

**JULKISEN SEKTORIN TIETOJEN UDELLEENKÄYTTÖ JA  
HENKILÖTIETOJEN SUOJA**

ANNA HÄNNINEN

Lapin yliopisto

Oikeustieteiden tiedekunta

Maisteritutkielma

Oikeusinformatiikka

Syksy 2014

## Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Julkisen sektorin tietojen uudelleenkäyttö ja henkilötietojen suoja

Tekijä: Anna Hänninen

Opetuskokonaisuus ja oppiaine: Oikeusinformatiikka

Työn laji: Tutkielma\_X\_Laudaturtyö\_\_Lisensiaatintyö\_\_Kirjallinen työ\_\_

Sivumäärä: XVI + 88

Vuosi: 2014

**Tiivistelmä:** Avoimen tiedon politiikalla on tarkoitus edistää julkisen sektorin tietojen saatavuutta, hyödynnettävyyttä ja uudelleenkäyttöä. Euroopan unionin tavoitteena on julkisen tiedon uudelleenkäyttömahdollisuuksien tehostaminen ja yhtenäistäminen. Tällä halutaan parantaa julkisin varoin tuotettuun tietoon perustuvien uusien koko yhteisön alueen kattavien palveluiden kehittämistä sekä edistää talouskasvua ja yhteiskunnallista osallistumista.

Viranomaisen tiedon julkisuutta koskeva keskeinen periaate on julkisuusperiaate, jonka nojalla kaikki viranomaisen hallussa oleva tieto on julkista, ellei sitä ole erikseen säädetty salassa pidettäväksi. Perinteisesti julkisuusperiaatteen nojalla kenellä tahansa on pyydettyessä oikeus saada tieto julkisesta asiakirjasta. Tietoyhteiskunnassa julkisuusperiaate tarkoittaa myös oikeutta hyödyntää viranomaistietoa kaupallisesti.

Henkilörekisteriin kuuluvien henkilötietojen vieminen avoimeen verkkoon on luonteeltaan tietojen sähköistä luovuttamista. Jos henkilötietoja julkaistaan avoimessa tietoverkossa, on kyse henkilötietojen automaattisesta käsittelystä, johon sovelletaan henkilötietojen suojaa koskevia säännöksiä. Henkilötietojen suojaan liittyvät riskit koskevat muun muassa anonyymien tietojen luovuttamista, profilointia ja rekisteröityjen oikeuksien toteutumista.

Avoimen julkisen datan aikakausi vaatii entistä parempaa tietojen ja tietojärjestelmien hallintaa viranomaisilta. Tietovarantojen avaamisessa korostuu viranomaisen hyvän tiedonhallintatavan noudattamisen tärkeys.

**Avainsanat:** avoin data, henkilötietojen suoja, julkinen sektori, julkisuusperiaate, oikeusinformatiikka, tietosuoja

Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön\_X\_

Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi\_X\_

Suostun tutkielman luovuttamiseen Lapin maakuntakirjastossa käytettäväksi\_X\_

(vain Lappia koskevat)

## Sisällys

Lähteet.....	IV
Oikeuskäytäntö ja viranomaisten ratkaisut .....	XIV
Lyhenteet.....	XV
1. Johdanto .....	1
1.1 Tutkimustehtävä.....	5
1.2 Tutkimusmetodi ja keskeiset oikeuslähteet.....	6
2. Keskeiset käsitteet.....	10
2.1 Avoin data, julkinen tieto ja tietoyhteiskunta.....	10
2.2 Henkilötieto ja anonyymi tieto.....	13
2.3 Henkilörekisteri ja rekisterinpitäjä.....	17
3. Julkisen sektorin tietojen uudelleenkäyttöä koskeva normisto .....	21
3.1 Julkisen sektorin tietojen uudelleenkäyttöä koskeva direktiivi.....	21
3.2 Julkisen sektorin tietojen uudelleenkäyttöä koskeva kansallinen normisto .....	24
4. Julkisuus ja yksityisyys perusoikeuksina .....	31
4.1 Oikeus tietoon .....	31
4.2 Oikeus yksityiselämän ja henkilötietojen suojaan.....	33
4.3 Rekisteröityjen oikeudet.....	35
4.4. Julkisuusperiaate .....	39
4.5 Hyvä tiedonhallintatapa .....	45
4.6 Julkisuuden ja yksityisyyden välinen suhde.....	48
5. Henkilötietojen suojaan kohdistuvat riskit.....	55
5.1 Julkinen sektori henkilötietojen julkaisijana .....	55
5.2 Anonyymien tietojen uudelleenkäyttö .....	58
5.3 Profilointi ja tietojen yhdistäminen .....	64
6. Henkilötietojen suojan huomioonottaminen .....	68
6.1 Oikeudelliset periaatteet.....	68
6.1.1 Suunnitteluvollisuus ja käyttötarkoitussidonnaisuus.....	69
6.1.2 Tietojen tarpeellisuus ja virheettömyys.....	75
6.1.3 Sisäänrakennettu ja oletusarvoinen tietosuojat.....	77
6.1.4 Tietotilinpäätös ja tilivelvollisuudenperiaate .....	78
6.2 Henkilötietojen siirto kolmansiin maihin.....	80
6.3 Käytännösäännöt .....	81
7. Lopuksi.....	84

## Lähteet

### Kirjallisuus

*Ahvenainen, Taisto ja Räty, Tapio.* Julkisuuslainsäädäntö; julkisuus ja salassapito kunnissa. Helsinki, Suomen kuntaliitto 1999.

*Arjen tietoyhteiskunnan neuvottelukunta.* Tietoyhteiskuntastrategia tuottava ja uudistuva Suomi, digitaalinen agenda vuosille 2011-2020. Juvenes Print Tampereen yliopistopaino Oy Vantaa 2010.

*Bygrave, Lee A.* Data Protection Law Approaching Its Rationale, Logic and Limits. Kluwer Law International. The Hague, London, New York 2002.

*Castrén, Kirsi.* Julkinen tieto ei aina ole avoin. Tietosuoja -lehti 2/2014. Hämeen kirjapaino Oy.

*van Dijk, Jan.* The Network Society 3rd Edition. SAGE Publications Ltd 2012.

*van Eechoud, Mireille ja Janssen, Katleen.* Rights of Access to Public Sector Information. Masaryk University of Law and Technology (MUJLT), Vol 6(3). Saatavissa: <http://ssrn.com/abstract=2213411> (katsottu 29.6.2014).

*Eklund, Mia. C ja Lilja, Johanna.* Kuluttajien profilointi markkinointitarkoituksiin – henkilötietojen käsittelyn ja tietosuojasääntelyn kehityssuuntia. Defensor Legis 2013/2 s.216. Asiantuntija-artikkeli.

*Floridi, Luciano.* Open Data, Data Protection and Group Privacy. Saatavissa: <http://link.springer.com/article/10.1007%2Fs13347-014-0157-8#page-1> (katsottu 29.6.2014).

*Hintikka, Kari A ja Kola, Petri ja Poikola, Antti.* Julkinen data -johdatus tietovarantojen avaamiseen. Liikenne- ja viestintäministeriön julkaisuja 15.3.2010.

*Konstari, Timo.* Asiakirja julkisuudesta hallinnossa; Tutkimus yleisten asiakirjain julkisuudesta hallinnon kontrollivälineenä. Vammalan kirjapaino Oy 1977.

*Konstari, Timo.* Henkilörekisterilaki; säännökset ja käytäntö. Lakimiesliiton kustannus 1992.

*Konstari, Timo ja Wallin, Anna-Riitta.* Julkisuus- ja salassapitolainsäädäntö; Laki viranomaisten julkisuudesta ja siihen liittyvät lait. Gummerus Kirjapaino Oy 2000.

*Korhonen, Rauno.* Perusrekisteri ja henkilötietojen suoja; Informaatio-oikeudellinen tutkimus yksityisyyden suojasta perusrekisteritietojen käsittelyssä. Rovaniemi: Lapin Yliopisto 2003.

*Korhonen, Rauno.* Sähköinen asiointi ja viestintä. Teoksessa: Tammilehto Timo (toim.): Oikeusjärjestys osa III 8. täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 60. Rovaniemi 2012.

*Mahkonen, Sami.* Oikeus yksityisyyteen. Werner Söderström Lakitieto Oy 1997.

*Mäenpää Olli.* Julkisuusperiaate. WSOY 2008.

*Neuvonen, Riku.* Viestintä- ja informaatio-oikeuden perusteet. Meedia Zone OÜ 2013.

*Neuvonen, Riku.* Yksityisyyden suoja Suomessa. Lakimiesliiton kustannus 2014.

*Niiniluoto, Ilkka.* Tieto, informaatio ja yhteiskunta. VAPK 1989.

*O'hara, Kieron.* Transparent Government, Not Transparent Citizens: A Report on Privacy and Transparency for the Cabinet Office. Saatavissa: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/61280/transparency-and-privacy-review-annex-b.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61280/transparency-and-privacy-review-annex-b.pdf) (katsottu 18.8.2014).

*Ohm, Paul.* Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Saatavissa: <http://ssrn.com/abstract=1450006> (katsottu 19.9.2014).

*Pitkänen, Olli ja Tiilikka, Päivi ja Warmma, Eija.* Henkilötietojen suoja. Talentum 2014.

*Pöysti, Tuomas.* Tehokkuus, informaatio ja eurooppalainen oikeusalue. Hakapaino Oy 1999.

*Rubinstein, Ira.* Big Data: The End Of Privacy or a New Beginning? International Data Privacy Law (2013 Forthcoming) NYU School of Law, Public Law Research Paper No. 12-56. 5.10.2012. Saatavissa: <http://ssrn.com/abstract=2157659> (katsottu 19.9.2014).

*Saarenpää, Ahti.* Verkkoyhteiskunta oikeutta –johdatusta aiheeseen. Saatavissa: <https://helda.helsinki.fi/handle/10224/3699> (katsottu 26.6.2014).

*Saarenpää, Ahti.* Henkilö- ja persoonallisuusosoikeus. Teoksessa: Tammilehto Timo (toim.): Oikeusjärjestys Osa I 8. täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 60. Rovaniemi 2012a.

*Saarenpää, Ahti.* Oikeusinformatiikka. Teoksesta: Tammilehto, Timo (toim.) Teoksessa: Tammilehto Timo (toim.): Oikeusjärjestys Osa I 8. täydennetty painos. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 60. Rovaniemi 2012b.

*Salo, Immo.* Big Data tiedon vallankumous. Docendo Oy 2013.

*Salokannel, Marjut.* Julkisesta datasta avoimeen dataan, julkisen datan lisensiointi. Elinkeinoelämän tutkimuslaitos, keskusteluaiheita No 1277 16.8.2012. Saatavissa: <http://www.etla.fi/wp-content/uploads/2012/09/dp1277.pdf> (katsottu 10.9.2014).

*Salokannel, Marjut.* Tutkimuksen perusteet: Tutkimusdatan ja muun primäärin tutkimusaineiston saatavuuteen liittyvä oikeudellinen sääntely. Julkaistu Edilexissä 21.11.2012 (katsottu 12.9.2014).

*Timonen, Pekka.* Johdatus lainopin metodiin ja lainopilliseen kirjoittamiseen. Helsinki: Helsingin yliopiston oikeustieteellinen tiedekunta 1998.

*Voutilainen, Tomi.* ICT-oikeus sähköisessä hallinnossa; ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely. Edita Publishing Oy 2009.

*Voutilainen, Tomi.* Palveluarkkitehtuuria tukeva lainsäädäntö, tutkimusraportti 22/2014. Juvenes Print – Suomen yliopistopaino Oy 2014.

*Vuorensyrjä, Matti ja Savolainen, Reijo.* Tieto ja tietoyhteiskunta. Gaudeamus 2001.

*Wallin, Anna-Riitta ja Nurmi, Pekka.* Tietosuojalainsäädäntö; Henkilörekisterilaki ja siihen liittyvät säännökset. Lakimiesliiton kustannus 1990.

## **Kotimaisia virallislähteitä ja viranomaisten julkaisuja**

*HE 309/1993 vp.* Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

*HE 30/1998 vp.* Hallituksen esitys Eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja eräksi siihen liittyviksi laeiksi.

*HE 96/1998 vp.* Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräksi siihen liittyviksi laeiksi.

*HE 171/2002 vp.* Hallituksen esitys Eduskunnalle laiksi ajoneuvoliikennerekisteristä.

*HE 20/2005 vp.* Hallituksen esitys Eduskunnalle laeiksi viranomaisten toiminnan julkisuudesta annetun lain muuttamisesta sekä kuntalain 50 §:n muuttamisesta.

*HE 246/2010 vp.* Hallituksen esitys Eduskunnalla laeiksi julkisen hallinnon tietohallinnon ohjauksesta sekä viranomaisen toiminnan julkisuudesta annetun lain 18 ja 36 §:n muuttamisesta.

*HE 154/2012 vp.* Hallituksen esitys eduskunnalle laeiksi tilastolain sekä maaseutuelinkeinotilastoista annetun lain 2 ja 3 §:n muuttamisesta.

*HE 195/2013 vp.* Hallituksen esitys eduskunnalle laiksi väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalvelusta annetun lain muuttamisesta

*Liikenne- ja viestintäministeriö.* Liikenteen ja viestinnän avoin tieto, työryhmän raportti 10/2013. Saatavissa: [www.lvm.fi/c/document\\_library/get\\_file?folderId=2497123&name=DLFE-19419.pdf&title=Julkaisuja%2010-2013](http://www.lvm.fi/c/document_library/get_file?folderId=2497123&name=DLFE-19419.pdf&title=Julkaisuja%2010-2013) (katsottu 1.8.2014).

*PeVL 25/1998.* Perustuslakivaliokunnan lausunto 25/1998 vp. Hallituksen esitys henkilötietolaiksi ja eräksi siihen liittyviksi laeiksi.

*PeVL 12/2002.* Perustuslakivaliokunnan lausunto 12/2002 vp. Hallituksen esitys ulosottolain muuttamisesta ja siihen liittyviksi laeiksi.

*PeVL 2/2008.* Perustuslakivaliokunnan lausunto 2/2008 vp. Hallituksen esitys laiksi maaseutuelinkeinohallinnon tietojärjestelmästä.

*Tietosuojavaltuutetun toimiston ohje.* Henkilötietojen käsittely suostumuksen perusteella, päivitetty 27.7.2010 (katsottu 5.8.2014).

*Tietosuojavaltuutetun toimiston ohje.* Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset, päivitetty 27.7.2010 (katsottu 5.8.2014).

*Tietosuojavaltuutetun toimiston ohje.* Henkilötietojen luovuttaminen viranomaisten henkilörekisteristä, päivitetty 27.07.2010 (katsottu 5.8.2014).

*Tietosuojavaltuutetun toimiston ohje.* Henkilörekisteriin talletettujen tietojen tarkastaminen, päivitetty 27.7.2010 (katsottu 5.8.2014).

*Tietosuojavaltuutetun toimiston ohje.* Laadi tietotilinpäätös, päivitetty 24.4.2012 (katsottu 6.8.2014).

*Tietosuojavaltuutetun toimiston ohje.* Tarkistuslista henkilötietojen luovutusmenettelyä suunniteltaessa huomioon otettavista asioista, päivitetty 27.7.2010 (katsottu 5.8.2014).

*Tietosuojavaltuutetun toimiston ohje.* Toimialakohtaisten käytännesääntöjen laatiminen, päivitetty 27.07.2010 (katsottu 5.8.2014).

Tietosuojavaltuutetun ohjeet ovat saatavissa osoitteessa:  
<http://www.tietosuoja.fi/fi/index/materiaalia/oppaat.html>.

*Valtioneuvoston kanslia.* Uudistuva, ihmisläheinen ja kilpailukykyinen Suomi. Kansallinen tietoyhteiskuntastrategia vuosille 2007-2015. Annettu 26.9.2006. Saatavissa: <http://vnk.fi/julkaisukansio/2006/tietoyhteiskuntaneuvosto/tietoyhteiskuntastrategia/fi.pdf> (katsottu 28.8.2014).

*Valtioneuvoston periaatepäätös.* Julkisen sektorin digitaalisten tietoineistojen saatavuuden parantamisesta ja uudelleenkäytön edistämisestä. Annettu 3.3.2011.

*Valtioneuvoston neuvottelutulos* vuoden 2011 hallitusohjelmasta. Annettu 17.6.2011. Saatavissa: [www.valtioneuvosto.fi/tiedostot/julkinen/hallitusneuvottelut-2011/neuvottelutulos/fi.pdf](http://www.valtioneuvosto.fi/tiedostot/julkinen/hallitusneuvottelut-2011/neuvottelutulos/fi.pdf) (katsottu 1.9.2014).

*Valtioneuvoston kirjelmä.* Eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta. Annettu 3.5.2012.



*Valtioneuvoston kanslia.* Pääministeri Jyrki Kataisen hallituksen ohjelma. Annettu 22.6.2011. Saatavissa: [www.valtioneuvosto.fi/tietoarkisto/aiemmathallitukset/katainen/hallitusohjelma/pdf/fi.pdf](http://www.valtioneuvosto.fi/tietoarkisto/aiemmathallitukset/katainen/hallitusohjelma/pdf/fi.pdf) (katsottu 22.8.2014).

*Valtioneuvoston kanslia.* Pääministeri Alexander Stubbin hallituksen ohjelma. Annettu 24.6.2014. Saatavissa: <http://valtioneuvosto.fi/hallitus/hallitusohjelma/pdf-stubb/fi.pdf> (katsottu 22.8.2014).

*Valtiovarainministeriön* julkaisu. Suomen avoimen hallinnon toimintasuunnitelma. Annettu 23.4.2013. Saatavissa: [www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/Avoin\\_hallinto\\_toimintasuunnitelma.pdf](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/Avoin_hallinto_toimintasuunnitelma.pdf) (katsottu 28.8.2014).

*Valtiovarainministeriön* julkaisu. Julkishallinnon tietoluovutusten periaatteet ja käytännöt, julkishallinnon tietovarantojen saatavuuden ja käytön edistäminen – työryhmän loppuraportti 2/2012. Juvenes Print Tampereen yliopistopaino 2012.

*Valtiovarainministeriön* julkaisu. Julkiset tietovarannot laajempaan käyttöön – esite. Saatavissa: [www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/01\\_julkaisut/076\\_ict/2014\\_0508Avoime/avoimen\\_tiedon\\_ohjelma\\_esite\\_FIN\\_low.pdf](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/076_ict/2014_0508Avoime/avoimen_tiedon_ohjelma_esite_FIN_low.pdf) (katsottu 17.8.2014).

*Valtiovarainministeriön* julkaisu. Tietoaineistojen käyttö lupa. Saatavissa: [http://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/20140902Avoime/Marjut\\_Salokannel\\_Avointen\\_tietoaineistojen\\_kaeyttoelupa.pdf](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20140902Avoime/Marjut_Salokannel_Avointen_tietoaineistojen_kaeyttoelupa.pdf) (katsottu 15.9.2014).

*Valtiovarainministeriön* muistio. EU/2022/2040 ja EU/2011/2041. Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta. Annettu 3.5.2012.

*Valtiovarainministeriön* raportti. VM041:00/2013, 885/00.01.00.01/2013. Julkisten tietovarantojen avaaminen, yhteenveto ministeriöiden vuosien 2014–2017 kehysvalmisteluiden yhteydessä tekemistä selvityksistä.

*Valtiovarainministeriön* raportti. Julkishallinnon kokonaisarkkitehtuuriraportti, julkisen hallinnon tietoarkkitehtuuri. Versio 0.95. Päivätty 4.4.2011. Saatavissa: [https://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/20110407Luo/12\\_JHKA\\_Tietoarkkitehtuuri\\_20110404.pdf](https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20110407Luo/12_JHKA_Tietoarkkitehtuuri_20110404.pdf) (katsottu 29.8.2014).

*Valtiovarainministeriö.* Palvelut ja tiedot käytössä, julkisen hallinnon ICT:n hyödyntämisen strategia vuosille 2012–2020. Annettu huhtikuussa 2013 Saatavissa: [https://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/julkict-strategia-2012-2020.pdf](https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/julkict-strategia-2012-2020.pdf) (katsottu 22.8.2014).

*Valtiovarainministeriö.* Julkisten tietovarantojen avaaminen ja kehysvalmistelut 2015–2018 ohje. Annettu 23.10.2013.

*Valtiovarainministeriön tiedote.* Annettu 12.9.2014. Saatavissa: <http://valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/fi.jsp?oid=424476> (katsottu 15.9.2014).

### **Ulkomaisia virallislähteitä ja muita julkaisuja**

*Article 29 Working Party* opinion 03/2013 on purpose limitation (00569/13/EN WP 230). Adopted on 2 April 2013. Saatavissa: [http://idpc.gov.mt/dbfile.aspx/Opinion3\\_2013.pdf](http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf) (katsottu 20.5.2014).

*The European Thematic Network on Legal Aspects of Public Sector Information (LAPSI), LAPSI Policy Recommendation N.4 Privacy and Personal Data Protection, LAPSI Working Group 2 Privacy Aspects of PSI.* Saatavissa: [http://www.lapsi-project.eu/lapsifiles/lapsi\\_privacy\\_policy.pdf](http://www.lapsi-project.eu/lapsifiles/lapsi_privacy_policy.pdf) (katsottu 29.6.2014).

*Euroopan neuvoston ministeriökomitean* suositus No R(91)10, julkisten viranomaisten hallussa olevien henkilötietojen luovuttamista ulkopuolisille, hyväksytty ministeriökomiteassa 9.9.1991.

*Euroopan tilasto-ohjelmakomitea.* Euroopan tilastoja koskevat käytäntesäännöt, tilasto-ohjelmakomitean hyväksymä 29.9.2011. Saatavissa: [http://epp.eurostat.ec.europa.eu/cache/ITY\\_OFFPUB/10425-FI/FI/10425-FI-FI.PDF](http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/10425-FI/FI/10425-FI-FI.PDF) (katsottu 20.9.2014).

*Henkilötiedodirektiivin 29 artiklan nojalla perustetun tietosuojatyöryhmän* lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83) annettu 12. joulukuuta 2003. Saatavissa

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83\\_fi.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_fi.pdf) (katsottu 28.7.2014).

*Henkilötiedodirektiivin 29 artiklan nojalla perustetun tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136) annettu 20. kesäkuuta 2007. Saatavissa:*

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_fi.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fi.pdf) (katsottu 10.7.2014).

*Henkilötiedodirektiivin 29 artiklan nojalla perustetun tietosuojatyöryhmän lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsitteijän käsitteestä (00264/10/FI WP 169) annettu 16. helmikuuta 2010. Saatavissa: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_fi.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fi.pdf) (katsottu 12.7.2014).*

*Henkilötiedodirektiivin 29 artiklan nojalla perustetun tietosuojatyöryhmän lausunto 3/2010 tilivelvollisuuden periaatteesta (00062/10/FI WP 173) annettu 13. heinäkuuta 2010. Saatavissa: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173\\_fi.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fi.pdf) (katsottu 5.8.2014).*

*Henkilötiedodirektiivin 29 artiklan nojalla perustetun tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207) annettu 5. kesäkuuta 2013. Saatavissa: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207\\_fi.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_fi.pdf) (katsottu 25.7.2014).*

*Henkilötiedodirektiivin 29 artiklan nojalla perustetun tietosuojatyöryhmän lausunto 5/2014 anonymisointitekniikoista (0829/14/FI WP 216) annettu 10. huhtikuuta 2014. Saatavissa: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_fi.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fi.pdf) (katsottu 25.7.2014).*

*Euroopan komission vihreä kirja. KOM (1998) 585. Julkisen sektorin tieto: Euroopan avainresurssi. Vihreä kirja julkisen sektorin tiedon käytöstä tietoyhteiskunnassa.*

*Euroopan komission ehdotus KOM (92) 422 lopullinen, annettu 28.10.1992. Amended proposal for a Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

*Euroopan komission tiedonanto KOM(2009)212.*

*Euroopan komission tiedonanto* Euroopan parlamentille, neuvostolle ja Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle. Avoin data Innovoiminnin, kasvun ja läpinäkyvän hallinnon moottori. KOM (2011) 882 lopullinen, Bryssel 12.12.2011.

*Euroopan komission ehdotus* Euroopan parlamentin ja neuvoston direktiiviksi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta, KOM (2011) 877 lopullinen, Bryssel 12.12.2011. Saatavissa: [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/com/com\\_com\(2011\)0877\\_/com\\_com\(2011\)0877\\_fi.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0877_/com_com(2011)0877_fi.pdf) (katsottu 4.7.2014).

*Euroopan komission päätös* komission asiakirjojen uudelleenkäytöstä (2011/833/EU). Annettu 12.12.2011. Saatavissa: <http://eurlex.europa.eu/legalcontent/FI/TXT/PDF/?uri=CELEX:32011D0833&from=FI> (katsottu 4.7.2014).

*Euroopan komission ehdotus* Euroopan parlamentin ja neuvoston asetukseksi: yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuojasetus)/ COM(2012) 11 Final, annettu 25.1.2012. Saatavissa: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FI:PDF> (katsottu 26.7.2014).

*LIBE-valiokunnan mietintöluonnos* yleisestä tietosuojasetuksesta: Draft report on proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0225/2012 – 2012/0011(COD)).

*Organisation for Economic Cooperation and Development (OECD)* Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information C(2008) 36. Saatavissa: <http://www.oecd.org/sti/44384673.pdf> (katsottu 14.8.2014).

*Opinion of the European Data Protection Supervisor* on the ‘Open-Data Package’ of the European Commission including a Proposal for Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the re-use of the Commission documents 18.4.2012. Saatavissa: <https://secure.edps.europa.eu/EDPSWEB/webdav>

/shared/Documents/Consultation/Opinions/2012/12-04-18\_Open\_data\_EN.pdf  
(katsottu 28.7.2014).

*Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to processing of personal data in the context of profiling*, adopted by the Committee of Ministers on 23 November 2010. Saatavissa: <https://wcd.coe.int/ViewDoc.jsp?id=1710949> (katsottu 04.9.2014).

## **Muut**

Valtiovarainministeriön Avoimen tiedon -ohjelman kotisivut saatavissa: [www.vm.fi/vm/fi/05\\_hankkeet/02381\\_avoin\\_tieto/index.jsp](http://www.vm.fi/vm/fi/05_hankkeet/02381_avoin_tieto/index.jsp).

Valtiovarainministeriön Avoimen tiedon -ohjelman hankesivut saatavissa: [www.hare.vn.fi/mHankePerusSelaus.asp?h\\_iID=19367&tVNo=1&sTyp=Selaus](http://www.hare.vn.fi/mHankePerusSelaus.asp?h_iID=19367&tVNo=1&sTyp=Selaus).

## Oikeuskäytäntö ja viranomaisten ratkaisut

Korkein hallinto-oikeus 20.5.2014/1619 KHO:2014:83

Korkein hallinto-oikeus 25.10.2012/2962

Korkein hallinto-oikeus 3.10.2012/2622 KHO:2012:88

Euroopan unionin tuomioistuin, asiassa C-131/12: Google SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González, annettu 13. toukokuuta 2014

Euroopan unionin tuomioistuin asiassa C-28/98: komissio v. The Bavarian Lager Co. Ltd., annettu 29. kesäkuuta 2010

Euroopan yhteisön tuomioistuin asiassa C-101/01: Bodil Lindqvist annettu 16. marraskuuta 2003

Eduskunnan oikeusasiamies dnro 2022/40/04

Apulaisoikeuskansleri päätös 07.2.2005 dnro 168/1/04

Apulaisoikeuskansleri päätös 18.11.2009 dnro OKV/1318/2007

Tietosuojalautakunnan päätös dnro 2/932/2009

Tietosuojavaltuutetun ohjaus dnro 2120/09/2013

Tietosuojavaltuutetun ratkaisu dnro 98/41/2007

## Lyhenteet

AOK	Apulaisoikeuskansleri
Dnro	Diaarinumero
EU	Euroopan unioni
EY	Euroopan yhteisö
HE	Hallituksen esitys
Henkilötietodirektiivi	Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
HetiL	Henkilötietolaki (532/1999)
Ibid.	Latinaa ibidem, samassa paikassa, edellinen alaviite on sama
ICT	Information and Communication Technology Tieto- ja viestintäteknikka
JUHTA	Julkisen hallinnon tietohallinnon neuvottelukunta
JulkL, Julkisuuslaki	Laki viranomaisten toiminnan julkisuudesta (621/1999)
KHO	Korkein hallinto-oikeus
KOM	Komission mietintö
LAPSI	Network on Legal Aspects of Public Sector Information
LIBE	Civil Liberties, Justice and Home Affairs, Kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta
OECD	Organisation for Economic Cooperation and Development, Taloudellisen yhteistyön ja kehityksen järjestö
PeVL	Perustuslakivaliokunnan lausunto

PeL	Suomen perustuslaki (731/1999)
PIA	Privacy Impact Assessment
PSI	Public Sector Information
PSI-direktiivi	Euroopan parlamentin ja neuvoston direktiivi 2003/98/EY, annettu 17 päivänä marraskuuta 2003, julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä ja Euroopan parlamentin ja neuvoston direktiivi 2013/37/EU, annettu 26. kesäkuuta 2013, julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta.
SopS	Sopimussarja
Trafi	Liikenteen turvallisuusvirasto Trafi
Vp.	Valtiopäivät



## 1. Johdanto

”Henkilötietojen sääntelyjärjestelmien toimivuus ja yleinen hyväksyntä on riippuvainen paitsi siitä, kuinka hyvin lainsäädännössä onnistutaan tasapainottamaan erilaiset tietoon ja sen saatavuuteen liittyvät arvot, myös siitä, kuinka hyvin rekisterinpitäjät ja muut henkilötietojen käsittelyyn osallistuvat ymmärtävät lainsäädännön tavoitteet ja sääntelyn taustalla olevat ihmisten perusoikeudet.”<sup>1</sup>

Julkisella sektorilla on hallussaan laadukkaita, julkisella rahoituksella tuotetut tietovarannot, joiden yhteydessä käsitellään ja tuotetaan suuria määriä erilaista dataa. Tavoitteena on, että näiden tietovarantojen käyttö ja uudelleenkäyttö koituu koko yhteiskunnan hyväksi. Julkisen sektorin tietovarannoilla tarkoitetaan taloudellisesti, sisällöllisesti tai yhteiskunnallisesti merkittäviä tietokokonaisuuksia.<sup>2</sup> Tietovarannot sisältävät huomattavan määrän tietoaineistoja, joiden uudelleenkäyttöön ei kohdistu rajoituksia.<sup>3</sup> Tietovarantojen avaamisella tai avoimella datalla tarkoitetaan tietovarantojen tarjoamista vapaasti hyödynnettäväksi ilman käyttörajoituksia. Avoimen tiedon ohjelmien tarkoituksena on saattaa koko tietokanta uudelleenkäytettäväksi standardoidussa elektronisessa muodossa, kaikille halukkaille, maksuttomasti ja mihin tahansa kaupalliseen tai ei-kaupalliseen tarkoitukseen.<sup>4</sup>

Ajatus julkisen sektorin tietovarantojen tehokkaasta hyödyntämisestä ei ole kansallisesti uusi. Tietojen yhteiskäyttö on ollut tavoitteena tietohallintoa ja tietoyhteiskunnan kehittämistä koskevissa linjauksissa jo yli 20 vuotta.<sup>5</sup> Tietovarantojen avaamiseen on sittemmin kiinnitetty huomioita tietoyhteiskunnan kehitystä koskevissa strategioissa, selvityksissä, periaatepäätöksissä ja ohjelmissa. Julkisten tietovarantojen avaaminen ja hyödyntäminen kuuluvat hallitusohjelman kestävän talouskasvun, työ-

---

<sup>1</sup> HE 96/1998 vp., osa 3.2.

<sup>2</sup> Valtiovarainministeriön raportti VM041:00/2013, 885/00.01.00.01/2013: Julkisten tietovarantojen avaaminen, yhteenveto ministeriöiden vuosien 2014–2017 kehysvalmisteluiden yhteydessä tekemistä selvityksistä s.2. Myös Korhonen 2003, s.9.

<sup>3</sup> Julkishallinnon tietoluovutusten periaatteet ja käytännöt 2/2012, s.27.

<sup>4</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 48.

<sup>5</sup> Tavoitteena on, että tieto kerätään sen syntymisen yhteydessä ja sitä käytetään sen jälkeen aina kun tietoa tarvitaan eri julkisorganisaatioissa. Periaatetta on jo pitkään toteutettu perusrekisterien tietojen ylläpidossa ja tietojen hyödyntämisessä. Julkishallinnon tietovarantojen saatavuuden ja käytön edistämisen -työryhmän loppuraportti Julkishallinnon tietoluovutusten periaatteet ja käytännöt 2/2012 s.15.

lisyiden ja kilpailukyvyen vahvistamisen kärkihankkeisiin.<sup>6</sup> Avoimet julkiset tietovarannot ovat hyvän hallinnon perusta.<sup>7</sup>

Euroopan unionin informaatioyhteiskuntahankkeen yhteydessä vuonna 1998 valmistui julkisen sektorin informaatiota koskeva vihreä kirja KOM (1998) 585, jossa korostetaan viranomaisten tuottaman tiedon merkitystä sisällöntuotantoteollisuudelle. Tällöin ajatus viranomaisten tuottaman tiedon käyttämisestä kaupallisessa tarkoituksessa oli vielä vieras. Tänä päivänä Euroopan unionin keskeisenä tavoitteena on Euroopan alueen talouden vakaan kasvun varmistaminen hyödyntämällä olemassa olevia innovaatiomahdollisuuksia ja resursseja. Komission tiedonannon mukaan Euroopan unionin alueella voitaisiin saavuttaa vuosittain 40 miljardin euron taloudellinen hyöty avaamalla julkisen sektorin tuottama tieto uudelleenkäytettäväksi.<sup>8</sup> Julkisen sektorin tiedon uudelleenkäyttöä koskeva direktiivi (PSI-direktiivi) velvoittaa jäsenvaltioita arvioimaan julkisen sektorin hallussa olevien tietojen uudelleenkäytettävyyttä sekä saattamaan sellaiset julkiset tietovarannot uudelleenkäytettäväksi, joihin ei kohdistu direktiivissä esitettyjä rajoituksia.<sup>9</sup>

Avoimen tiedon politiikalla on tarkoitus edistää julkisen sektorin tiedon laajaa saatavuutta, hyödynnettävyyttä ja uudelleenkäyttöä. Julkisen tiedon uudelleenkäyttömahdollisuuksia parantamalla ja yhtenäistämällä halutaan parantaa julkisin varoin tuotettuun tietoon perustuvien uusien koko yhteisön alueen kattavien palveluiden kehittämistä sekä edistää talouskasvua ja yhteiskunnallista osallistumista.<sup>10</sup>

Julkisen tiedon tehostettuun saatavuuteen ja uudelleenkäyttöön liittyy riskejä ja haasteita henkilötietojen suojan ja viime kädessä yksityiselämän ja yksityisyyden suojan kannalta.<sup>11</sup> Riskit liittyvät henkilötietojen yhdistelemiseen ja niiden käyttämiseen

---

<sup>6</sup> Neuvottelutulos hallitusohjelmasta annettu 17.6.2011, s.50. Valtioneuvosto, pääministeri Alexander Stubbin hallituksen ohjelma 24.6.2014, s.5.

<sup>7</sup> Valtiovarainministeriön Avoimen tiedon ohjelma - julkiset tietovarannot laajempaan käyttöön –esite, saatavilla osoitteessa:

[http://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/01\\_julkaisut/076\\_ict/20140508Avoime/avoimen\\_tiedon\\_ohjelma\\_esite\\_FIN\\_low.pdf](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/076_ict/20140508Avoime/avoimen_tiedon_ohjelma_esite_FIN_low.pdf).

<sup>8</sup> Esimerkiksi paikkatieto, tilastotieto, säätiedot, julkisrahoitteisissa tutkimushankkeissa tuotettu tieto ja kirjastojen digitoidut kirjat.

<sup>9</sup> Jäsenvaltioiden on PSI-direktiivin johdanto-osan 8 kohdan mukaan sallittava tietojen uudelleenkäyttö, jollei tietojen saatavuutta ole rajoitettu tai estetty kansallisilla asiakirjojen saatavuutta koskevilla lainsäädännöksillä tai direktiivissä säädetyillä poikkeuksilla.

