkilöistä sekä tietoturvaratkaisuja tarjoavat yritykset olivat sitä mieltä, että tietosuojatyöryhmän tulisi antaa asiassa lisäohjeita. Jotkut ehdottivat jopa henkilötietodirektiivin täydentämistä RFID:ta koskevilla erityissäännöksillä. Nämä erityissäädökset voisivat koskea esimerkiksi tiettyjä RFID-sovelluksia, kuten RFID:n käyttöä julkisessa liikenteessä, vähittäiskaupassa, ihmisen kehon sisällä tai passeissa. Jotkut vaativat erityislainsäädäntöä tiedottamisvelvollisuudesta käytettäessä RFID:ta kulutustavaroissa sekä kuluttajan mahdollisuudesta tuhota tunniste, jotka nähtiin tarpeellisina riippumatta siitä, sisältääkö RFID:n käyttö kulutustavaroissa henkilötietojen käsittelyä. Toiset taas vaativat erityissäännöksiä salakirjoituksen käyttövelvollisuudesta silloin, kun tunnisteelle tallennetaan henkilötietoja.[351]

Ne tahot, jotka uskovat, että erillistä RFID:ta koskevaa lainsäädäntöä ei tarvita, ovat sitä mieltä, että henkilötietodirektiivi kattaa riittävän hyvin RFID:n avulla tapahtuvan henkilötietojen käsittelyn ja keräämisen. Heidän mielestään erillinen RFID:ta koskeva lainsäädäntö ja lainsäädännöstä aiheutuvat kustannukset saattaisivat muodostaa esteen kyseisen teknologian kehitykselle. He katsovat, että erillislainsäädäntö johtaisi Euroopan epäedulliseen asemaan muihin talousalueisiin verrattuna.[352] Itse katson, että ainakin tässä vaiheessa on tärkeämpää antaa ohjeita alan toimijoille nykyisen tietosuojalainsäädännön soveltamisesta RFID-tekniikkaan, eikä vielä tule antaa

[351] Tiivistelmä lausunnoista, s. 1-2
[352] Tiivistelmä lausunnoista, s. 2

erillislainsäädäntöä. Kuten edellä on todettu, ala on tällä hetkellä erittäin nopean kehityksen vaiheessa ja niinpä tietosuojatyöryhmän tulee seurata alan kehitystä aktiivisesti.

Kiistellyksi kysymykseksi lausunnoissa nousi se, voiko tuotekohtainen EPCglobalin standardeihin perustuva tunnistaminen sisältää henkilötietojen käsittelyä. Kuluttajajärjestöt ja jotkut yliopistotahot olivat sitä mieltä, että henkilötietojen käsittely on mahdollista, kun taas elinkeinoelämä oli pääosin sitä mieltä, että henkilötietojen käsittely ei tässä kohtaa ole mahdollista. Kysymys on erityisen tärkeä siksi, että mikäli kyseisen järjestelmän avulla kerättyjä tietoja ei pidetä henkilötietoina, vähittäiskauppiailla ei ole velvollisuutta noudattaa henkilötietodirektiiviä. Tällöin vähittäiskauppiaalla ei olisi myöskään velvollisuutta tiedottaa kuluttajia RFID-tunnisteiden olemassaolosta tuotteissa, lukijoiden sijainnista tai niiden poistamismahdollisuudesta ilman erillislainsäädäntöä.[353] Vähittäiskauppiaat ovat kuitenkin Euroopassa tiedottaneet kuluttajia kyseisistä asioista, vaikka he kokevat, ettei direktiivi heitä siihen velvoita.

Toiseksi kiistanalaisena kysymykseksi nousi se, perustuuko tietosuojatyöryhmän työasiakirja liian tiukkaan henkilötieto-käsitteen määrittelyyn. Joidenkin lausunnonantajien mielestä tietosuojatyöryhmän käsitykset laajentavat henkilötiedon käsitettä siitä, miten se on määritelty henkilötietodirektiivissä. Erityisesti monet lausunnonantajat olivat sitä mieltä, että luvussa 6.3. esitellyissä skenaarioissa ei käsitellä henkilötietoja. Toistuvasti lausunnoissa kritisoitiin myös sitä, etteivät tietosuojatyöryhmän skenaariot edusta todellisuutta. Monet lausunnonantajat katsoivat, että tarkastelun tulisi pikemminkin keskittyä teknisten sovellusten tarjoamiin yhteiskunnallisiin hyötyihin arvioitaessa RFID-sovelluksia.[354] Itse katson kuitenkin, että RFID:hen liittyvät yksityisyydensuoja- ja tietosuojakysymykset on pidettävä esillä tekniikan ollessa nopeassa kehitysvaiheessa. Vaikka onkin myönnettävä, etteivät läheskään kaikki tietosuojatyöryhmän skenaariot ole tällä hetkellä teknisesti toteutettavissa, saattaa tilanne muuttua hyvin nopeasti. Niinpä tietosuojatyöryhmän on oltava valmiina antamaan lisäohjeistusta ja tarvittaessa käytettävä järeämpiä keinoja unionin kansalaisten yksityisyyden suojan takaamiseksi.

