Acta Universitatis Lapponiensis 325

Juhani Korja

Biometrinen tunnistaminen ja henkilötietojen suoja

Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta

Akateeminen väitöskirja,
joka Lapin yliopiston oikeustieteiden tiedekunnan suostumuksella
esitetään julkisesti tarkastettavaksi Lapin yliopiston luentosalissa 19
toukokuun 27. päivänä 2016 klo 12

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Rovaniemi 2016

Lapin yliopisto
Oikeustieteiden tiedekunta

Kansi: Pasi Kainulainen
Kannen alkuperäinen kuva: Igor Stevanovic © 123RF.com;
muokkaus Pasi Kainulainen
Taitto: Pasi Kainulainen

Myynti:
Lapin yliopistokustannus
PL 8123
96101 Rovaniemi
puh. 040 821 4242
julkaisu@ulapland.fi
www.ulapland.fi/lup

Hansaprint Oy, Turenki 2016

Painettu:
Acta Universitatis Lapponiensis 325
ISBN 978-952-484-899-2
ISSN 0788-7604

Pdf:
Acta electronica Universitatis Lapponiensis 193
ISBN 978-952-484-900-5
ISSN 1796-6310

Sisällys

LYHENTEET

CBPL	Belgian tietosuojaviranomainen
Dnro	Diaarinumero
EIF	Encyclopaedia Iuridica Fennica, oikeustietosanakirja
EIS	Euroopan neuvoston ihmisoikeussopimus; Euroopan neuvoston yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi
EIT	Euroopan neuvoston ihmisoikeustuomioistuin
EN	Euroopan neuvosto
EOA	Eduskunnan oikeusasiamies
EU	Euroopan unioni
EU:n henkilötietodirektiivi	Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta
EU:n passiasetus	Euroopan neuvoston asetus (EY) N:o 2252/2004, annettu 13 päivänä joulukuuta 2004, jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista
EU:n yleinen tietosuoja-asetus	Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta
Euroopan tietosuojasopimus	Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä 1981 (SopS 36/1992)
EY	Euroopan yhteisö
EYT	Euroopan yhteisöjen tuomioistuin
FBI	Yhdysvaltain liittovaltion keskusrikospoliisi
HaVM	Hallintovaliokunnan mietintö

HE	Hallituksen esitys
HenkRekL	Henkilörekisterilaki 471/1987
HetiL	Henkilötietolaki 22.4.1999/523
HM	Suomen Hallitusmuoto
ICAO	Kansainvälinen siviili-ilmailujärjestö
ILO	International Labour Organization, Kansainvälinen työjärjestö
IP-osoite	Internetin protokollaosoite
KHO	Korkein hallinto-oikeus
KKO	Korkein oikeus
KM	Komiteamietintö
N.Y.S.	New York State
PeL	Perustuslaki
PeVL	Perustuslakivaliokunnan lausunto
PeVM	Perustuslakivaliokunnan mietintö
PIN-koodi	Personal identification number, tunnusluku
PolHetiL	Laki henkilötietojen käsittelystä poliisitoimessa(22.8.2003/761); poliisin henkilötietolaki
PVN	Norjan tietosuojalautakunta (Personvernnemnda)
RF-siru	Radiotaajuuksia (radio frequency) hyödyntävä jäljitysmenetelmä
RL	Rikoslaki
SopS	Suomen säädöskokoelman sopimussarja
SOU	Statens Offentliga Utredningar (Ruotsin komiteanmietintö)
U.S.	United States
USA	The United States of America
TSL	Työsopimuslaki
TT	Työtuomioistuin
VP	Valtiopäivät
YK	Yhdistyneet kansakunnat
YksTL	Laki yksityisyyden suojasta työelämässä
YTL	Laki yhteistoiminnasta yrityksissä; yhteistoimintalaki

ALKUSANAT

Siitä lähtien, kun olin ala-asteen viimeisillä luokilla, olen halunnut juristiksi. En kyllä koskaan arvannut kiinnostuksen oikeustiedettä kohtaan kasvavan väitöskirjan tasolle asti. Niin vain kävi. Voisi sanoa nälän kasvaneen syödessä. Muutaman kerran olen väitöskirjaa kirjoittaessa miettinyt, ettei tämä ole järkevää touhua. Ajatusmaailma kuitenkin muuttuu kirjoittamisen aikana. Nyt en vaihtaisi hetkeäkään pois. Elämme vain kerran ja aika on kallisarvoista, ja väitöskirjan kirjoittaminen on muuttanut minua ihmisenä. Ymmärrän paremmin elämää, ja olen tyytyväinen saavuttamaani. Ei sitä kuitenkaan jokainen kirjaa kirjoita.

Väitöskirjan kirjoittamista prosessina on mahdollista kuvata lainaamalla Ridley Scottin Robin Hood elokuvan sanontaa: *"Rise and rise again until lambs become lions."* Sanonnalla viitataan siihen, että koskaan ei pidä antaa periksi, vaikka tehtävä tuntuisi kuinka mahdottomalta. Väitöskirjan kirjoittaminen on näet prosessi, joka vaatii pitkäjänteisyyttä, kärsivällisyyttä ja ennen kaikkea kykyä sietää turhautumista. Muistaa tulee kuitenkin se, että aika kultaa muistot. Tietyt asiat nimittäin ovat taistelemisen arvoisia. Ja lopussa kiitos seisoo. Väitöskirjan kirjoittamisessa tärkeintä on muistaa, että tärkeintä ei ole määränpää vaan matka.

Suuri kiitos kuuluu ohjaaville professoreille *Ahti Saarenpäälle* ja *Rauno Korhoselle*, jotka antoivat paljon hyödyllisiä neuvoja ja korvaamatonta apua väitöskirjan kirjoittamisen alusta lähtien. Jokainen kohtaa tieteellisiä ongelmia väitöskirjan kirjoittamisen aikana, mutta teiltä olen saanut apua tieteellisten kysymysten pohdinnassa ja ratkaisussa. Olette pitäneet huolta edellytysten säilymisestä tutkimuksen etenemiselle. Niin ikään olette olleet ohjaamassa tutkimustani vaativalla, mutta

palkitsevalla tavalla. En olisi voinut pyytää parempaa ohjaajaparivaljakkoa väitöskirjalleni.

Haluan kiittää myös esitarkastajina toimineita professori Päivi Korpisaarta ja dosentti Tuomas Pöystiä, jotka omilla neuvoillaan auttoivat väitöskirjan viimeistelyssä.

Kaikki, jotka ovat kirjoittaneet tai kirjoittamassa väitöskirjaa tietävät, ettei sen kirjoittaminen onnistu ilman taloudellista apua. Tästä avusta haluan kiittää Suomen Kulttuurirahaston Lapin rahastoa, joka myönsi minulle korvaamattoman ensimmäisen apurahan keväällä 2011. Ilman tätä apurahaa olisi todennäköisesti ollut huomattavasti hankalampaa saada työ valmiiksi.

Kiitos Lapin rahastolle alkusysäyksen antamisesta. Kiitos myös Suomen Lakimiesliitolle ja Suomalaiselle Lakimiesyhdistykselle, jotka tukivat työtäni apurahalla. Suomen Akatemia on myös myöhemmin myöntämällään tutkimusprojektirahoituksella mahdollistanut työni jatkumisen. Vuoden 2011 lopulla pääsin tutkijaksi Verkkoyhteiskunta oikeudellisen ja yhteiskunnallisen ajattelun paradigmana –tutkimushankkeeseen. Kiitän Suomen akatemiaa, joka tutkimushankkeelle myöntämällään rahoituksella on omalta osaltaan ollut mahdollistamassa tutkimukseni katkottoman jatkumisen.

Suuret kiitokset myös Lapin yliopiston oikeustieteiden tiedekunnalle, joka on ollut varmistamassa tutkimukseni etenemistä antamalla minulle tutkijan paikan tiedekunnassa.

Oman kokoisensa kiitokset ansaitsee myös Cornell Legal Information Instituten johtaja Thomas Bruce, joka auttoi Yhdysvaltojen lainsäädäntöä koskevan osion valmiiksi saamisessa. Thomasia haluan erityisesti kiittää mahdollisuudesta tehdä tutkimusta Cornell University Law Schoolissa. Ilman tätä mahdollisuutta ja tukea tutkimuksen tekeminen Yhdysvalloissa olisi ollut hankalaa. Thank You very much, Thomas!!

Unohtaa ei tule myöskään sitä, että väitöskirjan kirjoittaminen on sitä helpompaa mitä enemmän saa kannustusta ja tukea kaikkein lähimmiltä. On vähintään outoa lainata tieteellisen väitöskirjan alkusanoissa iskelmätähtiä, mutta tällä kertaa lausuma on niin osuva, ettei sitä voi olla ohittamatta. Matti ja Teppo ovat laulaneet: *"Kaiken takana on nainen"*. Niin on myös tämän tutkimuksen kohdalla. Haluankin siis kiittää vaimoani *Helenaa* kaikesta siitä tuesta, avusta ja ymmärryksestä, jonka olen saanut väitöskirjan kirjoittamisen aikana. Voin rehellisesti sanoa, etten välttämättä olisi saanut väitöskirjaa aikaiseksi ilman tätä tukea. Olet nähnyt minut väitöskirjan kirjoittamisen aikana huonoimmillani ja parhaimmillani. Olet jaksanut olla tukena ja apuna, kun olen sitä tarvinnut.

Haluan kiittää myös vanhemmiltani *Liisalta* ja *Anterolta* saamaani tukea. Te olette luoneet ne edellytykset, joiden avulla on ollut helppo pärjätä omin avuin. Tiedän myös, ettei ole ollut helppoa katsoa sivusta, kun oma lapsi tuskissaan tekee väitöskirjaa. Näin haluankin kiittää Teitä äiti ja isä aivan kaikesta. Ilman Teitä en olisi tässä, sillä Te olette luoneet turvallisen ympäristön kasvamiselle ja itsenäistymiselle.

Myöskään sisaruksiltani *Antilta* ja *Veeralta* saamaani tukea ei voi olla unohtamatta. Tiedän, etten ole ollut helppo tämän väitöskirjaprosessin aikana. Myös vaimoni vanhemmat *Marja* ja *Eero* ansaitsevat suuret kiitokset kaikesta kannustuksesta ja tuesta.

Lopuksi haluan kiittää koiraamme *Jetiä*, joka jatkuvalla leikkisyydellään on saanut ajatukseni muualle.

Omistan väitöskirjani vaimolleni Helenalle.

Hyvinkäällä ja Rovaniemellä syksyllä 2015

Juhani Korja

ESIPUHE

Uudet rikollisuuden muodot ja tarve yksilön vahvaan tunnistamiseen ovat korostaneet turvallisuuden merkitystä yhteiskunnassa. Eri maissa on kehitetty uusia valvontateknologioita ja otettu niitä käyttöön. Biometrinen tunnistaminen on esimerkki tällaisen uuden teknologian käytöstä. Sillä yleisesti tarkoitetaan ihmisen automatisoitua tunnistamista jonkin fysiologisen ominaisuuden tai käyttäytymispiirteen perusteella. Vaikka biometrinen tunnistaminen ei ole pelkästään valvontateknologia, aiheuttavat sen tuomat valvonta ja kontrollimahdolisuuksien yleityminen vastarintaa eri maissa.

Biometrinen tunnistaminen kuitenkin yleistyy. Kannettavat tietokoneet ja älypuhelimet ovat avattavissa sormenjäljellä, kuntosalille voi kirjautua sisään sormenjälkeä käyttäen ja EU-alueen sekä Yhdysvaltojen ja Kanadan passeissa hyödynnetään biometrisia tunnisteita.

Biometrisen tunnistamisen sanotaan olevan pettämätön ja erehtymätön ratkaisu nykymaailman ongelmiin oli kysymys sitten turvallisuudesta tai markkinoinnista. Biometrian hyödyntämättä jättämisen katsotaan nykymaailmassa olevan iso riski, jota ei ole varaa ottaa. Se myös nähdään nykymaailman välttämättömyytenä, jonka avulla on mahdollista suojautua vaarallisessa maailmassa. Väitetään, että tässä maailmassa tarvitaan lisääntyvää valvontaa turvallisuuden takaamiseksi. On myös esitetty, ettei siinä ole mitään pelättävää, jos ei ole mitään salattavaa.

Moderni biometrinen tunnistaminen on yksi verkkoyhteiskunnan tyypillisistä toimintamalleista. Teknologisen imperatiivin ajatuksen mukaisesti sekä hallinnon eri sektoreilla että myös yksityissektorilla erilaiset biologisen tunnistamisen toteutustavat kuuluvat usein välineisiin, joiden avulla tavoitellaan varmuutta, tehokkuutta ja hallintotaakkojen vähentämistä eri toiminnoissa. Tietoteknisten mahdollisuuksien

vastapainoksi on asetettu vähimmän puuttumisen periaate ihmisoikeusperusteisena ihmisen itsemääräämisoikeuden suojana. Jos tätä ei tunnisteta oikea-aikaisesti ja oikealla tavalla, syntyy merkittäviä jännitteitä tietoteknisen kehityksen ja ihmisoikeuksien välillä.

Nykyisin biometrisen tunnistamisen merkitys kasvaa. Teknologian kehitys on tehnyt mahdolliseksi biometristen tunnisteiden käytön. Tunnistamiseen liittyvät tietosuojaa ja yksityisyyden suojaa koskevat kysymykset ovat nousemassa huolestuttavasti esille julkisen sektorin ohella myös kaupan ja liikenteen alueella. Suomessa biometrisia tunnisteita on otettu käyttöön vuoden 2006 passilakiuudistuksen yhteydessä ja vuoden 2012 oleskelulupakortin muutoksella. Oikeusinformatiikkan ja persoonallisuusoikeuden yhteydessä on mahdollista puhua jo ns. tunnisteoikeuden erityskysmyksistä.

Kansainvälisesti biometrinen tunnistaminen on myös erittäin ajankohtainen. Vuodesta 2010 alkaen esimerkiksi intialaiset ovat saaneet käyttöönsä pelkän numeron, jonka avulla heidän sormenjälkensä ja iiristunnisteensa löytyvät jättimäisestä tietokannasta.

EU:ssa myös kiinnitetään entistä enemmän huomiota biometrisen tunnistamisen käyttöön ottoon. Tästä on osoituksena biometrinen passi. Se on otettu myös meillä Suomessa käyttöön passilain uudistuksella vuonna 2006. Toisena esimerkkinä on oleskelulupakortti, johon tallennetaan kortinhaltijan biometrisena tunnisteena kasvokuva ja sormenjälki.

Erityisesti Yhdysvalloissa biometrinen tunnistaminen on suuren kiinnostuksen ja kehityksen kohteena. Yhdysvalloissa myös on käytössä biometrinen passi, jossa biomterisena tunnisteena käytetään kasvokuvaa. Biometrisia tunnisteita käytetään myös osavaltiotasolla ajokorteissa sekä pankkien palveluissa. Biometrisen tunnistamisen kasvavasta merkityksestä on osoituksena se, että Yhdysvalloissa toimii erityinen puolustusministeriön alainen Biometrics Identity Management Agen-

cy, jonka tarkoituksena on toimia biometrisen tunnistamisen ”markkinajohtajana” ja kehittäjänä.

Biometrisesta tunnistamisesta on esitetty kahdenlaisia näkemyksiä sen vaaroista yksityisyyden suojalle ja ylipäätään demokratialle. Ensinnäkin biometrinen tunnistaminen nähdään teknologiana, joka uhkaa yksilöiden ja yhteiskunnan vapautta. Biometrisen tunnistamisen koetaan olevan persoonatonta, joka mahdollistaa erillään olevan informaation kokoamisen yhdeksi profiiliksi yksilöstä. Toisaalta biometrinen tunnistaminen nähdään yksityisyyttä suojaavana teknologiana, jonka avulla suojataan identiteettiä ja tiedollista koskemattomuutta.

Näiden näkemysten ytimessä on ihmis- ja perusoikeuksien tasapaino, erityisesti yksityisyyden suojan ja turvallisuuden tasapaino. Lisääntyvän valvonnan ja biometristen tunnisteiden aikakaudella tämä tasapaino joudutaan todennäköisesti etsimään uudestaan. Yksityisyyden ja turvallisuuden välinen tasapaino ei ole koskaan ollut staattinen. Päinvastoin se on jouduttu aika ajoin hakemaan uudestaan yleensä lisääntyvän turvattomuuden takia. Tällöin yksityisyys on yleensä ollut se, josta on joustettu. Tämä on myös yksi syy valvonnan lisääntymiselle yhteiskunnassa.

Biometriaa on hyvin vähän tutkittu oikeustieteen näkökulmasta. Ensiarvoisen tärkeää on kiinnittää huomiota biometrisen tunnistamisen mukanaan tuomiin perusoikeuskysymyksiin. Biometristen tunnisteiden käyttöönotto ilman riittävää tietoa tämän teknologian riskeistä aiheuttaa vaaran sen väärinkäytöstä.

Biometrisen tunnistamisen myötä on vaarana, että yksityisyyden suoja rapautuu ja että valvonta lisääntyy huomaamatta ja nopeasti. Kehityksen kannalta keskiössä ovat erilaiset tietojärjestelmät ja rekisterit sekä niissä olevat henkilötiedot ja näiden tietojen käsittely.

Demokraattisessa yhteiskunnassa yksilöillä tulee olla oikeus elää elämäänsä anonyymisti suhteessa julkiseen valtaan ja muihin organisaatioihin. Tämän vuoksi demokraattisessa yhteiskunnassa yksityisyydellä tulee olla korostunut merkitys. Koska biometrinen tunnistaminen yleensä koetaan uhkana yksityisyydelle, tulee siihen ja sen käyttöön suhtautua varauksella.

JAKSO I JOHDANTO

1. Teoreettinen viitekehys, teema ja näkökulma

”Tieteen tulee alkaa myyteistä ja niiden kritiikistä.”
Sir Karl Popper.

1.1. Tutkimustehtävä ja sen asettaminen

1.1.1. Tutkimustehtävä

Tämän tutkimuksen lähtökohtana on tarkastella biometrista tunnistamista henkilötietojen suojan, itsemääräämisoikeuden sekä yksityisyyden ja yksityiselämän suojan näkökulmasta. Tarkoituksena tutkimuksessa on tunnistaa yksityisyyden, yksityiselämän suojan ja henkilötietojen suojan käsitteiden kautta teknologisen kehityksen vaikutus näiden oikeuksien sisältöön. Teemana on lisäksi, miten biometristen sovellusten käyttöönotto vaikuttaa yksilöiden yksityisyyteen ja henkilötietojen suojaan.

Tarkasteltaessa lähemmin tutkimuksen pääalueita eli biometrista tunnistamista ja henkilötietojen suojaa, asetetaan muutama tarkentava kysymys, joihin tutkimuksessa on tarkoitus syventyä:

- Mitä on biometrinen tunnistaminen?
- Mitä tarkoitetaan henkilötiedoilla ja henkilötietojen käsittelyllä?
- Mitä vaikutuksia biometrisella tunnistamisella on henkilötietojen suojaan ja yksityisyydelle?
- Miten yksityisyyttä ja henkilötietojen suojaa säännellään Suomessa, EU:n lainsäädännössä ja Yhdysvalloissa?

Varsinainen oikeudellinen kysymys on esitettävissä seuraavasti: *Miten yksityisyyttä ja henkilötietoja suojataan lainsäädännössä biometrisen tunnistamisen kohdalla?* Lisäksi tutkimuksessa selvitetään niitä yhteiskunnallisia ja oikeudellisia taustatekijöitä, jotka ovat vaikuttaneet biometrisen tunnistamisen käyttöönoton lisääntymiseen. Niitä on tarkoitus käyttää tutkimuksen työkaluina paremman kuvan saamiseksi biometrisen tunnistamisen tarkoituksesta yhteiskunnassa.

Edellä mainittuihin tutkimuksen teemaa koskeviin kysymyksiin liittyen vastataan seuraavaan kysymykseen: Tarvitsemmeko yhteiskunnassa todella biometrista tunnistamista yhteiskunnan ja yksilöiden turvallisuuden parantamiseksi vai onko kysymyksessä vain yksi teknologisen imperatiivin[1] ilmentymä, jonka avulla on mahdollista kerätä entistä enemmän informaatiota yksilöistä esimerkiksi valvontaa varten? Kysymys on varsin oleellinen, sillä tunnistaminen on mahdollista nähdä valvonnan välineenä, ja valvonta puolestaan toimii vallankäytön välineenä yhteiskunnassa. Tämän näkökulman huomioiminen on ensiarvoisen tärkeää myös sen vuoksi, että yksilöillä on oikeus elää anonyymisti yhteiskunnassa. Eräänä kysymyksenä tutkimuksessa on myös, tarvitaanko uutta lainsäädäntöä biometriseen tunnistamiseen liittyen.