<sup>10</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 48 ja KOM(2011) 882 lopullinen, Bryssel 12.12.2011 s.2.

<sup>11</sup> Opinion of the European Data Protection Supervisor on the ‘Open-Data Package’ of the European Commission including a Proposal for Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the re-use of the Commission documents 18.4.2012 (‘Euroopan tietosuojavaltuutetun avoimen datan pakettia

tarkoituksiin, joita ei ole pystytty ennalta arvioimaan. Henkilötietojen suojaan liittyvät riskit koskevat muun muassa anonymien tietojen luovuttamista, profilointia ja rekisteröityjen oikeuksien toteutumista. Jos anonymiejä tietoja luovutetaan, on mahdollista, että henkilöitä voidaan edelleen tunnistaa tiedoista esimerkiksi yhdistelemällä tietoja muihin olemassa oleviin tietoihin. Teknologian nopea kehitys vaikeuttaa tunnistamisriskien analysointia. Lisäksi kaikki salassa pidettävät tiedot eivät sisällä henkilötietoja. Yksi keskeinen Avoimen tiedon – ohjelman periaate on se, ettei aineistojen avaaminen saa heikentää yksityisyyden suojaa.

Ihmistä kerätään suuria määriä tietoja siitä, ketä me olemme, missä me olemme, kenen kanssa me olemme, mitä syömme ja harrastamme. Käsitteinä ”Open Data”, ”Big Data” ja ”Internet of Things” ovat osa arkipäiväämme. Euroopan kuluttajasiames Maglena Kuneva totesi tietojen keräämistä ja profilointia koskevassa puheessaan 31.3.2009 ”Personal data is the new oil of the internet and the new currency of the digital world”.<sup>12</sup> Ihmisillä saattaa olla useita digitaalisia henkilöllisyyksiä, jotka saattavat muodostua myös virheellisistä tiedoista.

Omien tietojen hallinnoiminen on yhä vaikeampaa, emmekä todellisuudessa voi tietää, missä ja mitä tietoja meistä kaikkialla on tallennettuna. Ehdotuksessa yleiseksi tietosuoja-asetukseksi otetaan huomioon ihmisen oikeus tulla unohdetuksi myös digitaalisessa maailmassa.<sup>13</sup> Tietosuoja-asetukselle kohdistuu odotuksia, koska sen tarkoituksena on turvata yksityisyyden suoja henkilötietoja käsiteltäessä globaalien tietoverkkojen aikakaudella, jossa tiedon määrä ja saatavuus kasvaa eksponentiaalisesti. Lisäksi viime aikoina julkisuutta saaneet tarkkailu- ja valvontatoimet ja epäonnistuneet henkilötietojen anonymisoinnit ovat entisestään kiinnittäneet huomiota yksityisyyden asemaan perusoikeutena globaalissa tietoyhteiskunnassa.<sup>14</sup>

Henkilörekisteriin kuuluvien henkilötietojen vieminen avoimeen verkkoon on luonteeltaan tietojen sähköistä luovuttamista.<sup>15</sup> Jos henkilötiedot saatetaan uudelleenkäytettäväksi avoimeen verkkoon, on kyse henkilötietojen automaattisesta käsittelystä

---

koskeva lausunto 2012’) s.3 ja Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to processing of personal data in the context of profiling, adopted by the Committee of Ministers on 23 November 2010 (”Neuvoston profilointisuositus”), s. 1.

<sup>12</sup> Saatavilla osoitteesta [http://europa.eu/rapid/press-release\\_SPEECH-09-156\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm).

<sup>13</sup> COM(2012) 11 final artikla 17 ”oikeus tulla unohdetuksi ja poistaa tiedot”.

<sup>14</sup> Ohm 2010, Rubinstein 2012.

<sup>15</sup> Tietosuojavaltuutetun ohjaus dnro 908/41/2007, Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s.4.

tä, johon sovelletaan henkilötietojen suojaa koskevia säännöksiä.<sup>16</sup> Tietojen uudelleenkäytön perusteena voi olla tietyn tahon nimenomainen pyyntö tai sopimus. Henkilötietojen uudelleenkäytön taustalla voi olla myös julkisten rekisterien käyttö.<sup>17</sup> Kansallisia tietojen saatavuutta ja henkilötietojen suojaa koskevia säännöksiä sovelletaan täysimääräisesti silloin, kun julkisen sektorin tietovarantoja avataan uudelleenkäyttötarkoituksessa. Euroopan neuvosto on jo 1990-luvun alussa antamassaan suosituksessa kiinnittänyt huomiota viranomaisten henkilötietojen käsittelyyn liittyviin riskeihin yksityisyyden suojan kannalta.<sup>18</sup>

Viranomaisen tiedon julkisuutta koskeva keskeinen periaate on julkisuusperiaate, jonka nojalla kaikki viranomaisen hallussa oleva tieto on julkista, ellei sitä ole erikseen säädetty salassa pidettäväksi. Perinteisesti julkisuusperiaatteen nojalla kenellä tahansa on pyydetessä oikeus saada tieto julkisesta asiakirjasta. Tietoyhteiskunnassa julkisuusperiaate tarkoittaa myös oikeutta hyödyntää viranomaistietoa kaupallisesti. Olli Mäenpään sanoin ”julkisuusperiaate ei enää ole vain yhteiskunnallinen arvo, vaan sillä on myös (liike)taloudellista arvoa”.<sup>19</sup>

Oikeusvaltioperiaatteen mukaisesti julkisen vallan käytön on perustuttava lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia (PeL 2 §). Julkista valtaa käyttävien on aktiivisin toimenpitein suojaavat henkilöiden yksityisyyttä erityisesti silloin, kun tietojen saatavuus voi aiheuttaa tiettyjä uhkia yksityisyyden suojalle (PeL 22 §). Pyrkimyksenä on viranomaisen hallussa olevan tiedon avoimuus ja läpinäkyvyys sekä toisaalta taas kansalaisten yksityiselämän suojaaminen.<sup>20</sup>

Julkinen tieto ja avoin tieto eivät ole synonyymejä. Julkinen tieto voi olla avointa tietoa, riippuen kohdistuuko siihen lainsäädännöllisiä rajoituksia. Keskeiset julkisen sektorin tietojen uudelleenkäyttöön vaikuttavat rajoitukset liittyvät salassapitosäännöksiin, maksulainsäädäntöön, tekijänoikeuksiin ja henkilötietojen suojaan. Avoimen julkisen datan aikakausi vaatii entistä parempaa tiedon ja tietojärjestelmien hallintaa niin viranomaisilta kuin yksittäisiltä virkamiehiltäkin. Tietojen avaamiseen ja saata-

---

<sup>16</sup> Valtiovarainministeriön raportti VM041:00/2013, 885/00.01.00.01/2013: Julkisten tietovarantojen avaaminen, yhteenveto ministeriöiden vuosien 2014–2017 kehysvalmisteluiden yhteydessä tekemistä selvityksistä, s. 2. PSI-direktiivin johdanto-osan 11 kohdan mukaan direktiivin soveltamisessa on noudatettava kaikilta osin henkilötietojen suojaa koskevia periaatteita.

<sup>17</sup> Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s.4.

<sup>18</sup> Viranomaisten henkilötietojen luovuttamista koskeva suositus. Euroopan neuvoston ministeriökomitean suositus No R(91)10, julkisten viranomaisten hallussa olevien henkilötietojen luovuttamista ulkopuolisille, hyväksytty ministeriökomiteassa 9.9.1991.

<sup>19</sup> Mäenpää 2008, s.9.

<sup>20</sup> O'hara, Review of Privacy and Transparency, s.3.

vuuteen liittyvät riskit on otettava huomioon mahdollisimman hyvissä ajoin. Tietovarantojen avaamisen yhteydessä korostuu viranomaisen hyvän tiedonhallintatavan noudattamisen tärkeys.

## 1.1 Tutkimustehtävä

Maisteritutkielmassani haluan selvittää, minkälaisia vaatimuksia julkisen sektorin tietojen uudelleenkäyttöön kohdistuu kansallisten ja yhteisön alueen keskeisistä tietoyhteiskuntaa koskevista päätöksistä ja strategioista sekä säännöksistä ja direktiiveistä.

PSI-direktiivin nojalla Euroopan unionin jäsenvaltioiden on pääsääntöisesti mahdollistettava julkisen sektorin tietojen uudelleenkäyttö, mutta tietojen uudelleenkäyttö perustuu kansallisiin asiakirjojen saatavuutta koskeviin säännöksiin. Keskeinen julkisen sektorin tietojen uudelleenkäyttöä koskeva poikkeus liittyy henkilötietojen suojaan. Julkisen sektorin tietojen uudelleenkäytön yhteydessä sovelletaan täysimääräisesti henkilötietojen suojaa koskevia säännöksiä.

Tutkielmani tarkoitus on vastata siihen, mihin säännöksiin ja periaatteisiin julkisen sektorin tietojen uudelleenkäyttö perustuu sekä siihen, miten henkilötietojen suojaa koskevat säännökset ja periaatteet vaikuttavat julkisen sektorin tietojen uudelleenkäyttöön. Tutkielmassa tarkoitukseni on selvittää, mitä henkilötietojen suojaa koskevia säännöksiä ja periaatteita julkisen sektorin elimen on otettava huomioon, kun se harkitsee tietovarantojensa avaamista uudelleenkäyttöä varten. Tarkastelen julkisen sektorin tietojen uudelleenkäyttöä pääsääntöisesti yleislainsäädännön, eli julkisuuslain ja henkilötietolain, näkökulmasta.

Tutkielmassani esittelen tietojen saatavuuteen ja uudelleenkäyttöön kohdistuvia keskeisiä riskejä yksityisyyden ja henkilötietojen suojan kannalta. Tarkoitukseni on henkilötietojen suojaa koskevien periaatteiden ja säännösten kautta analysoida keinoja henkilötietojen suojaan kohdistuvien riskien minimoimiseen. Yhteisönoikeudella on tutkielmassani keskeinen asema ja sen tehtävänä on toimia ennen kaikkea soveltuvin osin tulkinnan apuna tutkielman keskeisten kysymysten hahmottamisessa.

Tutkielmassani en käsittele muita tietovarantojen avaamisen esteitä kuten maksuperustelainsäädäntöä tai tekijänoikeudellisia kysymyksiä. Keskeinen este julkisen tiedon

vapaalle hyödyntämiselle on valtion maksuperustelainsäädäntö, jonka nojalla tietojen luovutukset hinnoitellaan eri tavalla asiakkaan ja tiedon käyttötarkoituksen mukaan. Tietojen uudelleenkäyttöä koskevan periaatteen mukaisesti ensisijaisesti julkisen sektorin tietojen olisi oltava saatavilla maksutta.<sup>21</sup> Muutospaineita kohdistuu myös julkisen sektorin tekijänoikeuksia koskevaan säädäntöön ja käytäntöihin. Julkisen sektorin tietovarantojen tehokas hyödyntäminen edellyttää, että julkishallinnolla on käytössä uudelleenkäyttöä koskeva selkeä avoin lisenssi.<sup>22</sup>

## 1.2 Tutkimusmetodi ja keskeiset oikeuslähteet

Lainopilliselle tutkimukselle on tyypillistä oikeussäännösten systematisointi ja tulkinta. Lainopillisen tutkimuksen tarkoituksena on selvittää voimassaolevan oikeuden sisältöä. Systematisoinnin tarkoituksena ja tehtävänä on muun muassa ymmärtää oikeusjärjestelmää kokonaisuudessaan.<sup>23</sup> Lainoppi voidaan jakaa normikeskeiseen ja ongelmakeskeiseen lähestymistapaan, kysymyksen asettelusta riippuen. Ongelmakeskeisen lähestymistavan tehtävänä on muodostaa kokonaiskuva oikeudellisen ongelman sääntelystä ja normikeskeisen lähestymistavan tehtävä on muodostaa käsitys siitä, miten tiettyjä säännöksiä olisi tulkittava.<sup>24</sup> Tutkielmassani lähestyn julkisen sektorin tietojen uudelleenkäyttöä ja henkilötietojen suojaa sekä ongelma- että normikeskeisesti.

Euroopan unionin jäsenyydellä ja unionin tuottamalla säädännöllä on keskeinen vaikutus suomalaiseen laintulkintaan ja puhtaasti kansallisia normeja on yhä vähemmän. Normihierarkiassa kansalliset normit ovat alisteisia yhteisön normeille ja lainsäädännön ristiriitatilanteissa on yhteisöoikeus ensisijaisessa asemassa.<sup>25</sup> Tutkielmassani yhteisön normeilla on keskeinen asema erityisesti tulkinnan apuna.

Oikeudenalat jaetaan perinteisesti yksityisoikeuteen ja julkisoikeuteen.<sup>26</sup> Yksityisyyden- ja henkilötietojen suoja ovat keskeinen osa siviilioikeuden alaan kuuluvaa per-

---

<sup>21</sup> Julkishallinnon tietojen luovutusten periaatteet ja käytännöt 2/2012 s. 16.

<sup>22</sup> Salokannel 2012, s.34.

<sup>23</sup> Timonen 1998, s.12-13.

<sup>24</sup> Timonen 1998, s.13.

<sup>25</sup> Timonen 1998, s.24.

<sup>26</sup> Neuvonen 2013, s. 13.

soonallisuus oikeutta. Viranomaistoimintaa ohjaava julkisuuslainsäädännön katsotaan kuuluvan osaksi julkisoikeutta. Tietoyhteiskunnassa julkisuus ja yksityisyys ovat välttämättömässä vuorovaikutuksessa keskenään. Julkisuuslain salassapitosäännöksiin määritellään yksityisyyden rajat viranomaistoiminnassa erityisesti asiakirjojen saatavuutta koskevin säännöksiin.

Oikeustieteen alueella tutkimukseni sijoittuu oikeusinformatiikan ja tarkemmin informaatio-oikeuden alalle. Oikeusinformatiikka on uudehko, yhteiskunnan muutokseen reagoiva, tieteiden välinen ja kansainvälinen oikeustieteenala.<sup>27</sup> Oikeusinformatiikka poikkeaa perinteisestä oikeudenalajaottelusta. Oikeusinformatiikka voidaan nähdä teoreettisena ja metodologisena lähestymistapana oikeudellisen tiedon käyttöön, jonka tehtävänä on yksityisyyden suojan vahvistaminen.<sup>28</sup> Oikeusinformatiikan erityinen osa voidaan jakaa neljään osa-alueeseen: oikeudelliseen tietojenkäsittelyyn, oikeudelliseen informaatioon, informaatio-oikeuteen ja tietotekniikka-oikeuteen.<sup>29</sup>

Informaatio-oikeus on oikeudenala, joka tutkii verkkoyhteiskunnan muuttuvaa sääntelyä informaatioinfrastruktuurin, informaation ja informaatioprosessien valossa.<sup>30</sup> Informaatio-oikeuden on katsottu kuuluvan hallinto-oikeuden osa-alueelle.<sup>31</sup> Koska julkisten tietovarantojen avaaminen on koko yhteisön alueella vaikuttava pyrkimys, on tässä tutkielmassa piirteitä myös eurooppalaisesta hallinto-oikeudesta. Tämä näkyy tutkielmassani erityisesti perusoikeuksien keskeisenä roolina. Tutkielmani kannalta keskeisimmät henkilö- ja informaatio-oikeudelliset perusoikeudet ovat oikeus tietoon ja oikeus henkilötietojen suojaan (PeL 12 § ja 10 §). Henkilötietojen suoja ilmentää viime kädessä oikeutta yksityiselämän ja yksityisyyden suojaan henkilötietoja käsiteltäessä.

Konstari ja Wallin määrittelevät informaatio-oikeuden yleisesti oikeudenalaksi, joka tutkii yksilöiden ja yhteisöjen oikeuksia ja velvollisuuksia hankkia, käyttää, luovuttaa, julkaista ja muuten käsitellä informaatioita.<sup>32</sup> Neuvonen määrittelee informaatio-oikeuden oikeudenalaksi, joka tarkastelee informaatioon liittyviä ihmis- ja perusoikeuksia ja sen oikeudellista ja muunlaista sääntelyä systematisoimalla ja analysoimalla oikeudellista ainesta ja toimimalla välittäjänä oikeustieteen ja muiden yhteiskuntatie-

---

<sup>27</sup> Saarenpää 2012b, s. 415-424.

<sup>28</sup> Neuvonen 2013, s.15, Pöysti 1999, s.74.

<sup>29</sup> Korhonen 2013, s. 24.

<sup>30</sup> Saarenpää 2012b, s.507.

<sup>31</sup> Neuvonen 2013, s.14.

<sup>32</sup> Konstari, Wallin 2000, s. 32.

teiden kanssa viestintään liittyvissä keskusteluissa.<sup>33</sup> Pöystin mukaan informaation vapaa liikkuvuus on yksi eurooppalaisen informaatio-oikeuden systeemiperiaatteista. Euroopan yhteisön alueen tietoyhteiskunnanohjelmien ja informaatio-oikeudellinen sääntelyn tarkoituksena on edistää oikeusvaltion periaatteita ja perusoikeuksien suojaa kunnioittavien eurooppalaisten informaatiomarkkinoiden kehitystä.<sup>34</sup> Informaatio-oikeuden keskeisiä periaatteita ovat muun muassa julkisuusperiaate, tiedollinen itsemääräämisoikeus ja oikeus tietoturvaan sekä oikeus luottamukselliseen viestintään.<sup>35</sup>

Informaatio-oikeus oikeudenalana on keskeinen instrumentti tietoyhteiskunnan lain-säädännön tulkinnassa ja kehittämisessä. Informaatio-oikeuden keskeinen tehtävä on analysoida voimassa olevaa oikeutta ja yhteiskunnan informaatioon kohdistuvia tarpeita sekä varmistaa perusoikeuksien toteutuminen oikeudellista informaatiota käsiteltäessä. Informaatio-oikeuden puitteissa on luonnollista tarkastella eri tiedollisiin perusoikeuksiin liittyvien oikeuksien toteutumista. Tavoitteena on, että perusoikeudet toteutuvat mahdollisimman täysimääräisesti.

Tutkielmani oikeuslähteitä ovat aihepiiriin soveltuvat kansalliset lait ja asetukset, Euroopan unionin säädökset sekä Suomea sitovat kansainvälisoikeudelliset velvoitteet. Muita oikeuslähteitä ovat hallituksen esitykset, oikeuskäytäntö, viranomaisten ja eri työryhmien ohjeet sekä oikeuskirjallisuus. Tiedon uudelleenkäyttöön soveltuva kansallinen oikeudellinen säännöstö koostuu muun muassa Suomen perustuslaista (731/1999), laista viranomaisten toiminnan julkisuudesta (621/1999) (myöhemmin julkisuuslaki), henkilötietolaista (523/1999), valtion maksuperustelaista (150/1999) ja tekijänoikeuslaista (404/1961). Lisäksi tietosuojaa koskevia normeja on sisällytetty useisiin erityislakeihin. Julkisten tietovarantojen avaaminen linkittyy vahvasti myös viranomaisen hyvään tietohallintoon, jota koskeva laki, laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011), on annettu vuonna 2011.

Yhteisön tasolla keskeisiä julkisen sektorin tietojen uudelleenkäyttöön vaikuttavia normeja ovat henkilötietodirektiivi<sup>36</sup> ja PSI-direktiivi<sup>37</sup>. PSI-direktiiviä käsitellen henkilötietojen suojan näkökulmasta. PSI-direktiivillä ei ole vaikutusta tietosuojalain-

---

<sup>33</sup> Neuvonen 2013, s.16.

<sup>34</sup> Pöysti 1999, s.12-13.

<sup>35</sup> Neuvonen 2013, s.325-326.

<sup>36</sup> Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

<sup>37</sup> Euroopan parlamentin ja neuvoston direktiivi 2003/98/EY, annettu 17 päivänä marraskuuta 2003, julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä ja Euroopan parlamentin ja neuvoston direktiivi 2013/37/EU, annettu 26. kesäkuuta 2013, julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta.



säännösten soveltamiseen. PSI-direktiivin keskeiset säännökset liittyvät muun muassa tiedon maksuttomuuteen, uudelleenkäyttöperiaatteeseen, yhdenvertaisuuteen ja syrjimättömyyteen.

Tutkielman kannalta keskeinen ehdotus on Euroopan komission keväällä 2012 antama ehdotus yleiseksi tietosuoja-asetukseksi, jonka tarkoituksena on korvata yhteisön henkilötietodirektiivi. Muutosehdotuksen taustalla on teknologian nopean kehityksen tuomat haasteet henkilötietojen käsittelylle. Yleisen tietosuoja-asetuksen tarkoituksena on luoda vahva ja johdonmukainen tietosuojakehys, joka toimii alustana digitaalisen talouden kehittymiselle sisämarkkinoilla. Ehdotuksen lopullinen sisältö on vielä epävarma, mutta otan tutkielmassani huomioon, tutkielman kannalta relevantit, ehdotuksessa esitetyt keskeiset periaatteet.

Julkisen sektorin tietojen uudelleenkäytön ja henkilötietojen suojan välistä suhdetta on tarkasteltu lähemmin erityisesti henkilötietodirektiivin 29 artiklalla perustetun tietosuojatyöryhmän (myöhemmin tietosuojatyöryhmä), Euroopan tietosuojavaltuutetun ja temaattisen LAPSI 2.0 verkoston toimesta.<sup>38</sup> Lausunnoissa on esitetty julkisen sektorin tietojen saatavuuteen ja uudelleenkäyttöön liittyviä riskejä ja ratkaisuja henkilötietojen suojan näkökulmasta. Lausunnoissa on myös todettu, että henkilötietojen suoja ei saa olla esteenä toimivien julkisen sektorin tiedon uudelleenkäyttöä koskevien sisämarkkinoiden syntymiselle.<sup>39</sup>

Erityisesti henkilötietolain periaatteiden käsittelemiseen vaikuttaa työelämästä saamani kokemus. Olen ollut ensin kuusi kuukautta harjoittelijana ja tämän jälkeen kahdeksan kuukautta tarkastajana tietosuojavaltuutetun toimistossa.

---

<sup>38</sup> Henkilötietodirektiivin 29 artiklan nojalla perustetun tietosuoja työryhmän lausunnot: 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83) annettu 12. joulukuuta 2003 ja lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207) annettu 5. kesäkuuta 2013. LAPSI (The European Thematic Network on Legal Aspects of Public Sector Information, LAPSI Policy Recommendation N.4 Privacy and Personal Data Protection, LAPSI Working Group 2 Privacy Aspects of PSI sekä Euroopan tietosuojavaltuutetun avoimen datan pakettia koskeva lausunto 2012.

<sup>39</sup> Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s. 4.

## 2. Keskeiset käsitteet

### 2.1 Avoin data, julkinen tieto ja tietoyhteiskunta

*Avointa dataa* voidaan kuvata tahtotilaksi, lähestymistavaksi ja asenteeksi tietojen uudelleenkäyttöä kohtaan.<sup>40</sup> Avoimella datalla tarkoitetaan sellaista dataa, joka on vapaasti käytettävissä ilman teknisiä tai lainsäädännöllisiä rajoituksia. Datan avoimuuden mittarina voidaan käyttää aineiston teknistä saavutettavuutta, löydettävyyttä, kokonaisuutta, maksuttomuutta, lisensointiehtojen tasa-arvoisuutta, alkuperäisyyttä ja ajantasaisuutta, laillista ja vapaata uudelleenkäytettävyyttä, koneluettavuutta, formaatin avoimuutta ja ymmärrettävyyttä.<sup>41</sup>

PSI-direktiivissä julkisen tiedon avoimuuden reunaehdot liittyvät koko tietokannan saattamiseen avoimesti saataville, standardoidussa elektronisessa muodossa, kenelle tahansa, maksuttomasti, kaikkiin kaupallisiin ja ei-kaupallisiin tarkoituksiin. PSI-direktiivin mukaisella uudelleenkäyttöperiaatteella tarkoitetaan sitä, että kaikki julkisen sektorin tiedot, joihin ei nimenomaisesti kohdistu direktiivissä esitettyjä poikkeuksia, on saatettava uudelleenkäytettäväksi edellä mainitulla tavalla. Tässä tutkielmassa käytetään lähinnä käsitettä uudelleenkäyttö, jolla tarkoitetaan julkisen sektorin tietojen asettamista uudelleenkäytettäväksi edellä mainitulla tavalla. Lisäksi uudelleenkäytöllä voidaan tarkoittaa julkisen sektorin tietojen hyväksikäyttöä myös suppeammin kuin siten, että koko tietokanta asetettaisiin avoimesti saataville.

Data on käsite, joka arkikielessä yleensä sekoittuu muiden käsitteiden, kuten informaation ja tiedon, kanssa.<sup>42</sup> Data voidaan mieltää tiedon raaka-aineeksi, josta voidaan tuottaa informaatiota ja informaatiosta voidaan muodostaa tietoa.<sup>43</sup> Informaatiolla on arvostuksellinen merkitys ja taas tieto on jotain sellaista, mikä on perusteltavissa ja todennettavissa.<sup>44</sup>

---

<sup>40</sup> Hintikka, Kola, Poikola 2010, s. 16.

<sup>41</sup> Hintikka, Kola, Poikola 2010, s.34 ja Open definition avoimien tietovarantojen määritelmä, saatavilla osoitteessa <http://opendefinition.org/od/suomi/>.

<sup>42</sup> Hintikka, Kola, Poikola 2010, s.14.

<sup>43</sup> Julkisen hallinnon kokonaisarkkitehtuuri, julkisen hallinnon tietoarkkitehtuuri 2011, s.45.

<sup>44</sup> Hintikka, Kola, Poikola 2010, s.14.

*Viranomaisen asiakirja* on määritelty julkisuuslain 5 §:ssä, jonka mukaan ”viranomaisen asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteenkuuluvista merkinnöistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistotallenteiden taikka muiden apuvälineiden avulla”. Asiakirja on viranomaisen asiakirja, kun se on viranomaisen hallussa. Ei ole merkitystä, kuka asiakirjan on laatinut.

*Julkinen tieto* on viranomaisen hallussa olevaa tietoa, jonka luovuttamiseen ei kohdistu tiedon salassapitoa koskevia rajoituksia. OECD:n julkisen sektorin tiedon uudelleenkäyttöä koskevassa suosituksessa julkinen tieto määritellään ”informaatioksi, mukaan lukien tuotteita ja palveluita koskeva informaatio, jonka hallinto tai julkinen sektori on kehittänyt, luonut, käsitellyt, säilyttänyt, ylläpitänyt, levittänyt tai rahoittanut”.<sup>45</sup> Julkisuusperiaatteen mukaan viranomaisten asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä (JulKL 1.1 §). Julkisuuslain salassapitosäännökset on sijoitettu lain 24 §:ään. Vaikka julkisuuslaissa säädetään asiakirjoista, julkisuuslain lähtökohtana on, että viranomaisen hallussa oleva tieto on julkista. Sillä miten tieto on tallennettu, ei ole lähtökohtaisesti merkitystä.<sup>46</sup>

Avoimen tiedon ja julkisen tiedon käsitteelliset erot liittyvät tiedon saatavuuteen. Vielä se, että tieto on julkisuusperiaatteen nojalla julkinen, ei automaattisesti tarkoita sitä, että tieto voitaisiin saattaa avoimesti uudelleenkäytettäväksi.<sup>47</sup> Julkisen tiedon avoimuutta rajoittavat salassapitosäännösten lisäksi muun muassa tekijänoikeudet, tietojen maksullisuus ja henkilötietojen suoja. Käytän tässä tutkielmassa synonyymeina käsitteistä julkisen sektorin tieto ja julkisen sektorin data, jolla tarkoitetaan julkisuuslain mukaisesti julkisen sektorin hallussa olevia asiakirjoja ja tietoja.

Tutkielman kannalta keskeinen käsite on *tietoyhteiskunta* (*knowledge society*), jota ei ole yksiselitteisesti määritelty. Tietoyhteiskunta termiä ei yhteiskuntatieteellisenä käsitteenä ole pidetty riittävän informatiivisena kuvaamaan yhteiskunnan organisointumista, kehittymistä ja sosiaalisia rakenteita.<sup>48</sup> Tietoyhteiskunta on käsitteenä aika- ja paikkasidonnainen.<sup>49</sup> Niiniluodon mukaan tietoyhteiskunnalla voidaan tarkoittaa,

---

<sup>45</sup> OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information C(2008)36.

<sup>46</sup> Neuvonen 2013, s.148.

<sup>47</sup> Näin myös tietosuojavaltuutettu avointa dataa koskevassa ohjauksessa 2120/09/2013, saatavilla osoitteessa: <http://www.tietosuoja.fi/fi/index/ratkaisut/tietosuojavaltuutetunohjausavoimendatans.html>.

<sup>48</sup> Vuorensyrjä, Savolainen 2001, s.22.

<sup>49</sup> Vuorensyrjä, Savolainen 2001, s. 11.

näkökulmasta riippuen, esimerkiksi tietotekniikkayhteiskuntaa, inhimillisen tiedon ja inhimillisen pääoman yhteiskuntaa tai virtuaalisen kulttuurin yhteiskuntaa.<sup>50</sup> Tietoyhteiskunnassa tieto on tärkeä kilpailutekijä ja hyödyke yhteiskunnan kokonaistaloudessa. Tietoyhteiskunta käsitettä käytetään yleisesti hallinnossa kuvaamaan yhteiskunnan tieto- ja viestintäteknologian kehitykseen ja käyttöön liittyviä tavoitteita.<sup>51</sup>

Tietoyhteiskunnasta voidaan erottaa käsitteellisesti *informaatioyhteiskunta* (*information society*), jolla viitataan lisääntyneeseen teknologian käyttöön yhteiskunnassa ja teknologian vaikutukseen yhteiskunnan eri osa-alueille.<sup>52</sup> Van Dijk kuvaa informaatioyhteiskuntaa moderniksi yhteiskunnaksi, jossa on tyypillistä korkea tasoinen informaation liikkuvuus ja, jossa käytetään hyväksi informaatiota sekä informaatio teknologioita.<sup>53</sup>

*Verkkoyhteiskunnalla* (*network society*) tarkoitetaan yhteiskuntaa, jossa kansalaisen toimintaympäristö on pääasiassa digitaalinen ja riippuvainen tietoverkkojen hyödyntämisestä. Suurin osa niin sanotuista kehittyneiden maiden organisaatioista ovat täysin riippuvaisia verkkoinfrastruktuurin toiminnasta.<sup>54</sup> Verkkoyhteiskuntäkäsitettä käytettäessä painopiste on organisaation kehityksessä ja yhteiskunnan infrastruktuurissa.<sup>55</sup> Verkkoyhteiskunnassa viranomaiset nähdään aktiivisena informaation tuottajina.

Oikeudellisen verkkoyhteiskunnan tunnusmerkkejä ovat muun muassa infrastruktuurien muutokset, perusoikeuksien siirtyminen verkkovaikutteisiksi ja verkoissa hyödynnettäviksi, informaation ja sen käsittelyn oikeudellisesti muuttunut asema yhteiskunnassa, sähköinen asiointi ja hallinta, sähköinen kaupankäynti, tietorikokset ja tietoturvallisuuden uusi merkitys oikeuksien toteutumisessa.<sup>56</sup>

---

<sup>50</sup> Niiniluoto 1989, s.66-99.

<sup>51</sup> Tietoyhteiskuntastrategiat, Arjen tietoyhteiskunnan neuvottelukunta tms.

<sup>52</sup> Vuorensyrjä, Savolainen 2001, s. 82, Saarenpää 2012b, s. 433, Korhonen 2013, s. 28.

<sup>53</sup> Van Dijk 2012, s. 23.

<sup>54</sup> Van Dijk 2012, s.2.

<sup>55</sup> Van Dijk 2012, s.23.

<sup>56</sup> Saarenpää 2012b, s. 435-439.

## 2.2 Henkilötieto ja anonyymi tieto

Onnistunut yksityisyyden ja muiden perusoikeuksien suojaaminen henkilötietoja käsiteltäessä vaatii ymmärrystä *henkilötiedon* käsitteen sisällöstä. Henkilötietojen suoja koskevia säännöksiä sovelletaan lähtökohtaisesti ainoastaan tunnistettavissa olevan henkilön tietojenkäsittelyyn. Jos henkilö voidaan suoraan tunnistaa, esimerkiksi nimen tai muun suoran tunnisteen perusteella, voidaan henkilötiedon käsitteen määrittämistä pitää jokseenkin yksinkertaisena. Jos henkilö on välillisesti tunnistettavissa, henkilötiedon käsitteen määrittelemisen on haastavampaa. Henkilö on välillisesti tunnistettavissa esimerkiksi silloin, kun tietty tieto ei sinänsä ole riittävää henkilön tunnistamiseksi, mutta tietoja yhdistelemällä henkilö voidaan tunnistaa.

Henkilötietolain 3 §:n 1 momentin 1 kohdan mukaan henkilötiedolla tarkoitetaan ”kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi”. Henkilötietoja ovat kaikki tiedot, joista voidaan suoraan tunnistaa luonnollinen henkilö tai tiedot, joista luonnollinen henkilö on välillisesti tunnistettavissa. Henkilötiedon käsitteen määrittelyssä painotetaan tietyn henkilön tunnistettavuutta kyseisestä tiedosta.<sup>57</sup> Henkilötietoja ovat jollekin alustalle talletetut tiedot. Sille ei anneta merkitystä, millä tavalla tai mille alustalle tiedot on talletettu. Suullinen tieto ei ole henkilötieto, ellei se perustu henkilörekisterissä olevaan tietoon. Henkilötietolain 33 §:n vaitiolosäännös koskee myös suullista tietoa.<sup>58</sup> Julkisuuslain 23 §:n vaitiolovelvollisuutta ja hyväksikäyttökieltoa koskeva säännös koskee salassa pidettävää tietoa.

Henkilötietolain sananmuodossa on päädytty korostamaan perhe-elämänsuojaa ulottamalla henkilötiedon käsite elinolosuhteita, perhettä ja yhteisessä taloudessa koskeviksi. Henkilötietodirektiivin mukaista henkilötiedon käsitettä on tulkittava samalla tavalla. Tämä on myös pääteltävissä henkilötietolain ja henkilötietodirektiivin tarkoituksesta suojella yksityiselämää henkilötietoja käsiteltäessä. Yksityiselämän suojan ydin alueeseen kuuluu perhe-elämän kunnioittaminen.<sup>59</sup>

Henkilötiedon käsite on saman sisältöinen niin henkilötietolaissa kuin henkilötietodirektiivissäkin. Henkilötietodirektiivin 2 artiklan 2 alakohdan mukaan henkilötiedolla

---

<sup>57</sup> Bygrave 2003, s. 316.

<sup>58</sup> HE 96/1998 vp., s. 43.

<sup>59</sup> Euroopan unionin perusoikeuskirjan 7 artikla.

tarkoitetaan ”kaikenlaisia tunnistettua ja tunnistettavissa olevaa luonnollista henkilöä (”rekisteröity”) koskevia tietoja; tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti henkilönumeron taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”. Henkilötiedon käsitteen määritelmän tarkoitus on olla mahdollisimman laaja ja yleisluonteinen, jotta se kattaa kaikki tunnistettavissa olevaa henkilöä koskevat tiedot.<sup>60</sup>

Henkilötiedon käsitteen analysoinnissa on lähdettävä liikkeelle henkilötietojen suojaa koskevien säännösten tarkoituksesta. Henkilötietolain tarkoituksena on ”toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä, sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista” (HetiL 1 §). Henkilötietodirektiivin tarkoituksena on niin ikään taata luonnollisten henkilöiden perusoikeuksien ja vapauksien kunnioittaminen, kun henkilötietoja käsitellään sisämarkkinoilla (artikla 1). Henkilötietodirektiivi on markkinadirektiivi, jonka perimmäisenä tarkoituksena on taata henkilötietojen vapaa liikkuvuus yhteisön alueella. Henkilötietojen suojaa koskevilla säännöksillä halutaan viimekädessä turvata rekisteröidyn oikeutta yksityisyyteen.