[353] Tiivistelmä lausunnoista, s. 2
[354] Tiivistelmä lausunnoista, s. 2

Yleisesti ottaen tietosuojatyöryhmän työasiakirjaa on mielestäni pidettävä tervetulleena avauksena RFID-tekniikkaan liittyvien tietosuojakysymysten eurooppalaisessa käsittelyssä. Työasiakirjassa tietosuojaongelmat tuodaan esiin varsin realistisessa valossa, joskin osa luoduista skenaarioista on ainakin teknisesti vielä kaukana tästä päivästä. Yhdysvalloissa kuluttajansuojajärjestöt ovat ottaneet aktiivisen roolin tekniikkaan liittyvistä tietosuojakysymyksistä tiedotettaessa. Siellä tiedotus tuntuu kuitenkin keskittyvän *”isoveli valvoo”* -hysterian luomiseen. Yhdysvalloissa tiedotukseen on sisältynyt jopa tarkoituksellista valheellisen tiedon levittämistä ja samalla RFID-tekniikan tarjoamat hyödyt tuntuvat unohtuneen. Mielestäni tärkeintä on, että Euroopan unionissa kiinnitetään jatkuvaa huomiota tietosuojakysymyksiin alan kehittyessä – kuitenkin luomatta minkäänlaista hysteriaa ja pitäen mielessä myös tekniikan tarjoamat hyödyt jokapäiväiseen elämäämme.

10. Summary

This study deals with data protection issues related to Radio Frequency Identification (RFID) technology. RFID is said to be "a new and vastly improved barcode", which has been considered a replacement for barcodes. The use of RFID applications may benefit business, individuals and public services. For example, RFID can help retailers manage their inventory, enhance consumers' shopping experience and improve drug safety.

However, as with many other technologies, widespread deployment of the technology does not come without its potential drawbacks. The most commonly discussed drawbacks have been data protection and privacy issues related to RFID technology. My research function was to find out, what kinds of data protection issues are related to RFID technology, and how can we avoid conflicts between applications of RFID technology and data protection rights of individuals. In addition, I aimed to find out, how legislations of European Union and Finland should be applied to applications of RFID.

European Union has also reacted to these drawbacks of the technology. Working Party on the protection of individuals with regard to the processing of personal data set up under Article 29 of data protection Directive (95/46/EC) published the *Working Document on Data Protection Issues Related to RFID Technology* (WP105) in the spring 2005. In particular, Working Party was concerned about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals. The ability to surreptitiously collect a variety of data all related to same person, track individuals as they walk in public places, enhance profiles through the monitoring of consumer behaviour in stores, read the details of clothes and accessories worn and medicines carried by customers were all examples of uses of RFID technology that gave rise to privacy concerns in WP105. Working Party decided to put WP105 up for public consultation, which resulted to 34 responses.

Beginning with basics of the technology of RFID and general survey of privacy and data protection legislation, I proceed to more special data protection issues related to RFID technology. These issues are dealt with in the light of WP105 and responses received to it. Working Party and many referees disagreed if the personal data is processed in particular applications of RFID. A very controversial issue was whether

item level tagging based on EPC Global standards will usually entail a processing of personal data. Another very controversial point was whether the WP105 paper is based on an overstretched definition of personal data, which goes beyond the definition contained in the data protection Directive and which is used to support the application of the Directive in cases where the Directive should not apply. A repeated criticism of the WP 105 paper is that the examples of RFID applications given in the paper do not represent reality.

The conclusion of my study is that the data protection Directive adequately covers the processing of personal data gathered through RFID and no additional legislation is needed for RFID – at least not yet, when RFID is in fast evolution. However, Working Party must continue monitoring the technological developments in the field of RFID in collaboration with interested parties. Depending on the evolution of RFID technology and its applications, Working Party must be ready to provide additional guidance for specific applications to protect privacy of union's citizens.