Koska tutkimuksessa keskitytään biometrisen tunnistamisen oikeudelliseen puoleen ja biometriseen tunnistamiseen liittyviin oikeudellisiin ongelmiin, rajataan tutkimuksen ulkopuolelle biometrisen tunnistamisen tekninen puoli eli se, miten biometrisen tunnistamisen

1 Teknologisella imperatiivilla tarkoitetaan yleisesti kulttuurista, sosiaalista ja arkista painetta teknologioiden käyttöön sekä teknologioiden vallitsevuutta yhteiskunnassamme. Käsitteestä tarkemmin katso Georg Henrik von *Wright,* Tiede ja ihmisjärki – suunnistusyritys. Katso myös *Clarke,* Five Most Vital Privacy Issues, jossa Clarke ottaa kantaa teknologiseen imperatiiviin biometrian kohdalla.Artikkeli on saatavissa osoitteesta: http://www.rogerclarke.com/DV/VitalPriv.html

järjestelmät teknisesti toimivat. Samoin tutkimuksen ulkopuolelle jää biometrisen tunnistamisen käyttöturvallisuuteen liittyvä keskustelu. Siinä keskiössä on se, miten turvallista biometrian käyttäminen on ihmisen terveydelle.[2]

1.1.2. Tutkimusmetodi

Oikeustieteellisen tutkimuksen keskeinen asia on tutkimusmetodi. Jotta tieteellistä työtä on mahdollista arvioida, on tutkimusmetodi kerrottava avoimesti. Metodin avulla tutkija pystyy osoittamaan, että tutkimuksen johtopäätöksiin ja tutkimustuloksiin on päädytty tieteellisen tiedontuottamisen menetelmiä käyttäen eikä esimerkiksi omien uskomusten tai mielipiteiden kautta.[3]
Oikeustieteen tutkimusmetodi määräytyy tutkimuskohteen, tieteenalan ja valitun tiedonintressin mukaan.[4] Metodit eivät ole abstrakteja ideoita, vaan tutkijan välttämätön työkalu.[5] Metodien oppimisessa on ennen kaikkea kysymys tiedon hankkimisesta metodiin liittyen sekä harjaantuminen metodin käyttämiseen. Tämä edesauttaa tutkijan metodologista tieto-taitoa.[6]

Metodit nähdään tavallisesti kahden tutkimuksen keskeisen osatekijän välittäjänä. Ensinnäkin oivaltamisen logiikka on tutkijan yksilöllistä ja ainutkertaista, luovaa ja intuitiivista, osittain jopa ennakoimatonta ja irrationaalista toimintaa. Toiseksi yleistettävissä ja

2 Tästä keskustelusta tarkemmin katso esimerkiksi *Patrizio Campisi* (ed.), Security and Privacy in Biometrics.

3 *Hirvonen,* Mitkä metodit, s. 5.

4 *Siltala,* Oikeustieteen tieteenteoria, s. 137.

5 Häyhä on osuvasti todennut, että metodi on tieteenalan vakiintunut väline, työkalu, jonka avulla päästään käsiksi johonkin sen itsensä kannalta ulkopuoliseen *Häyhä,* Minun metodini, s.24

6 *Hirvonen,* Mitkä metodit, s. 4.

toistettavissa oleva perustelemisen logiikka on tiedeyhteisösidonnaista, jonka hyväksyntä tutkimustulosten on saatava. Metodi on tässä yhtälössä se yhdistävä tekijä. Metodi muodostuu niistä päättelysäännöistä, joiden kautta siirtymä oivaltamisesta perustelemiseen tapahtuu.[7]

Oikeustieteessä ollaan hyvin usein yksimielisiä siitä, että oikeustieteissä ei ole mitään yleispätevää, todettua ja standardisoitua metodisäännöstöä. Oikeustieteessä vain harvoin täsmennetään, mitä käsite metodi tarkoittaa.[8] Oikeustieteen metodissa ei ole kysymys mistään laskusäännöstöstä, jonka avulla päästään tulokseen, kun systeemiin syötetään asianmukaiset seikat.[9]

Oikeudellinen ajattelu ei ole mekaaninen, yksikäsitteisiä sääntöjä noudattava prosessi.[10] Oikeustieteen metodi osoittautuu enemmänkin näkökulmaksi oikeuteen kuin laskusäännöstöksi. Oikeudellisen ajattelun niin sanottu metodi on muuta kuin luonnontieteiden tai teknisen tutkimuksen menetelmä.[11]

Oikeusinformatiikan kohdalla on esitettävissä kysymys, onko oikeusinformatiikalla erityistä omaa tutkimusmetodia. Oikeusinformatiikka on perinteisessä oikeudenalajaottelussa niin sanottu uusi oikeudenala, jonka täytyy edelleen todistaa oman asemansa tärkeys yhteiskunnassa ja oikeustieteen kentässä. Oikeusinformatiikka tulee

---

7 *Siltala,* Oikeustieteen tieteenteoria, s. 473–474.

8 *Aarnio,* Luentoja lainopillisen tutkimuksen teoriasta s. 12

9 *Aarnio,* Tulkinnan taito, s. 237.

10 *Aarnio,* Oikeussäännön systematisointi ja tulkinta, s. 35 ja Tulkinnan taito, s. 237

11 Aarnion mukaan metodilla on normatiivinen sisältö. Se viittaa kovien tieteiden eli luonnontieteiden yhteydessä joukkoon käsitteitä, sitoumuksia ja normeja. Niitä on noudatettava, jotta saavutettaisiin tiedeyhteisössä hyväksyttävissä oleva tieteellinen väite, teoria tai kannanotto. *Aarnio,* Tulkinnan taito, s. 237. Katso myös von *Wright,* Explanation and Understanding.

nähdä perinteisten oikeudenalojen pikkuveljenä, jonka merkityksellisyyttä yhteiskunnallinen ja teknologinen kehitys kasvattaa.

Tästä huolimatta myös oikeusinformatiikalle on löydettävissä metodinen lähtökohta. Oikeusinformatiikan metodissa on kysymys siitä, että löydetään (uudelleen) teknologian taustalla oleva informaatio ja informaatiovirrat sekä kokeillaan, miten oikeudellinen sääntely näihin vaikuttaa. Tällainen metodi on sekä monivivahteinen että joustava: se sopeutuu niihin kysymyksiin, jotka kaipaavat vastausta arvioiden samalla omaa merkitystään.[12]

”Uudenlaisesta” luonteestaan huolimatta oikeusinformatiikan metodin tarkoituksena ei ole perinteisten metodien syrjäyttäminen, vaan sen on tarkoitus olla näitä täydentävä. Tarkoituksena on uuden näkökulman esille tuominen, ja tätä kautta informaatioon kohdistuvan oikeudellisen lähestymistavan arvioiminen ja optimoiminen. Oikeusinformatiikan metodin avulla on myös mahdollista korvata teknologiariippuvaisia lähestymistapoja sekä auttaa ymmärtämään teknologioiden luonnetta.[13] Ennen kaikkea metodissa on siis kysymys siitä, että osataan kysyä ajan ehdoilla. Konkreettisesti tämä tapahtuu arvioimalla biometristen tunnisteiden asemaa ja merkitystä yhtenä uutena teknologiana. Tällöin oikeustieteen on mahdollista vastata yhteiskunnasta nousevaan haasteeseen. Jännitteet turvallisuuden ja yksityisyyden suojan välillä ovat esimerkki tällaisesta haasteesta.

Toisinaan on katsottu, että oikeusinformatiikan kaltaiset monitieteiset oikeusopit olisivat lainopin aputieteitä. Näin ei kuitenkaan ole, sillä oikeusinformatiikka on itsenäinen oikeustieteen osa-alue omine teorioineen, metodeineen ja kysymyksenasetteluineen. Tästä ei kuitenkaan voi vetää johtopäätöstä, ettei oikeusinformatiikan tuottama tieto oikeudesta voisi tukea ja palvella lainoppia ja olla perusteena lainopin

12 *Burkert,* Information Law: From Discipline to Method, s. 399

13 *Burkert,* Information Law: From Discipline to Method, s. 399

tulkinnoille, punninnoille ja systematisoinneille tai ettei oikeusinformatiikka voisi itsessään esittää tulkinta-, punninta- tai systematisointikannanottoja.[14]

Tämän tutkimuksen aihepiirin ja tutkimuskysymysten kannalta keskeisessä asemassa on voimassa oleva lainsäädäntö. Tutkimusmetodiksi tutkimukseen on valittu lainopillinen eli oikeusdogmaattinen metodi[15], jota täydennetään oikeusinformatiikan metodilla. Lainopin tehtävänä on voimassaolevan oikeussäännösten systematisointi ja oikeussäännösten sisällöllinen selventäminen eli tulkinta.[16] Lainoppi on eräänlaista voimassa olevien oikeusnormien operointia, jossa suoritetaan eri oikeuslähteistä johdettujen oikeussääntöjen tulkintaa ja systematisointia sekä oikeusperiaatteiden punnintaa ja keskinäistä yhteensovittamista luomalla suosituksia perustelluiksi oikeudellisiksi ratkaisuiksi.[17] Oikeussäännöille pyritään toisin sanoen määrittämään merkityssisältö.

Tässä tutkimuksessa selvitetään lainopillisen tutkimuksen mukaisesti biometrista tunnistamista koskevan lainsäädännön sisältöä. Biometrista tunnistamista koskevan lainsäädännön systematisointi on tärkeässä asemassa tässä tutkimuksessa. Systematisoinnin keskeiseksi tehtäväksi muodostuu biometrista tunnistamista sääntelevän normikokonaisuuden systematisoiminen. Lainopillinen tulkintatehtävä tulee tutkimuksessa esiin lähinnä käsiteltäessä biometrista tunnistamista lainsäädännön kautta.

---

14 *Hirvonen,* Mitkä metodit, s. 29–30

15 Lainopin käsitteestä katso Aarnio Tulkinnan taito, s. 302–304 ja Makkonen, Luentoja yleisestä oikeustieteestä, s. 2.

16 *Peczenik,* Juridikens teori och metod, s. 33.

17 *Aarnio,* Tulkinnan taito, s.238. Lainopillisen tutkimuksen tehtävä on viime kädessä käytännön tarpeiden tyydyttäminen, esimerkiksi oikeuselämässä toimivien lakimiesten työn tukeminen

Lainoppi on sille asetettujen tehtävien perusteella jaettavissa ongelmakeskeiseen ja normikeskeiseen lähestymistapaan. Ongelmakeskeiselle metodille on keskeistä oikeudenalat ylittävä tutkimuksellinen ote, jossa muodostetaan kokonaiskuva jonkin oikeudellisesti mielenkiintoisen ongelman sääntelystä.[18] Kysymys on tällöin oikeudellisen tutkimuksen tavasta määrittää ja rajata tutkimusongelmat yhteiskunnasta eikä niinkään oikeusjärjestyksestä käsin.[19] Normikeskeinen tai normilähtöinen lähestymistapa puolestaan muodostaa perustellun käsityksen siitä, miten tiettyä säännöstä tai säännöksiä tulee tulkita.

Perinteinen lainoppi on lähtökohtaisesti normilähtöistä. Lainopin luokittelua ongelma- ja normikeskeiseen voidaan kuitenkin pitää kärjistettynä. Normikeskeisen ja ongelmakeskeisen lainopin välille ei synny sellaista eroa, joka ilmenisi erilaisena metodologiana.[20]

Lähes jokaista oikeustieteellistä tutkimusta on mahdollista pitää ongelmakeskeisen ja normikeskeisen lähestymistavan yhdistelmänä. Yhdistävänä tekijänä ovat kysymyksenasettelut ja ongelmat, joita käytetään kummassakin lähestymistavassa. Kysymys on painotuksista lainopin perustehtävien kesken, sillä ongelmakeskeinen lähestymistapa korostaa systematisoinnin merkitystä, mutta edellyttää tarkastelussa esiin tulleiden tulkintaongelmien ratkaisemista. Normikeskeinen

18 Kankaan mukaan ongelmakeskeinen lainoppi pyrkii systematisoimaan oikeusjärjestystä yleensä, ei vain jotain sen osaa, joten sen perusajatus on oikeusjärjestyksen ykseys. Ongelmakeskeisen lainopin ydin on siinä, että se systematisoi kokonaisuuden jonkin peruskysymyksen suhteen. *Kangas,* Lesken oikeudellinen asema, s. 385–386.

19 Kankaan mukaan perinteinen tulkintalainoppi tyytyy pääosin oikeusjärjestyksen sisäisen näkökulman korostamiseen yhteiskunnallisen näkökulman kustannuksella. *Kangas,* Lesken oikeudellinen asema, s. 385.

20 *Aarnio,* Laintulkinnan teoria, s. 61–63 ja *Timonen*, Johdatus lainopin metodiin ja lainopilliseen kirjoittamiseen, s. 14.

lähestymistapa puolestaan painottuu tulkintatilanteiden arviointiin, mutta siinä tarvitaan niin asiayhteyksien ymmärtämistä kuin oikeudellisesta järjestelmästä ja käsitteistöstä johdettuja argumentteja.[21]

Oikeusinformatiikan tutkimuksessa ei hyödynnetä pelkästään oikeusdogmaattisten oppien mukaisia oikeuslähteitä, vaan ominaista on myös muiden lähitieteiden tuottaman aineiston tai menetelmien hyödyntäminen. Tämä muodostaa oikeusinformatiikalle oman identiteetin, joka erottaa sen erityisesti puhtaasta oikeusdogmaattisesta tutkimuksesta.

Oikeusinformatiikka tarjoaa alustan tieteellisen tutkimuksen harjoittamiselle tieteenalojen ja oikeudenalojen välisissä rajapinnoissa. Oikeusinformatiikan tunnusomaisena piirteenä on sen tieteidenvälisyys tai monitieteellisyys, joka tekee oikeudellisesta tutkimuksesta nimenomaan oikeusinformatiikkaan kuuluvan tutkimuksen oikeustieteiden joukossa.

Tähän tutkimukseen on sen monialaisen tutkimuskohteen vuoksi valittu ongelmakeskeistä lähestymistapaa painottava tutkimusteema. Tutkimuksessa tarkasteltu ongelma on biometrinen tunnistaminen. Siinä selvitetään, mitkä säännökset koskevat biometrista tunnistamista. Yksinkertaistaen sanottuna tutkimuksessa kerätään biometrisia tunnisteita koskevia normeja eri yhteyksistä yhteen. Ongelmaan liittyvät kysymykset ovat suhteessa tosielämän tilanteisiin ja ongelmiin, joihin lakeja on tarkoitettu sovellettavaksi. Ongelmakeskeisessä lainopissa kysytään, mitä keinoja lainsäätäjällä on näiden ongelmien ratkaisemiseksi.[22]

---

21 *Timonen,* Johdatus lainopin metodiin ja lainopilliseen kirjoittamiseen, s. 14–15.

22 Toisaalta voidaan huomauttaa ongelman olevan hieman kärjistetty. Kysymys on pikemminkin ilmiöstä. Ongelmakeskeisen metodin sijaan tulisi ehkä puhua ilmiökeskeisestä lainopista.

Osana lainopillista tutkimusmetodia tutkimuksessa käytetään de lege lata ja de lege ferenda –analyyseja, jotka ovat läheisessä suhteessa toisiinsa, varsinkin kun tarkastellaan biometrisen tunnistamisen ja tietosuojalainsäädännön suhdetta. Tässä tutkimuksessa pääpaino on de lege lata –analyysillä, sillä tarkastelun kohteena on voimassa oleva lainsäädäntö. Tosin tutkimuksessa tehdään myös muutosehdotuksia, mikäli aihepiiriin liittyvä voimassa oleva lainsäädäntö on puutteellista.[23]

Vaikka tutkimuksessa käydään läpi useamman oikeudenkäyttöalueen lainsäädäntöä, ei tutkimus ole oikeusvertaileva tutkimus. Sen sijaan, että tutkimuksessa keskityttäisiin laajamittaiseen ja systemaattiseen oikeusvertailuun, tutkimuksessa esitellään esiin tulevia mahdollisuuksia ja ongelmia voimassa olevan muun kuin kansallisen lainsäädännön kautta.

1.1.3. Tutkijanideologia osana metodia

Käytettävään metodiin liittyy läheisesti tutkijanideologia eli tutkijanpositio. Tällä tarkoitetaan Siltalan mukaan tutkijan omaksumaa näkökulmaa oikeudellisesti määrittyneeseen tutkimuskohteeseensa. Tutkijanideologia jaetaan Siltalan mukaan analyyttis-deskriptiiviseen ja normatiivis-kriittiseen. Toisaalta tutkijanideologia voi myös olla näiden kahden yhdistelmä.[24]

Analyyttis-deskriptiivisessa tutkijanideologiassa ajatuksena on se, että tutkijan tulee mahdollisimman neutraalilla tavalla kuvata, analysoida ja selittää tutkimuskohdettaan sellaisena kuin se yhteiskunnal-

23 Bygrave on tähän liittyen todennut, että tietosuojan alueella tällaisen eron tekeminen on hankalampaa kuin muilla aloilla. *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 16. Katso myös *Sandström – Peterson,* Lex Lata – Lex Ferenda. Fakta eller Fiktion?, s. 159–177.

24 *Siltala,* Oikeustieteen tieteenteoria, s. 141.

lisena tosiasiana on. Kaikki ennakko-oletukset voivat nimittäin vääristää tieteen tuloksia. Sen vuoksi tutkijan tulee pysyä objektiivisena tai ainakin tiedostaa ennakko-oletuksensa Jos ennakko-oletuksia ei tiedosteta, tutkimuksesta tulee rajoittunutta eikä se voi asettua rohkeasti alttiiksi kritiikille ja tulostensa koettelulle.[25] Tutkijan tulee tämän vuoksi rajata omat näkemyksensä tieteellisesti hallittavissa olevan tutkimuksen ulkopuolelle ja pitäytyä objektiivisissa arviointikriteereissä. *Kriittis-normatiivisessa* tutkijanideologiassa puolestaan on kysymys siitä, että tutkija liittää sisäistämänsä näkemykset avoimesti osaksi toteutettua tutkimusta. Tällöin tavoitteena on perustella ideaalinen tulkinta voimassa olevasta oikeudesta.[26]

Tutkimus voi olla myös näiden edellä mainittujen ideologioiden yhdistelmä. Haasteena tällöin on se, miten kriittis-normatiivinen tutkijanideologia vaikuttaa tutkijan mahdollisuuksiin toteuttaa täydellisen analyyttis-deskriptiivistä tutkimusta. Onko mahdollista tehdä objektiivista tutkimusta, jos tutkijan omat näkemykset ovat avoimesti osana toteutettua tutkimusta?

Haasteellisuudesta huolimatta tässä tutkimuksessa on omaksuttu näiden kahden tutkijanideologian yhdistelmä. Tutkimuksessa kuvataan, analysoidaan ja selitetään biometrinen tunnistaminen yhteiskunnallisena tosiasiana, mutta de lege ferenda ja de lege lata -analyysien kautta esitetään voimassa olevaan lainsäädäntöön parannusehdotuksia eli perustella ideaalinen tulkinta voimassa olevasta oikeudesta. Nämä parannusehdotukset ovat aina tietyllä tavalla subjektiivisesti värittyneitä. Asiaan vaikuttaa myös se, että jokaisella tutkimuskohteella on aina tietynlainen yhteiskunnallinen arvo, joka omalta osaltaan vaikuttaa aina myös tutkijanideologiaan. Jokainen tutkimuskohde on omalla

25 *Aarnio,* Tulkinnan taito, s. 231

26 *Siltala,* Oikeustieteen tieteenteoria, s. 141–143.

tavallaan yhteiskunnallisten valintojen ja prosessien ohjaamaa, ja on tällä tavoin aina ideologista ja myös subjektiivista.

Oikeuden ja yhteiskunnan muutoksella on aina myös oma osansa tutkijanideologian valinnassa. Ideaalista ja parasta mahdollista tulkintaa tutkimuskohteesta on varsin mahdotonta antaa. Tulkinta voimassa olevasta oikeudesta on aina tiettyyn aikaan, paikkaan ja yhteiskunnalliseen tilanteeseen sidottu. Lait ovat kirjoitettavissa neutraaliin muotoon, mutta kukin laki edustaa aina lain antoajankohdan yhteiskunnallisia ja osin poliittisia näkemyksiä. Kysymys on toisin sanoen siitä, mitä on kulloinkin pidetty yhteiskunnassa säätämisen arvoisena ja näin yhteiskunnallisesti merkittävänä asiana.

1.1.4. Tutkimuksen lähteet

Oikeustiede nojautuu oikeuslähteisiin. Oikeuslähteillä tarkoitetaan niitä lähteitä, joista oikeussäännöt ovat löydettävissä. Nämä lähteet voivat olla kirjoitettuja tai kirjoittamattomia. Laajemmassa merkityksessä oikeuslähteillä tarkoitetaan niitä lähteitä, jotka kertovat jotakin oikeudesta, sen olemassaolosta ja merkityksestä yhteiskunnassa.

Oikeustiede käyttää oikeuslähteitä systematisoidakseen ja tulkitakseen useimmiten juuri oikeuslähteitä. Toisaalta oikeustiede itsessään myös on oikeuslähde. Tämä osoittaa sen, että *"oikeuslähteet eivät ole mikään staattinen tila tai kerrostuma, vaan jatkuvasti kehittyvä, normien ja oikeussysteemisten ajatusten sekä sovellusten hitaasti etenevä prosessi."*[27] Jokainen kannanotto oikeuslähteisiin luo samalla käsitystä oikeuslähteistä. Oikeuslähteitä tuleekin pitää oikeudellisen argumentoinnin lähtökohtana.[28]

Oikeuslähdeopin tehtävänä on oikeuslähteiden tyypittely ja niiden keskinäisten suhteiden ja etusijajärjestyksen erittely. Oikeuslähdeopin

27 *Tolonen,* H, Oikeuslähdeoppi, s. 8.

28 *Sandgren,* Vad är rättsvetenskap, s. 182.

sääntöjen avulla tunnistetaan oikeus, ja se on lakimiehen ammattitaidon kulmakivi. Kysymyksessä on sananmukaisesti oppi oikeuden lähteistä. Tässä tarkoituksessa oikeuslähdeoppi vetää rajan juridisen ja ei-juridisen välille.[29] Kysymys on toisin sanoen siitä, mille perusteille rakennetaan ja millä tavalla perustellaan kannanotto voimassa olevaan oikeuteen eli oikeuskysymykseen de lege lata. Vain oikeuslähteiden kautta on mahdollista määrittää oikeudellinen ja erottaa se ei-oikeudellisesta.[30]

Oikeuslähdeopissa on lähtökohtaisesti kysymys siitä, mistä kyseiseen oikeudelliseen ongelmaan liittyvät oikeusohjeet on mahdollista löytää. Oikeuslähteet myös auttavat käsillä olevan oikeudellisen ongelman tulkinnassa ja ratkaisussa. Tämän tutkimuksen kohdalla oikeuslähdeopin kautta pyritään vastaamaan siihen, mistä löytyvät biometriseen tunnistamiseen liittyvät oikeusohjeet. Valmis biometrista tunnistamista koskeva oikeus näin ollen syntyy biometrista tunnistamista koskevista oikeuslähteistä syntyvistä aineksista.