Henkilötietoa on tieto, joka koskee tiettyä henkilöä koskevaa tosiasiaa (objektiivinen tieto) tai tiettyä henkilöä koskevaa mielipidettä (subjektiivinen tieto). Tiedon ei tarvitse olla todennettu tai virheetön, jotta se olisi henkilötieto. Henkilötieto voi olla periaatteessa sisällöltään mitä vain ja käsite kattaa kaiken tiedon, jolla ilmaistaan jotain tunnistettavissa olevasta henkilöstä. Myös sähköisessä asiakirjassa olevat vapaaseen tekstiin sisällytetyt tiedot ovat olla henkilötietoja edellyttäen, että tiedot täyttävät henkilötiedon määritelmän ehdot.<sup>61</sup> Henkilötietojen suojaan liittyvän lainsäädännön soveltamisen edellytyksenä ei ole se, että henkilötiedot muodostaisivat teknisen henkilörekisterin. Olennaista on henkilötietojen käsittely tavalla, johon sovelletaan henkilötietolain säännöksiä. Henkilötietolakia sovelletaan henkilötietojen automaattiseen käsittelyyn sekä manuaaliseen henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa (HetiL 2.2 §).

---

<sup>60</sup> Näin mm. komissio ehdotuksessaan KOM (92) 422 lopullinen, 28.10.1992 s. 10 (2 artiklan perustelut).

<sup>61</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s. 8.

Henkilötietoa on tieto, joka koskee tiettyä henkilöä eli kertoo henkilöstä jotain. Henkilötietoja voivat olla myös esineitä koskevat tiedot, kuten kiinteistön arvoa koskevat tiedot tai auton huoltotiedot. Tietojen ei tarvitse koskea vain yhtä henkilöä, jotta ne katsottaisiin henkilötiedoiksi. Luciano Floridin mukaan tietovarantoja avatessa yksityisyyden suojaan liittyvät riskit kohdistuvat yleensä ryhmään, eikä niinkään tietosuojasäännösten mukaisesti tunnistettavissa oleviin luonnollisiin henkilöihin. Perinteisesti avointa dataa ja tietosuojaa koskeva keskustelu keskittyy luonnollisen henkilön yksityisyyden ja yhteiskunnan intressien väliseen punnintaan. Floridi katsoo, että anonyymien datan avaamiseen liittyvät riskit kulmineituvat erityisesti siihen, että yksilöt voidaan edelleen tunnistaa tiedoista ryhminä.<sup>62</sup> Jos tiedot koskevat useampaa henkilöä, on tämä otettava huomioon esimerkiksi tarkastusoikeutta toteutettaessa.

Henkilötiedosta voidaan erottaa sisältö-, tulos- ja tarkoitustekijä. Henkilötieto on tieto, joka kertoo sisältönsä perusteella jotain tietystä henkilöstä. Henkilötietoa on tieto, jonka käsittely todennäköisesti vaikuttaa tiettyyn henkilöön. Henkilötietoa on tieto, jonka käsittelyn tarkoituksena on arvioida tiettyä henkilöä. Nämä kolme tekijää eivät ole kumulatiivisia.<sup>63</sup> Huomioitava on myös, että tietojen ei tarvitse olla tosia, myös virheelliset tiedot voivat olla henkilötietoja muiden edellytysten täytyessä.

Henkilötieto on tieto, josta henkilö on suoraan (tunnistetaan) tai välillisesti (on mahdollista tunnistaa) tunnistettavissa. Jos henkilö on suoraan tunnistettavissa, tunnisteetaan hänet usein yksittäisten tietojen eli tunnisteiden perusteella. Nimiä käytetään tavallisesti henkilön tunnistamiseen, mutta henkilö voi olla tunnistettavissa myös muiden tunnisteiden kautta. Euroopan yhteisöjen tuomioistuimien on asiassa C-101/2001 todennut seuraavaa: ”Sitä, että internet-kotisivuilla viitataan henkilöihin ja yksilöidään heidät, joko nimeltä tai muulla tavoin, kuten ilmoittamalla heidän puhelinnumerosa tai antamalla tietoja heidän työsuhteestaan ja harrastuksista on pidettävä – direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna – henkilötietojen käsittelynä”. Tunnisteita voivat olla esimerkiksi henkilötunnus, valokuva, ääni, sormenjälki tai auton rekisteritunnus.<sup>64</sup>

Välillisellä tai epäsuoralla tunnistamisella tarkoitetaan sitä, että käytettävissä olevat tunnisteet eivät ole riittävät henkilön tunnistamiseen siinä tilanteessa. Jos käytettävissä olevat tunnisteet yhdistetään muihin tunnisteisiin tai tietoihin, on henkilön tunnis-

---

<sup>62</sup> Luciano Floridi, Open Data, Data Protection, and Group Privacy. Julkaistu verkossa 18.2.2014.

<sup>63</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s. 9-12.

<sup>64</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s. 12–13.

taminen mahdollista.<sup>65</sup> ”Muiden tarvittavien tietojen” ei tarvitse olla rekisterinpitäjän hallussa. Määrittävä seikka tunnistamassa on se, että tunnistaminen on mahdollista.<sup>66</sup> Tunnistamistekniikoiden kehitys ja tietojen saatavuuden parantuminen lisää välillisen tunnistamisen riskiä.<sup>67</sup>

Tietosuojalautakunta on päätöksessään Dnro 2/932/2009 tulkinnut tunnistamista niin, että sen määrittelemiseksi, onko henkilö tunnistettavissa on otettava huomioon kaikki kohtuullisesti toteutettavissa olevat keinot. Tietosuojalautakunta katsoi kyseisessä päätöksessä, että auton rekisteritunnus on henkilötieto. Liikenteen turvallisuusvirasto Trafín (myöhemmin Trafi) ylläpitämästä ajoneuvoliikennerekisteriä koskevasta tietopalvelusta on mahdollista saada auton rekisteritunnuksen avulla helposti lisätietoja auton omistajasta. Näin ollen henkilön tunnistaminen auton rekisteritunnuksen perusteella on tietosuojalautakunnan mukaan kohtuullisesti mahdollista.

Henkilötietojen suojaa koskevilla säännöksillä suojataan luonnollista henkilöä. Luonnollisen henkilön käsitteeseen viitataan esimerkiksi ihmisoikeuksien yleismaailmallisen julistuksen 6 artiklassa, jonka mukaan ”jokaisella ihmisellä on kaikilla oikeus siihen, että hänet henkilönä tunnustetaan lain edessä”. Henkilötietolaissa henkilötiedolla tarkoitetaan kaikkia luonnollista henkilöä koskevia tietoja.<sup>68</sup>

Korkeimman hallinto-oikeuden ratkaisussa 2012:88, tuomioistuin katsoi, että tietoa julkiseen EU-seminaariin osallistumisesta ei voitu pitää ”osallistujien yksityisyyden piiriin kuuluvana seikkana eikä osallistuja listaa henkilötietolain 3 §:n mukaisena henkilörekisterinä, eikä sen sisältämiä henkilötietoja henkilötietolain 3 §:ssä tarkoitettuina henkilötietoina”. Mielestäni korkeimman hallinto-oikeuden tulkinta on jokseenkin virheellinen. Kyseissä tapauksessa henkilötietojen luovuttamista voitiin sinänsä pitää hyväksyttävänä, mutta sillä missä asemassa luonnollinen henkilö kulloinkin toimii, ei ole merkitystä henkilötiedon käsitteen kannalta.<sup>69</sup>

Henkilötietolakia säädettäessä on lähdetty siitä, että kaikki luonnolliseen henkilöön liittyvät tiedot ovat henkilötietoja. Oikeushenkilöitä koskevia tietoja voidaan pitää luonnollista henkilöä koskevina esimerkiksi tilanteissa, joissa oikeushenkilön nimi on johdettu luonnollisen henkilön nimestä tai pientä yritystä koskevat tiedot, jotka saat-

---

<sup>65</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s.13–14.

<sup>66</sup> Bygrave 2003, s. 318.

<sup>67</sup> Bygrave 2003, s.317.

<sup>68</sup> HE 96/1998 vp., 34-35.

<sup>69</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s. 7.



tavat pikemminkin kuvata sen omistajaa luonnollisena henkilönä kuin oikeushenkilöä. Oikeushenkilöä tai yritystä koskevat tiedot ovat henkilötietoja, jos niiden voidaan ”sisällön”, ”tarkoituksen” tai ”tuloksen” perusteella katsoa ”koskevan” luonnollista henkilöä.<sup>70</sup>

Henkilötiedot ovat luonnollisia henkilöitä koskevia tietoja, joten henkilötietolain säännöksiä ei periaatteessa sovelleta syntymättömiin lapsiin tai kuolleisiin henkilöihin. Kuolleet henkilöt eivät ole yksityisoikeudellisia luonnollisia henkilöitä, mutta kuolleitten henkilöiden tiedot voivat saada välillisesti suojaa elossa olevien henkilöiden kautta. Lisäksi esimerkiksi potilastiedot ovat salassa pidettäviä vielä potilaan kuoleman jälkeenkin. Kuitenkin kuolleen henkilön elinaikanaan saamaan hoitoon liittyviä potilastietoja voidaan luovuttaa perustellun hakemuksen perusteella sille, joka tarvitsee tietoja tärkeiden etujensa tai oikeuksien selvittämistä tai toteuttamista varten. Syntymättömät lapset henkilötiedot voivat saada suojaa välillisesti äidin tietojen kautta.<sup>71</sup>

*Anonyymillä datalla* tarkoitetaan tietoa, josta luonnollinen henkilö on aiemmin ollut tunnistettavissa, mutta tunnistaminen ei olemassa olevien resurssien perusteella ole enää kohtuudella mahdollista. Arviointi tietojen mahdollisesta tunnistettavuudesta on tehtävä yksittäistapauksessa ja siihen vaikuttavat suoraan tietojenkäsittelyn asiayhteys ja olosuhteet.<sup>72</sup> Tietotekniikan kehittyessä on lähes mahdotonta antaa yksiselitteistä vastausta sille, milloin tiedot ovat aidosti anonyymejä. Henkilötietodirektiivin johdanto-osan 26 kappaleessa todetaan: ”[.tietosuojaa koskevia periaatteita ei sovelleta tietoihin, jotka on tehty anonyymeiksi siten, ettei rekisteröity enää ole tunnistettavissa...].”. Käsittelen anonyymien tietojen käsittelyä tarkemmin tutkielmani luvussa 5.2.

## 2.3 Henkilörekisteri ja rekisterinpitäjä

*Julkisen sektorin henkilörekisterit* muodostuvat tyypillisesti viranomaisen palvelutoiminnassa käytetyistä asiakasrekistereistä ja hakemusasioiden yhteydessä sähköises-

---

<sup>70</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s. 23.

<sup>71</sup> HE 96/1998 vp., s.35.

<sup>72</sup> Tietosuojatyöryhmän lausunto 5/2014 anonymisointitekniikoista (0829/14/FI WP 216), s. 8.

ti ylläpidettävistä asiakirjarekistereistä ja asianhallintajärjestelmistä.<sup>73</sup> Perusrekistereillä tarkoitetaan yhteiskunnan keskeisiä tietovarantoja, joihin sisältyy yhteiskunnan toiminnan kannalta keskeisiä tietoja.<sup>74</sup> Julkisten rekisterien tietoihin liittyy julkinen oletama tietojen luotettavuudesta, jolla tarkoitetaan sitä, että tietojen vastaanottajalla on oikeus olettaa tietojen olevan ajantasaisia ja virheettömiä.<sup>75</sup> Keskeisiä kansallisia perusrekistereitä ovat väestötietojärjestelmä (VTJ), kiinteistötietojärjestelmä (KTJ), kaupparekisteri, yhdistysrekisteri, säätiörekisteri ja yritys- ja yhteisötietojärjestelmä (YTJ).

Henkilörekisterillä tarkoitetaan ”käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta” (HetiL 3.1 §:n 3 kohta).

Henkilörekisterin käsite on juridinen ja looginen, joten automaattisen tietojenkäsittelyn avulla käsiteltävien henkilötietojen osalta henkilörekisteri muodostuu samaan käyttötarkoitukseen käsiteltävistä henkilötiedoista niiden tallennustavasta ja sijainnista riippumatta.<sup>76</sup> Henkilörekisterin käsitteen kannalta ei ole merkitystä sillä, onko henkilötiedot talletettu samaan tietotekniseen rekisteriin. Ratkaisevaa on henkilötietojen käsittely tiettyyn määriteltyyn tarkoitukseen, joko automaattisesti tai manuaalisesti niin, että tiettyä henkilöä koskevat tiedot ovat helposti ja kohtuuttomitta kustannuksitta löydettävissä. Yksi henkilörekisteri voi muodostua useista tietoteknisistä tai manuaalisista rekistereistä, mutta toisaalta yksi tietotekninen rekisteri saattaa sisältää useita henkilörekistereitä.<sup>77</sup> Rekisterinpitäjä voi käsitellä henkilötietoja useaan eri tarkoitukseen, jos tämä on asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Se onko kyse yhdestä vai useammasta rekisteristä riippuu siten henkilötietojen käsittelyntarkoituksesta.

Viranomaistoiminnassa käsitellään suuret määrät ”jollekin alustalle tallennettua tietoa”, joka on olennainen tekijä henkilötiedon ja viranomaisen asiakirjan käsitteen

---

<sup>73</sup> Tietosuojavaltuutetun toimiston ohje: Henkilötietojen luovuttaminen viranomaisten henkilörekistereistä, päivitetty 27.7.2010 s. 6-7.

<sup>74</sup> Korhonen 2003, s.224.

<sup>75</sup> Korhonen 2003, s.326.

<sup>76</sup> HE 96/1998 vp., s.4.

<sup>77</sup> Konstari 1992, s.71–73.

tunnusmerkistön kannalta (JulkL 5§ ja HetiL 3.1 §:n 1 kohta). Jos viranomaisen hallussa olevaa, jollekin alustalle tallennettua henkilötietoa, käsitellään automaattisen tietojen käsittelyn avulla, muodostuu automaattisen tietojenkäsittelyn avulla samaan tarkoitukseen käsitellyistä tiedoista pääsääntöisesti henkilörekisteri. Jos automaattisella tekstinkäsittely ohjelmalla laaditaan asiakirja, ei se sellaisenaan muodosta henkilörekisteriä. Edellytyksenä henkilörekisterin määritelmän täyttymiselle on se, että asiakirja säilytetään sähköisessä muodossa osana tietojenkäsittelyjärjestelmää.<sup>78</sup>

Loogisen henkilörekisterin käsitteen mukaisesti viranomaisen henkilörekisteriin kuuluvat myös ulkopuolisilta palveluntuottajilta rekisterinpitäjän lukuun hankituissa palveluissa käsiteltävät henkilötiedot.<sup>79</sup> Ulkopuoliseen palveluntuottajan (toimeksiantonsaajaan) toiminnassa syntyvien asiakirjojen käsittelyyn sovelletaan myös julkisuuslain säännöksiä (JulkL 5.2 §). Toimeksiannosta tapahtuvassa tietojenkäsittelyssä on viranomaistoiminnassa otettava huomioon myös toimeksiantosuhteen vaikutus tietojen julkisuudelle ja salassapidolle.<sup>80</sup>

*Rekisterinpitäjällä* tarkoitetaan ”yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty” (HetiL 3.1 §:n 4 kohta). *Viranomaisen* määritelmä on julkisuuslain 4 §:n mukaisesti laaja ja sillä tarkoitetaan lähtökohtaisesti kaikkia julkista valtaa käyttäviä tahoja.

Viranomaisen edellytys käsitellä henkilötietoja perustuu yleensä henkilötietolain 8 §:n 1 momentin 4 kohtaan, jonka mukaan henkilötietojen käsittely on sallittua, jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai veloitteesta tai henkilötietolain 16 §:ään, jossa säädetään henkilötietojen käsittelystä ilman 8 §:n mukaista perustetta, jos tietojen käsittely koskee viranomaisen suunnittelu- tai selvitystehtäviä. Jos viranomainen luovuttaa henkilötietoja, tulee tietojen luovutuksensaajasta rekisterinpitäjä, jos laissa säädetty edellytykset täyttyvät. Tässä yhteydessä on huomioitava henkilötietolain yksityistä käyttöä koskeva poikkeussäännös (HetiL 2.2 §).

Rekisterinpitäjän käsite on toiminnallinen käsite, jonka avulla vastuu henkilötietojen käsittelystä osoitetaan sinne, missä henkilötietojen käsittelyn todellinen vaikutus on.

---

<sup>78</sup> HE 96/1998 vp., s. 26.

<sup>79</sup> Tietosuojavaltutetun toimiston ohje: Henkilötietojen luovuttaminen viranomaisten henkilörekisteristä, päivitetty 27.7.2010, s. 6.

<sup>80</sup> Ibid.

Rekisterinpitäjän tunnistamisella halutaan varmistaa henkilötietojen käsittelyn ennakoitavuutta ja rekisteröidyn oikeuksien tehokasta toteutumista. Rekisterinpitäjän tunnistaminen on merkityksellistä myös rekisteröidyn oikeusturvan, lainvalinnan ja viiranomaisten toimivallan kannalta.<sup>81</sup>

Rekisterinpitäjän käsitteellä on siis ensisijaisesti tarkoitus jakaa vastuu henkilötietojen käsittelystä oikealle taholle. Jotta tietosuojasäännösten tavoitteet toteutuvat sekä, että mahdollisessa lainvastaisessa toiminnassa vastuu voidaan osoittaa oikealle taholle, on tärkeä varmistaa, että vastuu henkilötietojen käsittelystä on selkeästi määritelty.<sup>82</sup> On huomioitava, että rekisterinpitäjän käsite määritellään henkilötietojen suojaa koskevan lainsäädännön nojalla. Vaikutusta ei ole esimerkiksi sillä, mikä taho on mahdollinen immateriaalioikeuksien (esimerkiksi sui generis -suojan) haltija.<sup>83</sup>

---

<sup>81</sup> Tietosuojatyöryhmän lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteestä (00264/10/FI WP 169), s.9.

<sup>82</sup> Tietosuojatyöryhmän lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteestä (00264/10/FI WP 169), s.4.

<sup>83</sup> Tietosuojatyöryhmän lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteestä (00264/10/FI WP 169), s.9.

### 3. Julkisen sektorin tietojen uudelleenkäyttöä koskeva normisto

#### 3.1 Julkisen sektorin tietojen uudelleenkäyttöä koskeva direktiivi

Komission laatiman Euroopan unioni 2020 -kasvustrategian keskeinen päämäärä on Euroopan yhteisön alueen talouskasvun kiihdyttäminen ja vakauttaminen. Tavoitteen saavuttamiseksi julkisen sektorin tietovarannot tulisi avata uudelleenkäytettäväksi läpinäkyvin, toimivin ja syrjimättömin ehdoin.<sup>84</sup> Komission arvion mukaan julkisen sektorin tietovarantojen avaamisella voidaan saavuttaa noin 40 miljardin euron taloudellinen hyöty, lisätä yhteiskunnallista aktiivisuutta sekä tukea yhteisön eri politiikan osa-alueita.<sup>85</sup>

Euroopan digitaalistrategian tavoitteena on vahvistaa toimintalinjat, joiden tarkoituksena on yhtenäistää ja tukea tiedon saatavuutta koskevia periaatteita. Julkisen sektorin tiedon uudelleenkäytön yhteisön alueen kattavan oikeudellisen kehyksen mukauttamiseksi ja vahvistamiseksi, strategiaan sisältyy ehdotus tarkistetuksi direktiiviksi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä 2003/98/EY (PSI-direktiivi) sekä ehdotus tarkistetuksi komission päätökseksi komission asiakirjojen uudelleenkäytöstä. Komission strategiassa esitetään myös julkisen sektorin tietojen uudelleenkäyttöön liittyviä tavoitteita, joita ovat muun muassa jäsenvaltioiden välisen koordinoinnin ja kokemusten vaihdon helpottaminen sekä yleiseurooppalaisten dataportaalien käyttöönotto.

Yhteisön tasolla julkisen sektorin hallussa olevien tietovarantojen avaamisen taustalla on edellä mainittu 17.11.2003 annettu Euroopan parlamentin ja neuvoston direktiivi 2003/98/EY julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (PSI-direktiivi). Euroopan unionin perustamissopimuksissa ei anneta unionille sinänsä oikeutta puuttua jäsenvaltioiden kansalliseen viranomaisen hallussa olevien tietojensaantia koskevaan lainsäädäntöön.<sup>86</sup>

---

<sup>84</sup> KOM (2011/833/EU).

<sup>85</sup> KOM (2011) 822 lopullinen 12.12.2011, s.2-3.

<sup>86</sup> van Eechound, Janssen 2012, s. 7.

Direktiivi on yhteisöoikeudellinen instrumentti, joka sisältönsä mukaisesti asettaa jäsenvaltioille tavoitteen, mutta jolla ei itsessään ole lainsäädäntöä muuttavaa vaikutusta. Direktiivin tarkoituksena on lähentää ja yhdenmukaistaa yhteisön alueen lainsäädäntöä. Euroopan unionin perustamissopimuksen 189 artiklan mukaan direktiivi sitoo jäsenvaltioita siinä asetettuun tarkoitukseen ja päämäärään, mutta jäsenvaltion päätettävissä on, mitä keinoja päämäärän saavuttamiseksi käytetään.

PSI-direktiivi perustuu Euroopan unionin toiminnasta tehtyyn sopimukseen ja erityisesti sen 114 artiklaan, jonka perusteella jäsenvaltioiden lainsäädäntöä voidaan yhdenmukaistaa, jos se on tarpeellista toimivien sisämarkkinoiden kannalta. PSI-direktiivin perusperiaate on, että kaikki julkisen sektorin tiedot, joihin ei nimenomaisesti sovelleta direktiivin poikkeussäännöksiä, ovat uudelleenkäytettävissä kaupallisiin ja ei-kaupallisiin tarkoituksiin mahdollisimman kustannustehokkaasti. PSI-direktiivin tarkoituksena on helpottaa julkisen sektorin tietojen uudelleenkäyttöä harmonisoimalla uudelleenkäyttöön vaikuttavia olosuhteita sekä poistaa uudelleenkäyttöön liittyviä esteitä Euroopan unionin sisällä. Vuonna 2003 annettuun direktiiviin 2003/98/EY ei sisältynyt velvoitetta sallia asiakirjojen uudelleenkäyttöä, vaan tämä oli jäsenvaltioiden omassa harkinnassa.

PSI-direktiivin 2003/98/EY 13 artiklan mukaan direktiiviä oli tarkasteltava uudelleen ennen 1.7.2008. Komission tekemän tarkastelun tuloksena julkaistiin komission tiedoksi KOM (2009) 212.<sup>87</sup> Suurimmiksi esteiksi julkisen sektorin tietojen laajemmalle hyödyntämiselle tiedoksiannossa todetaan muun muassa datan avaamisesta perittävät maksut, julkisen sektorin kyvyttömyys nähdä tietojen uudelleenkäyttöön liittyviä taloudellisia mahdollisuuksia, julkisen ja yksityisen sektorin välinen kilpailu sekä uudelleenkäyttöä rajoittavat käytännön asiat.<sup>88</sup> Tiedoksiannossa todetaan, että komissio tekee direktiiviä koskevan toisen tarkastelun viimeistään vuonna 2012, jolloin on saatavilla enemmän näyttöä PSI-direktiivin soveltamisesta ja tuloksista.<sup>89</sup>

Tarkastelun tuloksena 12.12.2011 julkaistiin ehdotus Euroopan parlamentin ja neuvoston direktiivi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta KOM(2011)877. Muutosehdotuksen tarkoituksena on vahvistaa PSI-direktiiviä ja sen toimeenpanoa Euroopan unionin jäsenvaltioissa. Muutosehdotuksen mukaan PSI-direktiivin keskeinen haaste on luoda sellainen

---

<sup>87</sup> Saatavilla osoitteessa <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0212:FIN:FI:PDF>.

<sup>88</sup> KOM (2009) 212, s. 6.

<sup>89</sup> KOM (2009) 212, s. 7.

oikeudellinen kehys, joka vastaa mahdollisimman hyvin markkinoiden tarpeeseen ja, jolla lisätään julkisen sektorin hallussa olevien tietojen uudelleenkäyttöä sekä kaupallisessa että muussa tarkoituksessa.<sup>90</sup>

Euroopan unioni hyväksyi 26. kesäkuuta 2013, muuttamalla direktiiviä 2003/98/EY, Euroopan parlamentin ja neuvoston direktiivin 2013/37/EU julkisen sektorin datan uudelleenkäytöstä. Muutoksen johdosta jäsenvaltioilla on nyt velvollisuus sallia kaikkien julkisten asiakirjojen uudelleenkäyttö, jollei niiden saatavuutta ole rajoitettu tai estetty asiakirjojen saatavuutta koskevilla kansallisilla säädöksillä tai, jollei direktiivissä säädetä muista poikkeuksista. Vastaavasti PSI-direktiivin johdosta jokaisella on oikeus vaatia sitä, että julkinen sektori asettaa tiedot uudelleenkäytettäväksi.<sup>91</sup>

PSI-direktiivin täytäntöönpanossa ja soveltamisessa on täysimääräisesti noudatettava henkilötietojen suojaa koskevia periaatteita henkilötietodirektiivin mukaisesti (2013/37/EU johdanto-osan 11 kohta). Henkilötietodirektiivin mukaisesti jäsenvaltioiden on muun muassa määriteltävä olosuhteet, joissa henkilötietojen käsittely on laillista. PSI-direktiivillä ”[.]ei kajota eikä millään tavalla vaikuteta yhteisön ja kansallisen lainsäädännön säännösten mukaiseen yksilöiden suojan tasoon henkilötietojen käsittelyssä, eikä sillä muuteta henkilötietodirektiivissä säädettyjä velvollisuuksia ja oikeuksia” (artikla 1 kohta 4). Henkilötiedoilla tarkoitetaan henkilötietodirektiivin määritelmän mukaisia tietoja (artikla 2 kohta 5).

PSI-direktiivillä ei muuteta jäsenvaltioiden asiakirjojen saatavuutta koskevia järjestelmiä. Näin ollen tässä tutkielmassa tarkasteltava kansallinen julkisen sektorin tietojen uudelleenkäyttöä ja tietojen saatavuutta koskeva normisto muodostuu julkisuuslaista ja henkilötietolaista sekä mahdollisesti sovellettavasta erityislainsäädännöstä.

Vuonna 2013 PSI-direktiivin soveltamisalaa laajennettiin kirjastoihin, arkistoihin ja museoihin. Kulttuuriperintökokoelmien avaamisella tavoitellaan erityisesti uusien palveluiden ja tuotteiden kehittämistä matkailun ja oppimisen alalle (artiklat 1, 3 ja 11). Rahallinen korvaus julkisen sektorin tietoaineistosta rajoitetaan muutosdirektiivin myötä pääsääntöisesti kopioinnista ja jakelusta aiheutuviin irtiottokustannuksiin. Korvaus voi olla suurempi, jos viranomaisen toiminnan toimintakustannukset kateetaan tietojen luovutuksiin liittyvällä tuotolla (artikla 6). Riippumattomien viranomaisten on jäsenvaltioissa valvottava julkisen tiedon saantia ja hyödyntämistä koskevia

---

<sup>90</sup> KOM(2011)877, s. 3.

<sup>91</sup> Salokannel 2012, s.10.

muutoksenhakukeinoja (artikla 4). Jäsenvaltioita veloitetaan varmistumaan siitä, että käytettävissä on monikielisiä hakutyökaluja. Näitä työkaluja voivat olla esimerkiksi internetin kautta ja koneellisesti luettavassa saatavilla olevat luettelot ja portaalisivusto (artikla 9). Jäsenvaltioiden on raportoitava komissiolle julkisen sektorin tiedon uudelleenkäytön tilanteesta sekä riippumattoman viranomaisen toiminnasta vuosittain (artikla 12).

Kuten edellä on todettu, PSI-direktiivin uudelleenkäyttöperiaate ei ole automaattinen, eikä sillä ole vaikutusta henkilötietojen suojaan koskevien säännösten soveltamiseen tai pätevyyteen. Näin ollen uudelleenkäyttöperiaate ei luo uutta laillista henkilötietojen käsittelyn perustetta, eikä viranomainen voi vedota tarpeeseen noudattaa PSI-direktiiviä, jos se saattaa henkilötietoja sisältäviä tietoaineistoja uudelleenkäytettäväksi.<sup>92</sup>

Henkilötiedot eivät ole PSI-direktiivin kohteena, mutta henkilötietoja voidaan pyytää uudelleenkäytettäväksi. Kun henkilötietoja luovutetaan viranomaisten toimesta, on luovutuksen aineellisten edellytysten täytyttävä. Aineellisilla edellytyksillä tarkoitetaan luovutukseen oikeuttavaa lainsäädännöstä tai rekisteröidyn suostumusta tietojen luovuttamiseen tiettyyn tarkoitukseen.<sup>93</sup>

### **3.2 Julkisen sektorin tietojen uudelleenkäyttöä koskeva kansallinen normisto**

Julkisen sektorin tietohallinnon yleinen ohjaus kuuluu valtiovarainministeriölle sekä toimiala ja organisaatiokohtainen ohjaus ministeriöille ja eri virastoille. Valtiovarainministeriön asettaman Avoimen tiedon -ohjelman (17.5.2013–30.6.2015) tarkoituksena on koordinoita ja ohjata tietovarantojen avaamista sekä luoda yhteisiä tietojen uudelleenkäyttöä koskevia konkreettisia käytäntöjä koko valtion hallinnon alalle.<sup>94</sup>

---

<sup>92</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s. 6 ja s. 20.

<sup>93</sup> Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s. 4.

<sup>94</sup> Avoimen tiedon -ohjelman hankesivut saatavilla osoitteessa:  
[http://www.hare.vn.fi/mHankePerusSelaus.asp?h\\_iID=19367&tVNo=1&sTyp=Selaus](http://www.hare.vn.fi/mHankePerusSelaus.asp?h_iID=19367&tVNo=1&sTyp=Selaus).



PSI-direktiivi 2003/98/EY on implementoitu kansalliseen lainsäädäntöön julkisuuslailla ja julkisuuslain maksuja koskevaan 34 §:ään vuonna 2005 tehdyllä julkisuuslain muutoksella (495/2005).<sup>95</sup> Julkisuuslain 35 §:n maksuja koskevaa säännöstä tarkennettiin, koska käytännössä oli ilmennyt, että maksuja on ainakin osittain määritetty suuremmiksi kuin julkisuuslakia säädettäessä lainsäätaja on tarkoittanut.<sup>96</sup> Tietojen uudelleenkäytön tehostamisen kannalta vuonna 2005 tehty keskeinen muutos liittyy julkisuuslain hyvää tiedonhallintatapaa koskevaan 18 §:ään, jolloin sen 2 momentin valtuutussäännökset siirrettiin julkisuuslain 36 §:ään. Muutoksen myötä julkisuuslain 18 §:n 2 momentissa säädettiin nyt julkishallinnon tietohallinnon edistämisestä, joka sittemmin kumottiin vuonna 2011 annetulla lailla julkisen hallinnon tietohallinnon ohjauksesta (635/2011).<sup>97</sup>

Muuten vuonna 1999 tehtyä julkisuuslain kokonaisuudistusta pidettiin riittävänä toimenpiteenä PSI-direktiivi 2003/98/EY toimeenpanemiseksi ja halutun kansallisen tavoitteen saavuttamiseksi. Valtiovarainministeriö arvio vuonna 2012, että PSI-direktiivin muutosehdotus ei aiheuttaisi tarvetta muuttaa julkisuuslainsäädännön periaatteita. Arvioitavana kuitenkin on, voidaanko lainsäädännön avulla tehostaa tietojen uudelleenkäyttöä.<sup>98</sup>

PSI-direktiivin suurin vaikutus kansalliseen lainsäädäntöön näkyy tietojen luovutuksesta perittäviä maksuja koskevien säännösten tarkistamisessa. Periaatteena on, että viranomaisten välisestä tietojen vakiomuotoisista luovutuksista ei peritä maksuja ja muista tietojen luovutuksesta perittävien maksujen tulisi vastata aineiston irtiottokustannuksia. Ensisijaisesti julkisen sektori tietojen olisi oltava saatavilla maksutta.<sup>99</sup>

Vastauksena Euroopan unionin i2010 -puitestrategiaan hallitus laati vuonna 2006 kansallisen tietoyhteiskuntastrategian ”Uudistuva, ihmisläheinen ja kilpailukykyinen Suomi vuosille 2007–2015”.<sup>100</sup> Viimeisimmässä *tietoyhteiskuntastrategiassa* ”*Tuotava ja uudistuva Suomi Digitaalinen agenda vuosille 2011–2020*” valtioneuvoston asettama Arjen tietoyhteiskunnan neuvottelukunta esittelee kansallista tietoyhteiskun-

---

<sup>95</sup> Valtioneuvoston kirjelmä Eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta.

<sup>96</sup> HE 20/2005 vp., s. 16.

<sup>97</sup> HE 20/2005 vp., s. 10–20.

<sup>98</sup> Valtiovarainministeriön muistio EU/2011/2040 ja EU/2011/2041, s. 3.

<sup>99</sup> Julkishallinnon tietojen luovutusten periaatteet ja käytännöt 2/2012, s. 16.

<sup>100</sup> Lopullinen tietoyhteiskuntastrategia dokumentti saatavilla osoitteessa:

[http://www.tietoyhteiskuntaohjelma.fi/esittely/fi\\_FI/1142405427272/\\_files/75972407877173318/default/strategia\\_taitettu\\_final.pdf](http://www.tietoyhteiskuntaohjelma.fi/esittely/fi_FI/1142405427272/_files/75972407877173318/default/strategia_taitettu_final.pdf).

taa koskevia haasteita ja edellytyksiä, joita tarvitaan, jotta Suomi voi vastata digitaalisen toimintaympäristön luomiin haasteisiin. Keskeinen keino tietoyhteiskunnan palveluiden tehokkaan tuottavuuden ja laadun parantamiselle sekä työllisyyden lisäämiselle on tehokas tieto- ja viestintäteknologian (myöhemmin ICT) hyödyntäminen.<sup>101</sup>

Tämän tutkielman kannalta relevantein tietoyhteiskuntastrategian linjaus liittyy julkisen sektorin hallussa olevan tiedon tehokkaan käytön edistämiseen ja tietojen uudelleenkäyttöön. Verovaroin tuotetun tiedon on oltava vapaasti ja helposti uudelleenkäytettävissä. Strategiassa otetaan huomioon, että tietojen laadun säilyttäminen ja tietosuojaa koskevien oikeuksien huomioonottaminen ovat keskeisiä vaatimuksia tietoyhteiskunnassa. Strategiassa lisäksi todetaan, että yksityisyyden suojan turvaaminen on haaste tietovarantojen avaamisen yhteydessä. Tietojen anonymisointi on mahdollinen ratkaisu yksityisyyden suojan ja samalla tietojen julkisuuden turvaamiseksi.<sup>102</sup>

Tietoyhteiskuntastrategiassa esteenä julkisen tiedon uudelleenkäytölle nähdään tiukat viranomaisrajoitteet, siilomaiset hallintorakenteet, toiminnan rahoittaminen tiedon maksullisuudella ja viranomaisten varovaisuus tietojen luovuttamisessa. Tietovarantojen avaamisen demokraattinen ulottuvuus tunnistetaan strategiassa: julkisella tiedolla on keskeinen rooli yhteiskunnan päätöksenteon eri vaiheissa. Tietovarantojen avaamisella halutaankin ennen kaikkea tukea kansalaisten osallistumista yhteiskunnalliseen päätöksentekoon ja vaikuttamiseen.<sup>103</sup>

*Valtioneuvoston 3.3.2011 antamassa periaatepäätöksessä ”Julkisen sektorin digitaalisten tietoaineistojen saatavuuden parantamisesta ja uudelleenkäytön edistämisestä”* esitetään tavoitteet, linjaukset ja toimenpiteet, jotka kohdistuvat julkisrahoitteisten ja julkisen sektorin hallinnoimien julkisten ja sellaisenaan luovutettavissa olevien digitaalisten tietoaineistojen uudelleenkäytölle.

Periaatepäätöksessä esitettyjen toimenpiteiden tarkoituksena on lisätä ja edistää julkisen hallinnon tietovarantojen saatavuutta ja uudelleenkäyttöä yhteiskunnan jokaisella osa-alueella. Periaatepäätöksen tarkoituksena ei ole muuttaa tai tarkastella luovutukseen, käytettävyyteen tai tietojen käsittelyyn liittyviä lainsäädännöllisiä rajoituksia.

---

<sup>101</sup> Saatavilla osoitteessa:

[http://www.lvm.fi/c/document\\_library/get\\_file?folderId=1551286&name=DLFE-11771.pdf&title=Tuottava%20ja%20uudistuva%20Suomi.%20Digitaalinen%20agenda%202011-2020](http://www.lvm.fi/c/document_library/get_file?folderId=1551286&name=DLFE-11771.pdf&title=Tuottava%20ja%20uudistuva%20Suomi.%20Digitaalinen%20agenda%202011-2020) (tietoyhteiskuntastrategia 2011–2020).

<sup>102</sup> Tietoyhteiskuntastrategia 2011–2020, s.29.

<sup>103</sup> Ibid,

Kuitenkin periaatepäätöksessä esitettyjä linjauksia voidaan käyttää myös tällaisten tietoaisteistojen käytettävyyden parantamiseksi, siltä osin kun tietoaisteistot ovat viranomaisten toimintaa koskevien säännösten nojalla luovutettavissa.<sup>104</sup>

Valtioneuvoston periaatepäätöksessä esitettyjen linjausten tavoitteena on selkeyttää hallinnon tietopolitiikkaa ja siihen kohdistuvaa lainsäädäntöä, jotta julkisen sektorin tietovarannot olisivat avoimesti saatavilla uudelleenkäyttöä varten. Tavoitteena on, että uudelleenkäyttö tapahtuu yhtenäisin, selkein ja kaikille tasapuolisin ehdoin, kustannustehokkaasti ja kansatalouden kokonaisuutena ajatellen. Tietoaisteistojen tulisi olla saatavilla pääsääntöisesti maksutta.<sup>105</sup>

Valtioneuvoston periaatepäätöksessä linjataan tavoitteeksi kehittyvän tietoinfrastruktuurin luominen, jossa julkisen sektorin tietoaisteistoja tarjotaan uudelleenkäytettäväksi avointen rajapintojen kautta koneluettavassa muodossa. Julkisen sektorin organisaatioiden on tehtävä tietoaisteistoja koskeva inventaario ja kuvailtava sen hallussa olevien tietoaisteistojen sisältö. Tavoitteena on luoda datakatalogi, jonka yhteydessä julkisen sektorin tietovarannot on kuvailtu yhtenäisellä tavalla. Datakatalogien yhteyteen on luotava palveluhakemistot, joiden avulla tiedonhakija pystyy helposti löytämään tarvitsemansa tietoaisteistot. Tarkoituksena on myös luoda avoimen datan kulttuuri, jossa tuetaan kehittäjäyhteisöjen toimintaa, alan tutkimusta, kansainvälistä yhteistyötä ja kokeilevaa toimintaa.<sup>106</sup>

Valtiovarainministeriön alainen *Julkishallinnon tietovarantojen saatavuuden ja käytön edistämisen -työryhmä on 8.12.2011* julkaistussa loppuraportissa määritellyt ”Perusrekistereiden tietojen käsittelyä koskevat yleiset käyttöehdot”.<sup>107</sup> Käyttöehtojen tavoitteena on ”määritellä ja yhdenmukaistaa viranomaisten pitämistä yhteiskunnan perusrekistereistä luovutettujen tietojen käsittelyä ja perusrekistereiden tietoihin myönnettyjen käyttöoikeuksien yleiset ja yhteiset periaatteet”.<sup>108</sup>

Perusrekistereillä tarkoitetaan yhteiskunnan keskeisiä tietovarantoja, joihin sisältyy yhteiskunnan toiminnan kannalta keskeisiä tietoja.<sup>109</sup> Perusrekisterit ovat henkilötietolain mukaisia henkilörekistereitä ja niiden tietojen käsittelyyn sovelletaan henkilö-

---

<sup>104</sup> Periaatepäätös, s.1.

<sup>105</sup> Ibid.

<sup>106</sup> Periaatepäätös, s.1.

<sup>107</sup> Julkishallinnon tietoluovutusten periaatteet ja käytännöt 2/2012 s. 73 liite 7.

<sup>108</sup> Ibid.

<sup>109</sup> Korhonen, 2003 s.224.

tietolain säännöksiä. Perusrekistereihin liittyy myös erityisiä laadullisia kriteereitä kuten kattavuus, luotettavuus, monikäyttöisyys ja tietojen suojaus.<sup>110</sup> Työryhmän julkaisemia käyttöehtoja suositellaan käytettäväksi seuraavien perusrekistereiden tietojen käsittelyyn ja erityisesti luovuttamiseen: väestötietojärjestelmä (VTJ), kiinteistötietojärjestelmä (KTJ), kaupparekisteri, yhdistysrekisteri, säätiörekisteri ja yritys- ja yhteisötietojärjestelmä (YTJ).

*Julkisen hallinnon ICT:n hyödyntämisen strategiassa vuosille 2012–2020 ”Palvelut ja tiedot käytössä”*, määrittellään viisi linjausta julkisen hallinnon ICT:n kehitykselle. Linjaukset koskevat palveluinnovaatioiden ekosysteemiä, avointa tietoa ja tietojen yhteiskäyttöä, kykyä hyödyntää ICT:tä, selkeitä tietohallinnon rakenteita sekä toimintavarmaa ja kustannustehokasta ICT-infrastruktuuria. Linjauksissa esitetyt tavoitteet halutaan saavuttaa vuoteen 2020 mennessä.<sup>111</sup> Strategian toimeenpanosta vastaa valtiovarainministeriö.

Avoimen tiedon, tiedon yhteiskäytön ja julkisen sektorin tietojen uudelleenkäytön osalta strategiassa toimivan ICT-toimintaympäristön lähtökohdiksi esitetään periaatteita, joita ovat viranomaistoiminnan avoimuus, julkisen tiedon saatavuus, hyödynnettävyys ja luottamuksellisuus sekä tietojärjestelmien yhteiskäyttö ja toimivuus. ICT:n hyödyntämistä koskevan strategian tarkoituksena on tukea valtioneuvoston periaatepäätöksessä esitettyjen periaatteiden toteutumista julkisten tietovarantojen uudelleenkäytön edistämiseksi.<sup>112</sup>

Tavoitteena on, että tietojen uudelleenkäyttöön liittyvät esteet poistetaan ja, että keskeisimmät tietovarannot ovat tehokkaasti yhteiskunnan eri sektoreiden hyödynnettävissä vuoden 2015 loppuun mennessä. Tietovarantojen avaamisessa on otettava huomioon yksityisyyden suoja sekä tietosuojaa koskevat säännökset. Keskeiset muutokset liittyvät tiedon pääsääntöiseen maksuttomuuteen (irtiottokustannukset) ja tiedon tekniseen saatavuuteen rajapintojen kautta. Tavoitteena on, että perusrekisterien tiedot ovat kopioina julkisen hallinnon toimijoiden käytettävissä.<sup>113</sup>

*Valtiovarainministeriö on vuosien 2015–2018 kehysvalmisteluita koskevassa kirjeessä 23.10.2013 pyytänyt ministeriöitä selvittämään tietovarantojen avaamiseen liittyvät suunnitelmat. Suunnitelmasta on käytävä ilmi: mitä tietovarantoja avataan, millä*

---

<sup>110</sup> Korhonen 2003. s.228.

<sup>111</sup> ICT –strategia, s. 8 [https://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/julkict-strategia-2012-2020.pdf](https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/julkict-strategia-2012-2020.pdf).

<sup>112</sup> Ibid.

<sup>113</sup> ICT –strategia, s.9-10.

aikataululla ja mahdollisimman täsmälliset taloudelliset ja yhteiskunnalliset vaikutusarviointit.<sup>114</sup> Organisaatiomuutoksissa on otettava huomioon tietovarantojen uudelleenkäyttö. Digitalisoinnista aiheutuneet kustannukset on eriteltävä tietoaineistojen avaamisesta aiheutuneista määrärahakustannuksista. Tietovarantojen kartoittaminen ja organisointi on suositeltavaa liittää osaksi tietohallintolain (634/2011) kokonais- ja tietoarkkitehtuurityötä.

Julkisen sektorin tietovarantojen tehokas hyödyntäminen edellyttää, että julkishallinnolla on käytössä uudelleenkäyttöä koskeva selkeä avoin lisenssi.<sup>115</sup> Valtiovarainministeriö esitteli Avoin Suomi -messuilla 15.–16.9.2014 suositusluonnoksen julkisen hallinnon tietoaineiston käyttöluvasta (JHS-suositus). Suositeltavaa käyttö lupa on Creative Commons 0 tai Creative Commons BY 4.0, jossa myönnetään maailmanlaajuinen ja peruuttamaton ei-yksinomainen oikeus käyttää korvauksetta luvan kohteena olevaa aineistoa kaikilla mahdollisilla tavoilla. Aineistossa on mainittava tekijänoikeustiedot luvasta ilmenevällä tavalla. Käyttö lupa myönnetään tekijänoikeudellisesti suojattuun aineistoon, jonka kaikki oikeudet ovat viranomaisella. On syytä huomata, että henkilötietoja sisältäviä rekisteritietoja ei voida lisensoida kyseisellä käyttöluvalla. Suositus koskeva päätös tullaan tekemään tietohallinnon neuvottelukunta JUHTAssa syksyllä 2014.<sup>116</sup>

Henkilötietojen käsittelyn kannalta keskeisimmät, jo toteutuneet, lakienmuutokset liittyvät tilastolain (280/2004) ja lain väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalvelusta annetun lain (661/2009) muuttamiseen. Näiden lainmuutosten tarkoituksena on tehostaa julkisen sektorin hallussa olevien digitaalisten tietoaineistojen hyväksikäyttöä. Lailla tilastolain muuttamisesta (361/2013) toimeenpantiin Euroopan parlamentin ja neuvoston tilastoinnista annettu asetus (EY) N.o 223/2009 ja sen tarkoituksena on edistää tilastojen laajempaa hyväksikäyttöä erityisesti tieteellisessä tutkimuksessa.<sup>117</sup>

Väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalvelusta annetun lain muuttamisella (145/2014) on tarkoitus muun muassa edistää Väestörekisterikes-

---

<sup>114</sup> Julkisten tietovarantojen avaaminen ja kehysvalmistelut 2015–2018 ohje, s.1. Annettu 23.10.2013.

<sup>115</sup> Salokannel 2012, s.34.

<sup>116</sup> Valtiovarainministeriön tiedote 12.9.2014 saatavissa:

<http://valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/fi.jsp?oid=424476> ja [http://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/20140902Avoime/Marjut\\_Salokannel\\_Avointen\\_tietoaineistojen\\_kaeyttoelupa.pdf](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20140902Avoime/Marjut_Salokannel_Avointen_tietoaineistojen_kaeyttoelupa.pdf).

<sup>117</sup> HE 154/2012 vp., s.1.

kuksen rakennushanke ja rakennustiedostojen uudelleenkäyttöä.<sup>118</sup> Lain 34 §:ään li-  
sättiin säännös julkiseen käyttöön tarkoitettujen tiedostojen muodostamisesta ja käy-  
töstä. Rakennushanke ja rakennustiedostot sisältävät myös henkilötietoja, mutta julki-  
seen käyttöön luovutettavat tiedostot olisi anonymisoitava siten, että tiedoista ei voi-  
da tunnistaa luonnollista henkilöä.<sup>119</sup> Lain 34 § ei velvoita viranomaista muodosta-  
maan kyseisiä tiedostoja vaan mahdollistaa tiedostojen muodostamisen, jolloin on  
erityisesti otettava huomioon tiedostojen uudelleenkäytön vaikutus rekisteröityjen  
yksityisyyden suojalle.<sup>120</sup> Koska kyseessä on anonymin tiedon luovutus, ei tiedon  
luovutusta rajoita henkilötietojen suojaa koskevat periaatteet. Näin ollen tiedostojen  
muodostaminen ja käyttäminen olisi mahdollista yleislain eli julkisuuslain nojalla.<sup>121</sup>

---

<sup>118</sup> HE 195/2013 vp., s.1

<sup>119</sup> HE 195/2013 vp., s.9.

<sup>120</sup> HE 195/2013 vp., s.10.

<sup>121</sup> Tästä myös Voutilainen selvityksessään ”Palveluarkkitehtuuria tukeva lainsäädäntö 22/2014”, s. 34.

## 4. Julkisuus ja yksityiselämän suoja perusoikeuksina

### 4.1 Oikeus tietoon

Informaatio-oikeudellisen tutkimuksen keskeinen kysymys liittyy perusoikeuksien konkretisoimiseen ja turvaamiseen tietoyhteiskunnassa nyt ja tulevaisuudessa.<sup>122</sup> Ahti Saarenpään sanoin ”kokonaisuutena informaationaalisen työn oikeudelliset reunaehdot liittyvät yleensä välttämättä useampaan oikeudellisesti merkittävään perusoikeustasoiseen instituutioon. Niitä ovat ennen kaikkea henkilötietojen suoja, yksityisyys, julkisuus ja tietoturva”.<sup>123</sup>

Julkisen sektorin tietojen uudelleenkäytön ja henkilötietojen suojaa koskevat tiedollisten perusoikeuksien ryhmän muodostaa oikeus saada tietoa viranomaisten asiakirjoista (PeL 12.2 §), oikeus yksityiselämän ja henkilötietojen suojaan (PeL 10 §) ja sananvapaus (PeL 12.1 §). Perustuslain sanavapautta koskevaan 12 §:n 2 momenttiin on perusoikeudeksi määritelty oikeus saada tietoa viranomaisten hallussa olevista asiakirjoista ja muista tallenteista, jollei niiden julkisuutta ole välttämättömien syiden vuoksi erikseen rajoitettu. Julkisuuden rajoittamisen perusteena on niin sanottu välttämättömyyedellytys.<sup>124</sup>

Viranomaisille asetettiin perusoikeus uudistuksen myötä myös velvollisuus aktiivisesti turvata ja edistää oikeutta tietoon. Perustuslain 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen, jolloin viranomaisen on aktiivisin toimenpitein huolehdittava julkisuuden toteutumisesta. Perusoikeutta voidaan rajoittaa vain erityisestä syystä, joka voi olla esimerkiksi toisen perusoikeuden edistäminen.<sup>125</sup> Tiedonsaantioikeutta rajoitetaan yleisesti yksityisen tai yleisen edun vuoksi. Julkisuuslaki yleislakina turvaa jokaisen oikeutta viranomaisen hallussa olevaan tietoon.

Demokraattisessa yhteiskunnassa tiedon saatavuuteen, käyttöön ja luotettavuuteen liittyvät oikeudet ovat keskeisessä asemassa. Hallinnon julkisuutta pidetään edelly-

---

<sup>122</sup> Pöysti 1998, s.31.

<sup>123</sup> Saarenpää 2012b, s.445.

<sup>124</sup> Korhonen 2003, s. 82.

<sup>125</sup> PeVL 2/2008 vp., s.2.

tyksenä demokratian ja tasa-arvon toteutumiselle sekä hallinnon luotettavuudelle ja päätösten hyväksyttävyydelle. Jokaisella on oltava mahdollisuus saada luotettavaa tietoa viranomaisten toiminnasta, jotta demokraattisen yhteiskunnan keskeinen perusoikeus vapaasta mielipiteen muodostamisesta ja ilmaisemisesta toteutuisi.

Julkisen sektorin tietojen uudelleenkäytön näkökulmasta oikeus tietoon sisältää oikeuden hyväksikäyttää ja oikeuden levittää edelleen julkisuusperiaatteen nojalla saatua tietoa (PeL 12.1 §).<sup>126</sup> Jos oikeutta tietoon tarkastellaan laajemmasta näkökulmasta, voidaan oikeudesta löytää eri ulottuvuuksia ja tasoja, jotka ovat turvattu perusoikeustasolla.<sup>127</sup> Julkisuuslain julkisuusperiaate (JulkL1 §) toteuttaa konkreettisesti oikeutta julkisen sektorin hallussa olevaan tietoon.<sup>128</sup>

Yhteisön tasolla sanan- ja tiedonvälityksen vapautta koskevat Euroopan unionin perusoikeuskirjan<sup>129</sup> 11 artikla ja Euroopan ihmisoikeussopimuksen<sup>130</sup> 10 artikla sisältävät oikeuden saada tietoa. Euroopan unionin perusoikeuskirjan 41 artiklan 2 kohdassa tunnustetaan jokaisen oikeus tutustua häntä itseään koskeviin asiakirjoihin ottamatta huomioon oikeutetun luottamuksellisuuden, salassapitovelvollisuuden ja liikesalaisuuden vaatimukset. Euroopan unionin perusoikeuskirjan 42 artiklassa tunnustetaan kaikille unionin kansalaisille ja kaikille luonnollisille ja oikeushenkilöille, joiden asuinpaikka tai sääntömääräinen kotipaikka on jossain jäsenvaltiossa, oikeuden tutustua Euroopan parlamentin, neuvoston ja komission asiakirjoihin.

Julkisen sektorin tietojen uudelleenkäyttö on suunnattu pääsääntöisesti uusia innovatiivisia julkisen sektorin tuottaman tiedon varaan rakentuvia palveluita ja toimintoja varten. Tietosuojatyöryhmä on vuonna 2003 antamassa PSI-direktiiviä koskevassa lausunnossa katsonut, että direktiivi on liiketoiminnan kannalta keskeinen liiketaloudellinen tekijä, joten näin ollen direktiiviin ei liity ihmisoikeuksia tai avoimuutta koskevaa näkökohtaa.<sup>131</sup>

Taloudellisten hyötyjen ohella, julkisen sektorin tietojen uudelleenkäyttö lisää demokratiaa, kansalaisten vaikutusmahdollisuuksia ja osallistumista päätöksentekoon tietoyhteiskunnassa. Kun viranomaisen tieto saatetaan uudelleenkäytettäväksi ja näin

---

<sup>126</sup> Mäenpää 2008, s.23.

<sup>127</sup> Korhonen 2003, s. 6-7.

<sup>128</sup> Voutilainen 2009, s. 163.

<sup>129</sup> EYVL N:o C 364, 18.12.2000 (Euroopan union perusoikeuskirja, eng. The Charter of Fundamental Rights of the European Union).

<sup>130</sup> SopS 19/1990.

<sup>131</sup> Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s. 3.



myös yhteiskunnan eri sektoreiden tarkastelun alle, lisää tämä viranomaistoiminnan avoimuutta ja läpinäkyvyyttä. Mielestäni on perusteltua katsoa, että PSI-direktiivillä, ja viranomaistiedon saatavuutta lisäävillä muilla säännöksillä, on myös perusoikeuksia vahvistava ominaisuus ja vaikutus. Esimerkiksi Civicus ja Open Society Institute ovat kansalaisliikkeitä, joiden tarkoituksena on edistää viranomaisten hallussa olevan tiedon julkisuutta ja avoimuutta ihmisoikeusnäkökulmasta.<sup>132</sup>

## 4.2 Oikeus yksityiselämän ja henkilötietojen suojaan

Perustuslain 10 §:n mukaan ”jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja luottamuksellisen viestin salaisuus on loukkaamaton. Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen tai yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapauden menetyksen aikana”.

Yksityiselämän suoja ei ole eksaktisti määritelty laintasolla. Tämä on kannatettavaa sen vuoksi, että yksityiselämän suoja kattaisi mahdollisimman laajasti kaikki yksityiselämän piiriin kuuluvat oikeudet. Oikeus yksityiselämän suojaan ilmentää erityisesti oikeutta yksityisyyteen, perhe- ja yksityiselämän piiriin ilman ulkopuolisen tahon, erityisesti valtion, perusteetonta puuttumista. Perusoikeuksien merkitys yhteiskunnan perusarvoina korostavat yksityiselämän suojan merkitystä myös yksityishenkilöiden välisissä suhteissa.<sup>133</sup> Yksityiselämän suojaa käytetään toisinaan synonyymina yksityisyyden suojalle.<sup>134</sup>

Yksityisyyden suojalla tarkoitetaan muun muassa yksilöiden suoja ja oikeuksia tietojenkäsittelyssä. Yksityisyyden suojaan voidaan katsoa kuuluvaksi myös viestinnän luottamuksellisuus ja oikeus vaihtaa arkaluonteisiakin tietoja. Oikeus yksityisyyden

---

<sup>132</sup> Lisää tietoja järjestöjen toiminnasta osoitteista <http://www.opensocietyfoundations.org/> ja <http://civicus.org/index.php/en/>.

<sup>133</sup> HE 309/1993 vp., osa 3.4.

<sup>134</sup> HE 96/1998 vp., s. 3.

suojaan voidaan katsoa koostuvan yksityiselämän suojan lisäksi myös muista henkilö-tietojen käsittelyssä merkityksellisistä perusoikeuksista, joita ovat muun muassa oi-keus henkilökohtaiseen vapauteen, oikeus kunniaan, oikeus yhdenvertaiseen kohte-luun, oikeus henkilökohtaiseen koskemattomuuteen, oikeus ihmisarvoiseen kohte-luun, oikeus turvallisuuteen, oikeus vaikuttaa itseään koskeviin asioihin ja syrjinnän kieltö.<sup>135</sup>

Henkilötietojen käsittelyn osalta keskeisiä oikeuksia ovat tiedollinen itsemääräämis-oikeus eli oikeus vaikuttaa omien tietojen käyttöön ja päättää omien tietojensa käsitte-lystä mahdollisimman kattavasti sekä oikeus tulla arvioiduksi oikeiden ja tarpeellisten tietojen perusteella.<sup>136</sup> Itsemääräämisoikeus henkilötietojen käsittelyssä ilmenee siten, että tietojen käsittely on ensisijassa perustuttava rekisteröidyn suostumukseen. Jos henkilötietoja käsitellään ilman rekisteröidyn suostumusta, on käsittelyn perusteena oltava laintasoinen säännös.

Yksilön yksityisyyden suojan keskiössä on oikeus päättää omista asioistaan ja tehdä henkilökohtaisia päätöksiä omasta elämästään ulkopuolisten siihen puuttumatta. Pe-rustuslain 10 §:n 1 momentin mukaan henkilötietojen käsittelystä on säädettävä lailla eli henkilötietojen suojaan ei voida puuttua lakia alemman tasoisella säännöksellä. Valtiolla on velvollisuus huolehtia yksityisyydensuojan toteutumisesta lainsäädännöl-lä sekä muilla toimenpiteillä (PeL 22 §).

Yksityiselämän suojasta on erotettava yksityisyys, joka on käsitteellisesti vielä hanka-lampi hahmottaa kuin yksityiselämän suoja. Yksityisyyden käsitettä ei ole myöskään lainsäädännön tasolla selkeästi määritelty. Neuvonen näkee yksityisyyden vastakoh-tana julkisuudelle ja näkee yksityisyyden suojan siten, että se luo toiselle oikeuden yksityisyyteen ja toiselle velvollisuuden kunnioittaa tätä oikeutta<sup>137</sup>. Mahkonen näkee yksityisyyden näkökulma-, aika-, käsitteellis-, laki-, arvo- ja kulttuurisidonnaisena ilmiönä, joista laki määrittelee yksityisyyden ja siihen puuttumisen rajat.<sup>138</sup> Yksityi-syyden tai yksityiselämän suojan alaan kuuluvia toimintoja ei ole määritelty laintasol-la. Lakiteknisesti yksityiselämän suojan loukkaamisesta on päädytty rankaisemaan rikosoikeudellisella vastuulla esimerkiksi yksityiselämää loukkaavan tiedon levittä-misestä sekä kunnianloukkaamisesta.

---

<sup>135</sup> HE 96/1998 vp., s31.

<sup>136</sup> Neuvonen 2014, s.59.

<sup>137</sup> Neuvonen 2014, s.21 ja s. 28–29.

<sup>138</sup> Mahkonen 1997, s. 14–38.

### 4.3 Rekisteröityjen oikeudet

Rekisteröityjen oikeuksien turvaaminen ja toteuttaminen ovat keskeisiä henkilötietolain tavoitteita. Jos tietoja saatetaan uudelleenkäytettäväksi, on viranomaisen otettava huomioon rekisteröityjen mahdollisuus hyväksikäyttää tietosuojasäännöksissä heille turvattuja oikeuksia sekä toimenpiteiden vaikutukset näille oikeuksille. Rekisteröidyn keskeisiä henkilötietolain mukaisia oikeuksia ovat tarkastusoikeus (HetiL 26–28 §), tiedonsaantioikeus (HetiL 24 §), tiedon korjaaminen (HetiL 29 §) ja kiello-oikeus (HetiL 30 §). Rekisteröidyn julkisuuslain mukaisia oikeuksia ovat muun muassa asianosaisen tiedonsaantioikeus (JulkL 11 §) ja oikeus saada tietoa itseään koskevasta asiakirjasta (JulkL 12 §).

Henkilötietojen käsittelyn lähtökohtana on tietojenkäsittelyn avoimuus ja läpinäkyvyys. Rekisterinpitäjän on aktiivisesti informoitava rekisteröityjä henkilötietojen käsittelyn tarkoituksesta. Henkilötietolain 10 §:n mukaan rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste, joka on pääsääntöisesti pidettävä jokaisen saatavilla. Rekisteriselosteeseen on kirjattava rekisterinpitäjä, käsiteltävät tiedot ja tietoryhmät, henkilötietojen käsittelyn tarkoitus, tietojen mahdolliset säännönmukaiset luovutukset, tietojen mahdolliset siirrot Euroopan unionin ja Euroopan talousalueen ulkopuolelle ja kuvaus siitä, miten rekisterin suojaus on järjestetty.

Henkilötietolain 24 §:ssä säädetään rekisterinpitäjän yleisestä informointivelvoitteesta. Rekisterinpitäjän on pääsääntöisesti henkilötietoja kerätessään huolehdittava siitä, että rekisteröity voi saada tiedon muun muassa henkilötietojen käsittelyn tarkoituksesta. Jos henkilötiedot kerätään muualta kuin rekisteröidyltä itseltään ja henkilötietoja on tarkoitus luovuttaa, on tiedot annettava viimeistään silloin kun henkilötietoja luovutetaan ensimmäistä kertaa. Tiedonantovelvollisuutta on rajoitettu esimerkiksi valtion turvallisuuteen liittyvien syiden vuoksi. Erityisesti luovutettujen tietojen käsittelyn osalta tärkeä suoramarkkinointiin liittyvä informointivelvollisuutta koskeva säännös sisältyy henkilötietolain 25 §:n 3 momenttiin. Rekisterinpitäjän on suoramarkkinointiviestissä ilmoitettava tietolähde eli sen rekisterin nimi, josta tiedot on saatu suoramarkkinointitarkoitusta varten sekä rekisterinpitäjän nimi ja yhteystiedot. Puhelinmarkkinoinnissa vastaavat tiedot on annettava pyynnöstä.

Henkilötietolain 29 §:n mukaan ”rekisterinpitäjän on ilman aiheetonta viivytystä korjattava henkilötietojen käsittelyn kannalta virheellinen, tarpeeton tai vanhentunut tieto

joko oma-aloitteisesti tai rekisteröidyn pyynnöstä. Jos rekisterinpitäjä ei hyväksy vaatimusta tiedon korjaamisesta, hänen on annettava asiasta kirjallinen todistus. Rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi. Jos rekisterinpitäjä on saanut tai luovuttanut rekisteröityä koskevan virheellisen tiedon, on rekisterinpitäjän ilmoitettava tiedon korjaamisesta luovutuksensaajalle tai sille, jolta se on saanut virheellisen tiedon. Ilmoitusvelvollisuutta ei kuitenkaan ole, jos se on mahdotonta tai vaatii kohtuutonta vaivaa”.

Tietoyhteiskunnassa merkittävä rekisteröidyn yksityisyyttä ja oikeutta tulla arvioituksi oikeassa valossa turvaava oikeus on oikeus tulla unohdetuksi (*right to be forgotten*). Ehdotuksessa yleiseksi Euroopan unionin tietosuojasetukseksi tämä oikeus on kirjattu ehdotuksen 17 artiklaan. Ehdotuksen mukaan jokaisella on oikeus tulla unohdetuksi, jos tietojen säilyttäminen ei ole asetuksen säännösten mukaista. Rekisterinpitäjä olisi pääsääntöisesti ilmoitettava rekisteröidyn pyynnöstä kolmansille osapuolille tietojen poistamisesta ja pyytää poistamaan henkilötietoihin liittyvät linkit, tietojen kopiot tai jäljennökset. Ehdotuksessa otetaan huomioon erityisesti lapsena annettu suostumus tietojenkäsittelylle, jolloin tietojen poistamisen olisi pääsääntöisesti oltava mahdollista. Tämä koskee erityisesti internetissä olevia tietoja.

Euroopan unionin tuomioistuimen antama hakukonepalvelu Googlea koskeva ennakkoratkaisu vahvistaa kyseisen oikeuden olemassaoloa.<sup>139</sup> Ratkaisussa Euroopan unionin tuomioistuin katsoo, että Google Inc. ja sen Euroopassa toimivat tytäryhtiöt ovat rekisterinpitäjän asemassa, kun hakukonepalvelu indeksoi tietoja ja näin ollen määrittää henkilötietojen käsittelyn tarkoitukset ja keinot. Tiedot on poistettava hakukonepalvelusta silloin, kun tiedot eivät ole asianmukaisia, olennaisia tai ne ovat liian laajoja siihen tarkoitukseen, mihin hakukone niitä käsittelee.

Henkilötietolain 30 §:n mukaan rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä (muun muassa luovuttamasta), markkinatarkoitusta, markkina- ja mielipidetutkimusta sekä henkilömatrikkelia ja sukututkimusta varten.

Henkilötietolain mukaisesta tiedonsaantioikeudesta säädetään henkilötietolain 26-28 §:ssä. Henkilötietolain 26 §:n mukaan jokaisella on salassapitosäännösten estämättä oikeus saada tietää, mitä häntä itseään koskevia tietoja henkilörekisteriin on talletettu tai, että rekisterissä ei ole häntä koskevia tietoja. Tiedonsaantioikeus koskee kaikkia

---

<sup>139</sup> Euroopan unionin tuomioistuin, asiassa C-131/12, Google SL ja Google Inc vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González, annettu 13. toukokuuta 2014.

rekisteriin tallennettuja tietoja. Lisäksi rekisterinpitäjän on ilmoitettava rekisteröidylle rekisterin säännönmukaiset tietolähteet sekä, mihin rekisterin tietoja käytetään ja säännönmukaisesti luovutetaan. Jos rekisteröity on ollut automatisoidun päätöksenteon kohteena, on hänellä oikeus saada tieto automaattiseen tietojenkäsittelyyn liittyvistä toimintaperiaatteista. Tarkastusoikeutta koskevan pyynnön esittäminen on maksutonta kerran vuodessa, muuten tarkastusoikeuden toteuttamisesta voidaan periä kohtuullinen korvaus. Korvaus ei tällöinkään saa ylittää tiedon antamisesta aiheutuvia kohtuullisia kustannuksia.

Tarkastusoikeuden toteuttamisesta säädetään henkilötietolain 28 §:ssä. Tarkastusoikeus on henkilökohtainen oikeustoimi ja sitä koskeva pyyntö on esitettävä omakätisesti allekirjoitetussa tai muulla tavalla varmennetussa asiakirjassa tai henkilökohtaisesti rekisterinpitäjän luona. Pyyntö on oltava riittävän yksilöity ja sen voi rajata koskemaan tiettyjä rekisterinpitäjän hallussa olevia tietoja tai tiettyä rekisterinpitäjän ylläpitämää henkilörekisteriä. Rekisteröidyllä on oikeus tutustua tietoihin rekisterinpitäjän luona tai hän voi saada tiedot pyynnöstä kirjallisena.

Pyynnön esittämisessä ei voi käyttää asiamiestä, ellei rekisteröity ole edunvalvonnan tai holhouksenalaisena siten, että edunvalvoja tai huoltaja voi toimia rekisteröidyn puolesta tämän henkilökohtaisissa ja/tai taloudellisissa asioissa. Edunvalvojan oikeus perustuu hänelle annettuun määräykseen. Jos määräys koskee taloudellisten asioiden hoitamista, edunvalvojalla ei ole esimerkiksi oikeutta päämiehen puolesta tarkastaa hänen potilastietoja.<sup>140</sup>

Eduskunnan oikeusasiamies on potilastietojen tarkastamista koskevassa ratkaisussa 2022/40/04 katsonut, että tarkastusoikeutta koskevan pyynnön lähettämisessä tai asiakirjojen tilaamisessa voidaan käyttää asiamiestä. Kyseissä tapauksessa potilaan omakätisesti allekirjoittaman tarkastusoikeutta koskevan pyynnön on tämän puolesta lähettänyt hänen avoimella asianajovaltuutuksella valtuuttama asiamies. Alaikäisen lapsen osalta huoltajalla voi olla oikeus tarkastaa lasta koskevat tiedot, mutta lapsen tiedollinen itsemääräämisoikeus omiin tietoihinsa määräytyy yleisen ja erityisen lapsen oikeuksia koskevan lainsäädännön perusteella.<sup>141</sup>

---

<sup>140</sup> Tietosuojavaltuutetun toimiston ohje: Henkilörekisteriin talletettujen tietojen tarkastaminen, päivätty 27.7.2010, s. 4.

<sup>141</sup> Tietosuojavaltuutetun toimiston ohje: Henkilörekisteriin talletettujen tietojen tarkastaminen, päivätty 27.7.2010, s. 4 ja lapsen oikeuksien yleissopimus (20.11.1989) ja perustuslaki (731/1999) sekä mahdollinen erityislainsäädäntö.

Vastaus tarkastusoikeutta koskevaan pyyntöön on annettava ymmärrettävässä muodossa ja ilman aiheetonta viivytystä, kuitenkin viimeistään kolmen kuukauden kuluessa pyynnön esittämisestä. Jos rekisterinpitäjä kieltäytyy toteuttamasta rekisteröidyn tarkastusoikeutta, tästä on annettava kirjallinen kieltäytymistodistus, jossa on ilmoitettava syy kieltäytymiselle. Jos rekisterinpitäjä ei reagoi rekisteröidyn pyyntöön kolmen kuukauden kuluessa, katsotaan tämä kieltäytymiseksi. Rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi.

Tarkastusoikeuden rajoituksista säädetään henkilötietolain 27 §:ssä, jolloin tarkastusoikeutta on rajoitettu esimerkiksi tilanteissa, jolloin tiedon antaminen saattaa vahingoittaa valtion turvallisuutta, rekisteröidyn hoitoa tai terveyttä tai silloin, kun rekisterissä olevia henkilötietoja käytetään yksinomaan historiallista tai tieteellistä tutkimusta taikka tilastointia varten. Lisäksi tarkastusoikeutta on nimenomaisesti rajattu tiettyjen rekisterien osalta. Esimerkiksi lain henkilötietojen käsittelystä poliisitoimesta (761/2003) 45 §:n mukaan tarkastusoikeutta ei ole lainkaan muun muassa epäiltyjen tietojärjestelmän tietoihin, suojelupoliisin toiminnallisen tietojärjestelmän tietoihin eikä Schengenin tietojärjestelmä salaista tarkkailua ja erityistarkastuksia koskeviin tietoihin. Rekistereihin on kuitenkin niin sanottu välillinen tarkastusoikeus, jolloin tietosuojavaltuutettu tarkastaa rekisteröidyn puolesta rekisterimerkintöjen asian- ja lainmukaisuuden. Rekisteröidyllä ei kuitenkaan ole oikeutta saada tietää, onko häntä koskevia tietoja kyseisissä rekistereissä tai, että rekistereissä ei ole häntä koskevia tietoja.

Yleisen tietosuojasetuksen ehdotuksen 18 artiklassa säädettäisiin rekisteröidylle oikeus siirtää tietonsa yhdestä sähköisestä käsittelyjärjestelmästä toiseen rekisterinpitäjän estämättä, jäsennellyssä ja yleisesti käytetyssä sähköisessä muodossa (*right to data portability*).<sup>142</sup> Ehdotuksen mukaan oikeus koskee tietoja, jotka rekisteröity on antanut rekisterinpitäjälle sopimuksen tai suostumuksen perusteella.