Oikeuslähteitä on pyritty kategorisoimaan eri tavoilla. Suomessa on vakiintunut Alexander Peczenikin ja Aulis Aarnion omaksuma niin sanottuun staattiseen oikeuslähdeoppiin perustuva tapa. Tässä jaottelussa oikeuslähteet jaetaan kolmeen ryhmään niiden velvoittavuudesta riippuen. Oikeuslähteet ovat tällöin vahvasti ja heikosti velvoittavia sekä sallittuja oikeuslähteitä. Vahvasti velvoittavilla oikeuslähteillä tarkoitetaan lakia ja tapaoikeutta. Heikosti velvoittaviin oikeuslähteisiin kuuluvat lain esityöt ja oikeuskäytäntö. Sallittuihin oikeuslähteisiin luetaan yleiset oikeusperiaatteet, oikeuskirjallisuus sekä reaaliset argumentit.[31]

---

29 *Siltala,* Oikeustieteen tieteenteoria, s. 189.

30 *Aarnio,* Oikeutta etsimässä, s. 209.

31 *Peczenik,* The Basis of Legal Justification, s. 35-44 ja *Aarnio,* Oikeussäännösten tulkinnasta, s. 220-247. Peczenik käyttää skall – bör – får –kolmijakoa. *Peczenik,* Vad är rätt?, s. 214-221. Suomenkielinen

Perinteisen käsityksen mukaan oikeudellinen ratkaisu tulee siis perustaa ensisijaisesti lakiin tai lain puuttuessa tapaoikeuteen. Ellei laki anna vastausta oikeudelliseen tulkintakysymykseen eikä tapaoikeutta ole käytettävissä, haetaan vastausta heikosti velvoittavista oikeuslähteistä, kuten lain esitöistä. Vasta viimesijaisena keinona on mahdollista tukeutua sallittuihin oikeuslähteisiin, kuten oikeusperiaatteisiin.

Perinteinen oikeuslähdeoppi on kuitenkin saanut osakseen kritiikkiä. Eniten kritiikkiä on kohdistettu siihen, ettei jaottelu ota lainkaan kantaa Euroopan unionin oikeudellisen normiston oikeudelliseen ratkaisuarvoon. Nykyaikaisessa oikeuslähdeopissa myös Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioisuimen ratkaisuista ilmenevät oikeusohjeet vaikuttavat lainsoveltajan ratkaisuharkintaan.[32]

Esitetyn kritiikin vuoksi Aarnio on täydentänyt näkemystään perinteisestä oikeuslähdeopistaan. Täydennetyssä oikeuslähdeluettelossa vahvasti velvoittavat oikeuslähteet on jaettu kansallisen oikeuden ulkopuoliseen normistoon ja kansallisen oikeuden normistoon. Kansallisen oikeuden ulkopuoliseen normistoon on sisällytetty Euroopan unionin oikeuden sitovat osat, Euroopan ihmisoikeussopimuksen normit, Euroopan unionin tietyt prejudikaatit ja Euroopan ihmisoikeustuomioistuimen tietyt prejudikaatit.[33]

Oikeuslähdeluetteloissa kysymys on listauksesta, johon on pyritty sisällyttämään kaikki oikeudellisen ratkaisun perustana olevat lähteet. Näin ollen lain ja maan tavan ohella esimerkiksi esityöt ja oikeuskäy-

---

terminologia on peräisin Aarniolta. *Aarnio,* Laintulkinnan teoria, s. 220-221.

32 *Siltala,* Oikeudellinen tulkintateoria, s. 21–22, 100–101 ja 377.

33 *Aarnio,* Tulkinnan taito, s. 292–293

täntö saavat painoarvonsa ratkaisutoiminnassa sen mukaan, miten lainsoveltajalla on velvollisuus noudattaa niitä.[34]

Oikeudenalat ja oikeudelliset ongelmat ovat kuitenkin erkaantuneet toisistaan eikä kaikille oikeudenaloille yhteistä oikeuslähdeoppia enää välttämättä voida esittää. Tämän vuoksi on puhuttu oikeuslähdeoppien vaihtelevan oikeudenaloittain.[35] Tällöin myös tulkinta pitää suhteuttaa vallitsevaan oikeudenalakohtaiseen systematiikkaan.[36]

Informaatio-oikeudellisten ilmiöiden ymmärtämistä vaikeuttaa sääntelyn monipolvinen rakenne. Informaatio-oikeuden sääntelyjärjestelmä on monikerroksinen ja siihen sisältyy EU-lainsäädäntöön pohjautuvia kansainvälisiä ja ylikansallisia aineksia. Näitä täydennetään kansallisilla ja alueellisilla erityispiirteillä. Pelkistetysti informaatio-oikeuden sääntelyjärjestelmä (kuvio 1) on esitettävissä seuraavasti[37]:

34 *Muukkonen,* Perusoikeuslähtöisen laintulkinnan hahmottelua yhdistysoikeudessa, s. 4

35 *Syrjänen,* Oikeudellisen ratkaisun perusteista, s. 182.

36 *Siltala,* Oikeustieteen tieteenteoria, s. 337.

37 *Pöysti,* Future of Privacy in the Emerging Electronic Marketplace in Europe, s. 170.

Kuvio 1. Informaatio-oikeuden sääntelyjärjestelmä.

<table>
<tr><td colspan="2">Kansainväliset ja eurooppalaiset ihmisoikeusperiaatteet
Euroopan ihmisoikeussopimus</td></tr>
<tr><td>Yhteisöoikeuden perustavanlaatuiset periaatteet (muut kuin ihmisoikeudet)</td><td>Kansainvälisten sopimusten periaatteet</td></tr>
<tr><td colspan="2">Yhteisön lainsäädäntö (Henkilötietodirektiivi ja sitä täydentävät säädökset)
Euroopan Unionin tuomioistuimen oikeuskäytäntö
Yhteisön ”pehmeä sääntely” (käytännesäännöt, standardit)</td></tr>
<tr><td colspan="2">Kansallinen lainsäädäntö</td></tr>
<tr><td colspan="2">Kansalliset käytännesäännöt</td></tr>
</table>

Vastauksia informaatio-oikeudellisiin, kuten henkilötietojen suojaa koskeviin kysymyksiin on etsittävissä useista eritasoisista lähteistä. Näiden tarjoamat ratkaisuperusteet eivät aina ole keskenään johdonmukaisia tai yksiselitteisiä.

Informaatio-oikeuden monipolvinen sääntelytapa ja siitä johdettavissa oleva oikeuslähdeoppi noudattavat oikeuslähteiden polysentristä suuntausta. Tämän kehistyssuuntauksen mukaisesti käytettävissä ei enää ole vain yhtä yhtenäistä oikeuslähdeoppia, vaan monia erilaisia oikeuslähdeoppeja siitä riippuen, kenen kannalta asiaa tarkastellaan.

Yhtenäisen oikeuslähdeopin sijaan voidaan siksi puhua ongelma-, oikeudenala- tai tilannekohtaisesta oikeuslähdeopista.[38]

Polysentrinen oikeuslähdeoppi vastaa nykyaikaisen informaatioyhteiskunnan haasteeseen tosielämän dynaamisten tarpeiden huomioimiseksi. Erityisesti henkilötietojen käsittelyn toimintatapojen ja toimintaympäristön kehitys ovat olleet merkittävästi säädöskehitystä nopeampaa, mikä osaltaan oikeuttaa uusien ja vaihtoehtoisten oikeuslähdeoppien hyväksikäyttämisen oikeita ja oikeudenmukaisia ratkaisuja sekä tulkintatapoja etsittäessä.

Informaatio-oikeuteen liittyykin luontevasti dynaaminen oikeuslähdeoppi. Sen mukaan on mahdotonta esittää yleistä ennakollisesti velvoittavaa oikeuslähteiden hierarkiaa. Tämän sijaan oikeuslähteiden painoarvo on määritettävissä vain tapaus- ja tilannekohtaisesti. Ainoan poikkeuksen muodostavat perus- ja ihmisoikeusperiaatteet, joiden tulee nähdä olevan painoarvoltaan ensisijaisia muihin oikeuslähteisiin. Biometrisen tunnistamisen kohdalla tämä ilmenee esimerkiksi siten, ettei kaikissa tilanteissa ole välttämättä mahdollista käyttää kaikkia oikeuslähdeopin oikeuslähteitä eikä sen määräämässä järjestyksessä. Dynaamisuuteen tuleekin kuulua oikeuslähteiden tulkinnan kehittymisen lisäksi oikeuslähteinä toimivien aineistojen jatkuva kehittyminen.

Avarakatseisuuden vuoksi tässä tutkimuksessa käytetyt lähteet on jaoteltu *Ian Brownlien* oikeuslähdejaottelun mukaan. Hänen mukaansa termi oikeuslähde viittaa sekä virallisiin (formal sources) että materiaalisiin (material sources) oikeuslähteisiin.[39] Virallislähteillä

38 *Syrjänen,* Oikeudellisen ratkaisun perusteista, s. 207. Katso myös *Siltala,* Oikeustieteen tieteenteoria, s. 203 sekä *Aarnio,* Tulkinnan taito, s. 292.

39 *Brownlie,* Principles of Public International Law (2008), s. 3-4. Aarnion mukaan oikeuslähteeksi voidaan luonnehtia jokainen sellainen perustelu (argumentti), jonka nojalla ratkaisu tai oikeustieteellinen kannanotto joko löydetään tai oikeutetaan juridisena ratkaisuna tai

tarkoitetaan niitä oikeudellisia käytäntöjä ja metodeja, jotka ovat oikeudellisesti sitovia.[40] Esimerkkeinä virallislähteistä toimivat lait, oikeuskäytäntö, kansainväliset sopimukset sekä yleiset oikeusperiaatteet. Näiden lähteiden painoarvo vaihtelee sen mukaan, missä yhteydessä näitä lähteitä käytetään.

Virallislähteet. Tässä tutkimuksessa käytettyjen virallislähteiden kautta muodostuu kuvaus biometriseen tunnistamiseen ja yksityisyyteen liittyvästä oikeudellisesta sääntelystä. Näitä ovat:

a) kansainväliset säännökset, kuten Euroopan ihmisoikeussopimus ja Euroopan unionin tietosuojadirektiivi. Myös Euroopan unionin tuleva henkilötietoasetus on huomioitu tutkimuksessa.
b) yleinen yksityisyyden ja henkilötietojen suojaa koskeva lainsäädäntö sekä erityisesti biometrista tunnistamista koskeva lainsäädäntö Suomesta ja Yhdysvalloista.
c) oikeuskäytäntö. Tällä hetkellä biometrista tunnistamista koskeva oikeuskäytäntö on hajanaista ja harvinaista. EU-alueelta on löydettävissä jonkin verran oikeuskäytäntöä niin jäsenvaltioiden paikallisista tuomioistuimista kuin unionitasoltakin. Suuren ihmisoikeusvaikutuksensa vuoksi suuri merkitys on ihmisoikeuksia koskevalla oikeuskäytännöllä. Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä on otettu kantaa teknologioiden mukanaan tuomiin ihmisoikeuskysymyksiin. Yhdysvalloissa puolestaan biometrista

---

kannanottona. *Aarnio,* Oikeutta etsimässä, s. 221.

40 Näitä voidaan kutsua myös konkreettisiksi oikeuslähteiksi. Konkreettisia oikeuslähteitä ovat ne oikeuslähteet, joita lainkäyttötoiminnassa todellisuudessa käytetään hyväksi. *Aarnio,* Oikeutta etsimässä, s. 225

tunnistamista koskevaa oikeuskäytäntöä on saatavilla useammalta vuosikymmeneltä.

d) oikeusperiaatteet. Informaation sääntelyssä periaatteet ovat keskeisessä asemassa. Informaatio-oikeudessa periaatteet ovat jaettavissa neljään kokonaisuuteen: 1) justifikaatioperiaatteet, 2) aineelliset periaatteet, 3) infrastruktuuri- ja informaatiomarkkinoiden periaatteet sekä 4) yhteensovittamisperiaatteet.[41] Tässä tutkimuksessa tarkastelu kohdistuu informaation aineellisiin periaatteisiin lukeutuvaan henkilötietojen suojaan ja sen toteutumiseen biometristen tunnisteiden kohdalla. Periaatteilla on henkilötietojen suojan sääntelyssäkin erityinen merkitys, sillä henkilötietojen suoja on toteutettu hyvin pitkälti periaatteiden pohjalta.

Materiaaliset oikeuslähteet. Materiaalisilla oikeuslähteillä ei tarkoiteta varsinaista lainsäädäntöä. Materiaaliset oikeuslähteet tarjoavat näyttöä oikeussäännöistä, joilla todistetuksi tullessaan on yleisesti sovellettavissa olevan ja oikeudellisesti sitovan oikeuslähteen asema.[42] Esimerkiksi EU-säädösten preamblet usein sisältävät sellaista yhteiskunnallista arvo- ja tarkoituksenmukaisuuspohdintaa, jota voi pitää materiaalisena.

Varsinaisen tutkimusaihetta koskevan nimenomaisen lainsäädännön puuttuessa lainvalmisteluaineisto työryhmämietinnöistä hallituksen esityksiin muodostaa tärkeän oikeuslähteen. Niissä esitettyjä näkemyksiä ja perusteluja on mahdollista käyttää analyysin pohjana. Lisäksi eri viranomaisten, kuten tietosuojavaltuutetun antamat sovel-

41 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 399–505. Katso myös *Pöysti,* Future of Privacy in the Emerging Electronic Marketplace in Europe, s. 168–169

42 *Brownlie,* Principles of Public International Law (2008), s. 3.

tamisohjeet muodostavat tärkeän materiaalisten oikeuslähteiden joukon.

Kirjallisuus. Oikeudenalan tulkintakäytännön kehittyminen vaatii kuitenkin myös tutkimusta. Tieteen käytäntösuhteen kannalta tutkimus on tietyllä tavalla avainasemassa. Tieteen yhteiskunnallista edistystä tuottava voima perustuu nimenomaan tutkimuksen kykyyn tuottaa uusia tuloksia, joiden varaan voidaan rakentaa uusia teknologioita ja yhteiskunnallisia käytäntöjä. Tosiasiallinen tilanne on kuitenkin toinen. Käytännössä päätöksentekijät eivät aina ymmärrä tutkimusta eivätkä halua kuulla tuloksista, jotka edellyttävät vakiintuneiden toimintakehysten muuttamista. .[43]

(Oikeus)lähteenä tulee ottaa tämän vuoksi huomioon myös (oikeus)kirjallisuus. Nämä (oikeus)lähteet ovat varsin laajoja ja niitä on melko hyvin saatavissa. Yksinomaan biometrista tunnistamista ja yksityisyyden suojaa koskevaa (oikeus)kirjallisuutta ei etenkään suomen kielellä juuri ole löydettävissä. Tutkimuksessa käytetty oikeuskirjallisuus on jaoteltavissa seuraavasti:

a) biometriseen tunnistamiseen ja yksityisyyteen liittyvä oikeuskirjallisuus ja artikkelit;
b) artikkelit, jotka liittyvät yksityisyyteen ja henkilötietojen suojaan, valvontateknologioihin sekä biometriaan ja
c) kirjallisuus, joka liittyy valvontateknologioihin, biometrisen tunnistamisen teknologioihin, yksityisyyteen ja tietosuojaan.

43 *Heiskala,* Yhteiskuntatutkimuksen vaikuttavuus ja uusi uljas maailma, s. 29. Tieteessä tapahtuu, Vol. 34 Nro 1, 2016. s. 27–33.

1.1.5. Tutkimuksen rakenne

Tutkimus jakautuu kolmeen pääjaksoon. *Jaksossa I* käydään läpi tutkimuksen tieteellistä viitekehystä, teemaa ja näkökulmaa. Tämän jakson pääasiallisena tarkoituksena on selvittää tutkimuksen aihepiirin kannalta keskeiset lähtökohdat. Jaksossa selvitetään tieteen asemaa yhteiskunnassa sekä yhteiskunnan muutosta. Jaksossa käsitellään myös tunnistamisen merkitystä ja roolia yhteiskunnassa. Lisäksi esitellään oikeuden yleistieteisiin kuuluvaa oikeusinformatiikkaa ja informaatio-oikeutta sen osana. Näiden lisäksi keskitytään persoonallisuusoikeuteen ja sen keskeisiin periaatteisiin: itsemääräämisoikeuteen, yksityisyyden ja henkilötietojen suojaan sekä identiteettiin ja kontrollisidonnaisuuteen.

Jaksossa II puolestaan käydään läpi tutkimuksen ydinalue eli biometrinen tunnistaminen. Jaksossa selvitetään, mitä biometrisella tunnistamisella tarkoitetaan, käydään läpi biometrisen tunnistamisen historiaa sekä esitellään biometrisen tunnistamisen menetelmiä ja niiden vaikutuksia yksityisyyden suojalle. Lisäksi käsitellään biometristä tunnistamista ja identiteettiä sekä biometristen tunnisteiden käsittelyyn liittyviä periaatteita. Esille tuodaan myös biometrisessa tunnistamisessa huomioon otettavat oikeudelliset lähtökohdat. Jaksossa esitellään myös biometrisen tunnistamisen lainsäädännöllistä asemaaYhdysvalloissa.

Kolmannessa jaksossa esitetään kootusti tutkimuksen keskeinen sisältö. Jakson tarkoituksena on käydä ns. sisäistä dialogia tutkimuksen kanssa. Jakson lopuksi myös selvitetään yksityisyyden, henkilötietojen suojan ja tietojärjestelmien tulevaisuudennäkymiä perus- ja ihmisoikeuksien näkökulmasta sekä tietoteknisen kehityksen vaikutuksia henkilötietojen käsittelylle, yksityisyyden suojalle ja valvonnalle.

1.2. Tutkimuksen sijoittuminen oikeudenalajaotuksessa

1.2.1. Lyhyesti oikeudenalajaotuksesta

Perinteinen lähtökohta suomalaisessa oikeustieteessä on oikeusjärjestyksen jakaantuminen oikeudenaloihin, jotka yhdessä muodostavat systemaattisen kokonaisuuden. Perinteinen käsitys nojautuu ajatukseen kokonaisvaltaisesta ja koko oikeusjärjestyksen kattavasta oikeudenalajaotuksesta.[44] Oikeudellisen sääntelyn lisääntyminen ja kansainvälistyminen sekä oikeuslähteiden monipuolistuminen, yhteiskunnallinen oikeudellistumiskehitys ja oikeudellisten ongelmien paikantuminen useiden perinteisten oikeudenalojen leikkauspisteisiin ovat johtaneet tämän näkökannan kyseenalaistamiseen sekä uusien oikeudenalojen tai oikeudenalaehdokkaiden syntymiseen.[45] Tämä rikkoo perinteistä oikeudenalajaotusta, koska uudet oikeudenalat eivät yleensä kata yhtä tiettyä osaa oikeusjärjestyksen kokonaisuudesta. Ne pikemminkin levittäytyvät perinteisten oikeudenalojen päälle.[46]

Mikä sitten on oikeudenalajaotuksen merkitys? Oikeudenalajaotuksen ehkä suurin merkitys on siinä, että se auttaa jäsentämään oikeudellista normistoa ja paikantamaan oikeusongelmien ratkaisemisessa sovellettavan normiympäristön. Oikeudenalajaotusta voidaan pitää myös osana oikeuskulttuurista esiymmärrystä, jonka avulla oikeudellisia ongelmia on mahdollista lähestyä ja jonka avulla ongelmien

---

44 *Björne,* Oikeusjärjestelmän kehityksestä, s. 6 ja *Tuori,* Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota, s. 1197–1198.

45 *Tiilikka,* Sananvapaus ja yksilön suoja. Lehtiartikkelin aiheuttaman kärsimyksen korvaaminen, s. 71–76. Katso myös *Korpisaari,* Viestintäoikeus globaalissa verkkoyhteiskunnassa.

46 *Korpisaari,* Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta, s. 988.

määritteleminen ja paikannus on mahdollista aloittaa. Vasta tämän paikannuksen jälkeen voidaan aloittaa tarkastelemaan tapaukseen sovellettavaa normia, lain säännöksiä ja yleisiä oikeusperiaatteita. Oikeudenalajaotusta on tämän vuoksi hyödynnetty oikeustieteen opetuksessa, tutkimuksessa ja käytännön lainsoveltamistoiminnassa.[47] Tutkijan näkökulmasta oikeudenalajaotuksella on osansa myös tieteen tradition ylläpitämisessä, sillä oikeudenalajaotuksen kautta tutkija paikantaa asemansa suhteessa tieteelliseen traditioon tekemällä tietyn oikeudenalan tutkimusta.[48] Systemaattisen merkityksen lisäksi oikeudenalajaotuksella on myös oikeusnormeihin kohdistuva tulkintavaikutus kunkin oikeudenalan yleisten oppien kautta.[49]

1.2.2. Oikeusinformatiikka oikeuden yleistieteenä

Tieteelliseltä viitekehykseltään tämä tutkimus on ensisijaisesti oikeusinformatiikan alaan kuuluva tutkimus. Syynä on se, että yksityisyys, yksityiselämän suoja, henkilötietojen suoja ovat oikeusinformatiikan ja erityisesti oikeusinformatiikkaan kuuluvan informaatio-oikeuden keskeisiä tutkimuskohteita. Syynä on myös se, että tutkimuksessa tarkastellaan teknologian eli biometrisen tunnistamisen vaikutusta yhteiskunnan kehitykseen ja perus- ja ihmisoikeuksiin.

Erityisesti teknologian ja informaation oikeudellisia kysymyksiä tutkivana oikeudenalana oikeusinformatiikka myös luo vahvan poh-

47 *Tuori,* Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota, s. 1196, 1198 ja 1201.