Suomen tietoyhteiskuntastrategiassa ” Tuottava ja uudistuva Suomi, Digitaalinen agenda vuosille 2011-2020” vuodelle 2020 asetettu yksi visio koskee henkilötietojen omistusoikeutta ja tietojen siirtoa käsittelyjärjestelmästä toiseen. Tavoitteena on, että vuoteen 2020 mennessä ”[...]ihmisillä on helppo pääsy omiin tietoihinsa. Ihmistä itseään koskevat tiedot kulkevat hänen mukaan ja ovat siten hänen omaisuuttaan ja jous-

---

<sup>142</sup> Yleinen tietosuojasetus COM(2012) 11 final s.9. Euroopan parlamentin LIBE valiokunnan mietintöluonnoksessa oikeus siirtää tietoja kirjattiin 15 artiklaan (LIBE-valiokunnan mietintöluonnos yleisestä tietosuojasetuksesta / (COM(12)0011 – C7-0225/2012 – 2012/0011(COD)), s. 95.

tavasti käytettävissä”.<sup>143</sup> Suomen avoimen hallinnon toimintasuunnitelmassa esitetään mahdolliseksi viranomaisten välisen yhteisen viitetietokannan perustaminen, jossa jokainen voi tarkistaa itseään koskevat tiedot kustannustehokkaasti samasta paikasta.<sup>144</sup>

Yksilön oikeutta tietoon ja tiedollista itsemääräämisoikeutta turvaa henkilötietolain 2 §:n 3 momentti, jonka mukaan ”henkilötietolaki ei koske henkilötietojen käsittelyä, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiinsa”. Säännös mahdollistaa yksityisen henkilön tiedon keräämisen ja luovuttamisen lähes rajoituksetta. Henkilötietojen vieminen avoimeen tietoverkkoon ei koskaan täytä yksityisenkäytön poikkeuksen edellytyksiä.<sup>145</sup>

#### 4.4. Julkisuusperiaate

Perustuslain 12 §:n 1 momentissa säädetään viranomaistoiminnan julkisuudesta ja oikeudesta saada tietoa viranomaisen asiakirjasta jokaiselle kuuluvana perusoikeutena. Viranomaistoimintaa koskeva yleislaki julkisuuslaki sekä mahdollinen sovellettava erityislainsäädäntö muodostavat sääntelykehikon, jonka avulla voidaan arvioida viranomaisen hallussa olevien tietojen luovutusten lainmukaisuutta.

Julkisuusperiaatteen nojalla viranomaisen asiakirjat ovat julkisia, jollei julkisuuslaissa tai erityislainsäädännössä toisin säädetä (Julkl 1.1 §). Julkisuuslain 24 §:ssä säädetään salassa pidettävistä viranomaisen asiakirjoista, jotka ovat salassa pidettäviä, jollei toisin säädetä. PSI-direktiivissä veloitetaan jäsenmaita arvioimaan viranomaisten hallussa olevien tietovarantojen uudelleenkäytettävyyttä, mutta arvio perustuu kansalliseen tietojensaantia koskevaan lainsäädäntöön.

PSI-direktiiviä ei sovelleta sellaisiin asiakirjoihin, jotka eivät ole saatavilla viranomaisen asiakirjojen saatavuutta koskevien säännösten perusteella. Viranomaisten

---

<sup>143</sup> Tietoyhteiskuntastrategia 2011–2020, s. 10.

<sup>144</sup> Saatavilla osoitteessa:

[http://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/Avoin\\_hallinto\\_toimintasuunnitelma.pdf](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/Avoin_hallinto_toimintasuunnitelma.pdf)

<sup>145</sup> Euroopan yhteisön tuomioistuimen ratkaisu 16.11.2003 C 101/01 Bodil Lindqvist.

asiakirjojen saatavuutta koskeva lainsäädäntö vaihtelee jäsenvaltioiden välillä.<sup>146</sup> Uudelleenkäyttöä koskevien periaatteiden tehokas soveltaminen riippuu paljolti kansallisen tietojensaantia koskevan lainsäädännön ja käytäntöjen tehokkuudesta.<sup>147</sup> Henkilötietoja sisältävät viranomaisen asiakirjat voidaan saattaa uudelleenkäytettäväksi PSI-direktiivissä tarkoitettulla tavalla ainoastaan, jos tiedonsaanti asiakirjasta on mahdollista tiedonsaantia viranomaisten asiakirjoista koskevan kansallisen lainsäädännön nojalla.<sup>148</sup>

Uudelleenkäytön perusteita arvioitaessa toisistaan on erotettava viranomaisten asiakirja julkisuutta koskeva yleinen tiedonsaantioikeus viranomaisen asiakirjasta, rekisteröidyn tiedonsaantioikeus, joka koskee rekisteriin talletettuja häntä itseään koskevia tietoja sekä henkilötietoja sisältävän viranomaisen hallussa olevan tiedon saattaminen uudelleenkäytettäväksi.<sup>149</sup>

Vuonna 1999 voimaantulleen julkisuuslain uudistuksen yksi keskeinen muutos liittyy viranomaiselle asetettuun aktiiviseen tiedontuotanto- ja informaatiotehtävään. Julkisten tietovarantojen uudelleenkäyttöä koskeva keskeinen periaate on julkisuuslain mukainen julkisuusperiaate, joka mahdollistaa osaltaan julkisten tietovarantojen hyödyntämisen ja uudelleenkäytön.<sup>150</sup>

Julkisuudella viranomaistoiminnassa tarkoitetaan muun muassa oikeutta viranomaisen hallussa olevaan tietoon (*right of access to information*), viranomaisen velvollisuutta luovuttaa pyydetty tieto (*duty to disclose information*), viranomaismenettelyn avoimuutta ja viranomaisille asetettua velvollisuutta aktiivisesti tiedottaa toiminnastaan.<sup>151</sup> Viranomaistiedon julkisuus on osa hyvän hallinnon vaatimusta. Suomessa viranomaistoiminnan julkisuudella on pitkä historia, sillä jo vuoden 1766 painovapausasetuksen 10 § edellytti yleistä tiedon saatavuutta asiakirjoista.<sup>152</sup>

---

<sup>146</sup>Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.9.

<sup>147</sup> van Eechound ja Jansen 2012, s. 3.

<sup>148</sup> Opinion of the European Data Protection Supervisor on the “Open-Data Package” of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents. Saatavilla osoitteesta: [https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-04-18\\_Open\\_data\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_EN.pdf) s.6.

<sup>149</sup> Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s. 3.

<sup>150</sup> Mäenpää 2008, s. 8.

<sup>151</sup> Mäenpää 2008, s. 1-2.

<sup>152</sup> Mäenpää 2008, s.1. Julkisuusperiaatteen historiasta ja kehityksestä enemmän esimerkiksi Korhonen 2003, s.52–64.



Julkisuusperiaatteen kohde on viranomaisen hallussa oleva tieto, joka perustuslain 12 §:n 2 momentin mukaan pääsääntöisesti koskee viranomaisen hallussa olevia asiakirjoja ja muita tallenteita. Julkisuusperiaate kohdistuu viranomaisen hallussa olevaan tietoon sen tallennustavasta riippumatta.<sup>153</sup>

Julkisuusperiaate määritellään julkisuuslain 1 §:ssä, jonka mukaan ”viranomaisten asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä (*tallennejulkisuus*). Oikeudesta seurata eduskunnan täysistuntoa, valtuuston ja muiden kunnallisten toimielinten kokouksia sekä tuomioistuinten ja kirkollisten toimielinten istuntoja säädetään erikseen (*yleisöjulkisuus*)”. Julkisuusperiaate voidaan jakaa käsittelyjulkisuuteen, asiakirjajulkisuuteen ja asianosaisjulkisuuteen.<sup>154</sup> Julkisuuslain 9 §:n 1 momentin mukaan jokaisella on oikeus saada tieto julkisesta asiakirjasta.

Viranomaisen asiakirjat ovat joko julkisia, osittain julkisia tai salassa pidettäviä. Salassapidon on aina perustuttava lakiin ja viranomaisen on pystyttävä perustelevaan salassapidon syyt. Suhteellisuusperiaate ohjaa viranomaisen salassapitoa ja tietojen luovutusta koskevaa harkintavaltaa. Tietojen luovutusta ja julkisuutta ei saa rajoittaa ilman laissa säädettyä ja asianmukaista perustetta tai enempää kuin on tarpeen sen oikeushyvän suojelemiseksi, minkä vuoksi salassapidosta on säädetty (JulkL 17§).<sup>155</sup> Jos tietojen julkisuus ja salassapito määräytyvät viranomaisen harkintavallan mukaan, sovelletaan tietojen luovutukseen harkintaperiaatetta.<sup>156</sup>

Julkisuusperiaatteella on useita eri tehtäviä modernissa tietoyhteiskunnassa. Julkisuusperiaatteen keskeinen tehtävä on kiistatta demokratian ja oikeusvarmuuden edistäminen, sen ollessa keskeinen viranomaistoiminnan läpinäkyvyyttä ja avoimuutta sekä informaation vapautta koskeva periaate. Julkisuusperiaatteen tehtävänä on yhteiskunnallisen osallistumisen, vaikuttamisen ja valvonnan toteutuminen ja varmistaminen.<sup>157</sup> Mahdollisuus siitä, että viranomaisen toiminta asetetaan kritiikin ja julkisen arvostelun kohteeksi ennaltaehkäisee epäasianmukaista ja laitonta toimintaa.

Julkisuusperiaatteen tarkoituksena on edistää viranomaistoiminnan läpinäkyvyyttä siten, että se ylläpitää kansalaisten luottamusta viranomaistoimintaan. Ei ole riittävää, että hallinto toimii lainmukaisesti vaan jokaisen on pystyttävä mahdollisimman luo-

---

<sup>153</sup> Mäenpää 2008, s.5.

<sup>154</sup> Korhonen 2003, s. 50.

<sup>155</sup> Neuvonen 2013, s.148.

<sup>156</sup> Ibid.

<sup>157</sup> Konstari; Wallin 2000, s.29–31 ja s.35, Mäenpää 2008, s. 1-2, Konstari 1977, s. 93.

tettavan tiedon pohjalta toteamaan, että näin myös tapahtuu. Tätä kutsutaan myös julkisuusperiaatteen legitimaatiotehtäväksi.<sup>158</sup>

Perinteisten funktioiden ohella julkisuusperiaate mahdollistaa julkisten tietovarantojen tehokkaan uudelleenkäytön ja taloudellisen hyödyntämisen.<sup>159</sup> Tietoyhteiskunnassa viranomaistiedolla on arvoa taloudellisena hyödykkeenä, jolloin tiedon saatavuus ja käytettävyys myös kaupalliseen tarkoitukseen on tärkeässä asemassa julkisuusperiaatteen toteutumisen kannalta. Julkisuusperiaatteen merkitys ja tehtävä viranomaisen hallussa olevan tiedon uudelleenkäytön mahdollistajana laajentaa julkisuuden merkitystä ohi perinteisen arvoasetelman, jossa julkisuus nähdään demokratian ja viranomaistoiminnan legitimitetin takeena. Perinteisessä ajattelumallissa julkisuusperiaate ei sinänsä aseta viranomaiselle aktiivista tiedonjakelu velvoitetta, vaan julkisuusperiaate turvaa tiedonsaannin julkisesta asiakirjasta pyydettyä.

Jotta julkisuusperiaate toteutuu täysimääräisesti, on viranomaisen hallussa oleva tieto tuotava informaatiomarkkinoille hyödynnettäväksi (*access to market*).<sup>160</sup> Viranomaistoiminnan julkisuuden toteutuminen vaatii viranomaisilta aktiivisia toimenpiteitä myös tiedon uudelleenkäytön mahdollisuuksien arvioimiseksi ja lopulta uudelleenkäytön varmistamiseksi.

Tietojen uudelleenkäytön näkökulmasta on tärkeää painottaa julkisen ja julkaistun tiedon eroja. Jos tieto on julkista, ei se automaattisesti tarkoita sitä, että tiedon voisi julkistaa. Julkisen tiedon esille hakeminen vaatii tiedonhakijalta aktiivisia toimia, kun taas julkaistu tieto on aktiivisesti ja passiivisesti kaikkien saatavilla.<sup>161</sup>

Tietosuojavaltuutetun ohjaus dnro 98/41/2007 koskee ammattipätevyyttä koskevien rekisterin tietojen julkaiseminen internetissä hakupalveluna. Ratkaisu havainnollistaa sitä, miten julkisuuslain mukainen julkinen tieto ja tietojen julkistaminen avoimessa tietoverkossa voidaan helposti sekoittaa keskenään.

Tapauksessa X valvontaviranomainen vetosi siihen, että rekisteri on lailla säädetty lailla julkiseksi, jokaisella on oikeus saada tieto ko. rekisteristä ja tietojen luovuttamisesta on säädetty laissa. Rekisteristä pyydetään tietoja jatkuvasti eri tahojen toimesta.

---

<sup>158</sup> Konstari; Wallin 2000, s. 29.

<sup>159</sup> Mäenpää 2008, s.5 ja s.8-9.

<sup>160</sup> Mäenpään mukaan keskeistä ei ole yksittäinen viranomaisen hallussa oleva asiakirja tai siinä oleva tieto sinänsä, vaan ”viranomaisen hallussa oleva tieto hyödyntämättömänä, mutta potentiaalisen arvokkaana tietovarantona, joka soveltuu jalostuksen ja vaihdannan kohteeksi”, Mäenpää 2008, s.9.

<sup>161</sup> Neuvonen 2013, s.146.

Helpoin ja kustannustehokkain ratkaisu oli toteuttaa ammattipätevyysrekisterin tietojen haku internetpalveluna. Hakupalvelu oli poistettu käytöstä, kun epäily rekisterin tietojen julkaisemisen lainmukaisuudesta oli tullut X valvontaviranomaisen tietoon.

Ohjauksessaan tietosuojavaltuutettu katsoo, että henkilötietojen vieminen avoimeen tietoverkkoon on henkilötietojen sähköistä luovuttamista ja luovutuksensaajia ovat kaikki kyseisen sivuston käyttäjät. Jotta viranomainen voi luovuttaa sähköisesti henkilötietoja, on luovuttamiselle oltava laissa säädetty peruste. Rekisteröidyn nimenomainen suostumus voi oikeuttaa tietojen julkaisemisen, jos se on muuten tarpeellista ja asianmukaisesti perusteltua rekisterinpitäjän toiminnan kannalta. Lisäksi nimenomainen lainsäädännös voi oikeuttaa tietojen julkaisemisen. ”Oikeutta saada tietoja” on tietosuojavaltuutetun käsityksen mukaan vakiintuneesti tulkittava siten, että se kattaa oikeuden saada tietoja pyynnöstä.<sup>162</sup>

Toisenlaiseen lopputulokseen on päädytty terveydenhuollon ammattihenkilöitä koskevassa tietopalvelu JulkiTerhikissä, jossa on saatavilla hakupalveluna perustiedot terveydenhuollon ammattihenkilöistä. Hakupalvelun tarkoituksena on muun muassa lisätä potilasturvallisuutta.<sup>163</sup>

Julkisuuslain 20 §:ssä säädetään viranomaisen velvollisuudesta tuottaa ja jakaa tietoa. Pykälässä korostetaan viranomaisen velvollisuutta edistää tiedon saamista toiminnastaan julkaisu- ja tiedotustoiminnan avulla sekä käyttämällä sellaisia tiedonjakelukanavia, joiden avulla kansalaiset voivat helposti saada tietoa. Säännöksen tarkoituksena on tehostaa julkisuusperiaatteen toteutumista ja viranomaisen aktiivista asemaa tiedon tuottajana ja jakelijana sekä turvata yksilöiden ja yhteisöjen tiedonsaanti heidän oikeuksiinsa ja velvollisuuksiinsa liittyvissä asioissa. Kun kyse on viranomaisesta, jonka käsittelemät asiat ovat pääsääntöisesti salassa pidettäviä, on viranomaisella laajempi velvollisuus tuottaa esimerkiksi erilaisia tilastoja ja päätöksentekoa kuvaavia aineistoja. Tietojen jakelun osalta viranomaisen on huolehdittava siitä, että keskeiset asiakirjat ovat helposti saatavilla erilaisissa tiedonjakelukanavissa.<sup>164</sup>

Julkisuuslain 21 §:n mukaan ”viranomainen voi pyynnöstä tuottaa ja luovuttaa eri käyttötarkoituksia varten digitaalisessa muodossa olevan tietoaineiston, jos tietoai-

---

<sup>162</sup> Ohjaus saatavilla osoitteessa:

<http://www.tietosuoja.fi/fi/index/ratkaisut/ammattipatevyttakoskevanrekisterintieto.html>.

<sup>163</sup> JulkiTerhikkiä koskeva lehdistötiedote saatavissa:

[http://www.valvira.fi/valvira/lehdistotiedotteet/terveydenhuollon\\_ammattihenkilorekisteri\\_terhikin\\_internet-hakupalvelu\\_avautuu](http://www.valvira.fi/valvira/lehdistotiedotteet/terveydenhuollon_ammattihenkilorekisteri_terhikin_internet-hakupalvelu_avautuu).

<sup>164</sup> HE 30/1998 vp., s. 111–112.

neiston luovuttaminen ei sen muodostamisessa käytettyjen hakuperusteiden, tiedon määrän tai laadun taikka tietoaaineistojen käyttötarkoituksen vuoksi ole vastoin sitä, mitä asiakirjan salassapidosta ja henkilötietojen suojasta säädetään”. Julkisuuslain 21 §:n mahdollistaa julkisuusperiaatteesta erillisen mahdollisuuden tiedonsaantiin ja kaupalliseen hyödyntämiseen.<sup>165</sup> Tyypillistä on, että viranomaisen yhdistää sen hallussa olevia sähköisiä rekistereitä esimerkiksi markkinointi- tai tutkimustarkoitukseen.<sup>166</sup>

Eri käyttötarkoituksia varten digitaalisessa muodossa olevat tietoaaineistot eivät muodosta julkisuusperiaatteen kohteena olevaa julkisuuslain 5 §:ssä tarkoitettua asiakirjaa. Viranomaisella ei ole velvollisuutta tuottaa ja luovuttaa julkisuuslain 21 §:ssä tarkoitettuja tietoaaineistoja. Tietoaaineistoja ei saa luovuttaa, jos tietojen luovuttaminen vaarantaa tietojen salassapidon tai henkilötietojen suojaa (JulkL 21 §).

Julkisuusperiaatteen mukaisesta tiedonsaantioikeudesta on erotettava asianosaisen oikeus saada tietoa myös salassa pidettävästä asiakirjasta (JulkL 11 §), omien tietojen tiedonsaantioikeuden (JulkL 12 §) ja henkilötietolain 26-28 §:ssä säädetty tarkastusoikeus henkilörekisteriin tallennettuihin tietoihin. Asianosaisen tiedonsaantioikeuden tarkoituksena on taata oikeusturva itseään koskevan asian hallinnollisessa käsittelyssä.

Julkisuuslain 29 §:n 2 momentissa säädetään henkilötietojen luovuttamisesta toiselle viranomaiselle teknisen käyttöyhteyden välityksellä. Tämä on mahdollista, jos toisen viranomaisen on otettava nämä tiedot laissa säädetyn velvollisuuden perusteella huomioon päätöksenteossa.

Julkisuuden vastakohtana viranomaisten asiakirjojen osalta on tietojen salassapito. Julkisuuslain salassapitosäännösten (JulkL 24 §) ohella erityislainsäädäntöön on kirjattu tietojen salassapitoa koskevia erityisiä säännöksiä. Julkisuuslain nojalla salassa pidettävien asiakirjojen lista sisältää 36 kohtaa. Salassapidolla pyritään suojaamaan sekä yleisiä että yksityisiä intressejä.

---

<sup>165</sup> Konstari, Wallin 2000, s.80–81 ja s.304.

<sup>166</sup> Mäenpää 2008, s. 228.

## 4.5 Hyvä tiedonhallintatapa

Julkisuuslakia säädettäessä 1990-luvun lopussa tavoitteena oli tuoda hyvä tiedonhallintatapa osaksi viranomaisten toimintaa. Viranomaisten velvollisuutena on luoda, toteuttaa ja edistää hyvää ja avointa tiedonhallintatapaa, jonka tarkoituksena on tiedon ja asiakirjojen korkean laadun säilyttäminen koko informaation elinkaaren ajan.<sup>167</sup>

Viranomaisen hallussa olevan tiedon saatavuuteen ja käytettävyyteen kohdistuvat vaatimukset korostavat hyvän tiedonhallintatavan vaikutusta viranomaisen arkipäiväisessä toiminnassa. Julkisen sektorin tietojen uudelleenkäytön kannalta hyvä tiedonhallintatapa on keskeisessä asemassa arvioitaessa sitä, toteutuuko julkisen tiedon saatavuuteen kohdistuvat vaatimukset konkreettisesti ja viranomaiskohtaisesti.

Hyvän tiedonhallintatavan luominen ei ole kertaluonteinen prosessi, vaan viranomaisen on kiinnitettävä siihen jatkuvasti huomiota tiedon elinkaarimallin mukaisesti. Hyvällä tiedonhallintatavalla ei ole merkitystä vain viranomaisen omassa toiminnassa, vaan viranomaisen on tunnistettava sen tietovarantoihin kohdistuvat ulkopuoliset tarpeet ja intressit.<sup>168</sup> Hyvään tiedonhallintatapaan kuuluu myös viranomaisen velvollisuus ja kyky tunnistaa tietovarantoihin ja niiden saatavuuteen, käytettävyyteen, suojaukseen ja laatuun liittyvät uhat ja riskit.<sup>169</sup>

Hyvä tiedonhallintatapa edellyttää viranomaisia huolehtimaan asiakirjojen, tietojen ja tietojärjestelmien saatavuudesta, käytettävyydestä ja suojaamisesta (JulkL 18.1 §). Hyvän tiedonhallintatavan keskeinen tavoite on tiedon laadun säilyttäminen ja julkisuusperiaatteen vaivaton toteuttaminen, jotka voidaan saavuttaa suunnittelemalla huolellisesti tietojen käsittelyyn liittyvät prosessit.<sup>170</sup>

Asiakirjojen ja julkisen tiedon *saatavuudella* tarkoitetaan sitä, että jokaisella on todellisuudessa mahdollisuus saada tieto julkisesta asiakirjasta, joten tiedon on oltava helposti ja ilman kohtuutonta vaivaa löydettävissä.<sup>171</sup> Tietojen saatavuus on julkisuusperiaatteen toteutumisen edellytys.<sup>172</sup> Julkisen sektorin tietojen uudelleenkäytettävyyden näkökulmasta, sellaiset julkisen sektorin tiedot on saatattava jokaisen saataville, joihin ei nimenomaisesti kohdistu lainsäädännöllisiä rajoituksia.

---

<sup>167</sup> Mäenpää 2008, s. 251.

<sup>168</sup> Konstari, Wallin 2000, s.307.

<sup>169</sup> Konstari, Wallin 2000 s.308.

<sup>170</sup> Ahvenainen, Rätty 1999, s.115. Konstari, Wallin 2000, s. 304.

<sup>171</sup> Mäenpää 2008, s.252.

<sup>172</sup> Ibid.

Asiakirjojen ja tiedon *käytettävyydellä* on merkitystä erityisesti viranomaisen omassa toiminnassa ja siihen sisältyy vaatimus viranomaisen asiakirja- ja tietohallinnon toimivuudesta. Käytettävyydellä tarkoitetaan sitä, että jokaisella on mahdollisuus saada tietoa siitä, mitä asiakirjoja ja tietoa viranomaisen toiminnassa muodostuu. Jotta vaatimus käytettävyydestä toteutuisi, viranomaisella on oltava käytössään ajantasaiset ja oikeat tiedot sen hallussa olevista tietovarannoista.

Julkisen tiedon uudelleenkäytön kannalta on olennaista tietää, mitä tietovarantoja viranomaisella on. Näin ollen tiedon potentiaalinen käyttäjä voi myös pyytää viranomaisesta arvioimaan tietovarantojen uudelleenkäytettävyyttä myös sellaisten tietovarantojen osalta, joita ei ole avattu uudelleenkäytettäväksi. Tietojen ja asiakirjojen käytettävyydellä varmistetaan myös asianosaisen oikeusturvan kannalta merkityksellinen asioiden viivytyksetön käsittely.<sup>173</sup>

Viranomaisella on velvollisuus huolehtia siitä, että sen hallussa olevat tiedot ja asiakirjat ovat helposti *löydettävissä* esimerkiksi diaarin tai erilaisten asianhallintajärjestelmien avulla. Tätä varten viranomaisen on ylläpidettävä luetteloa sen käsiteltäväksi annetuista ja otetuista sekä ratkaistuista ja käsitellyistä asioista (Julkl 18.1 §:n 1 kohta).

Asiakirjojen ja tiedon *ehydeillä* tarkoitetaan vaatimusta viranomaisen hallussa olevan tiedon ja asiakirjojen oikeellisuudesta ja aitoudesta koko tiedon elinkaaren ajan. Tähän liittyy kiinteästi vaatimus tietoturvallisuudesta ja vaatimus säilyttää tiedot ja asiakirjat siinä muodossa kuin se on alun perin talletettu. Viranomaisella on velvollisuus varmistua siitä, että sen tietojärjestelmät toimivat virheettömästi.<sup>174</sup> Julkisuuslain tehtävänä on taata viranomaisten tiedon korkea laatu yksilöiden oikeusturvan toteuttamiseksi ja yhteiskunnallisen päätöksen teon tukemiseksi.<sup>175</sup> Viranomaisten on taattava muun muassa perusrekisterien julkinen luotettavuus.<sup>176</sup>

Asiakirjojen ja tiedon *suojaamisella* tarkoitetaan muun muassa sitä, että viranomaisen soveltaa oikein salassapitosäännöksiä ja ottaa huomioon henkilötietojen käsittelyä koskevat velvoitteet esimerkiksi henkilötietojen huolellisesta käsittelystä, tietoturvas- ta ja tietojen suojaamisesta asianmukaisella tavalla (myös HetiL 5 § ja 32 §). Suhteellisuusperiaatteen mukaisesti suojaamisvelvoite on korostettu silloin, kun käsitellään

---

<sup>173</sup> Mäenpää 2008, s. 252.

<sup>174</sup> Ibid.

<sup>175</sup> HE 30/1998 vp., s. 48.

<sup>176</sup> Mäenpää 2008, s.253.

arkaluonteisia tai salassa pidettäviä tietoja.<sup>177</sup> Hyvään tiedonhallintatapaan ja henkilötietolain tietojen suojaamisvelvoitteeseen kuuluu myös henkilöstön kouluttaminen niin, että he osaavat soveltaa oikein yksityisyyden ja yleisen edun suojaamiseksi tarkoitettuja säännöksiä (JulkL 18.1 §:n 5 kohta ja HetiL 32 §).<sup>178</sup>

Hyvään tiedonhallintatapaan sisältyy vaatimus pääsääntöisesti laatia ja pitää saatavilla kuvaukset viranomaisen ylläpitämistä tietojärjestelmistä ja niissä saatavilla olevista julkisista tiedoista (JulkL 18.1 §:n 2 kohta). Tietojärjestelmien kuvauksessa on otettava huomioon julkisuuslain 24 §:n mukaiset salassapitosäännökset. Kuvauksesta on myös käytävä ilmi, mitä henkilörekistereitä tietojärjestelmään sisältyy.<sup>179</sup> Viranomaisella on velvollisuus ottaa huomioon tietojen ja asiakirjojen julkisuus ja salassapito, kun viranomaisen tietohallintoa kehitetään ja valmistellaan lainsäädännöllisiä ja hallinnollisia uudistuksia. Samanaikaisesti on otettava huomioon tietojen laadun säilyminen ja tietojen suojaaminen sekä tiedollisten oikeuksien toteutuminen (JulkL 18.1 §:n 3 kohta).

Viranomaisen velvollisuutena on suunnitella ja käytännössä toteuttaa tietohallinto siten, että julkisuusperiaate on vaivattomasti toteutettavissa (JulkL 18.1 §:n 4 kohta). Jotta julkisuus toteutuu vaivattomasti, edellytetään viranomaiselta menetelmällisiä keinoja hyvän tiedonhallintatavan toteuttamiseksi. Keinoja ovat esimerkiksi asiakirjojen selkeä arkistointi ja viranomaisen verkkosivujen toimivuus.<sup>180</sup>

Julkisuuslain 18 §:n 2 momentissa säädettiin siitä, että hyvän tiedonhallintatavan toteutumisesta annetaan tarkempia säännöksiä valtioneuvoston asetuksella. Asetuksella voitiin myös säätää velvollisuudesta osallistua useammalle viranomaiselle yhteiseen yleisen tietoverkon avulla toteutettavaan asiakaspalvelujärjestelmään taikka yleisesti merkittävien asioiden valmistelun julkisuutta edistävien rekisterien ylläpitoon (JulkL 18.2 §:n 2 kohta). Tällaista asetusta ei kuitenkaan ole annettu ja kyseinen momentti kumottiin lailla julkisen tietohallinnon ohjauksesta (634/2011).<sup>181</sup> Hyvän tiedonhallintatavan toteuttamisesta säädetään tarkemmin asetuksella viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999).

---

<sup>177</sup> Mäenpää 2008, s. 207, Ahvenainen, Rätty, 1999 s. 115–116.

<sup>178</sup> Mäenpää 2008, s. 207, Voutilainen 2009, s. 166.

<sup>179</sup> Tietosuojavaltuutetun opas: ”Henkilötietojen luovuttaminen viranomaisten henkilörekistereistä”, Päivitetty 27.7.2010, s. 7.

<sup>180</sup> Mäenpää 2008, s. 255.

<sup>181</sup> HE 246/2010 vp., s. 4.

## 4.6 Julkisuuden ja yksityisyyden välinen suhde

Viranomaisten tietoon kohdistuva julkisuusperiaate koskee nimenomaisesti viranomaisen hallussa olevan tiedon julkisuutta, ei yksittäisten kansalaisten koskevia henkilötietojen ja yksityiselämän julkisuutta suhteessa yhteiskunnan eri toimijoihin. Henkilötietolain yleisvelvoitteita ja periaatteita sovelletaan viranomaisen harjoittamaan henkilötietojen käsittelyyn. Henkilötietolain ja julkisuuslain lisäksi henkilötietojen luovuttamista koskevia erityyssäännöksiä sisältyy useaan erityislakiin. Henkilötietolain 8 §:n 4 momentin mukaan ”oikeudesta saada tieto ja muusta henkilötietojen luovuttamisesta viranomaisten henkilörekistereistä, on voimassa mitä viranomaisen asiakirjojen julkisuudesta säädetään”. Vaikka julkisuuslaki ja henkilötietolaki ovat molemmat yleislakeja, sovelletaan julkisuuslakia erityislakina suhteessa henkilötietolakiin silloin, kun viranomainen luovuttaa henkilötietoja.<sup>182</sup>

Henkilötietojen suojan ja julkisuuden suhde näkyy konkreettisesti henkilötietojen luovuttamista koskevan sääntelyn osalta (HetiL 8.4 § ja JulkiL 13 § ja 16 §). Kun viranomaisen hallussa olevia tietoja pyydetään julkisuuslain 16 §:n 1 momentin nojalla nähtäväksi, jäljennettäväksi tai kuultavaksi julkisuuslain 13 §:n 1 momentin mukaan pyytäjän ei tarvitse perustella pyyntöään tai ilmaista henkilöllisyyttään. Jos tietoja pyydetään luovutettavaksi viranomaisen henkilörekisteristä, henkilötietolain säännöksistä johtuen, on tietojen käyttötarkoitus selvitettävä sekä tarvittaessa myös selvitys siitä, miten tietojen suojaus on järjestetty (JulkiL 13.2 § ja JulkiL 16.3 §).

Henkilötietojen uudelleenkäytön osalta keskeinen kysymys liittyy siihen, voiko viranomainen luovuttaa henkilötietoja uudelleenkäytettäväksi. Perustuslain 10 §:n 1 momentin mukaan henkilötietojen käsittelystä on säädettävä tarkemmin lailla. Lakisääteisyysvaatimuksesta johtuen henkilötietojen luovuttamisesta on aina säädettävä lain tasoisella säännöksellä. Jos henkilötietoja on passiivisesti saatavilla uudelleenkäytettäväksi avoimessa tietoverkossa, esimerkiksi julkisuuslain mukainen vaatimus tietojen käyttötarkoituksen selvittämisestä ei täyty. Koska henkilötietojen luovuttaja vastaa tietojen luovutuksen lainmukaisuudesta kokonaisuudessaan, on viranomaisen myös selvitettävä, millä perusteella tietojen luovutuksen saaja aikoo käsitellä tietoja

---

<sup>182</sup> Saarenpää 2012a, s. 361.



ja ennen kaikkea, että tietojen käsittely vaikuttaa kokonaisuutena arvostellen lainmukaiselta.

Julkisuuslain nojalla määräytyvät viranomaisen oikeus henkilötietojen ja muiden tietojen luovutukseen ja luovutuksen perusteet, tietojen salassapito ja poikkeukset tietojen salassapidosta (JulkL 24 §, 26 §), tietojen luovuttamiseen liittyvät menettelyt ja antamistavat (JulkiL 13.1 §, 13.2 §, 16.1 § ja 16.3 §), viranomaisen velvollisuus tuottaa ja jakaa tietoa (JulkL 20 §), viranomaisen oikeus tuottaa tietoaineistoja (21 §) ja edellytykset teknisen käyttöyhteyden avaamiselle (JulkiL 29.3).

Julkisuuslain 13 §:ssä ja 16 §:ssä säädetään erilaisesta menettelystä riippuen siitä, pyydetäänkö henkilötietoja nähtäväksi, jäljennettäväksi tai kuunneltavaksi (JulkL 13.1 § ja 16.1 §) vai luovutettavaksi (JulkL 13.2 § ja 16.3 §). Jos viranomainen luovuttaa sähköisesti henkilötietoja, sovelletaan tietojen luovutukseen julkisuuslain 16 §:n 3 momenttia, jonka mukaan ”julkisesta henkilörekisteristä voidaan luovuttaa pyytäjälle henkilötietoja otteina, kopion tai tiedot sähköisessä muodossa, jos luovutuksensaajalla on henkilötietojen suoja koskevien säännösten mukaan oikeus tallettaa ja käyttää tällaisia henkilötietoja. Suoramarkkinointiin tietoja voidaan luovuttaa ainoastaan asianomaisen suostumuksella tai erityislainsäännöksen nojalla” (JulkL 16.3 §).<sup>183</sup> Viranomaisen on pyydettävä selvitys muun muassa tietojen käyttötarkoituksesta ja muista tietojen luovuttamiseen liittyvistä seikoista, esimerkiksi siitä miten tietojen suojaus on järjestetty (JulkL 13.2 §).

Julkisen sektorin tietojen avaamisen ja uudelleenkäytön näkökulmasta, henkilötietojen saattaminen yleisesti saataville avoimeen verkkoon on henkilötietojen sähköistä luovuttamista ja henkilötietojen automaattista käsittelyä.<sup>184</sup> Viranomainen ei voi hallita tai kontrolloida henkilötietojen käsittelyä eli sitä, miten ja mihin tarkoitukseen tietoja käsitellään jatkossa kaikkien mahdollisten käyttäjien toimesta.

Viranomainen voi luovuttaa henkilötietoja rekisteröidyn nimenomaisen suostumuksen tai luovuttamiseen oikeuttavan lainsäännöksen nojalla. Suostumuksen käyttäminen henkilötietojen käsittelyn perusteena uudelleenkäyttötilanteissa on jokseenkin ongelmallinen, mutta henkilön tiedollisen itsemääräämisoikeuden kannalta riittävä peruste.

---

<sup>183</sup> Esimerkiksi väestötietojärjestelmästä tietoja voidaan luovuttaa ellei rekisteröity ole kieltänyt tietojen luovuttamista (opt-out).

<sup>184</sup> Tietosuojavaltuutetun ohjaus dnro 98/41/2007.