48 *Määttä,* Monitieteisyys ympäristöoikeudessa – oikeustieteen sisäiset ja ulkoiset yhteydet oikeustieteellisen tutkimuksen haasteena, s. 346. Määtän mukaan oikeudenalat ovat myös viestintää helpottavia yhteisöllisiä konventioita, jotka helpottavat ymmärretyksi tulemista.

49 *Korpisaari,* Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta, s. 987.

jan biometrisen tunnistamisen tarkastelulle. Syynä on se, että teknologiaan liittyvien käsitysten ja toiveiden ymmärtäminen toimii ikkunana normeihin, arvoihin ja odotuksiin sekä ohjaa järkevien käytäntöjen luomista. Sama ymmärrys toimii myös työkaluna yhteiskunnallisesti hyväksyttävissä olevien teknologioiden luomisessa.

Oikeusinformatiikka[50] on yksi niin sanotuista uusista oikeudenaloista, joka on vakiinnuttanut paikkansa oikeustieteen osana.[51] Tämä on mahdollista havaita tarkastelemalla niitä vaatimuksia, mitä on asetettu oikeudenalan itsenäistymiselle. Yhtenä tällaisena on pidetty oikeudenalan omia yleisiä oppeja, jotka ovat ymmärrettävissä oikeudenalan identiteetiksi.[52] Yleisten oppien avulla yhdistetään tietyn oikeudenalan eri osa-alueet käsitteiden ja periaatteiden avulla.[53] Yleiset

50 Nimityksellä oikeusinformatiikka halutaan osoittaa kysymyksessä olevan ensi sijassa oikeuden ja tietojenkäsittelytieteen välisestä suhteesta, jossa oikeustiede on merkitykseltään suuremmassa asemassa. Seipelin mukaan ”informatiikka” viittaa joukkoon informaatiotieteitä, joita ovat yleinen systeemiteoria, tietojenkäsittelytiede, kirjastotiede ja kognitiotiede. Lisäksi informatiikka viittaa yhteiskunnan informaatioprosessien ennakkoehtoihin ja seurauksiin sekä myös bioinformatiikkaan ja lääketieteelliseen informatiikkaan. *Seipel,* Legal Informatics Broad and Narrow, s. 18.

51 *Seipel,* Juristen och datorn, s. 200 sekä *Kuopus*, Hallinnon lainalaisuus ja automatisoitu verohallinto, s. 23. Vertaa *Voutilainen,* Oikeus tietoon, s. 45–46 ja ICT-oikeus sähköisessä hallinnossa, s. 24 ja 344, joissa Voutilainen katsoo oikeusinformatiikan olevan oma tutkimusalansa, mutta ei oikeudenala.

52 *Tuori,* Kriittinen oikeuspositivismi, s. 187 ja *Tuori,* Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota, s. 1203.

53 Yleiset opit ovat keskeisessä asemassa oikeudenalan kokonaisuuden hahmottamisessa. *Wilhelmsson,* Social civilrätt, s.19–20.

opit ovat oikeustieteen luoma järjestelmä, jota yksittäinen lainsäännös, oikeustapaus ja muu oikeudellinen lähdemateriaali voivat järjestää.

Yleisten oppien lisäksi uuden oikeudenalan itsenäistymisen merkkeinä on pidetty omaa yliopistollista oppituolia sekä tunnustettua asemaa lakimieskoulutuksen oppiainejaotuksessa.[54] Esimerkiksi Lapin yliopiston oikeustieteiden tiedekunnassa on vuodesta 2004 lähtien ollut oikeusinformatiikan professuuri, jonka lisäksi oikeusinformatiikka on kuulunut pakolliseen opetukseen jo 1980-luvulta lähtien. Lisäksi tiedekunnassa toimii maan ainoa oikeusinformatiikan instituutti.[55]

Oikeustiede on mahdollista nähdä määritelmärikkaana tieteenä. Oikeustieteessä on esimerkiksi tapana määritellä oikeudenalat. Tämä koskee myös oikeusinformatiikkaa, joka on mahdollista määritellä suppeasti ja laajasti. Suppean määritelmän mukaan oikeusinformatiikka on oikeuden ja informaation sekä oikeuden ja tietotekniikan suhdetta tutkiva tieteen- ja opetusala.[56]

Laajemmasta perspektiivistä katsottuna oikeusinformatiikka tulee nähdä oikeustieteellisenä tutkimus- ja opetusalana, jonka tutkimus- ja opetuskohteena ovat oikeuden ja informaation sekä oikeuden ja tie-

54 *Tuori,* Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota, s. 1209. Katso myös *Saarenpää,* Oikeusinformatiikka (1998), s. 215–216. Vertaa *Korpisaari,* jonka mukaan oppituoli pelkästään ei osoita, että kysymys olisi oikeudenalasta, eikä sen puuttuminenkaan tarkoita, etteikö jo voitaisi puhua oikeudenalasta. *Korpisaari,* Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta, s. 995.

55 *Korhonen,* Oikeusinformatiikan kansainvälisiä haasteita tietoverkkojen yhdentyvässä maailmassa, s. 178 ja Koivumaa – *Korhonen,* Ahti Saarenpää suomalaisen oikeusinformatiikan tienraivaajana, s. 241.

56 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 25.

totekniikan suhteet eri muodoissaan.[57] Edellä mainittujen alueiden lisäksi oikeusinformatiikassa tutkitaan näiden alueiden yhteydessä ilmeneviä oikeudellisia sääntely- ja tulkintakysymyksiä.[58]

Kuten molemmat määritelmät osoittavat, oikeusinformatiikka on voimakkaasti kiinnostunut tietotekniikasta, sekä tietojenkäsittelystä että tietoliikenteestä.[59] Edellä mainitulla, hyvin teknologiakeskeisellä tavalla kuvattuna, saattaa oikeuinformatiikan tavasta tarkastella oikeutta saada puuttellisen käsityksen.

Tornbergin väitöskirjassaan esittämän mukaan oikeusinformatiikka on luonnehdittavissa erilaisia lähestymistapoja sisältäväksi oikeudenalaksi, joka koostuu oikeusteoreettisesta näkökulmasta aina käytännön tarpeista lähtevään tutkimukseen koskien oikeuden, informaation ja

57 Siltala on määritellyt oikeusinformatiikan hieman suppeammasta näkökulmasta. Hänen mukaansa ”oikeusinformatiikka tutkii oikeutta informaatiojärjestelmänä eli oikeudellisen tiedon saatavuutta ja erilaisiin tietokantoihin liittyviä oikeudellisia kysymyksiä, kuten oikeudellisia tietojärjestelmiä, tiedonhakua ja tiedonsiirtoa. Erityisenä oikeusinformatiikan tiedonintressinä voi olla vaikka se, miten hyvin kansalaiset saavat tietoa lain heille takaamista oikeuksista ja miten tietokantojen valvonta ja väärinkäytösten estäminen on oikeudellisesti järjestetty.” *Siltala,* Oikeustieteen tieteenteoria, s. 112.

58 *Saarenpää,* Oikeusinformatiikka (2009), s. 1.

59 Tämän lisäksi oikeusinformatiikka on kiinnostunut niin informaatioteknologian käytöstä oikeustieteessä kuin niistä oikeudellisista kysymyksistä, joita informaatioteknologia synnyttää. *Seipel,* Juridik och IT. Introduktion till rättsinformatiken, s. 269 sekä *Seipel,* Juristen och datorn, s. 200. Magnusson-Sjöbergin mukaan oikeusinformatiikan keskeisiä alueita ovat hallinnon automatisointi sekä oikeudellisia informaatiojärjestelmiä koskeviin menetelmäkysymyksiin keskittyminen sekä informaatio-oikeus. *Magnusson-Sjöberg,* Rättsautomation, s. 20.

informaatioteknologian välistä suhdetta.[60] Oikeusinformatiikka yhdistääkin oikeuden ymmärrykseen informaation ja informaatioympäristön suhteesta, informaatioprosesseista ja informaatioteknologiasta. Oikeusinformatiikassa tehtävälle tutkimukselle onkin ominaista monitieteinen tutkimusote, joka yhdistää oikeudelliseen toimintaympäristöön siihen liittyvää ei-oikeudellista tietoa.[61] Monitieteisyys ei kuitenkaan ole itsetarkoitus vaan luonnollinen osa ja ilmenemismuoto oikeustieteiden ja yhteiskuntatieteiden vahvalle yhteydelle.[62]

Toinen ominaispiirre on se, että oikeusinformatiikassa yleensä tutkitaan teknologisen kehityksen mukanaan tuomia uusia ilmiöitä, joihin ei vielä ole perinteisen oikeustieteen piirissä reagoitu. Tyypillistä on se, että oikeusinformatiikassa uusia oikeudellisia ilmiöitä ei nähdä rasitteina, vaan pikemminkin mahdollisuutena luoda teknologiaa tukevia ratkaisuja.

Tässä tutkimuksessa tutkimuskohdetta ei tarkastella vain oikeustieteen näkökulmasta. Tutkimusaiheeseen liittyy vahvoja poliittisia ja yhteiskunnallisia tekijöitä, joita ei voi ymmärtää pelkästään oikeustieteen kautta. Kokonaisuuden ymmärtämiseksi on tärkeä tarkastella myös taustalla vaikuttavia tekijöitä. Oikeudellisesta näkökulmasta tutkimuskohde nähdään mahdollisuutena luoda biometrista tunnistamista ja sen käyttöä tukevaa tietoa.

---

60 *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 151 sekä *Pöysti,* Communicational Quality of Law, s. 465.

61 *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 151, *Seipel,* Juridik och IT. Introduktion till rättsinformatiken, s. 269 sekä *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 26.

62 *Aarnio,* Tulkinnan taito, s. 238. Oikeustieteen ja yhteiskuntatieteen suhteesta katso myös *Backman,* Oikeustiede yhteiskuntatieteenä, s. 11–13.

Teknologiakeskeisyydestä huolimatta oikeusinformatiikan perusta on kuitenkin oikeustieteessä. Juridinen intressi määrittelee ne ongelmat, jotka oikeusinformatiikka näkee mielenkiintoisina ja tutkimisen arvoisina.[63] Oikeusinformatiikka on tänä päivänä oikeudenala, jonka yleisinä viitekehyksinä ovat informaation ja informaatioteknologian oikeudellinen sääntely informaatioyhteiskunnassa sekä niiden hyödyntäminen oikeudellisessa elämässä.[64]

Oikeusinformatiikan eteenpäin katsova luonne ja kiinnostus teknisen kehityksen oikeudellisiin ongelmiin ja mahdollisuuksiin ovat tuoneet oikeusinformatiikan piiriin uusia tutkimuskohteita. Nykyään oikeusinformatiikalle ovat yhä suuremmassa määrin tunnusomaisia tutkimusaiheita myös riskien tunnistamisen ja lainsäädännön muutostarpeen tutkimus. Toisaalta verkkoyhteiskunnan oikeudellistuminen on merkittävästi lisännyt alan lainopillista, esimerkiksi henkilötietojen suojaa koskevaa tutkimusta käytännöllisen oikeustieteen pysyttämiseksi mukana verkkoyhteiskunnan kehityksessä.[65]

Oikeusinformatiikka on nykyisin tapana jakaa yleiseen ja erityiseen osaan. Yleisen osan puitteissa tutkitaan oikeudellisen verkkoyhteiskunnan kehitystä, informaatioinfrastruktuurin oikeudellista merkitystä, tietojärjestelmien käytön oikeudellisia reunaehtoja sekä lakimiesten tietoteknisiä valmiuksia. Oikeusinformatiikan erityisessä osassa tarkastellaan lähemmin oikeudellista tietojenkäsittelyä, oikeudellista informaatiota, informaatio-oikeutta sekä tietotekniikkaoikeutta.[66]

---

63 *Seipel,* Juristen och datorn, s. 200.

64 *Saarenpää,* Oikeusinformatiikka (1998), s. 212.

65 *Saarenpää,* Oikeusinformatiikka (2015), s. 44

66 *Saarenpää,* Oikeusinformatiikka (2009), s. 21–127 sekä *Saarenpää,* Oikeusinformatiikka (1998), s.212. Näin myös Magnusson-Sjöberg. Rättsautomation, s. 24–25. Vertaa *Voutilainen,* jonka mukaan infor-

Viimeksi mainittu on enenevässä määrin muuttumassa ensi sijassa tietoverkko-oikeudeksi.[67]

Moderni oikeusinformatiikka ja sen kehitys on yhteydessä nykyaikaisen tietotekniikan kehityksen kanssa.[68] Tietotekniikan vaikutukset yhteiskuntaan ovat suuret. Tietotekniikalle on ominaista myös jatkuva kehitys osana yleistä yhteiskunnan teknologista kehitystä.

Oikeusinformatiikan tarkoitus onkin löydettävissä merkittävämmästä ja syvällisemmästä muutoskehityksestä. Oikeusinformatiikan eriytyminen omaksi oikeudenalakseen liittyykin pitkälti yhteiskunnan tietoteknistymiseen, infrastruktuurin muutokseen sekä informaation määrän ja informaatiomarkkinoiden kasvuun. Yhteiskunnan muuttuessa oikeusinformatiikka onkin yhä tärkeämmäksi käyvä oikeustieteen

---

maatio-oikeus ja ICT – eli tietotekniikkaoikeus eivät kuulu itsenäisinä oikeudenaloina oikeusinformatiikkaan. *Voutilainen,* Oikeus tietoon, s. 46.

67 *Saarenpää,* Oikeusinformatiikka, s. 718. Vertaa *Seipel,* Jurister och Datorn. Introduktion till rättsinformatiken, s. 36–39. Katso myös *Korhonen,* Perusrekisterit ja henkilötietojen suoja, s. 23. Ruotsalaisessa katsannossa oikeusinformatiikan puitteissa tutkitaan tietoyhteiskuntaan, sähköiseen kaupankäyntiin, sähköiseen markkinointiin, sähköisiin sopimuksiin, sähköiseen maksamiseen ja taloushallintoon sekä sähköiseen hallintoon liittyviä kysymyksiä. Katso tarkemmin esimerkiksi *Magnusson-Sjöberg – Nordbeck – Nordén – Westman,* Rättsinformatik: inlickar i e-samhället, e-handel och e-förvaltning. Vertaa *Seipel,* Juristen och datorn – Introduktion till rättsinformatiken, s.201.

68 Oikeusinformatiikan historiasta ja kehitysvaiheista katso tarkemmin *Paliwala* (ed.) The History of Legal Informatics. Katso myös *Seipel,* Juristen och datorn, s. 206–212, jossa Seipel tiivistetysti esittää oikeusinformatiikan kehitysvaiheita sekä tulevaisuudennäkymiä.

osa-alue. Oikeusinformatiikka on oikeuden ja tietotekniikan sekä oikeuden ja informaation tiede.

Oikeusinformatiikan merkityksen kasvun syyt liittyvät nykyään entistä enemmän yhteiskunnan muutokseen. Yhteiskunta on muuttunut laajamittaisen tietoteknistymisen, informaatioinfrastruktuurien muutosten ja informaation kasvun myötä, joihin perustuen on mahdollista puhua myös laajemmasta oikeustieteellisestä muutoksesta. On tarve opettaa ja tutkia muutoksen näkökulmasta ja ottaa huomioon myös tulevaisuus [69]

Edellä kuvatut esimerkit puhuvat oikeustieteiden – ja oikeusinformatiikan – monialaisuudesta. Oikeusinformatiikkaa tulee suppea-alaisuuden sijaan nähdä monialaisena tieteenä, koska sen vaikutukset ulottuvat eri tieteiden- ja oikeudenaloille.[70]

Varhaisessa oikeusinformatiikassa tutkittiin erityisesti mahdollisuuksia hyödyntää tietotekniikkaa oikeudellisessa elämässä. Varsinkin nykyajan digitaalisessa toimintaympäristössä tämä tehtävä jatkuu edelleen. Mukaan ovat tulleet tietoturvallisuus ja tietosuoja osana yksityisyyden suojaa.[71] Tietosuoja on tullut osaksi oikeusinformatiikkaa sen vuoksi, että oikeusvaltion kehittyessä on entistä tärkeämpää seurata ja arvioida yksilön oikeuksien toteutumista digitaalisessa toimintaympäristössä, jossa oikeus yksityisyyteen on eräs merkittävimpiä yksilön perusoikeuksia.[72]

---

69 *Seipel,* Juridik och IT (2004), s.271.

70 Peter Seipelin sanonta ”finns det egentligen något inom rättsystemet som inte på ett eller sätt har anknytning till information” kuvaa hyvin oikeusinformatiikan asemaa nyky-yhteiskunnassa. Katso tarkemmin *Seipel,* Juridik och IT (2004), s. 275.

71 *Saarenpää,* Kansalaisen oikeudet tiedon valtatiellä, s. 148.

72 Tämän ajatuksen taustalla on ihmiskäsitys, joka on oikeusinformatiikan peruspilari. Toinen peruspilareista on tietotekniikan oikeudellinen merkitys. *Saarenpää,* Kansalaisen oikeudet tiedon valtatiellä,

Uutena oikeuden- ja tieteenalana oikeusinformatiikka yhä etsii rajojaan, sillä oikeusinformatiikan muutos seuraa yhteiskunnan muutosta. Nähtävissä on, että uudessa informaatioinfrastruktuurissa oikeusinformatiikka on entistä tärkeämpi.[73]

Oikeusinformatiikka on erikoitumisen tulosta. Tietotekniikka yhdessä informaation kanssa toimivat systematisoinnin avaimina. Esimerkkinä toimii tietosuojalainsäädäntö, joka on oikeusinformatiikan ja persoonallisuusoikeuden yhteinen tutkimusalue. Oikeusinformatiikka on myös yhdistävä ja yhteistyötä avaava tiede, jonka merkitys korostuu sitä enemmän, mitä suuremman merkityksen tietotekniikka yhteiskunnassa saa.

Verkkoyhteiskunnassa tämä on entistä tärkeämpää, sillä etenkin informaation ja verkkoviestinnän merkityksen kasvu edellyttävät ns. tiedon tien seuraamista kokonaisuudessaan. Vastaavasti myös yhteiskunnan muutos digitaaliseksi verkkoyhteiskunnaksi ja edelleen kohti valvontayhteiskuntaa vaatii oikeusinformatiikalta entistä tiiviimpää yhteistyötä muiden yhteiskunnan kehitystä ajantasaisesti seuraavien tieteiden kanssa. Tämä muutos myös korostaa oikeusinformatiikan merkitystä. Oikeusinformatiikka tieteenalana ei täytä yhteiskunnallista palvelutehtäväänsä, ellei se ota kantaa yhteiskunnan muutokseen ja muutosta seuraaviin oikeudellisiin ilmiöihin.

---

s.148

73 Infrastruktuurilla tarkoitetaan yleisesti yhteiskunnallisesti merkittävien toimintojen tarvitsemia rakenteita, palveluita, järjestelmiä ja väylästöjä. Ns. kriittisiä infrastruktuureja eli sellaisia, joiden toimimattomuus vaarantaa yhteiskunnan toimivuuden ovat erilaiset liikenne-, energia-, yhdyskuntatekniikka ja viestintäväylästöt. Verkkoyhteiskunnassa näiden rinnalle ja osin jopa ohi on noussut tietoverkkojen muodostama informaatioinfrastruktuuri, joiden ytimen muodostavat avoimet tietoverkot. *Saarenpää,* Oikeusinformatiikka (2009), s. 36–37.

Asiaa on mahdollista kuvata esimerkillä: Jalkapallossa syötön perusajatuksena on pallon syöttäminen sinne, missä pelaaja tulee olemaan, ei sinne, missä pelaaja jo on. Toisin sanoen pelin onnistuminen edellyttää ennakoimista ja muutoksen huomioimista. Samoin oikeusinformatiikka katsoo sinne, mihin kehitys on meitä viemässä, ei niinkään sitä missä tällä hetkellä olemme. Tällä tavoin oikeusinformatiikka ennakoi jo tulevaa muutosta, jotta oikeudellisiin ongelmiin on mahdollista reagoida ennen kuin ne ovat varsinaisesti ongelmia.

Oikeusinformatiikka siis edesauttaa oikeuden aikaistumista yhteiskunnassa. Samalla oikeusinformatiikan tehtävänä oikeuden yleistieteenä[74] on ottaa kantaa siihen, miten perinteiset oikeudelliset instituutiot sijoitetaan osaksi uutta digitaalista toimintaympäristöä[75] ja miten ne tässä uudessa toimintaympäristössä voivat toimia yksilön oikeuksia turvaavasti.

Oikeusinformatiikkaa on mahdollista pitää myös oikeuden yleistieteenä, sillä sen piirissä käsitellään perinteisen oikeusteorian alueelle kuuluvia kysymyksiä uudessa digitaalisessa toimintaympäristössä.[76] Oikeusinformatiikka pyrkii vastaamaan kysymyksiin yksilön oikeuksien ja oikeuden voimassaolosta ja niiden vaikuksista uuden digitaalisen

74 Yleisen oikeustieteen kohteista katso esimerkiksi Makkonen, Luentoja yleisestä oikeustieteestä, s. 2–3.

75 Digitaalinen toimintaympäristö voidaan suppeasti määritellä ympäristöksi, joka on sidoksissa tietotekniikkaan ja informaation käsittelemiseen. Katso *Saarenpää,* Oikeusinformatiikka (2011), s. 419.

76 Oikeusinformatiikka on oikeudellisen tiedon hakua ja tietosuojaa koskevilta osiltaan voimakkaasti sidoksissa oikeusteoriaan. *Saarenpää,* ATK ja yksilön suoja, s. 201–202 ja s. 208. Katso myös *Korhonen,* Informaatio-oikeuden asemasta oikeuksien kentässä, s.89. Vertaa *Aarnio,* Tulkinnan taito – ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta, s. 382.

toimintaympäristön ympärille rakentuvassa verkkoyhteiskunnassa.[77] Oikeusinformatiikka toimii uuden ja perinteisen oikeustieteen yhdistävänä siltana verkkoyhteiskunnassa.[78]

Perinteisesti suuntautuneelle juristille oikeuden ja tietotekniikan suhde saattaa näyttäytyä vaikeasti lähestyttävältä tai jopa yllätyksellisiltä. Tämän vuoksi oikeusinformatiikan välttämätön valistustehtävä jatkuu edelleen myös juristien keskuudessa.