Rekisteröidyn tietoisuuden suostumuksen käyttämiseen tietojen käsittelyn perusteena liittyy periaatteellisia ongelmia, joista keskeisin on erilaisten käytössä olevien tietosuojalausekkeiden (*privacy policies*) vaikeaselkoisuus.<sup>185</sup> Kansallisen lainsäädännön nojalla henkilötietoja voidaan julkaista avoimessa verkossa asianomaisen suostumuksen perusteella. Henkilötietolain 3 §:n 1 momentin 7 kohdan mukaan suostumuksella tarkoitetaan ”vapaaehtoista, yksilöityä ja tietoista tahdonilmausta, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn”.<sup>186</sup>

Ehdotuksessa yleiseksi tietosuojasetukseksi 7 artiklassa halutaan selkeyttää olosuhteita ja edellytyksiä, joiden perusteella suostumus muodostaisi pätevän oikeusperustan henkilötietojen lainmukaiselle käsittelylle. Ensinnäkin rekisterinpitäjälle asetettaisiin nimenomainen todistustaakka suostumuksen olemassa olosta. Toiseksi, jos rekisteröidyn on annettava suostumus kirjallisessa ilmoituksessa, joka koskee myös muita asioita, suostumuksen antamista koskeva vaatimus on esitettävä selkeästi erillään näistä muista asioista. Kolmanneksi säädettäisiin nimenomaisesti siitä, että rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa. Suostumuksen peruuttaminen ei kuitenkaan vaikuttaisi suostumuksen perusteella ennen sen peruuttamista suoritettujen käsittelyjen lainmukaisuuteen. Neljänneksi suostumus ei muodostaisi oikeusperustaa henkilötietojen käsittelylle, jos rekisteröidyn ja rekisterinpitäjän välillä on selkeä epäsuhta, jolloin voidaan kyseenalaistaa suostumuksen vapaaehtoisuus.<sup>187</sup>

Jotta suostumus muodostaisi lainmukaisen käsittelyn perusteen, on rekisteröidylle annettava riittävä informaatio suostumuksen perusteella tapahtuvasta henkilötietojen käsittelystä. Henkilötietolain 24 § velvoittaa rekisterinpitäjää yleisesti informoimaan rekisteröityjä henkilötietojen käsittelystä. Suostumusta pyydetessä rekisteröidylle on annettava tiedot ainakin siitä, kuka hänen tietojansa käsittelee, mihin tarkoitukseen, mitä tietoja kerätään, luovutetaanko tietoja, siirretäänkö tietoja kolmansiin maihin ja kauan tietoja säilytetään. Jos henkilötietoja luovutetaan, on suostumusta pyydetessä annettava tieto siitä, kenelle tietoja luovutetaan, mitä tietoja luovutetaan ja mihin käyttötarkoituksiin. Henkilötietolain 24 § velvoittaa rekisterinpitäjää lisäksi informoimaan rekisteröityjä heidän tietojenkäsittelyyn liittyvistä oikeuksista.

Suostumus ei syrjäytä henkilötietojen käsittelyn tarpeellisuusvaatimusta (HetiL 9.1 §). Tarpeellisuusvaatimusta on arvioitava objektiivisesti niin, että minkälainen käsit-

---

<sup>185</sup> Rubinstein 2013, s.2.

<sup>186</sup> Myös henkilötietodirektiivin 2 artiklan h kohta.

<sup>187</sup> COM (2012) 11 final.

tely on yleisesti arvioiden tarpeellista ja asianmukaista tietojenkäsittelyntarkoituksen kannalta ennalta määritellyn tarkoituksen saavuttamiseksi.<sup>188</sup> Uudelleenkäyttötilanteissa on tyypillistä muun muassa, että ei tiedetä kenelle tietoja luovutetaan ja, että tiedot luovutetaan ennalta määrittelemättömiin tarkoituksiin. Suostumuksen peruuttaminen on ongelmallista, jos tietoja luovuttanut viranomainen ei pysty tavoittamaan kaikkia tahoja, jotka käsittelevät henkilötietoja. Jos suostumus pyydetään lisensoituun tietojen luovutukseen tiettyjen ehtojen vallitessa, suostumuksen pätevyys laillisena käsittelyn perusteena on todennäköisempää.

PSI-direktiivin soveltamisalaan eivät kuulu saatavilla olevien asiakirjojen osat, jotka ovat ristiriidassa henkilötietojen suojaa koskevan lainsäädännön kanssa (1 artikla c alakohta). Näin ollen PSI-direktiivissä vahvistetaan periaate, jonka mukaan vaikka henkilötiedot olisivat saatavilla asiakirjojen saatavuutta koskevan lainsäädännön nojalla, voidaan tietojen julkaisemista ja saattamista uudelleenkäytettäväksi rajoittaa henkilötietojen suojaa koskevien seikkojen perusteella.

Julkisuuslain ja erityislainsäädännön salassapitosäännöksin suojataan yksityiselämän piiriä. Julkisuuslain nojalla salassa pidettäviä yksityisyyden suojan piiriin kuuluvia viranomaisen asiakirjoja ovat asiakirjat, jotka sisältävät tietoja henkilön sosiaalihuollon tarpeesta, terveydenhuollosta ja tiedot henkilön seksuaalisesta käyttäytymisestä ja suuntautumisesta (JulkL 24.1 §:n 25 kohta) sekä tietoja henkilön perhe-elämästä, elintavoista, vapaa-ajan harrastuksista ja muista niihin verrattavista henkilökohtaisista oloista ja tiedot henkilön poliittisesta vakaumuksesta, yksityiselämän piirissä esittämistä mielipiteistä ja osallistumisesta yhdistystoimintaan (JulkL 24.1 §:n 32 kohta). Yksityisyyteen, elintapoihin ja henkilökohtaisiin oloihin liittyvien tietojen salassapito ei ole harkinnanvaraista, vaan tiedot ovat salassa pidettäviä riippumatta siitä aiheutuuko tietojen luovuttamisesta haitallisia tai vahingollisia seurauksia rekisteröidylle.<sup>189</sup>

Psykologisia soveltuvuusarviointeja ja muita henkilökohtaisia ominaisuuksien arviointia koskevat tiedot ovat salassa pidettäviä, kuten myös oikeuspsykiatrisesta mielentilatutkimuksesta, nuoresta rikoksenteijästä tehdystä henkilötutkinnasta ja yhdyskuntapalvelun soveltuvuus selvitystä saadut tiedot ja tulokset (JulkL 24.1 §:n 29 ja 27 kohta).

---

<sup>188</sup> Lisätietoja henkilötietojen käsittelystä suostumuksen perusteella on saatavilla esimerkiksi tietosuojavaltuutetun toimiston laatimasta ohjeesta: ”Henkilötietojen käsittely suostumuksen perusteella”.

<sup>189</sup> Mäenpää 2008, s.286.

Henkilön taloudellista asemaa koskevat tiedot ovat yleensä salassa pidettäviä, jos tietojen perusteella voi saada laajempaa tietoa henkilön kokonaistaloudellisesta asemasta. Näin ollen salassa pidettäviä ovat tiedot henkilön vuosituloista ja kokonaisvarallisuudesta, tuen tai etuuden perustana olevista tuloista ja varallisuudesta tai muuten henkilön taloudellista asemaa kuvaavat tiedot. Salassa pidettäviä ovat myös tiedot luonnollisesta henkilöstä ulosottovelallisena (JulkL 24.1 §:n 23 kohta). Yksittäinen taloudellinen tieto, kuten yksittäistä tuloa tai omistusta koskeva tieto, ei ole salassa pidettävä.<sup>190</sup> Julkishallinnonpalveluksessa olevan palkkatietojen julkisuudesta säädetään nimikirjalain (1010/1989) mukaan, jolloin viranomaisen palkkaustiedot ovat julkisia.

Henkilön yhteystiedoista salassa pidettäviä ovat salainen puhelinnumero sekä matkaviestimen paikkatietoja koskevat tiedot (JulkL 24.1 §:n 31 kohta). Pakolaista ja turvapaikan hakijaa koskevat tiedot ovat pääsääntöisesti salassa pidettäviä (JulkL 24.1 §:n 24 kohta). Julkisuuslain rekisteröidyn itsemääräämisoikeutta korostava säännös sisältyy lain 26 §:n 1 momentin 2 kohtaan, jonka mukaan viranomaisen voi antaa tiedon salassa pidettävästä asiakirjasta, jos se, jonka etujen suojaamiseksi salassapitovelvollisuudesta on säädetty antaa siihen suostumuksensa.

Vaikka julkisuuslain nojalla yksityisyyteen, elintapoihin ja henkilökohtaisiin oloihin viittaavat tiedot on säädetty ehdottaman salassa pidettäväksi, tulkinnanvaraisuutta sisältävy juuri ”yksityisyyden, elintapojen ja henkilökohtaisten olojen” piirin hahmotamiseen.<sup>191</sup>

Korkein hallinto-oikeus on ratkaisussaan 20.5.2014 KHO:2014:83 katsonut, että lakisääteisiä vakuutuksia käsittelevän vakuutusyhtiön asiakirjoihin sisältynyt tieto julkista valtaa käyttävistä asiantuntija lääkäreiden henkilöllisyydestä, erikoisaloista tai erityspätevyyksistään, eivät olleet julkisuuslain 24 §:n 1 momentin 32 kohdassa tarkoitettuja henkilökohtaisia oloja kuvaavia salassa pidettäviä tietoja. Tuomioistuin katsoo, että tieto siitä, ketkä käyttävät julkista valtaa kuuluu julkisuusperiaatteen ydinalueeseen.

Apulaisoikeuskanslerin päätös dnro OKV/1318/2007 koskee kärjäoikeuden rikosasiassa antaman tuomion julkaisemista kärjäoikeuden verkkosivuilla. Kärjäoikeus oli julkaisut verkkosivuillaan tuomion, josta kävi ilmi muun muassa vastaajien nimet, henkilötunnukset ja osoitetiedot. Henkilötietolain 11 §:n 3 momentin nojalla rikollista

---

<sup>190</sup> Mäenpää 2008, s.289.

<sup>191</sup> Mäenpää 2008, s.286.

tekoa, rangaistusta tai muuta rikoksen seuraamusta koskevat tiedot ovat arkaluonteisia, eikä niitä saa käsitellä ilman henkilötietolain 12 §:n mukaista erityistä perustetta. Käräjäoikeus oli vedonnut oikeudellisen perusteen tueksi muun muassa viranomaisen tiedottamisvelvollisuutta koskevaan julkisuuslain 20 §:ään.

Apulaisoikeuskansleri on pyytänyt asiassa lausuntoa tietosuojavaltuutetulta. Tietosuojavaltuutettu toteaa lausunnossaan muun muassa, että julkisuuslain tiedon luovuttamista koskevia säännöksiä tulisi soveltaa tilanteissa, joissa tiedon luovuttamista on edeltänyt aktiivinen pyyntö. Tietosuojavaltuutetun mukaan henkilötietolain säännöksiä on sovellettava täydentävästi silloin, kun on kyse julkisuuslain 20 §:n mukaisesta tiedottamisesta. Tietosuojavaltuutettu katsoo, että tällöin ei ole kyse henkilötietolain 8 §:n 4 momentin tarkoittamasta julkisuuslain sääntelemästä henkilötiedon antamisesta tai luovuttamisesta. Tuomion pitäminen verkkosivuilla on sellaisenaan henkilötietojen automaattista käsittelyä, johon voidaan soveltaa henkilötietolakia.

Apulaisoikeuskansleri kyseenalaistaa päätöksensä perusteluissa sen, että ”[...]voidaanko julkisuuslain 20 §:ään perustuvaa tiedonjakovelvoitetta pitää sellaisena viranomaisen laissa säädettyinä tehtävänä, joka oikeuttaa henkilötietolain 8 §:n 4 momentin kohdan mukaiseen henkilötietojen käsittelyyn, henkilötietolain 12 §:n 5 kohdan mukaiseen arkaluontoisten henkilötietojen käsittelyyn tai henkilötietolain 13 §:n 1 momentin mukaiseen henkilötunnuksen käsittelyyn”. Apulaisoikeuskansleri kiinnittää käräjäoikeuden huomiota henkilötietolain soveltamiseen verkossa julkaistavien tietojen osalta, mutta ei ota tarkemmin kantaa julkisuuslain ja henkilötietolain väliseen suhteeseen. Koska yksityisyyttä ja yksityiselämän suoja koskevat tiedot ovat ehdottomasti salassa pidettäviä, ei julkisuuslain 20 §:n tiedottamisvelvollisuutta koskeva säännös voi mielestäni syrjäyttää tietojen salassapitoa. Tiedon julkaisemiselle tulisi olla jokin muu laissa säädetty peruste.

Yhteisön tasolla yksityiselämän ja henkilötietojen suojan sekä julkisuuden välistä suhdetta on käsitelty esimerkiksi Euroopan unionin tuomioistuimen 29.10.2010 antamassa ratkaisussa C-28/08 komissio v. Bavarian Lager. Asiassa tuomioistuimen ratkaistavana oli se, oliko komissio velvollinen luovuttamaan asiakirjoissa (kokouspöytäkirjoissa) esiintyneiden viiden henkilön nimen asiakirjapyynnön yhteydessä asiakirjojen saatavuutta koskevan asetuksen (EY) N:o 1049/2001 ja tietosuojasetuksen EY N:o 45/2001 perusteella. Ratkaisu on merkittävä yhteisön toimielinten asiakirjojen julkisuuden ja henkilötietojen suojan näkökulmasta.

Ratkaisussaan Euroopan unionin tuomioistuin katsoi, että asiakirjojen saatavuutta koskevalla asetuksella ”otetaan käyttöön erillinen ja vaativampi järjestely sellaisen henkilön suojaamiseksi, jonka henkilötiedot saatetaan joissain tapauksissa luovuttaa yleisölle”. Tuomioistuimen mukaan silloin, kun asiakirjojen saatavuutta koskevan asetuksen perusteella pyydetään hakemuksella saada oikeutta tutustua henkilötietoja sisältävään asiakirjaan, asiakirjojen saatavuutta koskevan asetuksen säännökset tulevat kaikilta osin sovellettaviksi.

Tuomioistuimen ratkaisun mukaan komissiolla oli peruste hylätä hakemus, joka koski kyseisen kokouksen täydellistä pöytäkirjaa. Bavarian Lager ei ollut esittänyt laillista ja nimenomaista tarkoitusta eikä minkäänlaisia vakuuttavia argumentteja osoittaakseen tarpeen näiden henkilötietojen luovuttamiselle. Näin ollen komissio ei voinut vertailla asianosaisten eri intressejä tai selvittää, voisiko rekisteröityjen oikeudet edut tietojen luovutuksen vuoksi vaarantua. Komissio oli täyttänyt avoimuusveloitteen luovuttamalla pöytäkirjan, josta viiden henkilön nimet oli poistettu.

## 5. Henkilötietojen suojaan kohdistuvat riskit

### 5.1 Julkinen sektori henkilötietojen julkaisijana

Julkisen sektorin tietovarantojen avaamiseen ja tietojen uudelleenkäytön tarkoituksena on pääsääntöisesti saattaa koko tietovaranto avoimesti saataville, standardoidussa elektronisessa muodossa, kenelle tahansa, maksuttomasti sekä kaikkiin kaupallisiin ja ei-kaupallisiin tarkoituksiin. Avoimen tiedon ohjelmissa on kyse sellaisen julkisen tiedon rajoituksettomasta saatavuudesta, johon ei kohdistu lainsäädännöllisiä rajoituksia.

Koska julkisen sektorin tietovarannot sisältävät myös huomattavan määrän henkilötietoja, aiheuttaa tietojen tehostettu saatavuus riskejä henkilötietojen suojan ja viime kädessä yksityisyyden suojan kannalta. Perustuslain 10 §:n 1 momentin lainsäätämivelvoitteesta johtuu, että henkilötietoja ei voida käsitellä ilman laissa säädettyä perustetta. Perustuslain 2 §:n 3 momentin oikeusvaltioperusteesta johtuen julkisen vallan käytön on perustuttava lakiin. Kun viranomaiset asettavat tietoja uudelleenkäytettäväksi, niiden on tunnistettava ja otettava asianmukaisesti huomioon mahdolliset rekisteröityjen yksityisyydensuojaan kohdistuvat uhat ja riskit.

Tärkeitä henkilötietojen käsittelyyn liittyviä sääntelykohteita ovat muun muassa rekisteröinnin tavoite, rekisteröitävien henkilötietojen sisältö, tietojen säilytys, henkilötietojen käyttötarkoitus sekä tietojen luovutettavuus.<sup>192</sup> Henkilötietojen käsittelyä koskevat keskeiset periaatteet liittyvät käsittelyn perusteeseen, tietojen käsittelyn ja käsiteltävien tietojen tarpeellisuuteen, käyttötarkoitussidonnaisuuteen, tietojen laatuun ja rekisteröidyn oikeuksiin. Periaatteiden toteutuminen olisi hyvin epävarmaa, jos henkilötietoja sisältävät tietovarannot avattaisiin rajoittamattomaan uudelleenkäyttöön.

Julkisen sektorin tietovarannot koostuvat yleensä tiedoista, jotka rekisteröity on lain nojalla velvollinen luovuttamaan viranomaiselle tämän hoitaessa laissa säädettyjä tehtäviä. Jos rekisteröity on lain nojalla velvoitettu antamaan henkilötietonsa rekiste-

---

<sup>192</sup> PeVL 25/1998 vp, s. 2, II. PeVL 12/2002 vp., s 5.

rinpitäjälle, esimerkiksi käyttötarkoituksen myöhempää yhteensopivuusarviointia on tarkasteltava suppeasti.<sup>193</sup>

Tietovarantoja avatessa on otettava huomioon rekisteröityjen oikeutetut odotukset tietojen käsittelylle. Viranomaisen rekisteröityjen oikeuksia kunnioittava tietojenkäsittely on keskeinen tekijä viranomaistoiminnan kohdistuvan luottamuksen kannalta.<sup>194</sup>

Euroopan tietosuojavaltuutettu on komission avoimen datan pakettia ja PSI-direktiivin muutosehdotusta koskevassa lausunnossa kiinnittänyt huomiota siihen, että ehdotuksessa ja direktiivin muutoksessa henkilötietojen suoja pitäisi nostaa tarkemmin esille.<sup>195</sup> Euroopan tietosuojavaltuutetun ehdotuksen mukaisesti muutos direktiiviin lisättiin 1 artiklan cc kohta, jonka mukaan PSI-direktiiviä ei sovelleta ”asiakirjoihin, jotka eivät ole saatavilla tai joiden saatavuutta on rajoitettu asiakirjojen saatavuutta koskevien järjestelmien perusteella henkilötietojen suojaamiseksi ja sellaisten kyseisten järjestelmien perusteella saatavilla olevien asiakirjojen osiin, jotka sisältävän henkilötietoja, joiden uudelleenkäyttö on ristiriidassa yksilöiden suojelusta henkilötietojen käsittelystä annetun lain kanssa”.<sup>196</sup>

Jos asiakirjassa olevat henkilötiedot eivät ole saatavilla kansallisen lainsäädännön perusteella, eivät ne kuulu myöskään PSI-direktiivin soveltamisalaan. Tietosuojatyöryhmä lausunnossaan WP 207 toteaa, että ”tietojen saatavuutta koskevissa järjestelmissä edellytetään tavallisesti tasapainotestiä, jossa verrataan yksityisyyden ja tietosuojasäännöillä suojeltuja etuja avoimuuden tuomiin hyötyihin”.<sup>197</sup> Periaatetta voidaan toteuttaa myös niin, että tietojen saatavuuteen sovelletaan tiettyjä suojatoimia, kuten hakuominaisuuksien ja massalatauksien teknisiä rajoituksia sekä tietojen anonyymisointia.<sup>198</sup>

Asiakirjojen ja viranomaisen hallussa olevien tietojen julkistamista koskeva säännös liittyy kuntalain (365/1995) 29 §:ään, jonka mukaan kunnan on tiedottava asukkailleen kunnassa vireillä olevista asioista, niitä koskevista suunnitelmista, asioiden käsittelystä, tehdyistä ratkaisuksista ja niiden vaikutuksista. Kyseiset asiakirjat ja tiedotteet

---

<sup>193</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.25.

<sup>194</sup> Euroopan tietosuojavaltuutetun avoimen datan pakettia koskeva lausunto 2012, s.5.

<sup>195</sup> Ibid.

<sup>196</sup> Euroopan tietosuojavaltuutetun avoimen datan pakettia koskeva lausunto 2012 s. 7.

<sup>197</sup> Ibid.

<sup>198</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.11.



voivat sisältää henkilötietoja. Kunnan tehokkaan tiedottamisvelvoitteen kannalta on perusteltua, että esimerkiksi kuntien kokouspöytäkirjoja julkaistaan kunnan verkkosivuilla, mutta vain sen ajan, mikä on tarpeellista tiedottamisvelvollisuuden toteuttamiseksi. Jos pöytäkirjat sisältävät arkaluonteisia henkilötietoja, ei niitä voida julkaista. Pöytäkirjan julkaiseminen kunnan verkkosivuilla on henkilötietojen automaattista käsittelyä, johon sovelletaan henkilötietolain säännöksiä.<sup>199</sup>

Apulaisoikeuskanslerin ratkaisu OKA 7.2.2005 koskee kaupunginhallituksen esityslistan ja pöytäkirjan julkaisemista kaupungin verkkosivuilla. Asiakirjoihin oli sisällytynyt erään henkilön kaupunkiin kohdistama korvausvaatimus, jossa oli ilmoitettu kyseisen henkilön nimi ja tilinumero. Ratkaisussaan apulaisoikeuskansleri katsoi, että pankkitilinumero voi olla yksilön elinpiiriin kuuluva julkisuuslain 24 §:n 1 momentin 32 kohdan perusteella salassa pidettävä tieto, mutta tämä ei suoraan ilmene laista. Näin ollen tiedon julkaiseminen ei ollut minkään nimenomaisen lainsäätösäännöksessä olevan kiellon vastainen.

Apulaisoikeuskansleri kiinnittää kunnan huomiota siihen, että esityslistojen ja pöytäkirjojen julkaisemissa tulisi arvioida ja punnita erisuuntaisin argumentein. Kyseessä olevassa tilanteessa tilinumeron julkaisemista ei voida perustella ainakaan perusoikeusargumenteilla tai muilla oikeudellisilla näkökohdilla. Henkilökohtaisten olojen suojaamisen tarpeen voitiin tässä tilanteessa katsoa olleen tilinumeron ilmaisesta puoltavia seikkoja painavampi.

Esimerkkinä henkilötietojen sähköisestä automatisoidusta luovuttamisesta voidaan käyttää Trafín ylläpitämää ajoneuvoliikennerekisteriä ja sitä koskevaa tietopalvelua. Tietopalveluna annetaan rekisteritunnuksen ja valmistenumeron perusteella tietoa rekisterissä olevien ajoneuvojen omistajista, haltijoista ja heidän osoitteistaan, katsastuksesta, teknisistä ominaisuuksista, käyttöönottopäivästä, vakuutusyhtiöstä ja maksamattomista veroista. Lisäksi henkilötunnuksen perusteella on saatavissa tietoja henkilöistä, joilla on ollut tai on ajo-oikeus.<sup>200</sup>

Ajoneuvoliikennerekisteristä annetun lain (541/2003) 14 §:n nojalla tapahtuva julkisten tietojen luovutus on mahdollista yksittäistapauksessa. Lainsäätäjä on yksittäisten julkisten tietojen osalta katsonut, että jokaisen yksittäin luovutettavan tiedon yhteydessä käyttötarkoituksen selvittäminen tai luovutuksensaajan identifioiminen ei ole

---

<sup>199</sup> Vrt. henkilörekisterin looginen määritelmä.

<sup>200</sup> HE 171/2002 vp., s. 25.

tarpeen.<sup>201</sup> Tietojen suojaamisessa on otettu huomioon tekniset rajoitukset esimerkiksi massalatausten estämiseksi. Lain 13 §:n 2 momentin mukaan muiden kuin yksittäin luovutettavien tietojen ja tilastotietojen tallettamiseen luovutuksen saajan tietojärjestelmiin vaaditaan rekisterinpitäjän lupa.

Näin ollen Trafín ajoneuvoliikennerekisteri ei voi olla saatavilla uudelleenkäyttöä varten täysin avoimessa muodossa. Trafín tekemän tietojen uudelleenkäyttöä koskevan selvityksen mukaan suurin uudelleenkäyttöä koskeva intressi kohdistuu ajoneuvoliikennerekisterin tietoihin, joiden luovuttaminen edellyttää pääsääntöisesti lupamenettelyä. Lisäksi tietojen luovuttaminen ajoneuvoliikennerekisteristä on sallittu vain laissa määriteltyihin käyttötarkoituksiin, joten tietojen avaaminen uudelleenkäytettäväksi ennakolta määrittelemättömiin tarkoituksiin ei ole mahdollista. Kuitenkin avoimen datan politiikka huomioon ottaen, Trafín tarkoituksena on tehostaa tietojen luovutukseen liittyviä sopimuskäytäntöjä ja yksinkertaistaa tietojen luovutukseen liittyviä toiminta malleja.<sup>202</sup>

Jotta viranomaisen voi julkaista henkilötietoja avoimessa tietoverkossa, on sillä oltava kyseisen henkilötietojen käsittelyn oikeutettava peruste. Peruste voi olla joko rekisteröidyn nimenomainen suostumus tai julkaisemisen oikeuttava lainsäädännös.

## 5.2 Anonyymien tietojen uudelleenkäyttö

Henkilötietojen käsittelyyn ja erityisesti luovutukseen kohdistuvien vaatimusten vuoksi henkilötunnisteellista dataa ei voida avata sellaisenaan kaikkien saataville ilman laissa säädettyä perustetta. Kuitenkin henkilötietoja sisältävään julkiseen dataan saattaa liittyä intressi saattaa se avoimesti kaikkien uudelleen hyödynnettäväksi esimerkiksi tilastotietona. Ohm esittää, että käyttökelpoinen henkilötietoja sisältävä tietovaranto ei ole koskaan täysin anonyymi.<sup>203</sup> Tietojen tunnistettavuuden riskiä lisäävät tunnistamisteknologioiden ja tunnistamistekniikoiden jatkuva kehitys sekä saatavilla olevan tiedon määrän eksponentiaalinen kasvu.<sup>204</sup> Julkiset ja yksityiset organi-

---

<sup>201</sup> Ibid.

<sup>202</sup> Liikenteen ja viestinnän avoin tieto 10/2013, s.22.

<sup>203</sup> Ohm 2010, s.1706.

<sup>204</sup> Salokannel 2012, s.2.

saatiot keräävät suuria määriä tietomassoja, jotka voidaan mahdollisesti yhdistää uudelleenkäytettäväksi saatettuun julkiseen anonyymiin tietoon.

Henkilötiedon laajasta määritelmästä johtuen anonyymisoinnille asetetaan korkeat vaatimukset. Henkilötiedodirektiivin 2 artiklan a alakohdan mukaan henkilötiedolla tarkoitetaan ”kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevia tietoja”. Tunnistettavissa olevalla henkilöllä tarkoitetaan luonnollista henkilöä, ”joka voidaan suoraan tai epäsuorasti tunnistaa, erityisesti henkilönumeron taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”. Henkilötietolaissa henkilötiedon käsitteen määritelmä on samansisältöinen. Määritelmässä on lisäksi korostettu henkilön yksityisyyden ja perhe-elämän suojaa: ”jotka voidaan tunnistaa häntä tai hänen perhettään, tai yhteisessä taloudessa eläviä koskevaksi” (HetiL 3.1 §:n 1 kohta).

Henkilötiedodirektiivin johdanto-osan 26 kappaleen mukaan ”sen määrittelemiseksi, onko henkilö tunnistettavissa, olisi otettava huomioon kaikki kohtuullisesti toteutettavissa olevat keinot, joita joko rekisterinpitäjä tai joku muu voi kyseisen henkilön tunnistamiseksi käyttää; tietosuojaa koskevia periaatteita ei sovelleta tietoihin, jotka on tehty anonyymeiksi siten, että rekisteröity ei ole enää tunnistettavissa”.

Anonyymillä datalla tarkoitetaan tietoa, josta luonnollinen henkilö on aiemmin ollut tunnistettavissa, mutta tunnistaminen ei olemassa olevien resurssien perusteella ole enää kohtuudella mahdollista. Arviointi tietojen mahdollisesta tunnistettavuudesta on tehtävä yksittäistapauksessa ja siihen vaikuttavat suoraan tietojenkäsittelyn asiayhteys ja olosuhteet.<sup>205</sup> Anonyymisointi on tehtävä mahdollisimman varhaisessa vaiheessa, joko rekisterinpitäjä tai luotettavan kolmannen tahon toimesta.<sup>206</sup>

Henkilötietojen suojaa koskevien säännösten soveltamisalaa ei pidä laajentaa liikaa sellaisiin tilanteisiin ja olosuhteisiin, joissa henkilöiden tunnistaminen ei ole kohtuullisesti toteutettavin keinoin mahdollista, eikä näitä keinoja todennäköisesti käytetä.<sup>207</sup>

---

<sup>205</sup> Tietosuojatyöryhmän lausunto 5/2014 anonymisointitekniikoista (0829/14/FI WP 216), s. 8.

<sup>206</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s. 14.

<sup>207</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s.5.

Pelkkä hypoteettinen mahdollisuus tunnistamiseen ei yksistään ole peruste tietosuojasäännösten soveltamiselle.<sup>208</sup>

Tunnistamisarviointi on aika- ja paikkasidonnainen, joten tietotekniikan ja yleisesti-kin tunnistamistekniikoiden kehitys on otettava huomioon tunnistamisriskiä arvioitaessa koko tiedon elinkaaren ajalta.<sup>209</sup> Tänä päivänä henkilöiden tunnistaminen suurista tietomassoista on helposti ja kustannustehokkaasti mahdollista. Tämä asettaa huomattavia vaatimuksia anonyymisointitekniikoille ja tietosuojalainsäädännölle. Voidaan perustellusti kysyä, onko tietosuojalainsäädännön soveltamisella enää ollenkaan rajoituksia?<sup>210</sup>

Tunnistettavuusarvioinnissa on otettava huomioon kaikki asiaan vaikuttavat tekijät ja tosiasiallinen mahdollisuus tunnistaa tietty luonnollinen henkilö kyseisistä tiedoista. Tunnistamiseen vaikuttavia tekijöitä ovat muun muassa: kustannukset, tunnistamisen tarkoitus, miten tietojenkäsittely on järjestetty, rekisterinpitäjän oletettu hyöty, henkilön yksityisyydelle aiheutuva vaara sekä organisatoristen häiriöiden ja teknisten vikojen riskit.<sup>211</sup> Tietojen anonyymisointiin liittyvä keskeinen ongelma on henkilötunnisteiden poistaminen niin, että tietovarannon käytettävyys ja eheys säilyy. Aidosti anonyymin, käyttökelpoisen datan tuottaminen on haasteellista.<sup>212</sup>

Olennaista on tietää eri anonyymisointitekniikoiden heikkoudet ja vahvuudet, jotta niistä voidaan valita juuri kyseisten tietojen, tilanteen ja tietojen käyttötarkoituksen kannalta sopivin. Anonyymisoinnin on oltava peruuttamatonta. Jos tiedot voidaan palauttaa, esimerkiksi rekisterinpitäjän hallussa oleviin tietoihin, ovat rekisteröidyt edelleen välillisesti tunnistettavissa tiedoista ja tietosuojalainsäädäntöä sovelletaan tällaisten tietojen käsittelyyn. Tietojen anonyymisointia ei ole pidettävä kertaluonteisena prosessina, vaan rekisterinpitäjän on säännöllisesti arvioitava tunnistamista koskevia riskejä.<sup>213</sup> Anonyymisointiprosessin jälkeen, säännöllisin väliajoin, rekisterinpitäjän on tehtävä riskiarviointi siitä, ovatko henkilöt kohtuudella toteuttavissa olevien

---

<sup>208</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s.5.

<sup>209</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s.15.

<sup>210</sup> Rubinstein 2013, s.5.

<sup>211</sup> Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä (01248/07/FI WP 136), s. 15.

<sup>212</sup> Tietosuojatyöryhmän lausunto 5/2014 anonyymisointitekniikoista (0829/14/FI WP 216), s. 3-5.

<sup>213</sup> Tietosuojatyöryhmän lausunto 5/2014 anonyymisointitekniikoista (0829/14/FI WP 216), s. 4.

keinojen avulla tunnistettavissa anonyymeistä tiedoista, jos esimerkiksi anonyymit tiedot yhdistettäisiin muihin olemassa oleviin tietoihin.<sup>214</sup>

Tunnistamiseen liittyvässä riskiarvioinnissa on otettava huomioon, mitä muuta tietoa on mahdollisesti olemassa. Muilla tiedoilla tarkoitetaan esimerkiksi julkisten tai yksityisten organisaatioiden hallussa olevia tietoja tai esimerkiksi internetissä julkaistuja tietoja. Esimerkiksi puhelinluettelossa julkaistuja tietoja voidaan mahdollisesti yhdistää riittämättömästi anonyymisoituihin tietoihin, mikä voi mahdollistaa henkilön tunnistamisen.<sup>215</sup>

Tietotekniikan kehittyessä on mahdotonta antaa yksiselitteistä vastausta sille, milloin tiedot ovat aidosti anonyymejä. Esimerkiksi pelkkien niin sanottujen tunnistetietojen, kuten nimen, henkilötunnuksen ja yhteistietojen poistaminen, ei yleensä johda siihen, että tiedot olisivat anonyymeja. Lisäksi anonyymien datan profiloimisella voi olla vaikutusta yksilöihin ja heidän oikeusasemaan.<sup>216</sup> Anonyymiä dataa sisältävien tietovarantojen avaamisessa yksi tunnistettavuutta lisäävä uhka on tietokantojen yhdistäminen ja henkilöiden profilointi tiettyjen ominaisuuksien perusteella.<sup>217</sup> Käsittelen tietojen profilointia tutkielman seuraavassa luvussa.

Anonyymien tietojen julkaisemisessa riskinä on luonnollisesti se, että henkilöt voidaan edelleen tunnistaa tiedoista. Riski ei vähene ajan kuluessa, vaan se päinvastoin kasvaa. Rekisterinpitäjä voi luulla, että tiedot ovat anonyymeja, mutta todellisuudessa kolmas osapuoli voi silti kyetä tunnistamaan henkilöitä, käyttämällä muita saatavilla olevia tietoja.<sup>218</sup> Anonyymisointiin kohdistuu haasteita, joista keskeisimpiä ovat teknologian ja tietojen saatavuuteen liittyvät kehitykset.

Tietosuojatyöryhmä esittelee *motivoituneen tunkeutujan testin*, jonka avulla pyritään määrittelemään ensinnäkin, onko olemassa tahoja, jolla on intressi tunnistaa henkilöitä anonyymeistä tiedoista ja toiseksi, voiko tunnistaminen onnistua tai kuinka todennäköisesti tunnistaminen onnistuu, jos hänellä on käytössään kohtuulliset resurssit. Jotkut tietotyypit ovat alttiimpia tunnistamisyrittäjille, kuten esimerkiksi tiedot, joilla

---

<sup>214</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s. 15.

<sup>215</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s. 15–16.

<sup>216</sup> Neuvoston profilointisuositus s.1.

<sup>217</sup> Bygrave 2003, s. 302. Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.3-5.

<sup>218</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.14.

on huomattava kaupallinen arvo. On huomioitava, että testi on rajoittunut ja teoreettinen. Jos organisaatio testin avulla tulee sellaiseen lopputulokseen, että ”tunkeutujia” ei ole, voi se johtaa siihen, että anonyymisointitekniikoihin ei välttämättä panosteta vaaditulla tavalla.<sup>219</sup>

Tunnistamistestauksen kohteena ovat tietovarannot, joita aiotaan julkistaa uudelleenkäytettäväksi. Julkisen sektorin elimen on ensin määritettävä, mitä muita sellaisia tietoja on saatavilla, jotka voitaisiin mahdollisesti yhdistää julkaistaviin tietoihin. Tunnistamistestauksen haasteena on, että se edellyttää organisaatiolta asiantuntemusta, lisäresursseja ja tietoa siitä, mitä muita tietoja on tosiasiallisesti saatavilla. Jos tunnistamistestaus onnistuu, tietosuojalainsäädännökset soveltuvat edelleen ja mahdolliset vaarantuneet tiedostot on poistettava. Jos tiedot on saatettu uudelleenkäyttöä varten, tunnistamisesta on myös tiedotettava tietojen uudelleenkäyttäjiä.<sup>220</sup> Viranomaisen on varmistuttava siitä, että sillä kykenee tehokkaasti vastaanottamaan mahdolliset tunnistamista koskevat ilmoitukset.