1.2.2.1. Informaatio-oikeus osana oikeusinformatiikkaa

Yhteiskunnan muuttuessa on informaation merkitys muuttunut olennaisesti. Verkkoyhteiskunnassa se on entistä tärkeämpi eri toimintojen raaka-aine. Informaatiotuotannon sekä viestinnän merkitys ovat myös kasvaneet yhteiskunnassa niin taloudellisesti kuin sosiaalisestikin. Informaatiotuotteisiin sekä viestintään liittyvät taloudelliset ja oikeudelliset jännitteet ovat tulleet aikaisempaa merkittävämmiksi niin eettisesti kuin taloudellisestikin, mikä on johtanut informaatio-oikeuden merkityksen voimistumiseen yhteiskunnassa.[79]

Informaatio-oikeuden lähtökohta on varsin selkeä. Kysymys on ensisijaisesti ihmisen oikeuksista ja niiden tukemisesta oikeusvaltiossa. Informaatio-oikeus turvaa osaltaan itsemääräämisoikeuden toteutumista käsiteltäessä informaatiota, kuten yksilön biometrisia tietoja verkkoyhteiskunnassa.

---

77 Tämän kautta on nähtävissä myös yhteiskunnan ja oikeuden välinen vuorovaikutus, sillä yhteiskunta ja sen muutokset vaikuttavat myös oikeuteen. Vertaa *Tolonen,* Oikeuslähdeoppi, s. 8.

78 Vertaa *Kuopus,* Hallinnon lainalaisuus ja automatisoitu verohallinto, s. 23–24. Kuopuksen mukaan oikeusinformatiikalle on ollut ominaista siteiden katkeaminen ”vanhaan” oikeustieteeseen.

79 *Saarenpää,* Oikeusinformatiikka (2011), s. 507.

Verkkoyhteiskunnassa sääntely jatkuvasti täsmentyy. Yhä enenevässä määrin sekä informaatioinfrastruktuurista että informaatiosta ja informaatioprosesseista säädetään lain tasolla. Tämä johtaa tiedollisen toimintaympäristön merkittävään muuttumiseen. Viimeistään verkkoyhteiskuntakehitys on tuonut välttämättömäksi arvioida lähemmin informaatiota, sen sääntelyä sekä erityisen informaatio-oikeuden tarvetta.

Lainsäädäntöön sisältyy mitä erilaisimpia informaatioon liittyviä, eri tavoin toteutettuja ja myös erilaisia funktioita omaavia säännöksiä. Informaatiota koskeva lainsäädäntö on kuitenkin hajanaista. Esimerkiksi biometristen tietojen käsittelystä säädetään meillä useissa henkilötietojen käsittelyn erityislaeissa, kuten henkilötietojen käsittelystä poliisitoimessa annetussa laissa. Aiheen hajanaisuus perinteisen systematiikan puitteissa toimittaessa ei kuitenkaan voi olla esteenä informaatiota tutkivan erityisen oikeudenalan olemassaololle ja kehitykselle. Näin siksi, että tieteen keskeisiin tehtäviin kuuluu asioiden järjestäminen ja tarvittaessa järjestyksen muuttaminen. Verkkoyhteiskunnassa oikeustieteen velvollisuutena on ottaa kantaa informaatioon ja sen myötä informaatio-oikeuteen oikeudenalana.

Informaatio-oikeus yhdistää normijärjestyksenä oikeusnormit, oikeudellisten toimintojen käytännöt sekä oikeuskielen rakenteet. Informaatio-oikeudellisen järjestelmän avulla pyritään hahmottamaan ja jäsentämään tiettyyn kokonaisuuteen liittyvät oikeudelliset normistot ja oikeudelliset kysymykset. Tässä tutkimuksessa käsiteltävä kokonaisuus on biometriset tunnisteet ja näiden asema henkilötietojen suojaa koskevassa lainsäädännössä. Informaatio-oikeudessa lähestymistapa onkin usein ongelma- tai ilmiökeskeinen sekä monitieteinen.[80] Tämä

80 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 369–371 sekä *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 154.

johtaa siihen, että informaatio-oikeudella on teoriassa mahdollisuus kattaa kaikki oikeudenalat. Edellytyksenä tosin on että informaatio-oikeutta käytetään määrittelemään aluetta, jolla on jokin yhteys dataan tai informaatioon.[81] Syynä on se, että informaatio-oikeus normijärjestelmänä sisältää informaatiota, sen käsittelyä ja käyttöä sekä informaatiomarkkinoita ja muita informaatiota välittäviä tai käsitteleviä instituutioita säänteleviä normeja.[82]

Edellä esitetty jättää kuitenkin informaatio-oikeudesta täsmentymättömän ja varsin laaja-alaisen kuvan, ja antaa näin aiheen lähemmälle tarkastelulle. Informaatioon kohdituva oikeudellinen sääntely on jaettavissa seitsemään säädöstyyppiin: 1) informaatiosidonnaiset, 2) informaatioperusteisia tuotteita koskevat, 3) viestintää koskevat, 4) yksilöön liittyvää informaatiota koskevat, 5) julkista informaatiota koskevat, 6) informaatioinfrastruktuuria koskevat sekä 7) informaation säilyttämistä koskevat säädökset.[83] Tämä tutkimus keskittyy yksilöön liittyvää informaatiota koskevaan sääntelyyn. Tutkimuksessa keskity-

81 *Bing,* Information Law?, s.38.

82 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 375. Saman on todennut informaatio-oikeuden isänä pidetty Egbert Dommering teoksessaan An Introduction to Information Law vuodelta 1991. Katso *Dommering,* An Introduction to Information Law, s. 20.

83 Tämän jaon on Ahti Saarenpää esitellyt yleisesityksessä Oikeusinformatiikka. Huomionarvoista on se, että jakoa ei ole tarkoitettu tarkkarajaiseksi eikä tyhjentäväksi. Esimerkkinä tästä on se, että vuoden 2009 yleisesityksessä ei vielä ollut informaation säilyttämistä koskevaa sääntelyä mainittu. Tämä on osoituksena myös informaatio-oikeuden dynaamisesta luonteesta. Informaatio-oikeuden tutkimuskohteet muuttuvat yhteiskunnan muuttuessa. Katso *Saarenpää,* Oikeusinformatiikka (2009), s. 93–95 ja Oikeusinformatiikka (2011), s. 500.

tään biometristen tietojen käsittelijän oikeuksiin ja velvollisuuksiin sekä biometristen tietojen subjektin oikeuksiin ja velvollisuuksiin yksilönä.[84]

Informaatio-oikeus määritellään oikeudenalaksi, jossa tutkitaan informaation tuottamisen, käsittelemisen, välittämisen, markkinoinnin, suojaamisen ja säilyttämisen oikeudellista sääntelyä sekä sääntelyn tarvetta ja mahdollisuuksia.[85] Toisaalta informaatio-oikeutta on mahdollista lähestyä myös laajemmasta näkökulmasta. Laajemman ja yksityiskohtaisemman näkökulman mukaisesti informaatio-oikeuden tehtävät ja tutkimuskohteet ovat seuraavat: 1) *informaation ja viestinnän erityispiirteiden selvittäminen oikeudellisen sääntelyn ja oikeuden soveltamisen edellyttämällä tavalla,* 2) *informaation tuottamista, käsittelyä, varastointia, toisintamista, muuntamista, välittämistä, käyttöä ja varastointia sekä hävittämistä ohjaavien sääntelyperiaatteiden ja oikeusnormien muotoilu sekä tällaisten normien systematisointi ja tulkinta;* sekä 3) *informaatiotekniikan ja informaatioteorian kehityksestä informaatio-oikeudellisille normeille sekä informaatio-oikeuden yleisille opeille aiheuttamien muutostarpeiden tunnistaminen ja analysointi sekä kehityksen myötä syntyvien uusien oikeudellisten instituutioiden sijoittaminen osaksi oikeusjärjestelmän kokonaisuutta.*[86]

Informaatio-oikeuden teoreettista perusteista on johdettavissa sen oikeudellinen tehtävä. Sen avulla informaatiota ja viestintää koskevien oikeusnormien, oikeuskielen lauseiden sekä oikeuden yleisten oppien

---

84 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 375. Näin myös *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 155.

85 *Saarenpää,* Informaatio-oikeus, s. 206. Informaatio-oikeudellisista näkökulmista katso myös *Bing,* A background analysis for information law, s. 43–59. Vertaa *Voutilainen,* Oikeus tietoon, s. 31. ja *Voutilainen,* ICT-oikeus sähköisessä hallinnossa, s. 18.

86 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 372.

joukko on kohdennettavissa tiedollisesti hallittavissa olevaksi oikeuden järjestelmäksi.[87]

Informaatio-oikeus on samalla oikeustieteen metodinen paradigma, jolla on sille ominainen tutkimuskohde ja tutkimuksellinen lähestymistapa. Tutkimuskohteen ominaispiirteet heijastuvat informaation sääntelyn ja samalla sääntelyä toteuttavien oikeuden normien ja instituutioiden tutkimukseen.[88] On varsin mahdoton ajatus, että lainopin harjoittajan olisi mahdollista operoida jollain yhtenäisellä välineistöllä, joka kohteesta ja sääntelykontekstista riippumatta toimisi kaikilla oikeudenaloilla. Varsin helppoa on yhtyä siihen, että metodis-teoreettisesti ja tieteenhistoriallisesti informaatio-oikeus on osa oikeusinformatiikkaa. Oikeusinformatiikka määrittää informaatio-oikeuden paradigmaa.[89]

Oikeussystemaattisesti informaatio-oikeus on osa oikeusinformatiikkaa. Informaatio-oikeuden eriytyminen omaksi oikeudenalakseen osana oikeusinformatiikkaa on kuitenkin uudehko, oikeudellisen informaatioyhteiskunnan kehitykseen liittyvä oikeussystemaattinen ilmiö. Oikeusinformatiikan piirissä keskustelu informaatio-oikeudesta

87 Informaatio-oikeudesta tietyllä tapaa rajattuna oikeusnormien joukkona, katso *Dommering,* An Introduction to Information Law, s. 6 ja 10–12.

88 *Dommering,* An Introduction to Information Law, s. 10–12 ja 20–28 sekä *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 358. Vertaa *Voutilainen,* Oikeus tietoon, s. 31.

89 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 299–302. Vertaa *Voutilainen,* Oikeus tietoon, s. 46, *Konstari,* Matkalla kohti eurooppalaista tietosuojaa, s. 22 sekä Wallin – *Konstari,* Julkisuus- ja salassapitolainsäädäntö…, s. 32–33. Wallin, Konstari ja Voutilainen katsovat informaatio-oikeuden omaksi erilliseksi oikeudenalakseen.

alkoi varsin pian sen jälkeen, kun keskustelu tietotekniikan laajamittaisen käytön vaikutuksista oli käynnistynyt.

Vasta 1990-luvulla informaatio-oikeuden merkitys kasvoi olennaisesti.[90] Tuolloin informaatio-oikeus saavutti oikeudellisen informaatio-yhteiskunnan tärkeän ja ajankohtaisen oikeudenalan aseman. Informaatio-oikeudellisen lainsäädännön kasvun ohella syynä oli yhteiskunnan eri toimintojen tietoteknistyminen, tietoverkkojen käyttömahdollisuuksien ja käytön kehitys, informaatiomarkkinoiden kansallinen ja kansainvälinen kehitys sekä ihmis- ja perusoikeuksien merkityksen kasvu. Kaikki nämä tekijät antavat aiheen puhua informaatio-oikeudesta yhtenäisenä oikeudenalana. Yhteiskunnallisessa keskustelussa on välttämätöntä tarkastella yksilöiden, yhteisöjen ja yhteiskunnan informaatioriippuvuutta siihen liittyvine oikeuksineen ja velvollisuuksineen sekä etuineen ja riskeineen.

Nykyisin informaatio-oikeus on vakiintunut, tärkeä osa oikeusinformatiikkaa ja yleisemmin verkkoyhteiskunnan modernia oikeustiedettä. Informaation merkityksen kasvaessa on myös syytä puhua informaatio-oikeudesta keskeisten oikeusperiaatteiden varaan rakentuvana oikeudenalana.[91] Se on informaatiomarkkinoiden ja tietoverkkojen kehityksen myötä noussut tärkeäksi oikeusinformatiikan osa-alueeksi. Informaatio ilmenee ja sitä käsitellään mitä erilaisimmin tavoin mitä erilaisimmissa tarkoituksissa. Vastaavasti informaation sääntely sekä informaatioon liittyvä sääntely ovat monitahoisia asioita.

---

90 Kuopuksen näkemyksen mukaan jo 1980-luvulla on voitu puhua perustellusti informaatio-oikeudesta. Katso *Kuopus* Hallinnon lainalaisuus ja automatisoitu verohallinto, s. 24–25.

91 Pöystin mukaan informaatio-oikeuden nousu on pitkälti yhdistettävissä Euroopan yhteisön eurooppalaisten informaatiomarkkinoiden kehittämistä koskeviin aloitteisiin ja jo toteutuneisiin säädöksiin. *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 366.

2000-luvulla informaatio-oikeuden asema on edelleen voimistunut ja jossain määrin se on myös eriytynyt oikeusinformatiikasta.[92] Tämä ei kuitenkaan ole vaikuttanut informaatio-oikeuden merkitykseen yhteiskunnassa. Tulevaisuudessa informaatio-oikeus tulee nuoren oikeudenalan tavoin hakemaan uutta muotoa ja uudenlaisia vivahteita muuttuvassa maailmassa joko osana oikeusinformatiikkaa tai omana erillisenä oikeudenalanaan. Informaatio-oikeus tullee myös yhä vahvemmin vaikuttamaan perinteisten oikeudenalojen sisällä eräänlaisena informaatiota ja tietotekniikkaa koskettelevien oikeudellisten ongelmien työvälineenä.

1.2.3. Persoonallisuusoikeus oikeustieteen alana

Tässä tutkimuksessa biometrista tunnistamista tarkastellaan erityisesti henkilötietojen suojan näkökulmasta. Henkilötietojen suojaan liittyviä käsitteitä ovat intimiteettisuoja[93], salassapito, yksityisyys, yksityiselämän suoja[94] ja itsemääräämisoikeus. Laajemmasta näkökulmasta katsottuna kysymys on persoonallisuusoikeuden alueesta.[95] Tämän

92 *Saarenpää – Korhonen – Råman,* Sähköinen viestintä, tietoturvallisuus ja perusoikeudet, s. 8.

93 Intimiteetti on Konstarin mielestä yhteydessä yksityisyyteen, tietosuojaan ja henkilötietojen salassapitoon. *Konstari,* Asiakirjajulkisuudesta hallinnossa – tutkimus yleisten asiakirjain julkisuudesta hallinnon kontrollivälineenä, s. 339–340 ja 352–356. Intimiteettisuojasta katso erityisesti *Melander,* Intimiteetin oikeussuojasta. LM 1964, s. 785–799.

94 Yksityisyydestä ja yksityiselämän suojasta puhuttaessa on huomioitava näitä lähellä oleva käsite yksilön suoja. Käsite ei juurikaan ole yleistynyt suomalaisessa oikeuskielessä. Yksilön suojasta tarkemmin katso erityisesti *Saarenpää,* Yksityisyys, yksityiselämä, yksilön suoja – yksityisyyden käsitteellistä kuvausta, s. 326.

95 *Korhonen,* Perusrekisterit ja henkilötietojen suoja, s. 98.

vuoksi tässä tutkimuksessa biometrista tunnistamista lähestytään myös persoonallisuusoikeuden näkökulmasta. Monipuolista ja monioikeudellista lähestymistapaa voidaan perustella sillä, että nykyään ei ole enää välttämättä mielekästä liittää tiettyä oikeudellista kysymystä vain yhden oikeudenalan piiriin.[96] Syynä on se, että oikeudellisen ongelman sijoittamisella tietylle oikeudenalalle saatetaan alitajuisesti rajata pois ongelman ratkaisemisessa tarvittavia normeja, periaatteita tai yleisiä oppeja vain, koska ne kuuluvat toisen oikeudenalan piiriin. Tulkintaongelman tarkasteleminen laajemmasta eli yhden perinteisen oikeudenalan ylittävästä näkökulmasta taikka useiden oikeudenalojen kautta on usein mahdollista saada sekä lisää perspektiiviä ongelmanratkaisuun että tasapainoisen ratkaisun tekemiseen tarvittavia oikeudellisesti päteviä argumentteja kunkin oikeudenalan yleisten oppien kautta. Tällä tavoin toimimalla edistetään sekä muodollista että aineellista oikeudenmukaisuutta.[97]

Persoonallisuusoikeudella on pitkä historia takanaan. Henkilöoikeus tunnettiin jo roomalaisessa oikeudessa.[98] 1800-luvun alkupuolen saksalaisessa oikeussystematiikassa henkilöoikeutta pidettiin yhtenä yksityisoikeuksista velvoite-, esine, sekä perhe- ja jäämistöoikeuden rinnalla. Tämän saksalaisen mallin kautta myös suomalaisessa yksityisoikeudessa persoonallisuusoikeudella on ollut ja tulee aina olemaan oma sijansa.

---

96 Näin myös *Korpisaari,* Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta, s. 990.

97 *Tuori,* Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota, s. 1215 ja 1219–1220 sekä *Tammi-Salminen,* Vanha ja uusi esineoikeus, s. 456.

98 Yksi varhaisimmista roomalaisen oikeuden oikeussystemaattisista jaotteluista oli jako henkilöoikeuksien, varallisuusoikeuksien ja perheoikeuksien välillä. *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2009), s. 267.

Vielä 1970-luvulla Suomessa esiintyi erimielisyyttä siitä, oliko ihmisellä katsottava olevan oma subjektiivinen oikeus vaatia suojaa persoonaansa lähimmin liittyville elämänalueille.[99] Ajassa ja kehityksessä on kuitenkin menty eteenpäin. Kehitys on johtanut siihen, että persoonallisuusoikeus on saanut suuremman merkityksen. Syynä ovat yhteiskunnan kehitys, ihmiskäsityksen muuttuminen, institutionaalisten suojasäännösten lainsäädännöllinen kehitys ja niiden reaalisen käytön kasvava kunnioitus. Nämä tekijät ovat myös vaikuttaneet siihen, että etualalle on noussut ihminen, hänen tarpeensa ja oikeutensa.

Perustuslain 1 §:n 1 momentista käy ilmi se, että demokraattisen oikeusvaltion oikeusjärjestyksessä lähtökohtana on ihminen. Yhteiskunta on ihmistä ja ihmisten yhdessä toimimista varten, ja oikeus ihmistä varten. Demokratiassa ihminen on kaikkein tärkein.[100]

Pidettäessä persoonallisuusoikeutta pelkästään teoriana oikeuskelpoisuudesta, oikeustoimikelpoisuudesta ja oikeussubjekteista saadaan vääränlainen kuva tästä oikeudenalasta. Määritelmässä unohtuu täysin ihmisen merkitys. Persoonallisuusoikeus on ollut ja tulee olemaan oikeudenala, jossa ihminen ja ihmiskäsitys ovat ensi arvoisen tärkeitä.[101]

Ihmiskäsityksen näkökulmasta perinteinen persoonallisuusoikeus asettuu luontevasti osaksi laajempaa oikeussystemaattista kokonai-

---

99 *Kivimäki – Ylöstalo,* Suomen siviilioikeuden oppikirja, s. 18.

100 Saarenpää huomauttaakin siitä, että oikeusjärjestys on järjestys yksilön vapauden ja oikeuksien toteuttamiseksi oikeudenmukaisella tavalla, ja kaikki muu on alisteista yksilön oikeuksille. *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2011), s. 232.

101 Myös Tornberg on väitöskirjassaan ottanut tähän kantaa sanomalla persoonallisuusoikeuden kohteen olevan pääsääntöisesti elävä ihminen, riippumatta hänen iästään, terveydentilastaan, sukupuolestaan, kansalaisuudestaan, rodustaan, etnisestä alkuperästään, uskonnostaan tai sosiaalisesta asemastaan. *Tornberg,* Edunvalvonta, itsemääräämis-

suutta, jonka perustana on yksilön persoonallisuuden suoja yhteiskunnassa. Kysymys ei ole vain siitä, miten lakiteknisesti liitymme yhteiskuntaan, vaan millaisina yksilöinä liitymme siihen ja millaista suojaa persoonallisuutemme eri yhteyksissä saa.[102]

Persoonallisuusoikeudella on vahva liittymä ihmisoikeuksiin. Suojattavana kohteena on nimenomaan itsemääräämisoikeus, oikeus määrätä omasta persoonastaan, saada kunnioitusta henkilökohtaista ja sosiaalista identiteettiään kuin julkista kuvaansakin kohtaan sekä oikeus kehittää omia yksilöllisiä ominaisuuksiaan. Persoonallisuusoikeuksien avulla ihmisoikeuksien tavoitteita tuodaan perusoikeuksien kautta tavanomaisen lainsäädännön tasolle.[103] Ihmisarvoa suojattaessa suojataan myös henkilön identiteettiä, jonka todenmukainen tunnistaminen on ihmisarvon perusta.[104]

Kansainvälisestä perspektiivistä katsottuna persoonallisuusoikeuden on käsitteenä tunnetuin Pohjoismaissa ja erityisesti Saksassa. Saksan toisen maailmansodan jälkeen annetun vuoden 1949 perustuslain mukaan jokaisella on oikeus ihmisarvoon ja vapaaseen persoonan kehittämiseen.[105]

---

oikeus ja oikeudellinen laatu, s. 118. Katso myös *Saarenpää* Henkilö- ja persoonallisuusoikeus (2011), s. 235–236 sekä *Götting – Schertz – Seitz,* Handbuch des Persönlichkeitsrechts, s. 593.