Anonyymien tietojen uudelleenkäyttöön voitaisiin liittää tiettyjä ehtoja, joiden avulla tunnistamisriskiä voitaisiin minimoida. Ehdossa olisi otettava huomioon ainakin seuraavat seikat: tiedot ovat anonyymisoituja, kiellettävä tietojen uudelleenkäyttäjää tunnistamasta henkilöitä, kiellettävä tietojen uudelleenkäyttäjää käyttämästä tietoja mihinkään henkilöä koskevaan päätöksentekoon tai toimenpiteeseen sekä velvoitettava tietojen uudelleenkäyttäjää ilmoittamaan, mikäli tiedoista tunnistetaan tai voidaan tunnistaa tiettyjä henkilöitä.<sup>221</sup>

Anonyymien tietojen uudelleenkäyttöä koskevien ehtojen yhteydessä olisi määriteltävä menettely, jonka avulla viranomainen voi perua vaarantuneen tiedoston käyttöluvan. Viranomaisen on toteutettava kaikki kohtuulliset toimet sen varmistamiseksi, että tietojen uudelleenkäyttäjä lopettaa vaarantuneiden tietojen käyttämisen. Tietosuojatyöryhmän mukaan rekisteröityminen olisi varmin tapa varmistua siitä, että uudelleenkäyttäjät tavoitetaan ja vaarantuneet tiedostot poistetaan käytöstä. Tähän ei kuitenkaan tietosuojaryhmän mukaan voida kannustaa, jos se edellyttää uusien henkilöiden keräämistä uudelleenkäyttäjiltä ja haittaa tai vaikeuttaa uudelleenkäyttöä

---

<sup>219</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.17.

<sup>220</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.18–19.

<sup>221</sup> Ibid.

varten perustettujen verkkosivustojen tai palvelujen käyttöä.<sup>222</sup> Ehtojen hyväksyttäminen on kuitenkin kannatettavaa, koska tällöin niillä on sopimuksen täytäntöönpanokelpoisuus.<sup>223</sup>

Tietojen yhdistelemiseen ja anonyymien tietojen luovuttamiseen mahdollisesti liittyvää tunnistamisen riskiä on oikeastaan mahdotonta arvioida ennalta. On mahdotonta arvioida pätevästi ja kaikenkattavasti, mitä tietoja on jo saatavilla tai, mitä tietoja on mahdollisesti saatavilla tulevaisuudessa.<sup>224</sup> Lisäksi ihmiset jakavat vapaaehtoisesti yhä enemmän tietoja itsestään, ystävistään ja lapsistaan sosiaalisessa mediassa. Tiedot voivat olla hyvinkin arkaluonteisia, joita monet eivät haluaisi käytettävän heitä koskevassa päätöksenteossa.<sup>225</sup> Päätöksenteko voi koskea esimerkiksi luottokelpoisuutta tai vakuutuksenottamiseen liittyviä ehtoja.<sup>226</sup> Julkisten lähteiden ja rekisteröidyn itse antamien tietojen lisäksi esimerkiksi matkapuhelimiin asennettavat applikaatiot keräävät ja jakavat tietoja useiden eri tahojen kanssa eksponentiaalisella vauhdilla.<sup>227</sup> Tunnistamisriski luonnollisesti kasvaa tiedon määrän kasvaessa. Viranomaiset voivat pienentää tunnistamisriskiä esimerkiksi julkiasemalla vain tiedot, jotka ovat tarpeellisia tietyn tarkoituksen saavuttamiseksi.<sup>228</sup> Tämä on perusteltua myös tietojen minimoinninperiaatteen näkökulmasta.

Anonyymistä datasta on erotettava niin sanottu pseudonyymidata, jolla tarkoitetaan tunnistetietojen salaamista niin, että henkilö ei ole tiedoista suoraan tunnistettavissa, mutta palauttamalla tiedot tai yhdistämällä pseudonyymitieto johonkin muuhun olemassa olevaan tietoon tunnistaminen on edelleen mahdollista. Pseudonyymien tietojen käsittelyyn sovelletaan tietosuojalainsäännöksiä.<sup>229</sup>

---

<sup>222</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s. 27.

<sup>223</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s. 27.

<sup>224</sup> Ohm 2010, s.1724.

<sup>225</sup> Ohm 2010, s.1725.

<sup>226</sup> Rubinstein 2013, s.4.

<sup>227</sup> Ibid.

<sup>228</sup> Ibid.

<sup>229</sup> Välillisestä tunnistamisesta tutkielman jaksossa 2.2.

### 5.3 Profilointi ja tietojen yhdistäminen

Yksi mahdollinen yksityisyyden suojalle riskejä aiheuttava tekijä on henkilöiden profilointi. Tietojen tehostettu saatavuus lisää mahdollisuutta, että henkilöt voidaan tunnistaa myös anonyymeista tiedoista ja uudelleenkäytettäväksi tarkoitettu tieto voidaan lisätä rekisteröidystä mahdollisesti laadittuun käyttäjäprofiliin.<sup>230</sup>

Automatisoidun päätöksenteon rajoittamisen periaate on tietosuojalainsäädännön keskeisiä periaatteita.<sup>231</sup> Automatisoitua päätöksentekoa koskeva kansallinen normi on kirjattu henkilötietolain 31 §:ään, jonka mukaan ”sellaisen rekisteröidyn tiettyjen ominaisuuksien arviointiin tarkoitettun päätöksen tekeminen, joka tapahtuu ainoastaan automatisoidun tietojenkäsittelyn perusteella ja josta aiheutuu rekisteröidylle oikeudellisia vaikutuksia tai joka muuten vaikuttaa häneen merkittävällä tavalla, on sallittu vain, jos: 1) siitä on laissa säädetty; tai 2) päätös tehdään sopimuksen tekemisen tai täytäntöönpanon yhteydessä edellytyksellä, että rekisteröidyn oikeuksien suojaaminen varmistetaan tai, että päätöksellä täytetään sopimuksen tekemisestä tai täytäntöönpanoa koskeva pyyntö.”

Säännöksen ongelmana on sen rajoitettu soveltuvuus, sillä se ei sinänsä rajoita henkilöiden profilointia, ainoastaan sitä, milloin automatisoidusti rakennettua profiilia voidaan käyttää päätöksenteossa. Säännöksen soveltamisen ehtona on, että automatisoidusta päätöksentekoprosessista aiheutuu rekisteröidylle oikeudellisia vaikutuksia tai sen on vaikutettava häneen merkittävällä tavalla. Oikeudellisilla vaikutuksilla tarkoitetaan vaikutuksia, joiden perusteella arvioidaan henkilön oikeuksia tai velvollisuuksia.<sup>232</sup> Säännöstä ei sovelleta, jos luonnollinen henkilö osallistuu päätöksentekoprosessiin millään tavalla.<sup>233</sup> Henkilötiedodirektiivissä automatisoitua päätöksentekoa koskeva säännös on direktiivin 15 artiklassa, joka on saman sisältöinen henkilötietolain 31 §:n säännöksen kanssa. Profilointia voidaan käyttää esimerkiksi vakuutuksenhakijaan liittyvien riskien arvioinnissa, luotonannossa tai rikosten ehkäisemisessä.<sup>234</sup>

---

<sup>230</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.14.

<sup>231</sup> Saarenpää 2012a, s.340. Saarenpää näkee ko. periaatteen merkittävänä ihmisoikeusperusteisena metaperiaatteena.

<sup>232</sup> Bygrave 2003, s.322.

<sup>233</sup> Rubinstein 2013, s.6.

<sup>234</sup> Bygrave 2003, s.304.



Automatisoidusta päätöksenteosta on erotettava profilointi, jolla tarkoitetaan muita prosesseja kuin päätöksentekoa.<sup>235</sup> Muita profiloinnin tarkoituksia voi olla esimerkiksi mainonnan kohdentaminen kuluttajan ostotottumuksia seuraamalla ja pyrkimällä ennustamaan tulevaa ostoskäyttäytymistä.<sup>236</sup>

Profiloinnin keskeinen ongelma on se, että rekisteröidyn käyttäytymistä ja toimintatapoja seurataan usein rekisteröidyn tietämättä ja näiden päätelmien avulla tehdään rekisteröidyn oikeusasemaan vaikuttavia päätöksiä tai jatkopäätelmiä. Rekisteröity ei pysty esimerkiksi tehokkaasti vastustamaan profilointia, jos rekisteröity ei ole tietoinen profiloinnista.<sup>237</sup>

Rekisteröidyn oikeusaseman kannalta ongelmana ovat myös profiloinnin tuloksena syntyneiden päätelmien ja tietojen virheellisyys ja laatu kokonaisuudessaan. Profilointiprosessin tuloksena syntyneet profiilit perustuvat yleensä todennäköisyyksiin ja sisältävät tietynlaisen virhemarginaalin.<sup>238</sup> Näkymättömät profilointiprosessit ovat riski rekisteröidyn yksityisyyden suojan kannalta.<sup>239</sup> Profiloinnin lopputulos saattaa myös johtaa syrjintään.<sup>240</sup> Profilointi on tietojen käsittelyä, joka yleensä johtaa tietojen käsittelyntarkoituksen uudelleen määrittelyyn.<sup>241</sup> Käyttötarkoitussidonnaisuuden periaate huomioon ottaen, uudelleen määriteltä käyttötarkoitusta ei saa olla yhteensopimaton alkuperäisen käsittelyn tarkoituksen kanssa (HetiL 7 §).

Ehdotuksessa Euroopan unionin yleiseksi tietosuojasetukseksi profilointiin on kiinnitetty laajempaa huomiota. Yleistä tietosuojasetusta koskevassa LIBE-komitean mietinnössä profiloinnille ehdotetaan määritelmää, jonka mukaan ”profilointi tulisi määritellä kaikenlaiseksi automatisoiduksi henkilötietojen käsittelyksi, jonka tarkoituksena on tiettyyn luonnolliseen henkilöön liittyvien henkilökohtaisten ominaisuuksien arvioiminen tai erityisesti hänen ammatillisen suorituskykynsä, taloudellisen tilanteensa, sijaintinsa, terveytensä, henkilökohtaisten mieltymyksensä, luotettavuutensa tai käyttäytymisensä analysoiminen tai ennakoiminen.”<sup>242</sup>

---

<sup>235</sup> Bygrave 2003, s. 321.

<sup>236</sup> Eklund, Lilja 2013, s.216.

<sup>237</sup> Rubinstein 2013, s.6.

<sup>238</sup> Bygrave 2003, s.307.

<sup>239</sup> Neuvoston profilointisuositus, s. 1.

<sup>240</sup> Neuvoston profilointisuositus, s.2.

<sup>241</sup> Bygrave 2003, s.305.

<sup>242</sup> LIBE –komitean mietintöluonnoksen muutosehdotus 87 koskien tietosuojasetuksen artiklaa 4 s.69.

Yleisen tietosuojasetuksen 20 artiklassa on nimenomaisesti otettu huomioon oikeus olla joutumatta profilointia koskevan toimenpiteen kohteeksi. Rekisteröidyn profilointi on sallittua ainoastaan, jos 1) se perustuu sopimuksen täytäntöönpanoon, 2) se perustuu rekisteröidyn suostumukseen tai 3) siitä on laissa erikseen säädetty. Profilointia koskeva 20 artikla korvasi henkilötietodirektiivin automatisoitua päätöksentekoa koskevan 15 artiklan. Automatisoitu päätöksenteko määritellään säännöksessä laajemmin, joten se soveltuu useampiin tilanteisiin kuin aikaisemmin. Ehdotuksen 20 artiklassa kielletään automatisoitu päätöksenteko, joka perustuu ainoastaan arkaluonteisiin tietoihin. Lähtökohtana profiloinnin oikeudellisen perusteen arvioinnissa on profiloinninkohteen tietoinen päätös sallia omien tietojen profilointi tiettyyn tarkoitukseen.

Profilointi ja tietojen yhdistely ovat haaste myös silloin, kun käsitellään anonyymia dataa, sillä profilointi ja tietojen yhdisteleminen lisäävät tunnistamisriskiä.<sup>243</sup> Big data on käsite, jolla viitataan muun muassa eksponentiaalisesti kasvavaan datan määrään ja sen tuomiin haasteisiin ja mahdollisuuksiin yhteiskunnalle.<sup>244</sup> Big datalla voidaan tarkoittaa myös eri organisaatioiden suorittamaan tietokantojen yhdistelemistä ja jalostamista, jolloin tiedon louhinta tekniikoiden avulla tiedoista etsitään tiettyä organisaatiota kiinnostavaa informaatioita.<sup>245</sup>

Tietojen louhinnalla tarkoitetaan tietovarantojen systemaattista yhdistämistä, analysointia ja muokkausta. Louhinnan tarkoituksena on tuottaa uutta tietoa. Tiedon avoin ja helppo saatavuus muodostavat hedelmällisen alustan tietojen louhinnalle.<sup>246</sup> Tiedon tehokkaan hyväksikäytön mahdollistaa teknologian ja tietojen analyysipalveluiden (kuten Apache Hadoop) kehitys sekä tietojen säilyttäminen ja käsittely pilvipalveluissa, jolloin tiedon käsittely ja säilyttäminen on kustannustehokasta.<sup>247</sup> Suuret internetiyhtiöt kuten Google, Facebook, Amazon, eBay, Microsoft ja Yahoo! käyttävät tavalla tai toisella hyväksi big dataa luomalla tietopohjaisia uusia hyödykkeitä ja lisäämällä omien palveluiden kustannustehokasta hyödyntämistä.<sup>248</sup>

Big data mahdollistaa henkilöiden tehokkaan profiloinnin laajentamalla käytettävissä olevaa tietoa. On huomioitava, että tietoaaineistoista saatavat taloudelliset hyö-

---

<sup>243</sup> Neuvoston profilointisuositus, s. 1.

<sup>244</sup> Salo 2013, s. 10

<sup>245</sup> Rubinstein 2013, s.1.

<sup>246</sup> Salokannel 2012, s.25

<sup>247</sup> Rubinstein 2013, s.4.

<sup>248</sup> Rubinstein 2013, s.3.

dyt syntyvät todellisesti silloin, kun tietoja yhdistellään toisiinsa ja olemassa oleviin palveluihin.<sup>249</sup> Toisin kuin esimerkiksi evästeisiin, eli profiloinninkohteen verkkokäyttäytymiseen perustuvassa profiloinnissa, big datan avulla suoritettava profilointi voidaan ulottaa koskemaan laajaa joukkoa verkossa ja muuta kautta saatavilla olevaa tietoa.<sup>250</sup>

---

<sup>249</sup> Castrén, Tietosuoja –lehti 2/2014 s.27.

<sup>250</sup> Rubinstein 2013, s.4.

## 6. Henkilötietojen suojan huomioonottaminen

### 6.1 Oikeudelliset periaatteet

Kun tavoitteena on julkisten tietojen tehokas käyttö ja uudelleenkäyttö, viranomaisten on analysoitava niiden hallussa olevat tietoaineistot. Tietoaineistoista on tunnistettava aineistot joiden käyttöön liittyy oikeudellisia rajoituksia, kuten henkilötietoja sisältävät tietoaineistot. Aineiston sisällön perusteella viranomaisen on tehtävä päätös siitä, voiko se saattaa sen hallussa olevat tietovarannot uudelleenkäytettäväksi. Olennaista tässä yhteydessä on tunnistaa henkilötietojen luovutukseen liittyvä lainsäädäntö sekä henkilötietojen luovuttamiseen kohdistuvat riskit.

Pääsääntöisesti henkilötietojen luovuttaminen on sidottu niiden käyttötarkoitukseen ja siihen, että henkilötietojen vastaanottajalla on henkilötietojen käsittelyä koskevien säännösten perusteella lainmukainen oikeus käsitellä luovutuksena saatuja henkilötietoja. Poikkeuksellisesti lainsäätäjällä on katsonut, että tietojen käsittelyntarkoitusta tai luovutuksensaajaa ei ole tarpeellista selvittää yksittäisten tietojen luovutusten osalta. Näin on esimerkiksi silloin, kun tietoja luovutetaan Trafín ylläpitämästä ajoneuvoliikennerekisteristä.

Henkilötietojen suojaa koskevat oikeudelliset periaatteet ovat keskeisiä tekijöitä yksityisyyden suojan toteutumisessa henkilötietoja käsiteltäessä. Sekä viranomaisen että tietojen luovutuksensaajan on otettava huomioon näiden keskeisten periaatteiden toteutuminen toiminnassaan. Esimerkiksi avoimessa tietoverkossa julkaistujen henkilötietojen osalta on otettava huomioon, että tietojen käsittelyyn sovelletaan henkilötietojen suojaa koskevia säännöksiä täysimääräisesti.<sup>251</sup>

Rekisterinpitäjän on varmistuttava siitä, että rekisteröidyt voivat tehokkaasti käyttää hyväkseen tietosuojalainsäädännön mukaisia oikeuksiaan. Viranomaisten on varmistuttava hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan toteutumisesta sekä tietojen suojaamisesta ja tietoturvasta. Julkisen sektorin tietojen osalta korkein hallinto-oikeus on 25.10.2012 antamassaan ratkaisussa 1694/1/11 katsonut, silloin kun

---

<sup>251</sup> <sup>251</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 48.

henkilötietojen luovuttaminen on lainsäädännössä sidottu niiden käyttötarkoitukseen, merkitsee tämä julkisuusperiaatteen rajoitusta.

### 6.1.1 Suunnitteluvollisuus ja käyttötarkoitussidonnaisuus

Henkilötietolain huolellisuusvelvoite edellyttää, että rekisterinpitäjä käsittelee henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojen käsittelytapaa sekä toimii muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta (HetiL 5 §). Perusedellytyksenä henkilötietojen käsittelyä sisältävälle toiminnalle on, että toiminta on lainmukaista.<sup>252</sup> Lainmukaisuudella tarkoitetaan sitä, että henkilötietojen käsittely ei saa olla minkään lain tai säännöksen vastaista.

Rekisterinpitäjällä on oltava henkilötietolain mukainen peruste käsitellä henkilötietoja (HetiL 8 §, 12 §, 13 § ja 4 luku). Vaikka rekisterinpitäjällä olisikin lainmukainen peruste käsitellä henkilötietoja, ei tämä legitimoisi henkilötietojen käsittelyä. Rekisterinpitäjän on otettava huomioon myös muiden henkilötietolain tietosuojaperiaatteiden toteutuminen henkilötietojen käsittelyssä.<sup>253</sup>

Rekisteröityjen oikeusturvan kannalta keskeisimpiä periaatteita ovat vullisuus määritellä henkilötietojen käsittelyntarkoitus sekä käyttötarkoitussidonnaisuus (HetiL 6 § ja 7 §).<sup>254</sup> Rekisterinpitäjän on ensimmäiseksi määriteltävä laillinen tarkoitus, jota varten henkilötietoja on tarpeellista käsitellä. Tämän jälkeen voidaan arvioida muiden tietosuojaperiaatteiden toteutumista vertaamalla periaatteita määriteltyyn käsittelyn tarkoitukseen.<sup>255</sup>

---

<sup>252</sup> Konstari 1992, s. 96.

<sup>253</sup> PSI-direktiivin johdanto-osan 11 kohdan mukaan direktiivin soveltamisessa on noudatettava kaikilta osin henkilötietojen suojaa koskevia säännöksiä. Erityisesti on kiinnitettävä huomiota lailliseen käsittelyn perusteeseen ja käyttötarkoitussidonnaisuuden periaatteeseen.

<sup>254</sup> Bygrave 2003, s.337.

<sup>255</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.11. . Viranomaisten luovuttaessa tietoja käsittelyntarkoitusta koskeva määrittely vullisuus koskee erityisesti luovutuksen saajaa. Kuten edellä todettu, viranomaisen peruste käsitellä henkilötietoja on pääsääntöisesti lakiin tai laissa säädettyyn tehtävään.

Jos viranomainen luovuttaa sähköisesti henkilötietoja julkisuuslain 16 §:n 3 momentin nojalla, jos luovutuksensaajalla on henkilötietojen suoja koskevien säännösten mukaan oikeus tallettaa ja käyttää tällaisia henkilötietoja. Viranomaisen on pyydyttävä selvitys muun muassa tietojen käyttötarkoituksesta ja muista tietojen luovuttamiseen liittyvistä seikoista, esimerkiksi siitä miten tietojen suojaus on järjestetty (JulKL 13.2 §).

Henkilötietojen käsittelyä sisältävät toiminnot ja niiden tarpeellisuus arvioitava etukäteen, jotta rekisterinpitäjä pystyy määrittelemään tietojen asianmukaisen käsittelyntarkoituksen.<sup>256</sup> Käsittelyntarkoitus on määriteltävä niin, että siitä käy selkeästi ja yksiselitteisesti ilmi, minkälaisen rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään ja miksi henkilötietojen käsittely on tarpeellista kyseisten tehtävien hoitamisen kannalta.<sup>257</sup>

Henkilötietojen käsittelyntarkoitus on määriteltävä ennen kuin rekisterinpitäjä ryhtyy käsittelemään, esimerkiksi keräämään, henkilötietoja. Jos yksi tietotekninen rekisteri sisältää useita loogisia henkilörekistereitä, rekisterinpitäjän on määriteltävä eri osatiedostojen käyttötarkoitus ja tietosisältö yksilöidymmin. Tämä on tarpeen esimerkiksi sen vuoksi, että rekisterinpitäjä pystyy määrittämään henkilöt, joiden tehtäviin henkilötietojen käsittely kulloinkin kuuluu.<sup>258</sup>

Henkilötietolain 7 §:n mukaan henkilötietoja saa käyttää tai muutoin käsitellä tavalla, joka ei ole yhteensopimaton 6 §:ssä tarkoitettujen käsittelyn tarkoitusten kanssa. Myöhempiä käsittelyä historiallista tutkimusta taikka tieteellistä tai tilastointitarkoitusta varten ei pidetä yhteensopimattomana alkuperäisen käsittelyn tarkoituksen kanssa.

Käyttötarkoitussidonnaisuuden periaatteen tarkoitus on toteuttaa henkilötietojen käsittelyn avoimuutta sekä varmistaa tietojen laatua koskevien periaatteiden toteutuminen. Jos tiedot irrotetaan alkuperäisestä käyttötarkoituksestaan, erityisesti riski tietojen virheellisyydestä kasvaa. Rekisteröidyn oikeusturvan kannalta ei ole riittävää, että rekisteröidyllä on mahdollisuus käyttää henkilötietolain mukaisia oikeuksiaan, vaan

---

<sup>256</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 15.

<sup>257</sup> Konstari 1992 s. 99, Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.15.

<sup>258</sup> Wallin, Nurmi 1991, s.43.

rekisteröidyllä on oltava mahdollisuus tietää, mitä häntä koskeville tiedoille tapahtuu ja mihin niitä käytetään.<sup>259</sup>

Käyttötarkoitussidonnaisuuden periaatteen tarkoitus on suojalla rekisteröityjen yksityisyyttä asettamalla rajat sille, miten ja mihin tarkoitukseen rekisterinpitäjä voi käsitellä henkilötietoja sekä edistää tietojen käsittelyn oikeudenmukaisuutta. Periaatteen tarkoitus on estää rekisterinpitäjää käsittelemästä tietoja tavalla, joka on odottamatonta, asiattonta tai muuten perusteetonta. Periaate sisältää tiettyä joustavuutta tietojen käsittelyssä, koska kiellettyä käsittelyä on alkuperäisen tarkoituksen kanssa yhteensopimaton henkilötietojen käsittely.<sup>260</sup> Viranomaisten suorittaman henkilötietojen käsittelyn osalta on otettava huomioon, että henkilötietojen käsittelyntarkoitus määrittyy pääsääntöisesti viranomaisen toimivallan perusteella.<sup>261</sup>

Käyttötarkoitussidonnaisuuden periaate ei edellytä, että rekisterinpitäjä pystyisi määrittelemään kaikki mahdolliset tietojen käsittelytavat etukäteen. Myöhempi käsittely eri tarkoitusta varten ei välttämättä tarkoita sitä, että käsittely olisi yhteensopimatonta alkuperäisen käsittelyn tarkoituksen kannalta. Käsittelyn yhteensopivuus on ratkaistava tapauskohtaisesti.<sup>262</sup>

#### **6.1.1.1 Käyttötarkoituksen yhteensopivuusarviointi**

Myöhemmän käsittelyn arvioinnissa on kiinnitettävä huomiota siihen hetkeen, jolloin tiedot on rekisteriin kerätty ja talletettu ja muun henkilötietojen käsittelyn eroihin. Kaikki muu henkilötietojen käsittely kuin kerääminen on ”myöhempää käsittelyä”.<sup>263</sup> Niin direktiivissä kuin henkilötietolaissa on valittu sanamuoto, joka kieltää yhteensopimattoman käytön, jolloin myöhempi käsittely on sallittua, jos se täyttää yhteensopivuuden ja laillisuuden vaatimukset.

Henkilötietolain tarkoituksena on, että rekisterinpitäjä pystyy itse arvioimaan oman toimintansa lainmukaisuutta. Näin ollen on oltava olemassa viitekehys, jonka avulla rekisterinpitäjä voi myöhemmän arvioida tietojen käsittelyn lainmukaisuutta ja sitä,

---

<sup>259</sup> Wallin, Nurmi 1991, s.100-101.

<sup>260</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 11.

<sup>261</sup> Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83),

<sup>262</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.3.

<sup>263</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 22.

että myöhempi käsittely on alkuperäisen käsittelyntarkoituksen mukaista.<sup>264</sup> Tarkoituksen kannalta yhteensopimattoman käytön kieltä asettaa rajat henkilötietojen myöhemmälle käytölle ja samalla velvoittaa rekisterinpitäjää määrittelemään ja erottamaan toisistaan yhteensopimaton ja yhteensopiva henkilötietojen käsittely.<sup>265</sup>

Jos henkilötietoja käsitellään muuhun kuin alun perin suunniteltuun ja määriteltyyn tarkoitukseen, ei siitä automaattisesti seuraa sitä, että henkilötietojen käsittely olisi tietosuojasäännösten vastaista yhteensopimatonta henkilötietojen käsittelyä.<sup>266</sup> Kerätyt henkilötietoja voi olla tarpeellista käsitellä johonkin muuhun tarkoitukseen, jota ei kuitenkaan ole alun perin tarkasti määritelty yhdeksi rekisterin käyttötarkoitukseksi.<sup>267</sup> Selkeästi yhteensopimattomana käsittelynä pidetään esimerkiksi sitä, että tutkimusta, suunnittelua ja tilastointia varten kerätyt henkilötietoja käytetään rekisteröityä koskevaan valvontaan.<sup>268</sup>

Tietosuojatyöryhmän käyttötarkoitussidonnaisuuden periaatteesta antamassa lausunnossa on nostettu esille keskeiset yhteensopivuusarviointiin vaikuttavat tekijät. Ensinnäkin on kiinnitettävä huomiota siihen, mikä on alkuperäisen ja myöhemmän käsittelyn suhde. Arvioinnissa huomiota on kiinnitettävä tosiasialliseen alkuperäiseen käsittelyntarkoituksen ja myöhemmän tosiasiallisen käsittelyn väliseen suhteeseen.<sup>269</sup> Mitä suurempi ero näiden välillä on, sitä todennäköisempää on, että käsittely todetaan yhteensopimattomaksi.

Toiseksi yhteensopivuusarviointiin vaikuttava tekijä on tietojen tosiasiallinen keräyskonteksti eli miten ja missä yhteydessä henkilötiedot on kerätty. Arviointiin vaikuttaa myös se, mitä rekisteröity voi ja on tietoja kerätessä voinut, objektiivisesti ja kohtuudella odottaa henkilötietojensa käsittelyltä. Jos myöhempi tietojenkäsittely katsotaan yllättäväksi tai kohtuuttomaksi rekisteröidyn kohtuullisten odotusten kannalta, on todennäköistä, että tietojenkäsittely on myös käyttötarkoitussidonnaisuuden periaatteen vastaista.<sup>270</sup>

Kolmanneksi yhteensopivuusarviointiin vaikuttaa rekisteröidyn ja rekisterinpitäjän välinen mahdollinen sopimus sekä rekisterinpitäjän toimialalla valitsevat yleiset käy-

---

<sup>264</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.20.

<sup>265</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.13.

<sup>266</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.12.

<sup>267</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.4.

<sup>268</sup> Ibid.

<sup>269</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 23.

<sup>270</sup> Ibid.



tännöt.<sup>271</sup> Jos rekisteröity on lain nojalla velvoitettu antamaan henkilötietonsa rekisterinpitäjälle, yhteensopivuusarviointia on tarkasteltava suppeasti. Jos henkilötietojen käsittely perustuu suostumukseen, rajaa se minkälaiseen henkilötietojen käsittelyyn suostumus on annettu henkilötietojen myöhempää käsittelyä. Yhteensopivuusarviointiin vaikuttaa myös se, kuinka läpinäkyvää ja avointa henkilötietojen käsittely on, sekä se perustuuko henkilötietojen myöhempi käsittely esimerkiksi lakiin.<sup>272</sup>

Yksi tärkeimmistä yhteensopivuusarviointiin liittyvistä seikoista on tietosuojalainsäädännön tarkoituksen huomioon ottaminen: yksityiselämän suojan ja muita yksityisyyden suojaa turvaavien perusoikeuksien toteuttaminen henkilötietoja käsiteltäessä. Jos henkilötietojen myöhempi käsittely vaikuttaa negatiivisesti rekisteröidyn yksityiselämän suojaan, on todennäköistä, että henkilötietojen myöhempi käsittely ei ole yhteensopivaa alkuperäisen käsittelyn tarkoituksen kanssa.<sup>273</sup> Lain tarkoituksena on suojella rekisteröityjä henkilötietojen käsittelyltä, joka on tarpeettoman laajaa ja epäasiallista. Jos käsitellään arkaluonteisia henkilötietoja, on yhteensopivan käsittelyn ala suppea.

Yhteensopivuusarvioinnissa on lisäksi kiinnitettävä huomiota rekisterinpitäjän omaksumiin turvatoimiin sekä siihen, miten rekisterinpitäjä on pyrkinyt estämään rekisteröidylle käyttötarkoituksen muutoksesta aiheutuvat mahdolliset haitat. Henkilötietojen anonyymisointia voidaan pitää keskeisenä turvatoimena silloin, kun käyttötarkoitus ei todennäköisesti ole yhteensopivaa alkuperäisen käsittelyntarkoituksen kanssa. Uusi oikeudellinen peruste voi myös kompensoida käyttötarkoituksen muutosta, vaikka se ei sinänsä legitimoisi yksinään muuten yhteensopimatonta käsittelyä.<sup>274</sup>

Tietojen uudelleenkäytön kannalta on syytä ottaa huomioon, käyttötarkoitussidonnaisuutta koskeva tarkennussäännös, jonka mukaan henkilötietojen käsittelyä tilastollista, historiallista tai tieteellistä tutkimusta varten ei pidetä yhteensopimattomana määritellyn käyttötarkoituksen kannalta (HetiL 7 §). Tällöinkin on huolehdittava yksityisyydensuoja- ja oikeusturvaloukkausten ehkäisemisestä.<sup>275</sup>

Henkilötietoja ei voi käsitellä vapaasti esimerkiksi tieteellistä tutkimusta varten. Tieteellinen tutkimus voi perustua esimerkiksi, joko rekisteröidyn suostumukseen (HetiL 8.1 §:n 1 kohta) tai lain 14 §:ään, jonka mukaan henkilötietoja voidaan tietyin ehdoin käsitellä tutkimustarkoituksessa ilman lain 8 §:stä johtuvaa perustetta. Erityisesti tut-

<sup>271</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 24.

<sup>272</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.25.

<sup>273</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.26.

<sup>274</sup> Ibid.

<sup>275</sup> Wallin, Nurmi 1991, s.105 ja HE 96/1998 vp., s.39.

kimuksessa, joka perustuu rekisteröidyn antamaan suostumukseen, määräytyy tietojen sallittu käsittelyntarkoitus sen mukaan, minkälaiseen käsittelyyn suostumus on annettu. On siis syytä huomata, että tarkennussäännöksen tarkoituksena on mahdollistaa rekisterintietojen myöhempi käyttö 7 §:ssä mainittuihin tarkoituksiin.

Rekisterinpitäjän on huolellisen kokonaisarvioinnin kautta otettava huomioon vallitsevat olosuhteet, tekijät ja tietojen kyseessä olevan käsittelyn vaikutus rekisteröityjen yksityisyyden suojaan. Erityisesti on kiinnitettävä huomiota siihen, että tietojen käsittely ei vaikuta rekisteröidyn oikeusasemaan. Jos henkilötietoja ei ole tarpeellista käsitellä kyseessä olevassa uudessa tarkoituksessa, henkilötiedot on muutettava tunnistettomiksi.<sup>276</sup>

Tarkennussäännöstä on tulkittava nimenomaisesti tarkennuksena eikä poikkeuksena käyttötarkoitussidonnaisuuden periaatteeseen. Tällöin on mahdollista, että muutkin kuin alkuperäiset henkilötietojen käsittelyntarkoitukset voidaan mieltää yhteensopiviksi.<sup>277</sup> Käyttötarkoitussidonnaisuuden periaatteen tulkinnassa on omaksuttu ns. tasapainoinen lähestymistapa, jossa otetaan huomioon rekisteröityjen oikeudet odotukset ja tietojenkäsittelyn oikeudellinen varmuus sekä toisaalta tarve tiettyyn joustavuuteen tietojenkäsittelyssä.<sup>278</sup>

### **6.1.1.2 Käyttötarkoituksen muutos**

Henkilörekisterin käyttötarkoitus ja säännönmukaiset tietojensiirrot voidaan myöhemmin määritellä uudelleen, jos se on muuttuneiden olosuhteiden vuoksi tarpeen eikä näin määritelty käyttötarkoitus olennaisesti poikkea alkuperäisestä käyttötarkoituksesta.<sup>279</sup> Jos rekisterinpitäjä ei ole määritellyt henkilötietojen käsittelyntarkoitusta riittävän täsmällisesti tai, jos käyttötarkoitus muuttuu olennaisesti, rekisterinpitäjä voi mahdollisesti kompensoida puutteita tietyillä suojaustoimilla. Valitut keinot voivat olla teknisiä tai organisatorisia.

Yhteensopivuusarvioinnin kautta ratkaistaan ovatko valitut keinot olleet riittäviä takaamaan oikeudenmukaista tietojenkäsittelyä. Ensimmäiseksi rekisterinpitäjän on

<sup>276</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 28.

<sup>277</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 13.

<sup>278</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s. 5.

<sup>279</sup> HE 96/1998 vp., s.39.

uudelleen määriteltävä henkilötietojen käsittelyntarkoitus niin, että se vastaa todellista asiantilaa. Toiseksi rekisterinpitäjän on informoitava rekisteröityjä muuttuneesta henkilötietojen käsittelyntarkoituksesta ja kolmanneksi rekisterinpitäjän on mahdollisesti pyydyttävä rekisteröityjen suostumus henkilötietojen käsittelyyn tähän uuteen tarkoitukseen. Suostumus henkilötietojen käsittelyyn uutta käyttötarkoitusta varten on pyydyttävä siten, että rekisteröidyllä on mahdollisuus kieltää henkilötietojen käsittely uudessa tarkoituksessa.<sup>280</sup>

Mitä suurempi erotus on alkuperäisen ja myöhemmän käsittelyntarkoituksen välillä, sitä laajemmat suoja-toimet rekisterinpitäjän on suoritettava tietojenkäsittelyn lainmukaisuuden varmistamiseksi. Edellä esitettyä yhteensopivuusarviointia voidaan käyttää yleisenä mittapuuna.