102 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 222–223

103 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2009), s. 12–13. Tähän on Saarenpään mukaan syynä siirtyminen sääntökeskeisestä rutiinilegalismista ihmiskeskeiseen legalismiin. Katso tarkemmin *Saarenpää,* Potilas, oikeus, ihminen – näkökohtia itsemääräämisoikeuden suojasta, s. 272.

104 *Kateb,* Human Dignity, s, 10.

105 *Lögdberg,* Personlighetsrätt, s. 11–12 ja 25–29. Saksan henkilöoikeus on hakenut muotonsa erityisesti oikeuskäytännössä. Erityisen merkittävä on ns. Schacht-tapaus vuodelta 1954. *Stoll,* The General

Persoonallisuusoikeus on jaettavissa muodolliseen ja materiaaliseen osaan.[106] *Muodollinen* persoonallisuusoikeus tutkii ensi sijassa oikeussubjekteja: niiden syntyä, olemassa oloa, suhteita muihin oikeussubjekteihin, tunnistamista ja lakkaamista. Keskeinen tutkimusaihe on yksilön erilaiseen tunnistamiseen liittyvä tunnisteoikeus. Yksilön tunnistaminen on erilaisten oikeussuhteiden ja valvonnan kannalta merkittävä oikeudellinen asia. *Materiaalinen* persoonallisuusoikeus puolestaan keskittyy tarkastelemaan lähemmin niitä vapauksia ja oikeuksia sekä erilaisia suojasäännöksiä, jotka koskevat meitä ja meidän toimintaamme itsemääräämisoikeutemme puitteissa yksilöinä yhteiskunnassa. Havainnollisen esimerkin tarjoaa yksityisyyden suoja.

Materiaalisen persoonallisuusoikeuden keskeinen lainsäädäntö yksityisyys- ja tietosuojalainsäädännöstä nimi- ja tunnistelainsäädäntöön on lainsäädäntöä, joka jossain vaiheessa koskee kaikkia kansalaisia. Kysymys on tässä mielessä itsemääräämisoikeutta koskevasta yleislainsäädännöstä, joka on kaikille tärkeää ja oikeudellisessa viestinnässä erityistä huolenpitoa edellyttävää lainsäädäntöä.[107]

Right to Personality in German Law, s. 31–34.

106 Saksassa persoonallisuusoikeus on ollut tapana jakaa yleiseen ja erityiseen osaan. Yleisestä persoonallisuusoikeudesta puhutaan silloin, kun lähtökohtana on yksilön persoonallisuuden perustuslaillinen suoja. Erityisellä persoonallisuusoikeudella puolestaan tarkoitetaan niiden säädösten ja säännösten muodostamaa kokonaisuutta, joilla ihmisen persoonallisuutta suojataan tai annetaan mahdollisuuksia rajoittaa sitä. *Götting – Schertz – Seitz,* Handbuch des Persönlichkeitsrechts, s. 4, 594 ja 598 sekä *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 223. Suomen oikeustieteessä käytössä oleva jaottelu kuvaa ehkä jonkin verran paremmin persoonallisuusoikeuden yhteiskunnallista merkitystä ja erilaisia käytännön ulottuvuuksia.

107 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 228.

Tässä tutkimuksessa keskitytään niin materiaalisen kuin muodollisen persoonallisuusoikeuden alueelle, sillä biometrisella tunnistamisella on suuria yhtymäkohtia molemmille persoonallisuusoikeuden alueille. Materiaalisen persoonallisuusoikeuden alueelta tutkitaan itsemääräämisoikeutta, erityisesti tiedollista itsemääräämistä. Muodollisen persoonallisuusoikeuden alueelta keskitytään yksilön tunnistamiseen liittyvään tunnisteoikeuteen.

1.2.3.1. Tunnisteoikeus osana persoonallisuusoikeutta

Nimi- ja tunnisteoikeus persoonallisuusoikeuden osana on selkeästi jaettavissa kahteen eri osaan. Nimioikeuden keskeisiä tutkimuskohteita ovat nimien määräytymiseen, niiden yksilöllisyyteen, pysyvyyteen sekä muuttamiseen liittyvät kysymykset. Nimioikeus on ennen kaikkea yksilön perusoikeuksiin ja nimikultuuriin liittyvää oikeutta.[108] Tunnisteoikeus on puolestaan yksilön luotettavaan tunnistamiseen, identiteettiin, yksityisyyteen sekä anonymiteettiin liittyvää uudempaa perusoikeuksiin sidoksissa olevaa persoonallisuusoikeutta. Toisin kuin nimet, tunnisteet eivät lähtökohtaisesti ole julkisia ja julkisesti käsiteltäviä. Nimestä poiketen ne ovat myös yleensä täysin yksilöllisiä tai ainakin siihen pyrkiviä.[109]

Tunnisteesta esimerkkinä on kaikille suomalaisille syntymän jälkeen annettava henkilötunnus, jonka tehtävänä on yksilöiden erottaminen toisistaan. Henkilötunnus on yksilöimiskeino, joka yksilöi kansalaiset vielä tarkemmin kuin nimi. Täysin samannimisiä ihmisiä löytyy, mutta ei kahta, joilla olisi täysin sama henkilötunnus. Se säilyy muuttumattomana koko elinajan.

---

108 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2009), s. 349.

109 *Saarenpää*, Henkilö- ja persoonallisuusoikeus (2009), s. 349 sekä *Saarenpää,* Personrätt – Integritetsrätt (2013), s. 79.

Henkilötunnus otettiin Suomessa käyttöön 1960-luvulla. Ajan saatossa henkilötunnuksesta on kuitenkin muodostunut keskeinen väline yksilöiden tunnistamisessa. Sitä ei kuitenkaan ole tarkoitettu henkilöiden tunnistamiseen, vaan henkilöiden erottelemiseen toisistaan. Henkilötunnusta ei kuitenkin saa käyttää yhtenä tietona muiden joukossa, joita henkilöltä kysytään tunnistamistarkoituksessa hänen soittaessaan esimerkiksi yrityksen asiakaspalveluun, terveydenhuollon toimintayksikköön tai viranomaiselle. Kukaan rekisterinpitäjä ei saa rakentaa tunnistamiskäytäntöjään yksinomaan henkilötunnuksen ja nimen kysymisen varaan. Tämä on vastoin henkilötunnuksen alkuperäistä tarkoitusta.

Tunnisteoikeuden merkitys verkkoyhteiskunnassa on varsin kiistaton. Yksilön tunnistaminen ja yksilöiden erottaminen toisistaan ovat myös juridisesti entistä tärkeämpiä verkoissa toimittaessa. Perinteisen fyysisen yhteiskunnallisen toimimisen rinnalle on tullut sähköinen yhteiskunnallinen toimiminen.

Palvelut – niin yksityiset kuin julkiset – ovat siirtyneet enenevässä määrin tietoverkoissa toimiviksi ja toteutettaviksi. Yksilön luotettavaan tunnistamiseen liittyvät oikeudelliset kysymykset saavat korostuneen merkityksen myös persoonallisuusoikeuden alueella. Itsemääräämisoikeuteen keskittyvänä oikeudenalana persoonallisuusoikeuden sisällä on myös havahduttu yksilön luotettavan tunnistamisen kysymyksiin verkkoyhteiskunnassa. Biometrinen tunnistaminen on tästä näkyvä esimerkki. On jo syystä mahdollista puhua tunnisteoikeuden erityiskysymyksistä.

2. Lähtökohdat tutkimusaiheen tarkastelulle

2.1. Oikeustiede ja yhteiskunnallinen kehitys

Eräs oikeutta koskevista lausumista on väite siitä, että lainsäädännön kehitys ei etene yhtäaikaisesti yhteiskunnan kehityksen kanssa. Lainsäädännön sanotaan kulkevan jälkijunassa.[110] Tämä korostuu uusien teknologisten ilmiöiden, kuten biometrisen tunnistamisen kohdalla. Syynä se, että uutta kohdattaessa altistutaan herkästi vaatimuksille myös uudesta sääntelystä. Taustalla on ajatus siitä, että lainsäädännössä tulee olla selkeä viesti asiaan reagoimisesta.

Yksipuolinen ajatus oikeuden kulkemisesta vain jälkijunassa on kuitenkin harhaanjohtava, sillä lainsäädäntö yleensä avaa mahdollisuuden yhteiskunnan kehitykseen. Tyyppitilanteessa lainsäädäntö abstraktisuudessaan kulkee yhteiskunnan edellä. Vapauksia rajoitetaan vain, kun se on välttämätöntä ja uusia ilmiöitä sovitetaan olemassa olevaan lainsäädäntöön tulkinnan avulla.

Lähtökohtana on lainsäädännön ja yhteiskunnan kehityksen sopusuhta. Tätä tasapainoa uhkaa ennen kaikkea riski lainsäädännön jälkeenjääneisyydestä. Mikäli lainsäätäjä ei havahdu uuteen ajoissa, oikeus jää jälkeen yhteiskunnan kehityksestä.[111] Tämän vuoksi on aiheellista tarkastella oikeuden ja yhteiskunnan muutosta.

110 Katso esimerkiksi *Kuopus,* Hallinnon lainalaisuus ja automatisoitu verohallinto, s. 6.

111 *Saarenpää,* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 35.

2.1.1. Oikeus digitaalisessa toimintaympäristössä

Oikeustiede on tiedettä oikeudesta. Tällainen määritelmä jättää kuitenkin avoimeksi sen, mitä tieteellisyydellä tarkoitetaan. Avoimeksi jää myös tutkimuksen kohde. Kohteen määrittelyn täsmentäminen on mahdollista aloittaa toteamalla oikeustieteen selvittävän voimassa olevien oikeussääntöjen sisältöä. Oikeuden lisäksi oikeustieteen tutkimuskohteena ovat oikeudenmukaisuus ja oikeudet. Mutta ymmärtääkseen oikeudenmukaisuutta ja oikeuksia, tulee nähdä näiden taakse eli oikeuteen.

Oikeus on luonteensa vuoksi haastava käsite. *Aarnio* kuvaa sitä historiallisesti ja yhteiskunnallisesti määräytyneeksi pakkojärjestykseksi. Hänen mukaansa on kaksi tapaa nähdä oikeus. Ensinnäkin sitä on mahdollista pitää luonteeltaan valtajärjestyksenä, jolloin keskiössä on joko itse valta käsitteenä tai sitten oikeus vallan välikappaleena. Toiseksi oikeus on tulkittavissa normijärjestelmäksi. Tällöin keskeistä ovat säännöt ja niiden seuraaminen. Säännöt antavat kansalaisille ja viranomaisille käyttäytymismallin, jota noudatetaan tai rikotaan, mutta käyttäytyminen kvalifioidaan oikeudeksi juuri näiden sääntöjen avulla.[112]

Oikeutta ei kuitenkaan ole mahdollista nähdä vain jommalla kummalla tavalla. Se on harhaanjohtavaa, sillä tällainen näkemys yksipuolistaa oikeuden käsitteenä. Ymmärtääkseen oikeutta käsitteenä tulee huomioida oikeuden ja yhteiskuntatodellisuuden olevan keskenään

112 *Aarnio,* Laintulkinnan teoria s. 15. Vertaa *Tolonen* Oikeuslähdeoppi, jossa Tolonen kuvaa oikeutta toiminnaksi, joka on virallisesti ja formaalisti ohjattua. *Tolonen* Oikeuslähdeoppi s. 3. Katso myös *Pöyhönen,* Oikeus, s. 693, jossa hän kuvaa oikeutta sanomalla sen olevan ihmisyhteisöille ominainen, niiden yhteisöllisyyttä ilmaiseva ulottuvuus.

vuorovaikutussuhteessa. Tällöin päästään siihen, että oikeus ei ole vain valtajärjestys tai pelkkä sääntöjärjestelmä.

Oikeus on hyvin moniulotteinen ja monikerroksinen käsite. Onko oikeutta edes tarpeen ehdottomasti määritellä?[113] Oikeuteen on luonteensa vuoksi mahdollista muodostaa rajattomasti erilaisia näkökulmia, ja eri näkökulmista oikeus näyttäytyy erilaisina hahmoina.[114] Nämä erilaiset näkökulmat eivät ole toisiaan poissulkevia vaan täydentäviä. Ne auttavat hahmottamaan oikeutta käsitteenä ja valottavat oikeuden kokonaisuuden eri puolia. Kysymys on lopulta oikeuden ymmärtämisestä eli tiedollisesta suhteesta oikeuteen.

Oikeutta ei dynaamisen luonteensa vuoksi ole järkevää ehdottomasti määritellä, sillä oikeus on aina vuorovaikutuksessa yhteiskunnan kanssa. Liian jäykkä, ehdoton määritelmä supistaisi oikeuden mahdollisuutta selvitä ajan ja kehityksen mukana. Oikeuden täytyy antaa elää vapaana eikä liiaksi sitoa sitä tiettyyn aikaan ja paikkaan.[115]

Oikeuden määrittelemisen sijaan oleellista on keskittyä siihen ympäristöön, missä oikeus kohdataan. Tähän on syynä se, että oikeus on sidoksissa tilaan ja ympäristöön, jossa se kohdataan. Tila, oikeuden ja sen ohjaamien toimintojen ympäristö, on läsnä oikeuden ja koko inhimillisen olemisen ja ymmärryksen perusrakenteissa. Verkkoyhteiskunnassa tällaisena tilana toimivat tietoverkot ja informaatioteknologia,

113 Näin myös *Kangas,* Minun metodini, s.91.

114 Hannu Tolonen käyttää tästä termiä oikeuden kaleidoskooppi. *Tolonen,* Oikeuden kaleidoskooppi, s. 150–165. Vertaa *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 106–107, jossa hän puhuu oikeuden näkökulmasidonnaisuudesta.

115 Näin myös *Morawetz,* jonka mukaan oikeus on radikaalisti tulkinnanvarainen yhteiskunnallinen käytäntö, jonka episteeminen, käsitteellinen, konstitutiivinen ja metodinen identiteetti on vain heikosti jäsentynyt ja aina avoin uusille tulkinnoille. *Morawetz,* Epistemology of Judging, s. 19–23.

jolloin verkkoyhteiskunnan oikeudessa olennaista on ihmisen ja hänen asioidensa kohtaaminen tässä tilassa ja ympäristössä.[116] Kysymys on siis oikeustieteen peruskäsitteen sijoittamisesta uuteen digitaaliseen toimintaympäristöön[117] eli tietoverkoissa toimivaan digitaaliseen verkkoympäristöön.[118]

Tämä näkökulma on perusteltu myös siksi, että digitaalinen teknologia vaikuttaa myös kulttuuriimme. Se on aiheuttanut perustavaa laatua olevan muutoksen muun kulttuurin ohella myös oikeuskulttuuriin. Digitaalisesta teknologiasta on tullut koko modernin elämäntavan punainen lanka ja se vaikuttaa siksi monin tavoin myös oikeuskulttuurin sisältöön ja tulkintaan.

Teknologia sekä sitä koskevat käsitykset ja asenteet ovat osa oikeuden ja sen soveltajan elämän- ja elämysyhteyttä. Tämä elämänyhteys koostuu tilanteen tai ilmiön ymmärtämistä edistävistä tai rajoittavista sekä ymmärtämiseen pyrkivän subjektin ja ympäristön väliseen vuorovaikutukseen liittyvistä seikoista.[119]

Nyky-yhteiskunnassa teknologiaa ja sen sovelluksia pidetään itsestäänselvyyksinä. Kulttuurille onkin ominaista teknologisen imperatiivin mukainen ajatusmaailma: teknologian ajatellaan olevan ratkaisu

116 *Pöysti,* Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet, s. 38.

117 Digitaalinen toimintaympäristö voidaan suppeasti määritellä ympäristöksi, joka on sidoksissa tietotekniikkaan ja informaation käsittelemiseen. *Saarenpää,* Oikeusinformatiikka (2011), s. 419.

118 Outi Korhosen kehittämä oikeuden situaation teoria tarkastelee oikeuden sidonnaisuutta sen soveltajan ja sovellusten kohteiden tai osapuolten elämän- tai elämysyhteyteen sekä niistä aiheutuviin oikeuden mahdollisuuksiin ja rajoituksiin. Katso *Korhonen,* International Law Situated…

119 *Pöysti,* Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet s. 39

kaikkiin ongelmiin. Tämä on alkanut näkyä myös oikeuskulttuurissa, sillä yhä useammin lainsäädännössä viitataan johonkin tiettyyn teknologiaan yhteiskunnallisen tai oikedellisen ongelman ratkaisuna. Esimerkkinä toimii biometrisen tunnistamisen vahventuva lainsäädännöllinen asema yksilön tunnistamisessa käytettävänä ratkaisuna. Tällainen antaa myös enenevässä määrin mahdollisuuksia yksilöiden valvontaan.

Tämä osoittaa sen, että myös digitaalisessa oikeuskulttuurissa oikeus ja valta ovat monin tavoin kietoutuneet toisiinsa.[120] Modernin oikeuden positiivisuus avaa mahdollisuuden sen käyttämiselle yhteiskunnan tietoisen ja suunnitelmallisen ohjauksen välineenä. Lainsäädännön kautta yksilöt ohjataan toimimaan halutulla tavalla digitaalisessa toimintaympäristössä ja käyttämään tiettyjä teknologisia ratkaisuja. Tällöin modernin oikeuden positiivisuus myös asettaa uudella tavalla kysymykset oikeuden suhteesta yhtäältä moraaliin ja toisaalta sekä valtaan että vallankäyttöön.[121]

Digitaalisen ajan oikeuskulttuuria leimaavia ominaisuuksia ovat oikeuden irtoaminen kansallisvaltion kontekstista, oikeudellisten prosessien massamuotoisuus, oikeudellisten järjestelmien jopa globaali laajuus, niiden entistä herkempi haavoittuvaisuus, samanaikaisuus ja etäisyyden merkityksen vähentyminen.[122] Digitaalinen teknologia heijastuu tällöin sekä oikeuden sisältöön että prosesseihin. Digitaalisen aikakauden oikeuskulttuurin ymmärtämiseksi onkin aivan välttämätöntä tunnistaa niitä sosiaalisia ja kulttuurisia voimia, jotka ovat

120 Tuori erottaa kolme oikeuden ja vallan suhteen ulottuvuutta: 1) oikeusjärjestys itsessään on tietynlainen valtajärjestys, 2) valta toimii oikeuden perustana ja 3) oikeus toimii myös vallan rajoituksena. *Tuori,* Oikeus, valta ja demokratia, s. 114.

121 *Tuori,* Oikeus, valta ja demokratia, s. IX ja s. 3.

122 Digitaalisen kulttuurin ominaisuuksista katso *van Dijk,* The Network Society, s.210–233

olleet muokkaamassa nykyilmiöitä. Mitä vähemmän nykyistä tilannetta muokanneista tekijöistä tiedetään, sitä vaikeampaa on vastustaa valtarakenteita.

Digitaalinen kulttuuri määrittää ja hallitsee oikeuskulttuuria ja sen merkitys kasvaa entisestään. Yksilöön kiinteästi yhdistetty tieto, henkilörekisterit ja jopa biometriset tunnistetiedot ovat tallennettuna digitaaliseen muotoon. Uuden teknologian lupaukset kiinnostavat niin, ettei niihin kätkeytyvää valtaa ja kontrollia huomaa. Digitaalisen teknologian levittäytyminen kaikkialle ja lisääntyvä näkymättömyys saavat sen vaikuttamaan luonnolliselta.[123]

Digitaalisen kulttuurin heterogeenisen luonteen ymmärtäminen on entistä tärkeämpää, sillä sitä ylläpitävä teknologia työntyy yhä enemmän elämäämme ja samalla uhkaa muuttua näkymättömäksi. Esimerkiksi kurinpidon ja tarkkailun panopticon ei enää ole pelkästään tulevaisuuden kauhukuva, vaan oleellinen ja toteutunut osa arkipäivää. Digitaaliseen teknologiaan perustuvassa maailmassa yksilön anonyymi elämä on käytännössä lähes mahdotonta.

Aikakaudellemme on tyypillistä kaksi ominaisuutta. Ensimmäinen ominaisuus on teknologian suuri merkitys yhteiskunnassa. Samalla ominaista on oikeuksien voimakas korostaminen. Verkkoyhteiskunnan oikeusajatukselle tulee olla ominaista se, että asianmukaisella infrastruktuurien järjestämisellä on mahdollista optimoida yhtä aikaa yk-

123 Digitaalisen kulttuurin vallan ja kontrollin olemukseen voi Paasilehdon mukaan pyrkiä perehtymään ”digitaalisen kulttuurin arkeologialla”, jolloin paikannetaan niitä kulttuurisia alusrakenteita, jotka määrittävät digitaalista kulttuuria. Paasilehto, Digitaalinen kulttuuri – tulevaisuuden oikeuskulttuuri?, s. 333. Paasilehdon esittämä digitaalisen kulttuurin arkeologia pohjaa Michel Foucault’n aikanaan esittämään tiedon arkeologiaan. Tiedon arkeologiasta katso tarkemmin *Foucault,* The Archeology of Knowledge.

silön vapaudet ja oikeudet sekä yhteisön tavoitteet ja yhteisöllisyyden arvot ja hyveet.[124]

2.1.2. Informaatioyhteiskunnasta valvontayhteiskuntaan

Nyky-yhteiskunnassa informaatio on saanut keskeisen merkityksen. Informaatiota, tietojenkäsittelyä ja tietoliikennettä pidetään yhteiskunnan tärkeänä voimavarana. Tällä tavoin informaatio on muuntunut keskeiseksi tuotannontekijäksi ja hyödykkeeksi.[125] Informaatioteknologian kehityksestä seurannut yhteiskunnallinen muutos on siirtänyt meidät uudelle aikakaudelle, informaation aikakaudelle.

Informaation kasvava merkitys on johtanut siihen, että 1990-luvulta lähtien on lisääntyvässä määrin puhuttu yhteiskunnan muutoksesta kohti *tieto- tai informaatioyhteiskuntaa*.[126] Kiistämätöntä on, että

124 *Pöysti,* Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet, s. 40.