Käyttötarkoituksen muutos ei siis aina tarkoita sitä, että käsittely olisi henkilötietolain vastaista ja näin ollen kiellettyä. Käyttötarkoituksen muutosta on arvioitava myös suhteellisuusperiaatteen nojalla niin, että otetaan huomioon käsittelyn peruste sekä se, miten rekisteröityjä on informoitu henkilötietojen käsittelystä.

Julkisen sektorin tietojen uudelleenkäytön yhteydessä käyttötarkoitussidonnaisuuden periaate on pääsääntöisesti otettava täysimääräisesti huomioon. Poikkeuksesta on säädettävä nimenomaisesti laintasoisella säännöksellä.

### 6.1.2 Tietojen tarpeellisuus ja virheettömyys

Tietojen laatua koskevat periaatteet sääntelevät, mitä tietoja on tarpeellista käsitellä määritellyn henkilötietojen käsittelyn tarkoituksen kannalta sekä rekisterinpitäjälle asetetusta velvollisuudesta huolehtia siitä, ettei se käsittele virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja (Hetil 9 §).

Tietojen tarpeellisuusvaatimus määräytyy henkilörekisterin käyttötarkoituksen mukaan ja tarpeellisuusvaatimuksen tarkoituksena on edistää käsiteltävien henkilötietojen minimoinnin periaatetta.<sup>281</sup> Rekisteröidyn suostumus ei syrjäytä tarpeellisuusvaa-

---

<sup>280</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.26.

<sup>281</sup> Wallin, Nurmi 1991, s. 67.

timusta.<sup>282</sup> Tietojen käsittelyn tarpeellisuutta on arvioitava tietojen keräys hetkellä olemassa olevan todellisen tarpeen mukaan.<sup>283</sup>

Viranomaistoiminnassa henkilötietojen käsittelyn tarpeellisuus kulminoituu yleensä laissa säädettyyn velvollisuuteen ylläpitää tiettyä rekisteriä tai viranomaiselle laissa säädetyn tehtävään, jonka nojalla henkilötietoja on tarpeellista käsitellä. Toki viranomainen käsittelee esimerkiksi myös palveluksessaan olevien työntekijöiden ja virkamiesten tietoja yhteysvaatimuksen perusteella.

Julkisen sektorin hallussa olevien tietojen uudelleenkäytön näkökulmasta, jos viranomainen huolellisen arvioinnin jälkeen toteaa, että on perusteltua sallia henkilötietojen uudelleenkäyttö esimerkiksi julkisuuslain 21 §:n nojalla, on sen arvioitava, mitä tietoja on tarpeellista ja asianmukaisesti perusteltua saattaa uudelleenkäytettäväksi. On otettava huomioon, että julkisuuslain nojalla ei ole perusteltua sallia henkilötietojen uudelleenkäyttöä ilman erillisiä suojaamistoimia kuten tietojen anonyymisointia.<sup>284</sup>

Tietojen laatua koskevat periaatteet liittyvät keskeisesti rekisteröityjen oikeuksiin. Rekisterinpitäjän on oma-aloitteisesti tai rekisteröidyn pyynnöstä poistettava tietojen käsittelyn kannalta tai muuten virheellinen tai harhaanjohtava tieto (HetiL 29 §). Rekisterinpitäjän on ilmoitettava tiedon korjaamisesta sille, jolta se on saanut tai jolle se on luovuttanut kyseisen virheellisen tiedon. Ilmoittamisvelvollisuutta ei ole, jos se on mahdotonta tai vaatii kohtuutonta vaivaa (HetiL 29.3 §). Jos henkilötietoja saatetaan uudelleenkäytettäväksi avoimesti tietoverkkoon, on yleensä mahdotonta tietää, kuka tietoja käsittelee. Näin ollen esimerkiksi tehokas ilmoittaminen tietojen virheellisyydestä ei näin ollen olisi kohtuudella mahdollista.

---

<sup>282</sup> Wallin, Nurmi 1991, s.68.

<sup>283</sup> Konstari 1992, s.146.

<sup>284</sup> Article 29 Working Party opinion 03/2013 on purpose limitation (00569/13/EN WP 230), s.50 ja Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s.6.

### 6.1.3 Sisäänrakennettu ja oletusarvoinen tietosuojaja

Rekisterinpitäjänä viranomaisten on noudatettava sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita (*privacy by design ja privacy by default*) sekä huolehdittava siitä, että tietosuojaa ja henkilötietojen suojaa koskeviin kysymyksiin puututaan mahdollisimman varhaisessa vaiheessa.

Välineenä periaatteiden toteuttamisessa voidaan käyttää tietosuojaa koskevaa vaikutusarvioinnin tekemistä (*Privacy Impact Assessment PIA*). Henkilötietojen käsittelyä koskevassa arvioinnissa on otettava huomioon ainakin tietojen julkaisemisen ja uudelleenkäytön oikeusperusta, käyttötarkoitussidonnaisuudenperiaate, tietojen minimoinnin ja suhteellisuuden periaate, arkaluonteisten tietojen erityissuoja sekä tietojen julkaisemisen vaikutukset rekisteröidyn oikeuksiin.

Vaikutusarvioinnin tarkoituksena on ohjata julkisen sektorin elintä siinä, voiko se julkaista henkilötietoja uudelleenkäyttötarkoituksessa ja, jos voi minkälaiset suoja-toimet sen on otettava huomioon. Vaikutusarvioinnin avulla voidaan myös arvioida anonyymien tiedon luovutukseen liittyviä riskejä.

Komission ehdotuksessa uudeksi yleiseksi tietosuojaja-asetukseksi säädettäisiin sisäänrakennetusta ja oletusarvoisesta tietosuojasta sekä vaikutusarviointien tekemisestä. Rekisterinpitäjän velvollisuuksia koskevassa ehdotuksen 23 artiklan mukaan ”rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, asetuksessa asetettujen vaatimusten toteuttamiseksi ja rekisteröidyn oikeuksien suojelemiseksi. Toimenpiteiden toteuttamisessa on otettava huomioon uusin tekniikka sekä toimenpiteiden ja menettelyjen toteuttamisesta johtuvat kustannukset. Rekisterinpitäjän on varmistuttava siitä, että käsiteltävät henkilötiedot ovat välttämättömiä käsittelyntarkoituksen kannalta, eikä se säilytä tietoja kauemmin kuin on välttämätöntä käsittelyntarkoituksen toteuttamiseksi. Keinojen ja menettelyjen avulla on varmistettava, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville”.

Yleisen tietosuojaja-asetuksen 23 artikla nimenomaisesti kieltäisi sen, että henkilötietoja oletusarvoisesti saatettaisiin kaikkien saataville. Yleisen tietosuojaja-asetuksen 23 artiklan 3 ja 4 kohdat koskevat komissiolle delegoitua valtaa määrittellä asian-

mukaisia toimenpiteitä ja teknisiä standardeja sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseksi.

Henkilötietolain 32 § edellyttää rekisterinpitäjää toteuttamaan tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi. Henkilötietolain 9 §:n 1 momentin tarpeellisuusvaatimus rajaa sitä, että rekisterinpitäjä saa käsitellä vain henkilötietoja, jotka ovat tarpeellisia määritellyn käsittelyn tarkoituksen kannalta. Henkilötietolain huolellisuus- ja suunnitteluvelvollisuus (HetiL 5 § ja 6 §) sekä julkisuuslain hyvää tiedonhallintapaa koskeva 18 § velvoittavat viranomaista suunnittelemaan huolellisesti kaikki henkilötietojen käsittelyyn liittyvät prosessit elinkaarimallin mukaisesti.

Euroopan tietosuojavaltuutettu suosittelee ennakoivaa ja tasapainoista lähestymistapaa uudelleenkäyttöä koskeviin kysymyksiin, jotta henkilötietojen suojeleminen ja uudelleenkäyttöperiaate voitaisiin toteuttaa mahdollisimman täysimääräisesti. Tällöin julkisen sektorin organisaation on analysoitava ennalta, jo tietojen keräämisvaiheessa, niiden luovuttamisiin ja mahdolliseen uudelleenkäyttöön liittyvät seikat ja riskit sekä informoitava rekisteröityjä heidän oikeuksistaan.<sup>285</sup>

#### 6.1.4 Tietotilinpäättös ja tilivelvollisuudenperiaate

Henkilötietolain hyvä tietojenkäsittelytapa (HetiL 1 §) ja julkisuuslain hyvä tiedonhallintatapa (JulkL 18 §) ilmentävät rekisterinpitäjän itseohjautuvuuden merkitystä henkilötietoja käsiteltäessä. Käsitteitä ei ole laintasoisesti määritelty eksaktisti, vaikka julkisuuslainsäädännön mukainen hyvä tiedonhallintatapa on lainsäädännön tasolla yksityiskohtaisemmin määritelty kuin henkilötietolain mukainen hyvä tietojenkäsittelytapa. Hyvä tietojenkäsittelytapa ja hyvä tiedonhallintatapa edellyttävät, että rekisterinpitäjä noudattaa soveltuvia tietosuojalainsäädännöksiä ja erityisesti varmistuu siitä, että rekisteröityjen oikeudet toteutuvat tehokkaasti. Julkisen sektorin tietojenkäsittelyssä on yhdistettävä hyvä tietojenkäsittelytapa ja hyvä tiedonhallintatapa.

---

<sup>285</sup> Euroopan tietosuojavaltuutetun avoimen datan pakettia koskeva lausunto 2012, s. 5 Euroopan tietosuojavaltuutetun mukaan julkisen sektorin tietojen uudelleenkäytössä on kyse tasapainosta henkilötietojen suojaamista koskevan oikeuden ja oikeuden saada tieto viranomaisen asiakirjasta välillä.

Julkisen sektorin tietojen uudelleenkäyttöä ja avoimen datan politiikkaa suunniteltaessa tietotilinpäätöksen kaltaisen yhteenvedon ja toimintasuunnitelman tekeminen on välttämätöntä. Viranomaisen on kartoitettava sen hallussa olevat tietovarannot ja mahdollisuus niiden avaamiselle uudelleenkäytettäväksi. Organisaation on kriittisesti tarkasteltava tarpeellisin väliajoin sen tietoinfrastruktuurin toimivuutta ja sitä, miten henkilötietojen suoja toteutuu tietojenkäsittelyssä. Vaatimus kohdistuu myös anonyymiin tietoon, koska erilaisten tunnistamistekniikoiden kehittyessä, mahdollisuus anonyymin tiedon tunnistettavuudesta kasvaa.

Tietotilinpäätöksellä tarkoitetaan organisaation suorittamaa tarkastelua, jonka kohteena ovat sen tietovarannot, tietojohdaminen, tietojen käsittely ja tietoturvallisuus. Tietotilinpäätöksen tarkoituksena on toimia dynaamisena tehokuutta ja kilpailukykyä lisäävänä työkaluna organisaatiolle.<sup>286</sup> Viranomaistoiminnassa hyvä hallintotapa ja julkisuuslain 18 §:n hyvä tiedonhallintatapa edellyttävät, että organisaation tietojärjestelmät toimivat moitteettomasti, tehokkaasti ja tietoturvallisesti.

Tilivelvollisuuden periaate (*accountability*) edellyttää, että rekisterinpitäjä pystyy näyttämään täyttäneensä kaikki tietojenkäsittelyyn kohdistuvat laissa säädetyt velvollisuudet. Ehdotuksessa yleiseksi tietosuoja-asetukseksi tilivelvollisuuden periaate on huomioitu ehdotuksen 22 artiklassa, jonka mukaan ”rekisterinpitäjän on hyväksyttävä toimintamenetelmät ja toteutettava tarvittavat toimenpiteet sen varmistamiseksi ja osoittamiseksi, että henkilötietojen käsittelyssä noudatetaan yleistä tietosuoja-asetusta”. Velvollisuuden tarkoituksena on saattaa tietosuojaperiaatteet konkreettisiksi toimintatavoiksi. Rekisterinpitäjän on huolehdittava tietosuojaperiaatteiden tehokkaasta toimeenpanosta ja tarvittaessa todistettava, että se on huolehtinut laissa säädettyistä velvollisuuksista.<sup>287</sup> Henkilötietolain huolellisuusvelvoite, suunnitteluvelvoite ja suojaamisvelvoite edellyttävät vastaavanlaisen arvioinnin tekemistä (HetiL 5 §, 6 § ja 32 §).

---

<sup>286</sup> Tietosuojavaltuutetun toimiston opas: ”Laadi tietotilinpäätös” päivätty 24.10.2014, s. 3.

<sup>287</sup> Tietosuojatyöryhmän lausunto 3/2010 tilivelvollisuuden periaatteesta (00062/10/FI WP 173), s.9.

## 6.2 Henkilötietojen siirto kolmansiin maihin

Jos tietojen vastaanottaja on sijoittautunut Euroopan unionin tai Euroopan talousalueen ulkopuolelle on otettava huomioon henkilötietojen siirtoa kolmansiin maihin koskevat erityiset edellytykset. Jos henkilötietoja saatetaan avoimesti uudelleenkäytettäväksi, on hyvin mahdollista, että osa tietojen vastaanottajista on sijoittautunut Euroopan unionin tai Euroopan talousalueen ulkopuolelle. Henkilötietojen siirtona pidetään esimerkiksi käyttöyhteyden avaamista henkilörekisteriin. Ei ole välttämätöntä, että henkilötiedot fyysisesti siirrettäisiin kolmannen maan alueelle.

Jotta henkilötietojen siirto kolmansiin maihin on laillista, henkilötietojen luovutuksen yleisen edellytyksen (Hetil 8§, 12 §, 13 § ja 4 luku) on täyttyvä. Lisäksi tietojen siirron on täytettävä siirrolle asetetut erityiset edellytykset. Lähtökohtana on, että vastaanottavassa maassa on turvattu riittävä tietosuojan taso. Henkilötietodirektiivissä tietojen siirtyä koskevat säännökset ovat sen 25 ja 26 artikloissa ja henkilötietolaissa lain 22 §, 22a § ja 23 §:issä.

Kaikissa henkilötietojen siirroissa rekisterinpitäjän on riittävällä tavalla varmistuttava siitä, että vastaanottajalla on peruste käsitellä henkilötietoja. Henkilötietojen siirroksi katsotaan myös tilanne, jossa Euroopan unionin tai Euroopan talousalueen ulkopuolelle sijoittautunut kolmas osapuoli voi teknisen yhteyden avulla käsitellä henkilötietoja Euroopan unionin tai Euroopan talousalueen ulkopuolella, vaikka tiedot tosiasiallisesti sijaitsevat Euroopan unionin tai Euroopan talousalueen alueella.<sup>288</sup> Tietosuojatyöryhmä on lausunnossaan kiinnittänyt huomiota henkilötietodirektiivin 26 artiklan 1 kohdan f alakohtaan, jonka mukaan siirto voidaan suorittaa tietyin edellytyksin, jos se tehdään tietyistä julkisista rekistereistä. Näin ollen kolmansiin maihin sijoittautuneita toimijoita ei aseteta huonompaan asemaan, kun on kyse oikeudesta saada tiettyjä julkisesti saatavilla olevia tietoja. Tässäkin tapauksessa tietojenkäsittelyn muut laillisuuden edellytysten on täyttyvä.<sup>289</sup>

<sup>288</sup> Tietosuojavaltuutetun opas: Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset s.11.

<sup>289</sup> Tietosuojatyöryhmän lausunto 7/2003 julkisen sektorin tiedon uudelleenkäytön ja henkilötietojen suojan välisestä tasapainosta (10936/03/FI WP 83), s.6.



## 6.3 Käytänneseännöt

Henkilötietolain 42 §:n mukaan ”rekisterinpitäjät tai näitä edustavat yhteisöt voivat laatia toimialakohtaisia käytänneseäntöjä henkilötietolain soveltamiseksi ja hyvän tietojenkäsittelytavan edistämiseksi. Tietosuojavaltuutettu voi tarkastaa, että käytänneseännöt ovat henkilötietolain ja muiden henkilötietojen käsittelyyn vaikuttavien säännösten mukaiset”. Käytänneseäntöjen tarkoituksena on luoda ohjeistuksia ja suosituksia siitä, miten viranomaisten on otettava huomioon henkilötietojen käsittelyn vaikutukset rekisteröityjen yksityisyyden suojalle ja muille yksityisyyttä turvaaville perusoikeuksille.

Käytänneseäntöjen tarkoituksena on tulkita normien sisältöä ja auttaa viranomaisia kehittämään hyvää tietojenhallintatapaa ja tietojenkäsittelytapaa.<sup>290</sup> Käytänneseäntöjä voidaan käyttää apuna, kun viranomainen arvioi tietojen uudelleenkäyttöä ja laajemmin tietojen luovutusten vaikutuksia rekisteröidyn yksityisyyden ja henkilötietojen suojalle. Käytänneseäntöjen avulla voidaan ottaa huomioon toimialakohtaiset erityisyydet.<sup>291</sup>

Käytänneseäntöjä voitaisiin luoda esimerkiksi tunnistamisriskien arviointia varten. Tällöin käytänneseäntöjen avulla voitaisiin ottaa huomioon tietyn viranomaisen tietovarantojen henkilötietojen suojaan kohdistuvat erityiset riskit sekä ohjata viranomaisista arvioimaan tietojen uudelleenkäytön vaikutuksia yksityisyyden kannalta. Käytänneseännöt perustuisivat ”oletusarvoisen ja sisäänrakennetun tietosuojan” periaatteille. Huomioon otettavia seikkoja ovat ainakin julkistamisen oikeusperusta, käyttötarkoitussidonnaisuus ja käyttötarkoituksen rajaaminen, suhteellisuusperiaate ja tietojen laatua koskevat periaatteet.<sup>292</sup>

Hyvään tiedonhallintatapaan kuuluu viranomaiselle asetettu velvollisuus huolehtia siitä, että sen palveluksessa olevilla on tarvittava tieto asiakirjojen julkisuudesta sekä tietojen antamisesta ja käsittelyssä sekä niiden asiakirjojen ja tietojärjestelmien suojaamisesta noudatettavista menettelyistä, tietoturvajärjestelyistä ja tehtävänjaosta,

---

<sup>290</sup> Saarenpää 2012a, s.342.

<sup>291</sup> Tietosuojavaltuutetun toimiston ohje: Toimialakohtaisten käytänneseäntöjen laatiminen, päivitetty 27.7.2010.

<sup>292</sup> Tietosuojatyöryhmän lausunto 6/2013 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä (1021/00/FI WP 207), s.7.

samoin kuin siitä, että hyvän tiedonhallintatavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan (JulkL 18.1 §:n 5 kohta).

Hyvän tiedonhallintatavan toteuttamisesta säädetään tarkemmin asetuksella viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999). Asetuksen 4 §:n mukaan ”viranomaisen on julkisuuslain 18 §:n 1 momentin 5 kohdassa tarkoitettuja toimenpiteitä suunniteltaessa erityisesti pidettävä huolta siitä, että 1) määritellään kenellä on oikeus tehdä asiakirjan antamista koskevia päätöksiä, 2) annetaan riittävät ohjeet asioiden ja asiakirjojen kirjaamisesta sekä asiakirjojen, tietojärjestelmien ja niissä olevien tietojen asianmukaisesta käsittelystä ja suojaamisesta eri käsittelyvaiheissa sekä 3) keskeneräisiä asioita kuvaavat ja niitä koskevat tiedonantovelvollisuuden toteuttamiseksi laaditut luettelot ja asiakirjat pidetään ajan tasalla. Ohjeiden ja toimenpiteiden toteutumista on tarpeellisessa laajuudessa valvottava sekä arvioitava sopivin väliajoin niiden toimivuutta ja muutostarpeita sekä ryhdyttävä toimenpiteisiin puutteiden korjaamiseksi”.

Esimerkkinä viranomaisen käytäntesäännöistä voidaan käyttää Euroopan tilastojen käytäntesääntöjä. Laadukkaan tilastotoiminnan edellytys on luottamus tilastoviranomaisen toimintaan ja korkeaan tietosuojan tasoon. Euroopan unionin komissio on vahvistanut vuonna 2005 Euroopan tilastojen käytäntesäännöt, jotka Euroopan tilastojärjestelmäkomitea on hyväksynyt 28.9.2011. Käytäntesäännöt perustuvat 15 toimintaperiaatteeseen, jotka kattavat institutionaalisen ympäristön, tilastojen tuotantoprosessit ja käytettävyyden.<sup>293</sup>

Tietosuojaa koskevia periaatteita käytäntesäännöissä on 1 kohdan mukainen vaatimus siitä, että tilastotietojen keräämisen ja käsittelemisen on perustuttava lakiin. Käytäntesääntöjen 5 kohdan mukaan tilastojen toimittajien yksityisyys on taattava ja rajataan tietojen tilastollinen käyttötarkoitus. Tilastotietojen tietosuojaa koskevan kohdan mukaan 1) tietosuoja taataan laissa, 2) työntekijän on allekirjoitettava salassapitoa koskeva sitoumus, 3) tietosuojan tahallisuudesta rikkomuksesta seuraa rangaistus, 4) henkilökuntaa on ohjeistettu tietojen suojaamisesta tilastoja laadittaessa ja nämä tietosuojaperiaatteet on oltava kaikkien saatavilla, 5) tilastotiedot suojataan teknisin ja organisatorisin menetelmin ja 6) yksikötason havaintoaineistojen tutkimuskäyttöön sovelletaan tiukkoja toimintasääntöjä ja teknisiä järjestelyitä.<sup>294</sup>

---

<sup>293</sup> Euroopan tilastojen käytäntesäännöt s.1.

<sup>294</sup> Euroopan tilastojenkäytäntesäännöt s. 4.

Tällaisia käytäntöjä voitaisiin luoda myös muille viranomaistahoille, jotka käsittelevät tietomassoja, jotka sisältävät henkilötietoja tai joiden perusteella henkilöiden tunnistaminen on mahdollista. Julkisen sektorin tietojen uudelleenkäyttöä koskevien käytäntöjen luominen on luonnollinen jatkumo viranomaisen tietovarantojen kartoitukselle ja tunnistamiselle.

## 7. Lopuksi

Julkisen sektorin tietovarantojen avaaminen on kovassa vauhdissa vuonna 2014. Tietojen avaamiseen liittyviä lainsäädännöllisiä ja teknisiä esteitä poistetaan ja viranomaisia veloitetaan kartoittamaan ja tunnistamaan avattavia tietovarantoja ja tietojärjestelmiä.<sup>295</sup> Lainsäädännöllisten muutosten tarkoituksena on tehostaa yleisestikin viranomaisen hallussa olevien tietojen käytettävyyttä ja saatavuutta.

Sekä Euroopan unionin että kansallisissa tietoyhteiskuntaa koskevissa strategioissa, päätöksissä ja linjauksissa on otettu huomioon tietojen avaamisen mahdollinen vaikutus tietosuojaan, niin yksityisyyden kuin muutenkin salassa pidettävien tietojen osalta. Strategioiden ja päätösten linjaukset liittyvät kuitenkin pitkälti tekijänoikeuksiin liittyvän lisensoinnin, tietojen maksuttomuuden ja teknisten käyttöyhteyksien arviointiin, parantamiseen ja helpottamiseen. Henkilötietojen suojan osalta on pääsääntöisesti tyydytty toteamaan, että tietovarantojen avaaminen uudelleenkäytettäväksi ei saa heikentää yksityisyyden suojaa. Julkista valtaa käyttävien on pyrittävä aktiivisesti minimoimaan kansalaisten yksityisyyden suojaan kohdistuvat riskit.

PSI-direktiivissä veloitetaan Euroopan unionin jäsenvaltioita arvioimaan tietovarantojen uudelleenkäytön mahdollisuuksia ja avaamaan sellaiset julkisen sektorin tietoaineistot uudelleenkäytettäväksi, joihin ei liity lainsäädännöllisiä rajoituksia. PSI-direktiivi ei muodosta erillistä henkilötietojen käsittelyn perustetta, joten jäsenvaltiot eivät voi sen nojalla avata henkilötietoja sisältäviä tietoaineistoja uudelleenkäytettäväksi. PSI-direktiivissä nimenomaisesti säädetään siitä, että tietovarantoja avatessa on otettava huomioon henkilötietojen suojaa koskevat säännökset täysimääräisesti. Tietovarantojen avaaminen ja uudelleenkäyttö perustuu jäsenvaltioiden julkisen sektorin tietojen julkisuutta ja tietojen luovuttamista koskeviin säännöksiin.

Oikeus tietoon ja oikeus yksityiselämän ja henkilötietojen suojaan ovat perusoikeus-tasoisia oikeuksia, joiden aktiivinen turvaaminen on perustuslain nojalla julkisen vallan tehtävä. Julkisen sektorin tietojen uudelleenkäytön yhteydessä viranomaisten on pystyttävä tasapainottamaan nämä oikeudet keskenään niin, että ne molemmat toteutuvat mahdollisimman täysimääräisesti. Tiedon julkisuudella tarkoitetaan viranomaisen tuottaman tiedon julkisuutta, ei yksittäisen kansalaisen henkilötietojen tai yksi-

---

<sup>295</sup> Julkisten tietovarantojen avaaminen ja kehysvalmistelut 2015-2018 ohje, annettu 23.10.2013.

tyiselämän julkisuutta suhteessa muuhun yhteiskuntaan. Henkilötietolain säännöksistä johtuen, henkilötunnisteellista dataa tai tietoa, josta henkilö on tunnistettavissa, ei voida saattaa avoimesti uudelleenkäytettäväksi. Poikkeuksellisesti tästä tulisi säätää laintasoisella säädöksellä.

On selvää, että julkisen sektorin tietojen uudelleenkäyttö ja tietovarantojen avaaminen eivät saa heikentää henkilötietojen suojaa. Henkilötietojen käsittelyn on aina perustuttava lakiin (PeL 10.1 §). Rekisteröidyn oikeudet on otettava huomioon julkisen sektorin tietojen käsittelyssä. Huomiota on kiinnitettävä siihen, miten eri julkisen tiedon saatavuuteen vaikuttavat ohjelmat, toimenpiteet ja lainmuutokset vaikuttavat rekisteröityjen mahdollisuuteen hallinnoida oikeuksiaan. Vaikka julkinen sektori julkistaisi henkilötietoja, esimerkiksi erilaisten tietopalveluiden yhteydessä, on luovutuksensaajan otettava täysimääräisesti huomioon henkilötietolain säännökset. Kun luonnollisen henkilö käsittelee henkilötietoja henkilökohtaisiin tarkoituksiinsa, ei henkilötietojen käsittelyyn sovelleta henkilötietolain säännöksiä (HetiL 2.3 §).

Kaiken tiedon, erityisesti henkilötietojen, ei tule olla vapaasti saatavilla ja uudelleenkäytettävissä. Tiedon julkisuutta ja julkaistavuutta rajoitetaan ja on rajoitettava yksityisyyden suojelemiseksi. Avoimen tiedon ja julkisuusperiaatteen kohteena on viranomaisen tuottama tieto, ei yksittäistä henkilöä koskevat henkilötiedot. Valtiovarainministeriön neuvotteleva virkamies Mikael Vakkari toteaa, että ”virastojen mukaan yksi keskeisistä tunnistetuista ongelmista datan avaamisessa on juuri tietosuojarit”<sup>296</sup>.

Yksityisyyden ja henkilötietojen suojaan kohdistuvat riskit liittyvät yleisesti henkilötietojen käsittelyyn ennalta määrittelemättömiin tarkoituksiin ja käsittelyjen tulosten vaikuttaminen rekisteröidyn elämään tavalla tai toisella. Riskit eivät liity pelkästään henkilötietojen saatavuuden parantamiseen vaan myös anonyymien tietojen luovutuksiin. Tietovarantoja yhdistelemällä voidaan luoda päätelmiä, jotka voivat vaikuttaa yksittäisten kansalaisten elämään. Henkilötiedoilla on taloudellista arvoa vaihdannan hyödykkeenä. ja välineenä. Näin ollen on mahdollista, että eri tahot pyrkivät hyödyntämään kasvavia tietomassoja henkilöiden tunnistamisessa.

Tietojen saatavuuden parantamisessa on haasteena muun muassa se, ettei yksityisyyden suojaan liittyvät vaikutuksia välttämättä pystytä näkemään ennalta tai välittömästi. Kun viranomaiset tietovarantojaan avatessa ovat tietoisia keskeisistä uhista ja ni-

---

<sup>296</sup> Castrén, Tietosuoja –lehti 02/2014, s.29.

menomaan niistä, mitkä kohdistuvat heidän hallussa oleviin tietovarantoihin, pysytään haasteisiin vastaamaan tehokkaasti. Viranomaisten tulee tuntee keskeiset henkilötietojen käsittelyyn vaikuttavat periaatteet ja säännökset. Tämä edellyttää hyvää tietojenhallintatapaa sekä erilaisten vaikutusarviointien, kuten tietotilinpäätöksien, tekemistä. Viranomaisten on arvioitava myös anonyymien tietojen luovutukseen kohdistuvia henkilöiden tunnistamiseen liittyviä riskejä. Tunnistamisriskiä on arvioitava koko tiedon elinkaaren ajalta.

Tutkielmassa esitettyjen henkilötietolain periaatteiden tarkoituksena on hyvän tietojenkäsittelytavan omaksuminen osaksi henkilötietojen käsittelyä sekä taata rekisteröityjen yksityiselämän suoja henkilötietoja käsiteltäessä. Näin ollen periaatteiden turvaaminen ja huomioonottaminen ovat keskeisiä tekijöitä aina, kun tietojenkäsittelyyn liittyy henkilötietojen käsittelyä. Jos henkilötietoja asetettaisiin uudelleenkäytettäväksi avoimesti ja mihin tahansa tarkoitukseen, olisi periaatteiden toteutuminen hyvin epävarmaa.

Julkisuuslain nojalla henkilötietoja sähköisesti luovutettaessa, viranomaisen on varmistuttava siitä, että tietojen vastaanottajalla on henkilötietojen suoja koskevien säännösten perusteella oikeus käsitellä kyseisiä tietoja. Keskeinen henkilötietojen suoja koskeva periaate on käyttötarkoitussidonnaisuuden periaate, joka sitoo henkilötietojen myöhemmän käsittelyn sen alkuperäiseen käsittelyn tarkoitukseen. Erityisesti viranomaistoiminnassa henkilötietojen suoja koskevien periaatteiden toteutumisella on merkitystä myös kansalaisten luottamuksen kannalta. PSI-direktiivissä nimenomaisesti huomioidaan se, että vaikka henkilötiedot ovat kansallisten asiakirjojen saatavuutta koskevien säännösten nojalla julkisia, voidaan henkilötietojen uudelleenkäyttöä rajoittaa henkilötietojen suojaamiseksi silloin, kun tietojen uudelleenkäyttö on ristiriidassa henkilötietojen suoja koskevan lainsäädännön kanssa.

Julkisuusperiaatteen asema modernissa tietoyhteiskunnassa liittyy myös tietojen taloudellisen hyödyntämisen mahdollistamiseen. Perinteisesti viranomaisen tiedon julkisuus ja avoimuus toteutetaan tietoja pyydettyäessä. Tosin julkisuuslain 20 § velvoittaa viranomaisia oma-aloitteiseen aktiivisuuteen tiedon tuottamisessa ja jakamisessa. Lähtökohtana tietojen uudelleenkäytölle ovat olemassa olevat viranomaisen hallussa olevien tietojen luovutuksia koskevat säännökset. Säännöksiä liittyy julkisuuslain ohella useaan erityissäännökseen, joissa henkilötietojen luovutukset on yleensä sidottu tiukasti niiden käsittelyntarkoitukseen. Henkilötietojen luovuttamisen osalta lähtö-

kohtana on, että vastaanottajalla on henkilötietolain mukainen oikeus käsitellä vastaanotettavia tietoja.

Jotta viranomaisella voisi saattaa henkilötietoja uudelleenkäytettäväksi tai yleensä luovuttaa henkilötietoja, on tästä säädettävä nimenomaisesti laissa. Julkisuuslain henkilötietojen luovuttamista koskevat yleissäännökset eivät oikeuta henkilötietojen rajattomaan uudelleenkäyttöön ilman rekisteröidyn suostumusta. Korkein hallinto-oikeus on 25.10.2012 antamassaan ratkaisussa 1694/1/11 katsonut, silloin kun henkilötietojen luovuttaminen on lainsäädännössä sidottu niiden käyttötarkoitukseen, merkitsee tämä julkisuusperiaatteen rajoitusta. Näin on esimerkiksi silloin, kun tietoja pyydetään viranomaisen henkilörekisteristä julkisuuslain 13.2 §:n mukaan.

Julkisuuslain 21 §:n mukaan viranomaisella voi pyynnöstä tuottaa ja luovuttaa eri käyttötarkoituksia varten digitaalisessa muodossa olevan tietoaineiston, jos tietoaineiston luovuttaminen ei sen muodostamisessa käytettyjen hakuperusteiden, tiedon määrän tai laadun taikka tietoaineistojen käyttötarkoituksen vuoksi ole vastoin sitä, mitä asiakirjan salassapidosta ja henkilötietojen suojasta säädetään.

Julkisuuslain 21 §:n mahdollistaa julkisuusperiaatteesta erillisen mahdollisuuden tiedon saantiin ja kaupalliseen hyödyntämiseen.<sup>297</sup> Tyypillistä on, että viranomaisella yhdistää sen hallussa olevia sähköisiä rekistereitä esimerkiksi markkinointi- tai tutkimustarkoitukseen.<sup>298</sup> Pykälän sananmuodon mukaisen tulkinnan perusteella tietoaineiston luovuttaminen myös julkisuuslain 21 §:n perusteella edellyttäisi tiedon haki- jalta erityistä aktiivista pyyntöä. Pyyntöä esittäminen on mahdollista, jos pyynnön esittäjä tietää, mitä tietoaineistoja ja tietovarantoa viranomaisella on hallussaan. Julkisuuslain 18 §:n 1 momentin 2 kohdan mukaan viranomaisella on laadittava ja pidettävä saatavilla kuvaukset pitämistään tietojärjestelmistä ja niissä saatavissa olevista julkisista tiedoista, jollei tiedon antaminen ole vastoin 24 §:n tai muun lain säännöstä.

Viranomaisella on julkisuuslain 20 §:n 1 momentin nojalla edistettävä toimintansa avoimuutta ja tässä tarkoituksessa laadittava oppaita, tilastoja ja muita julkaisuja sekä muita tietoaineistoja palveluistaan, ratkaisukäytännöstään sekä yhteiskuntaoloista ja niiden kehityksestä toimialallaan. Jos kyse on henkilötunnisteita sisältävän tiedon

---

<sup>297</sup> Konstari, Wallin 2000, s.80–81, s.304.

<sup>298</sup> Mäenpää 2008, s. 228.

käsittelystä, viranomaisen on otettava huomioon henkilötietojen suoja koskevat säännökset.

Henkilötietolain säännöksistä johtuen lainmukaiset edellytykset henkilötietojen luovutukselle eivät julkisuuslain nojalla täyty, jos viranomainen julkaisee henkilötietoja avoimessa tietoverkossa. Julkisuuslain 20 § ja 21 § mahdollistaisivat viranomaisen hallussa olevan tiedon julkaisemisen esimerkiksi anonyymina tilastotietona. Anonyymintiedon luovuttamisessakin on käytettävä harkintaa ja arvioitava, mikä on se riski, että henkilöt voitaisiin edelleen tunnistaa uudelleenkäytettäväksi annetuista tiedoista. Viranomaisilta vaaditaan hyviä tiedonhallintataitoja ja resursseja hyvän tiedonhallintatavan varmistamiseen ja ylläpitämiseen. Julkisen vallan on taattava perusoikeuksien täysimääräinen toteutuminen. Liika varovaisuus ei saa kuitenkaan olla esteenä tietovarantojen avaamiselle.

Julkisten sektorin tietojen uudelleenkäyttöä koskevan normiston ymmärtäminen vaatii laaja perspektiiviä avoimen datan politiikkaan ja sen vaikutuksiin yhteiskunnassa. Avoimen tiedon politiikka tukee myös viranomaistoiminnan läpinäkyvyyttä ja tietojen tehokasta hyödyntämistä ohi perinteisen avoimen datan ajattelumallin, jossa tietovarannot avataan uudelleenkäytettäväksi kokonaisuudessaan ilman teknisiä rajoituksia sekä, mihin tahansa ennalta määrittelemättömään tarkoitukseen.