125 Katso tästä kehityksestä tarkemmin *Bell,* The Social Framework of the Information Society (1980) sekä *Webster,* Theories of Information Society (1995).

126 Käsitteitä tietoyhteiskunta ja informaatioyhteiskunta käytetään toistensa synonyymeina. Saarenpää huomauttaa kuitenkin siitä, että kysymys on Suomessa lähinnä käännös- ja ajatusvirheestä. Tietoyhteiskunnalla tarkoitetaan tämänpäiväisestä yhteiskunnasta paljon pidemmälle kehitettyä, informaation nykyistä älykkäämmälle käsittelylle rakennettua yhteiskuntaa. *Saarenpää,* Kansalaisen oikeudet tiedon valtatiellä, s.141. Katso myös *Korhonen,* Perusrekisterit ja tietosuoja, s. 14, *Niiniluoto,* Informaatio, tieto ja yhteiskunta, s. 67–72 ja 100, *Karvonen,* Elämmekö tieto- vai informaatioyhteiskunnassa?, s. 81–83 ja 107–108.

olemme jo jonkin aikaa eläneet informaatioyhteiskunnan aikaa.[127] Osoituksena tästä ovat informaatiomarkkinoiden ja tietotekniikan käytön huima kasvu sekä informaatioinfrastruktuurin monitasoiset muutokset. Informaatioyhteiskunnan tunnuspiirteinä ovat informaation strateginen merkitys, tietotekniikan runsas käyttö sekä riippuvuus tietotekniikasta ja informaation käsittelystä.[128]

Riippuvuus tietotekniikasta sekä informaatiosta ja sen käsittelystä eivät kuitenkaan vielä oikeuta puhumaan informaatioyhteiskunnasta. Ilmaisut tieto- ja informaatioyhteiskunta viittaavat ilmiöiden laskennallisen hallittavuuden teknisten ratkaisujen luomiin uusiin yhteiskunnallisiin rakenteisiin ja niiden vaikuttavuuteen ihmisen elämysmaailmassa. Tällä hallittavuudella ja sen teknisillä ratkaisuilla ei kuitenkaan ole mitään tekemistä tiedon eikä informaation kanssa. Tämän vuoksi tulisi ennemmin puhua teknologisesta yhteiskunnasta, joka on laskennallisen hallittavuuden varaan rakentunut arvovapaa materiajärjestelmä.[129]

Informaatioyhteiskuntanimitys ei liity pelkästään teknologian mukanaan tuomiin mahdollisuuksiin käsitellä informaatiota eikä riippuvuuteen informaatiosta ja sen käsittelystä. Syyt ovat syvemmällä yhteiskunnan rakenteissa. Informaation luonne on muuttanut tapamme elää. Informaatiosta on tullut niin merkittävä osa yhteiskuntaa, että se ohjaa käyttäytymistämme. Katsottaessa informaatioyhteiskuntaa vain teknologian näkökulmasta saadaan puutteellinen kuva informaation

---

127 Informaatioyhteiskunnan sanotaan kehittyneen 1970-luvulla siirryttäessä jälkiteollisesta yhteiskunnasta palveluyhteiskuntaan, jolloin myös tiedon ja informaation merkitys kasvoi tietotekniikan kehittyessä. *Bell,* The Coming of Postindustrial Society: a venture in social forecasting, s. 14. Katso myös *Lyon,* The Information Society, s. 2–4 sekä *van Dijk,* The Network Society, s. 43.

128 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s.295

129 *Juti,* Tiedon filosofia antiikista nykyaikaan, s. 422–423.

merkityksestä yhteiskunnassa. Teknologian näkökulman lisäksi tulee huomioida se, että informaatio on vaikuttanut yhteiskuntaan myös taloudellisesti, ammatillisesti, alueellisesti ja kulttuurisesti.[130] Näiden syiden vuoksi on aiheellista puhua informaatioyhteiskunnasta teknologisen yhteiskunnan sijaan. Teknologia on vain yksi osa informaatioyhteiskuntaa.

Informaatioyhteiskunta on oikeudellisesta näkökulmasta tarkasteltuna oikeudellinen informaatioyhteiskunta. Tällä tarkoitetaan yhteiskuntaa, missä tietotekniikan hyödyntämisen ja informaatioinfrastruktuurin sekä informaatiomarkkinoiden muutokset johtavat yhteiskunnan informaatio-oikeudelliseen oikeudellistumiseen, missä oikeudellinen viestintä muuttuu voittopuolisesti elektroniseksi viestinnäksi ja missä tietotekniikan sekä tietojärjestelmien käyttö johtavat päätetyöskentelyyn oikeudellisessa elämässä.[131]

Oikeudelliseen informaatioyhteiskuntaan siirtyminen on vaikuttanut keskeisesti ja muuttavasti työ- ja menettelytapoihin, oikeudellisiin tietovarastoihin, oikeus- ja informaatiolähteisiin, lainsäädäntöön, oikeussystematiikkaan, ihmiskäsityksiin sekä oikeutta koskevaan viestintään.[132] Oikeuden uudistumista ja selkeitä informaation, informaatioinfrastruktuurin ja informaatiomarkkinoiden pelisääntöjä tarvitaan tällöin yksityisten aseman ja oikeuksien suojaamiseksi, uusien, informaatiokeskeisten toimintavälineiden luomiseksi ja uudenlaisten ristiriitojen ratkaisemiseksi.[133]

---

130 Katso esimerkiksi *Webster,* Theories of the Information Society (2014).

131 *Saarenpää,* Verkkoyhteiskunnan oikeutta - johdatusta aiheeseen, s. 3

132 *Saarenpää,* Verkkoyhteiskunnan oikeutta - johdatusta aiheeseen, s. 3–4.

133 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 296–297.

Termi informaatioyhteiskunta ei kuitenkaan riittävästi kuvaa tämän päivän maailmaa. Yhteiskunta on muuttunut rakenteellisesti siten, että toimintaympäristö on saanut yleisen informaatioinfrastruktuurin.[134] Yhteiskunnan toiminnot ja asiointi ovat siirtyneet tietoverkkoihin.

Seuraava askel yhteiskunnan kehityksessä onkin ollut *verkkoyhteiskunta*. Erilaisten tietoverkkojen käyttö on tullut kiinteäksi osaksi viestintää ja tiedonkäsittelyä. Tietotekniikka on tullut osaksi arkipäivää. Informaatioyhteiskunnan ja verkkoyhteiskunnan välinen ero on kuvattavissa sanomalla informaatioyhteiskuntaa staattiseksi yhteiskunnaksi, kun verkkoyhteiskunta puolestaan on dynaaminen ja entistä interaktiivisempi yhteiskunta. [135]

Verkkoyhteiskunnalla tarkoitetaan yhteiskuntaa, jonka merkittävät toiminnot ja prosessit ovat järjestäytyneet erilaisten toisiinsa liittyneiden verkkojen muotoon.[136] Sille ominaisia piirteitä ovat tietotekniikkasidonnaisuus ja digitaalisten tietovarantojen sekä informaation muodossa olevien hyödykkeiden lisääntyvä käyttö julkisen ja yksityisen toiminnan perusvoimavarana ja -tuotteena.[137] Tyypillistä verkkoyhteiskunnalle on myös konvergenssi eli median, teknologian ja taloudellisen toiminnan muotojen lähentyminen ja sulautuminen yhdeksi,

---

134 Infrastruktuurilla tarkoitetaan yleisesti sitä järjestelmää, jonka varaan yhteiskunnallisesti merkittävät toiminnot, palvelut ja väylästöt rakentuvat. Näin ollen verkkoyhteiskunnassa tulee ensisijaisesti kiinnittää huomiota infrastruktuuriin. *Saarenpää,* Kansalaisen oikeudet tiedon valtatiellä, s. 142.

135 *Saarenpää,* Information Government and Legal Information, s. 182 ja *van Dijk,* The Network Society, s. 45-46.

136 *van Dijk,* The Network Society, s. 24. Katso myös *Saarenpää,* Oikeudellinen informaatioyhteiskunta, s. 554–562.

137 Havainnollisena esimerkkinä kansalaisten verkkosidonnaisuudesta voidaan pitää korkeimman hallinto-oikeuden ennakkoratkaisua KHO 2006:18, jossa oli kysymys julkisin varoin vammaiselle han-

avointen tietoverkkojen ja matkaviestimien avulla käytettäväksi kokonaisuudeksi.[138]

Verkkoyhteiskunnan lisäksi on mahdollista puhua *oikeudellisesta verkkoyhteiskunnasta.*[139] Yhteiskunta on nopeasti oikeudellistumassa uudenlaisesti.[140] Infrastruktuurin oikeudellistuminen näkyy lainsäädännön nopeassa kehittämisessä ja oikeudellisen elämän viestintätapojen muutoksessa. Oikeudellista informaatiota – ja informaatiota ylipäätään – käytetään uusissa muodoissaan, eikä nykypäivänä juristit voi enää välttyä verkkoyhteiskunnan uudistuksiin tutustumiselta ja niiden hyödyntämisestä työssään.[141]

---

kittavista tietokoneen käytön mahdollistavista apuohjelmista. Katso myös korkeimman hallinto-oikeuden 12.4.2006 antama ratkaisu (876/2006).

138 *Pöysti,* Julkisen vallan velvollisuus edistää… s. 92–93 ja *Saarenpää,* Verkoissa, verkoista… s. 210–214. Saarenpää huomauttaa, että teknologista konvergenssia seuraa oikeudellinen konvergenssi, joka näkyy monin tavoin lainsäädännön uudistuksissa ja uudessa lainsäädännössä. *Saarenpää,* Kansalaisen oikeudet tiedon valtatiellä, s. 146.

139 Oikeudellisen verkkoyhteiskunnan käsitteestä katso esimerkiksi *Saarenpää,* Oikeusinformatiikka (2008), s. 8.

140 Yhteiskunnan oikeudellistumisella tarkoitetaan oikeudellisen sääntelyn ja sen merkityksen vahvistumista yhteiskunnassa. Se voi ilmetä 1) säännösten määrän kasvuna, 2) oikeudellisen sääntelyn kohteena olevien asioiden lisääntymisenä ja 3) oikeudellisten ratkaisuperusteiden voimistumisena ristiriita- ja ongelmatilanteissa. *Tarasti,* Yhteiskunnan oikeudellistuminen, s. 575. Vertaa *van Aerschot* Oikeudellistuminen julkishallinnossa, s. 1036–1037. Verkkoyhteiskunnan ja oikeusvaltion suhteesta katso *Saarenpää,* Oikeusvaltio ja verkkoyhteiskunta sekä Saarenpää Kansalaisen oikeudet tiedon valtatiellä, s. 146.

141 *Saarenpää,* Verkkoyhteiskunnan oikeutta... s. 5–6 ja *Saarenpää,* Verkoissa, verkoista, verkkoon, s. 214–218.

Jatkuvat yhteiskunnalliset muutokset ovat tuoneet mukanaan myös uuden tavan tarkastella yhteiskuntaa. Verkkoyhteiskunnan ohella – tai sijasta – on mahdollista puhua *valvontayhteiskunnasta*. Halukkuus lisätä tietotekniikan ja tietoverkkojen käyttöä erilaisiin ohjaus- ja valvontatarkoituksiin on muuntamassa verkkoyhteiskuntaa enenevässä määrin valvontayhteiskunnaksi. [142]

WTC:n terrori-iskua on omalta osaltaan mahdollista pitää tämän yhteiskunnallisen kehityksen vauhdittajana. Kyseisen terrori-iskun jälkeen valvonnan, tiedonhallinnan, tiedonhaun ja älykkäiden teknologioiden yhdistely ja kehittäminen alkoivat saada uutta vauhtia. Sovellukset valvonnan tarpeisiin lisääntyivät. Tiedonhallinnan ja valvonnan intressit ja teknologiat kietoutuivat uudessa vaiheessa nopeasti yhteen. Viimeistään tämän jälkeen valvonnasta ja tiedonkeruusta, etenkin julkishallinnon tarpeisiin, tuli tuottava ja kasvava liiketoiminnan alue.

WTC:n terrori-iskut toivat esiin valvontateknologioita, jotka olivat kehittyneet pikkuhiljaa ilman suurempaa huomiota. Iskut merkitsivät lisäksi mahdollisuutta kehittää täysin uusia teknologioita ja politiikkoja valvontaa varten. Esimerkkinä tällaisesta toimii kameravalvonta ja biometrinen tunnistaminen, joiden kehitys ja käyttö ovat lisääntyneet näiden iskujen jälkeen. [143]

Uuden teknologian ja infrastruktuurin keskeisiä ominaisuuksia ovat mahdollisuudet valvoa ihmisiä, heidän ominaisuuksiaan sekä toimintojaan samoin kuin yhteisöjen toimintoja. Tämän on mahdollistanut tekninen lähentyminen eli konvergenssi, joka erilaisten toimintojen yhdentäjänä tarjoaa tekniset valmiudet myös tietoverkkojen valvontakäyttöön.

Uuden läsnä-älyn eri sovellukset lisäävät myös mahdollisuuksia valvontaan langattomia verkkoja hyödyntäen. Uusi teknologia ja uusi

142 *Saarenpää,* Oikeusinformatiikka (2011), s. 420–421.

143 *Lyon,* Surveillance after September 11, s. 4–5.

infrastruktuuri sekä luovat houkutuksia että tosiasiallisesti käytettyinä ja säänneltyinä voivat viedä ja ovat jo vieneet kehitystä vähin erin avoimesta yhteiskunnasta valvonnan yhteiskuntaan. Valvonnan lisääminen on usean vuoden ajan ollut näkyvä erilaisia julkisen sektorin tietoteknisiä kehittämishankkeita yhdistävä tunnusmerkki.

2000-luvulla kehitys on kulkenut kohti valvontayhteiskuntaa. [144] Ihmiset ovat perustellusti huolissaan valvonnan lisääntymisestä, koska seurauksena on yksityisyyden vaarantuminen. Huolta aiheuttaa sekä yksityinen että julkinenkin valvonta, sillä niiden vaikutukset ulottuvat ihmisten jokapäiväiseen elämään.[145]

Tietoverkot tarjoavat väylän tietovarastojen ja näihin sisältyvien tietojen käytölle valvontaan.[146] Verkot myös ovat valvonnan kannalta

144 Valvontayhteiskunnan kehittymistä pohjusti Vance Packard vuonna 1964 julkaistussa teoksessaan The Naked Society. Valvonayhteiskunta (engl. surveillance society) käsitteenä juontaa juurensa sosiologi Gary T. Marxin ajatuksiin 1980-luvun puoliväliin. Katso tarkemmin *Marx,* The Surveillance Society: the threat of 1984-style techniques (Futurist-lehti vuodelta1985). Katso myös *Gandy,* The Surveillance Society: Information Technology and Bureaucratic Social Control. Journal of Communication Vol 39, No.3. 1989. s. 61–76

145 Valvonta on nykyään niin monelle taholle eriytynyt toiminto, että sen määrittely on hankalaa. Perinteisesti valvonnalla on ymmärretty julkisen vallan turvallisuuden ja järjestyksen sekä laillisuuden varmistamiseen tähtäävää toimintaa. Laajassa merkityksessä valvontaan kuuluu myös poikkeavien käytösten määrittely. Heinonen ja Hannula huomauttavat siitä, että valvonta on ihmisen seurantaa erityistä tarkoitusta varten. Tämä tarkoittaa sitä, että pelkkä päämäärätön havainnointi ei ole valvontaa. *Heinonen – Hannula,* Valvonta tietoyhteiskunnassa, s. 10.

146 Tietovarantojen, rekistereiden ja tietojärjestelmien sisältämien tietojen käsittelyyn liittyy monenlaisia ja monitahoisia, ongelmallisia kysymyksiä. Voidaan esimerkiksi kysyä, miten näiden tietojen käsit-

tärkeä tekijä, tehokkaan valvonnan edellytys ja valvontaa kiihdyttävä tekijä. Tietoverkot ja rekisterit mahdollistavat kansalaisten silmällä pidon ja tekemisten kirjaamisen.[147]

Tiedon hallitseminen on demokratian toteutumisen kannalta keskeinen asia. Tieto on se, joka ohjaa yksilöiden päätöksentekoa. Tiedolla on kuitenkin varjopuolensa. Se ohjaa yhteiskunnallisen vallan käyttöä. Uuden tietojenkäsittelyn aika on kiistatta lisännyt yhteiskunnan julkisten ja yksityisten valtarakenteiden ja turvallisuusjärjestelmien tarkkailumahdollisuuksia. Samanaikaisesti se on vähentänyt kansalaisten tosiasiallista tiedollista itsemääräämisoikeutta.

Oikeus tietoon on valvonnan tautalla oleva yhteikunnallinen perusperiaate.[148] Uteliaan luonteensa vuoksi ihmisellä on aito tarve tietää ja käyttää tietoa.[149] Oikeudessa tietoon on erotettavissa kaksi tärkeää näkökulmaa: oikeus jakaa tietoa rajoituksetta sekä oikeus ottaa tietoa vastaan avoimesti ja ilman rajoituksia. Nämä kaksi näkökulmaa ovat vastavuoroisia ja ne vaikuttavat toisiinsa (yhden toteutuminen edellyt-

---

tely säännellään ja kuinka sitä valvotaan? *Korhonen,* Perusrekisterit ja tietosuoja, s. 21

147 Pelkästään se, että yhteiskunnalle on määritetty perusrekisterit, kuvastaa valvonnan mahdollisuuksien lisääntymistä. Perusrekistereistä tarkemmin katso Korhonen Perusrekisterit ja tietosuoja sekä Karimaa Perusrekisterit.

148 Oikeus tietoon on käsitteenä kuitenkin paljon monitahoisempi. Korhosen mukaan se voidaan ymmärtää laajemmasta ja suppeasta näkökulmasta. *Korhonen,* Perusrekisterit ja tietosuoja, s. 16–17.

149 Oikeudessa tietoon on pohjimmiltaan kysymys yksilön itsemääräämisoikeuden yhdestä ulottuvuudesta: tiedollisesta itsemääräämisoikeudesta. On vakiintuneesti katsottu, että yksilön on mahdotonta käyttää itsemääräämisoikeuttaan ilman oikeutta tietoon, niin itseään kuin yhteiskuntaa koskevaan tietoon.

tää myös toisen toteutumista): jos tiedonkulku ei ole vapaata, yhteiskunta ei voi taata oikeutta tietoon.

Modernissa valtiossa pääsy tietoon ja valta liittyvät kiinteästi toisiinsa. Tätä kytköstä on vauhdittanut ja vahvistanut nimenomaan tietojenkäsittelyn kehittyminen. Puhutaan uudesta panoptisesta valvonnasta, joka yhdistää tietoteknologian ja ennen kaikkea tietoverkkojen avulla tietoa ja valtaa. Tällaisen uuden valvonnan kautta ihmistä arvioidaan ja luokitellaan yhä enemmän heidän tietoimagonsa, digitaalisen persoonansa eli heistä rekistereihin talletettujen tietojen ja heidän jättämien sähköisten jälkien perusteella. [150]

Digitaalisen persoonan käsite on tärkeä nykymuotoisen valvonnan prosessin ymmärtämiseksi, sillä valvova organisaatio rakentaa käytettävissään olevan tiedon avulla valvottavasta yksilöstä mallin, jota pidetään tarkkana kuvana yksilöstä. Keräämänsä tiedon perusteella organisaatio rakentaa yksilöstä digitaalisen vastineen, joka voi olla kaukana täydellisestä tai edes oikeasta, mutta jota pidetään riittävänä. Tiedon tulee kuitenkin olla liitettävissä tiettyyn yksilöön ja oltava jossain ymmärrettävässä suhteessa tähän yksilöön ollakseen hyödyllistä valvonnan kannalta. Teknologia on antanut tietämisen vallan niiden käsiin, jotka kontrolloivat teknologiaa ja sen takana olevaa tietoa.[151]

---

150 Daniel Solove puhuu digitaalisesta persoonasta tai digitaalisesti henkilöstä. Tämän digitaalisen persoonan hän katsoo muodostuvan kaikesta yksilöön liittyvästä digitaalisesta datasta ja informaatiosta tallennuspaikasta riippumatta. *Solove,* Digital Person. Technology and Privacy in the Information Age, s. 1. Katso myös *Heinonen,* Digitaalinen minä, s. 13 ja 253. Verkkoyhteiskunnan identiteettikäsityksistä katso tarkemmin tutkimuksen jakso 4.5.1.

151 *Heinonen,* Digitaalinen minä, s. 112. Tärkeää kuitenkin on huomata, että oikeudella tietoon on oltava kohde. Tässä tapauksessa kohde on tieto tai informaatio. Laajemmin kysymys on tietoyksiköistä,

Biometristen tunnisteiden lisääntyvä käyttö edesauttaa yksilöiden tarkkailua ja valvontaa. Biometristen tunnisteiden käyttö esimerkiksi osana sähköistä identiteettiä mahdollistaa yksilön tehokkaan tarkkailun sähköisen identiteetin käytöstä jäävien yksilöllisten digitaalisten jalanjälkien kautta. Biometrisen tunnistamisen avulla yksilöä on mahdollista seurata hänen tietämättään.

Valvontayhteiskunnan kehittyminen tulee nähdä informaatioyhteiskunnan sivutuotteena. Nykyajan valvonta käyttää hyväksi informaatioyhteiskunnan mukanaan tuomia digitaalisia infrastruktuureja.[152] Valvontayhteiskunta on kuvattavissa yhteiskunnaksi, jonka toiminta perustuu osittain yksilöitä koskevan information laajamittaiseen keräämiseen, tallettamiseen, analysointiin ja käyttämiseen.[153] Siihen liittyy kuitenkin myös harhakäsityksiä. Yleisenä käsityksenä valvontayhteiskunnasta on niin sanottu ”Iso Veli valvoo”-yhteiskunta, jossa jokin yksittäinen taho on valvonnan takana. Totuus on kuitenkin, että yhteiskunta valvoo hyvin monenlaisin tavoin kansalaisiaan. Valvontaa harjoittavat myös monet eri tahot. Ratkaisevaa valvonnan kehittyessä on kuitenkin se, mitä valvonnan välineet ja käytännöt mahdollistavat, ei niinkään pelkästään toteutunut valvonta.

Kehittyneissä yhteiskunnissa on viimeisen kolmenkymmenen vuoden aikana tapahtunut merkittävä muutos valvontamahdollisuuksien tehostumisessa. Tietoteknologian aikaansaaman vallankumouksen ohella on alettu puhua valvonnan vallankumouksesta. Suomi on tässä yksi maailman edelläkävijöistä. Ensinnäkin rekistereitä on lisätty

---

joita ovat tietokannat, -pankit, -varastot, -varannot, -järjestelmät ja rekisterit, joihin tietoa ja informaatiota tallennetaan, varastoidaan ja rekisteröidään.

152 *Lyon,* Surveillance, Power, and Everyday Life, s. 452–453.

153 Surveillance Studies Network, An introduction to the surveillance society. Artikkeli saatavilla osoitteessa: http://www.surveillance-studies.net/?page_id=119.

perustamalla kerättäviä tietoja varten uusia rekistereitä. Biometristen tunnisteiden kohdalla tämä näkyy esimerkiksi passirekisterin perustamisella passilain yhteydessä. Toiseksi valvontamahdollisuuksia ovat tehostaneet tietojen käyttötarkoitusten ja -tapojen laajentuminen ja monipuolistuminen, mistä biometrinen tunnistaminen on yksi esimerkki. Biometrisen tunnistamisen teknologiaa ei käytetä enää pelkästään yksilöiden tunnistamiseen, vaan myös yhä enemmän yksilöiden valvontaan ja tarkkailuun. Lisäksi viime vuosikymmenien aikana verkottuminen on lisääntynyt ja tietovarastojen muokkaus- ja analysointivälineet ovat kehittyneet.[154] Suomalaista yhteiskuntaa on jo perusteltua kutsua valvontayhteiskunnaksi, kun otetaan huomioon rekistereissä olevat tiedot, teknologian tuomat mahdollisuudet tietojen käyttämiselle valvontaan, rekisteröinnin vaikutus ihmisten elämään ja yhteiskunnan poliittinen tahto valvoa.[155]

Yhteiskunnallisen kehityksen lisäksi on huomioitava myös toimintaympäristössä tapahtunut muutos. Fyysinen toimintaympäristö on saanut rinnalleen uuden digitaalisen toimintaympäristön. Tässä uudessa toimintaympäristössä perus- ja ihmisoikeudet ovat helpommin lou-

154 *Heinonen,* Arjen tietoyhteiskunnassa ei ole yksityisyyttä, s. 173.

155 Heinonen ja Hannula huomauttivat tästä muutoksesta jo vuonna 1999 julkaistussa teoksessa Valvonta tietoyhteiskunnassa. Heidän mukaansa jo valvonnan määrällisten muutosten laajuus oikeuttaa puhumaan uudesta valvonnasta tai valvontayhteiskunnasta. Katso tarkemmin Heinonen – Hannula Valvonta tietoyhteiskunnassa, s. 20. Katso myös *Lyon,* Surveillance, Power, and Everyday Life, s. 449–450, jossa Lyon toteaa: "systematic surveillance became a routine and inescapable part of everyday life in modern times and is now, more often than not, dependent on information and communication technologies (ICTs). Indeed, it now makes some sense to talk of 'surveillance societies,' so pervasive is organizational monitoring of many kinds."

kattavissa, ehkä jopa unohdettavissa. Näin ei kuitenkaan saisi tapahtua, sillä kysymys on vanhojen oikeusnormien tulkinnasta uudessa ympäristössä. Digitaalisessa toimintaympäristössä perus- ja ihmisoikeudet saavat korostuneen merkityksen juuri niiden helpon loukkaamisen ja haavoittuvan luonteen vuoksi. Toimintaympäristön muutos on myös osaltaan vaikuttanut valvonnan ja sen mahdollisuuksien lisäämiseen yhteiskunnassa.

Oma osansa valvontayhteiskuntakehitykseen on ollut myös oikeudellistumisella, sillä sen kautta verkkoyhteiskunta on muuttumassa toisaalta ylisääntelyn ja toisaalta lisääntyvän valvonnan yhteiskunnaksi. Pelkästään säännösmäärän ja sekavan lainsäädäntötekniikan perusteella on nyky-yhteiskunta kuvattavissa keinotekoiseksi.[156] Tämä yhteiskunta on samalla myös enenevässä määrin valvonnan ja erilaisten valvontojen yhteiskunta.

Oikeudellistumisen vuoksi valvontayhteiskunnan rinnalla on mahdollista puhua oikeudellistuvasta valvontayhteiskunnasta. Viime vuosina valvonta, valvonnan mahdollisuudet sekä valvonnan riskit ovat lisääntyneet niin lakisääteisesti kuin tosiasiallisestikin. Lakisääteisiä vapausoikeuksien nimenomaisia rajoituksia kontrollin tehostamiseksi edustavat esimerkiksi telekuuntelua ja pankkitietojen luovuttamista koskevat säädökset sekä erityissäännökset sosiaaliviranomaisen oikeudesta saada salassapitosäännösten estämättä eri tahoilta asiakassuhteen kannalta välttämättömiä tietoja. Havainnollisen esimerkin uusista mahdollisuuksista valvonnalle tarjoaa myös biometristen ominaisuuksien käyttö ihmisen tunnistamisessa, jonka passilaki ja ulkomaalaislaki mahdollistavat.[157]

---

156 *Saarenpää,* Oikeusinformatiikka (2011), s. 441 ja Henkilö- ja persoonallisuusoikeus (2011), s. 232.

157 On myös huomattava, että poliisin taholta on jo esitetty kattavan DNA-rekisterin kokoamista kaikista kansalaisista. Katso YLEn uutinen: KRP esittää kansallista DNA-rekisteriä. Löytyy osoitteesta

Teknologian nopea kehitys yhdessä hallinnollisten ja kaupallisten strategioiden kanssa ovat saaneet aikaan uusien valvontamahdollisuuksien nopean lisääntymisen. Tämän seurauksena valvonnan lisääntymistä on vaikea seurata, jäsentämisestä ja sääntelemisestä puhumattakaan. Uuden oikeudellistuvan valvontayhteiskunnan suurimpana haasteena on se, miten tätä lisääntyvää valvontaa tulisi säädellä.[158]

2.1.3. Oikeusvaltiokehityksestä

Perustuslaki mainitsee oikeusvaltioperiaatteet sekä ihmisarvon loukkaamattomuuden, yksilön vapauden ja oikeudet sekä oikeudenmukaisuuden valtiojärjestyksemme perusteina. Käsitteenä oikeusvaltio on kuitenkin vaikeammin ymmärrettävissä. Yleinen käsitys oikeusvaltiosta ei kuitenkaan vastaa sen todellista olemusta. Käsitteenä oikeusvaltio on enemmän kuin vain julkisen vallan lainalaisuus.

Oikeusvaltiossa valtiovallan käyttö tapahtuu oikeusjärjestyksen mukaisesti. Yksilöllä on valtioltakin suojattu oikeuspiiri, jonka perustuslaissa vahvistetut yksilön perusoikeudet turvaavat. Tämän lisäksi yksilöllä on riittävää ja todellista oikeussuojaa sen varalta, että hänen oikeuksiinsa puututaan. Virkakoneiston tulee muodollisesti ja asiallisesti olla lakiin sidottu.[159] Oikeuvaltion ajankohtaisuutta korostaa huoli turvallisuudesta ja tulevaisuudesta, ja sen merkitys kestävän kehityksen ja hyvinvoinnin perustana ymmärretään taas paremmin.

Tuori määrittelee oikeusvaltion oikeudellisesta näkökulmasta seuraavasti: oikeusvaltio on valtio, jossa oikeuden itserajoitus toimii, jossa oikeudelliset käytännöt välittävät pinnanalaisten kerrostumien pintatason tapahtumiin nähden harjoittamaa normatiivista sensuuria.[160]

---

http://yle.fi/uutiset/krp_esittaa_kansallista_dna-rekisteria/5222321

158 Näin myös *Lyon,* Surveillance, Power, and Everyday Life, s. 450.

159 KM 1974:27, s. 9.

160 *Tuori,* Kriitinen oikeuspositivismi, s. 256.

Saarenpää puolestaan luonnehtii oikeusvaltiota valtioksi, jossa oikeuskulttuuri pyrkii edistämään kansalaisten ja yhteisöjen oikeuksien optimaalista määräytymistä, tuntemusta ja toteutumista.[161]

Oikeusvaltio voidaan ymmärtää monella tavalla. Sitä koskevat teoriat on perinteisesti jaettu kahteen: materiaaliseen ja muodolliseen. Materiaalisen oikeusvaltioajattelun lähtökohdaksi on ymmärrettävissä se, että valtio saa toteuttaa tarkoituksiaan vain oikeuden rajoissa ja sen välinein. Näin ollen oikeuden periaate rajoittaa valtion suvereniteettia. Oikeuden ja valtion välisissä suhteissa oikeus on valtion yläpuolella.[162]

Muodollisessa oikeusvaltioteoriassa valtion ja oikeuden käsitteitä tulkitaan toisin kuin materiaalisessa teoriassa, samoin kuin valtion ja oikeuden keskinäissuhdettakin. Muodollisessa oikeusvaltioajattelussa valtio on yksityisoikeuden subjekteihin rinnastettava tahtoyhteisö, ja suvereeni valtiovalta kuuluu tälle tahtoyhteisölle. Oikeus puolestaan nähdään vain positiivisena, valtiosäännön määräämässä järjestyksessä asetettuna oikeutena. Sitä ei enää voida asettaa valtion yläpuolelle, vaan valtio määrää oikeutta.[163]

Muodollisen oikeusvaltiokäsitteen mukaan valtiolla on lupa käyttää valtaansa vain oikeudellisesti määritellyn toimivallan nojalla ja kansalaisten oikeuksia kunnioittaen. Kansalaisten oikeuksista erityisesti perusoikeudet on otettava huomioon. Julkisen vallankäytön takeina on siten kaksi toisiaan täydentävää tekijää: 1) perusoikeudet ja 2) hallinnon lainalaisuus. Kansalaisilla on muodollisen oikeusvaltioajattelun mukaan perusoikeuksien turvaama vapauspiiri, johon viranomaisilla on lupa puuttua vain lain antaman valtuutuksen nojalla.[164]

---

161 *Saarenpää,* Oikeusvaltio ja verkkoyhteiskunta, s. 113.

162 *Tuori,* Oikeusvaltio, s. 933.

163 *Tuori,* Oikeusvaltio, s. 934.

164 *Tuori,* Oikeus, valta ja demokratia, s. 114–115.

Muodollinen oikeusvaltio on mahdollista nähdä prosessipainotteisena oikeusvaltiona, joka jättää huomiotta kansalaisen oikeuksien ydinalueen. Tällä ydinalueella tarkoitetaan materiaalista oikeutta perusoikeuksista lakisääteisiin ja lailla sääntelemättömiin oikeuksiin. Suhteessa materiaaliseen oikeusvaltiokäsitykseen muodollinen oikeusvaltiokäsitys muodostaa ikään kuin kehykset.[165] Materiaalinen oikeusvaltiokäsitys tuo tähän omana lisänä oikeuksien tehokkuuden sekä lain yleisten periaatteiden ja perustavanlaatuisten oikeuksien optimaalisen toteutumisen.[166]

Oppihistoriallisesti oikeusvaltion käsite on korostuneesti saksalainen[167], jonka sisällöstä on esitetty monia eri tulkintoja. Näitä kaikkia kuitenkin yhdistää kaksi teemaa: 1) vaatimus valtion puuttumisilta suojatusta yksityisautonomian alueesta ja 2) vaatimus valtion toiminnan sitomisesta oikeuteen.[168]

Vaatimus valtion toiminnan sitomisesta oikeuteen on oikeusvaltion ydin. Se juontaa juurensa jo antiikin Kreikasta. Nykyisen muotonsa se sai osin Montesquieun hahmottelemassa valtiovallan kolmijako-opis-

165 *Saarenpää,* Oikeusvaltio ja verkkoyhteiskunta, s. 112–113.

166 *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 29.

167 Vaikka oikeusvaltiokäsite on saksalaisen oikeuskulttuurin tuote, sillä on vastineensa myös muissa oikeuskulttuureissa. Angloamerikkalaisessa oikeuskulttuurissa vastaava käsite on rule of law –periaate ja ranskalaisessa traditiossa voidaan viitata legaliteettiperiaatteeseen (principe de legalité). Nämä periaatteet kuvastavat Tuorin mukaan sitä modernien länsimaisten demokratioiden oikeusajatteluun kuuluva käsitystä, että oikeus sitoo ja rajoittaa yksityisten subjektien ohella myös valtioelinten toimintaa. *Tuori,* Oikeus, valta ja demokratia, s. 115.

168 *Tuori,* Oikeusvaltio, s. 932.

sa ja saksalaisessa Rechtsstaat-ajattelussa.[169] Montesquieu teki valtiotyyppijaon tasavaltaan, monarkiaan ja despotiaan jaotteluperusteenaan laillisuusperiaatteen noudattamisen taso. Laillisuusperiaatteen lisäksi Ranskan vallankumous nosti esiin ajatuksen lain merkityksestä yhdenvertaisuuden toteuttajana.[170]

Nykyinen ajatus oikeusvaltiosta on peräisin valistusajalta.[171] Sen eräs ensimmäinen teoreettinen perustelu on löydettävissä John Locken Second Treatise –teoksesta. Käytäntöön sitä ryhdyttiin soveltamaan vasta 1800-luvulla.[172] Keskeinen ajatus oli valtionpäämiehen toiminnan sitominen lakiin.

Euroopan ihmisoikeussopimus vuodelta 1950 ja Euroopan unioinin perusoikeuskirja 2000-luvulla ovat osana eurooppalaista oikeusvaltion käsitteen kehitystä. Huomionarvoinen on myös Lissabonin sopimus, sillä siinä oikeusvaltio määriteltiin Euroopan kulttuurisesta, uskonnollisesta ja humanistisesta perinteestä kehittyneeksi yleismaail-

169 *Aarnio,* Oikeusvaltio – tuomarivaltio, s. 1. Montesquieu kehitteli kolmijako-oppinsa teoksessaan ”Lakien henki” (1748). Työnsä pohjana hän käytti Englannissa 1600-luvun loppupuolella käytössä ollutta poliittista järjestelmää. Montesquieusta katso myös *Jyränki,* Montesquieu: miksi lakeja ja mitä lakien takana, s. 153–168.

170 *Jyränki,* Oikeusvaltio ja demokratia, s. 18–19.

171 Vertaa *Jyränki,* Oikeusvaltio ja demokratia. Jyrängin mukaan oikeusvaltion idea syntyi uudella ajalla, jolloin oikeusvaltio nähtiin reaktiona mielivaltaiseen ja ennalta ennustamattomaan hallintoon ja lainkäyttöön, joka uhkasi ihmisten henkeä ja henkilökohtaista koskemattomuutta sekä haittasi tavaroiden vaihdantaa ja muuta liiketoimintaa.. Tavoitteena oli turvallisuus ja ennustettavuus.

172 *Tolonen,* Oikeusvaltio ja oikeustiede, s. 29.

malliseksi arvoksi, joka toimii myös Euroopan unionin perustana olevana arvona.[173]

Nykyään oikeusvaltiokehityksessä on nähtävissä ihmiskäsityksen muutos, joka korostaa itsemääräämisoikeuden merkitystä. Tämä kehitys on ollut seurausta erityisesti kansainvälisiin ihmisoikeussopimuksiin liittymisestä, Euroopan unionin jäsenyydestä ja unionin kehityksestä sekä Suomen perusoikeusjärjestelmän ja perustuslain uudistamisesta. Itsemääräämisoikeuden korostuminen käy erityisen hyvin ilmi Euroopan unionin perusoikeuskirjasta, jonka johdanto-osassa ajatus ihmisen itsemääräämisoikeudesta on sisällytetty demokraattiseen oikeusvaltioon. Perusoikeuskirjan mukaan siinä mainittuihin oikeuksiin ei ole lupa puuttua muutoin kuin lakitasoisella sääntelyllä, joka täyttää suhteellisuusperiaatteen vaatimukset.

Euroopan unionissa on muutoinkin tuettu eurooppalaisen yhteiskunnan kehittymistä, joka perustuu perusoikeuksien ja unionin kansalaisuudesta johtuvien oikeuksien kunnioittamiselle. Tärkeä osa tätä ajatusta on kansalaisten mahdollisuus omalta osaltaan vaikuttaa tähän kehitykseen niin yksilöinä kuin esimerkiksi erilaisten järjestöjen ja muiden toimijoiden kautta.[174]

Nykyistä oikeusvaltiota on edellä mainittujen syiden vuoksi mahdollista kuvata demokraattiseksi oikeusvaltioksi. Siinä erilaiset po-

---

173 Katso Lissabonin sopimus 2007/C 306/01, s. 10–11. Muina unionin perustana olevina arvoina pidetään ihmisarvon kunnioittamista, vapautta, kansanvaltaa, tasa-arvoa ja ihmisoikeuksien kunnioittamista. Myös vähemmistöihin kuuluvien oikeudet huomioidaan unionin perustana olevien arvojen joukkoon. Barroso, Human Rights: A Thread of Light Through Europe´s History, s. 8.

174 Katso Neuvoston päätös, tehty 19 päivänä huhtikuuta 2007, perusoikeuksia ja kansalaisuutta koskevan erityisohjelman perustamisesta vuosiksi 2007–2013 osana perusoikeuksien ja oikeusasioiden yleisohjelmaa (2007/252/YOS).

liittiset oikeudet yhdistyvät yksilön muihin oikeuksiin. Yksilöllä on mahdollisuus osallistua oikeuksiensa toteuttamiseen ja toisaalta myös vaatia niiden toteuttamista. Oikeusvaltioperiaatteessa ei näin ollen ole kysymys vain yksilön suojaamisesta julkista valtaa ja toisia yksilöitä vastaan, vaan myös yhteisön demokraattisen legitimaatiorakenteen suojaamisesta.[175]

Erityisesti henkilötietojen suojan kohdalla sääntelyssä on havaittavissa se, että oikeusvaltio ei nykyisellään tarkoita vain kansalaisen ja valtion suhteen määrittelemistä. Pikemminkin kysymys on yksilön lähtökohtaisesta oikeudesta määrätä itsestään, elämästään ja myös itseään koskevasta informaatiosta. Saarenpää onkin osuvasti sanonut, ettei kysymys ole enää yksilön oikeuksien rajoittamisesta julkisen vallan avulla vaan siitä, että yksilön oikeudet rajoittavat viranomaisen oikeuksia.[176]

Perusoikeuksien merkityksen voimistuminen korostaa omalta osaltaan yksilön itsemääräämisoikeutta. Tämän vuoksi onkin perusteltua puhua ihmis- ja perusoikeusvelvoitteisesta demokraattisesta oikeusvaltiosta, jossa kaiken julkisen vallan käytön lähtökohtana tulee olla yksilön ihmis- ja perusoikeudet oikeudenmukaisuuden mittarina. Keskeinen osa tätä on käsitys yksilön itsemääräämisoikeudesta ja sen kunnioittamisesta kaikissa tilanteissa.[177]

Yhteiskunnan ja sen käsitysten muuttuessa vaikuttavat muutokset myös oikeuteen. Tämän kehityksen tulisi näkyä lain soveltamisessa niin, että ihmiskäsityksen muutos tuodaan osaksi käytännön ratkai-

175 *Jyränki,* Oikeusvaltio ja demokratia, s. 13–14.

176 *Saarenpää,* Kansalainen, yksilö oikeudellisesti kaiken keskipisteenä, s. 80 ja 83.

177 *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s.34.

sutoimintaa. Oikeusvaltioajattelun toteuttaminen käytännön elämän tasolla on kiinni lainsoveltajan todellisuusperspektiivistä.[178]

Oikeusvaltiokehityksestä puhuttaessa on muistettava, että perinteinen oikeusvaltioajatus on saanut alkunsa ajalla ennen digitaalista toimintaympäristöä. Oikeuvaltiokehityksen seuraavana haasteena on yksilön oikeuksien turvaaminen verkkoyhteiskunnaan digitaalisessa toimintaympäristössä. Tässäkin lähtökohdaksi tulee ottaa ihmis- ja perusoikeusvelvoitteisuus. Verkkoyhteiskunnan palveluja ja toimintoja suunniteltaessa, rakennettaessa ja toteutettaessa tulee huolehtia yksilön oikeuksien turvaamisesta oikeusvaltioajattelun mukaisesti.[179]

2.1.4. Oikeustiede muuttuvassa yhteiskunnassa

Yhteiskunnan tavoin tiede on jatkuvassa muutoksessa. Tiede onkin dynaaminen yhteiskunnallinen ilmiö. Tässä muutoksessa on kysymys tieteen yhteiskunnallisesta palvelutehtävästä ja tieteen harjoittamisen institutionaalisista edellytyksistä yhteiskunnassa. Tieteen tarkoituksena on palvella yhteiskuntaa, mikä on myös sen harjoittamisen perusedellytys.[180] Tieteen olemassaolo ei kuitenkaan ole itseisarvo, sillä tieteen eriytyessä liikaa yhteiskunnasta se käy ainakin osittain hyödyttömäksi.

178 *Tolonen,* Oikeusvaltio ja oikeustiede, s. 36

179 Näin myös *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s.34.

180 *Saarenpää,* Oikeusinformatiikka (2011), s. 412. Näin myös *Merton,* jonka mukaan tiede ja yhteiskunta ovat yhteenkietoutuneita, mutta kuitenkin toisistaan erillisiä kokonaisuuksia. *Merton,* The Sociology of Science, s. 175–176

Vaikka tieteellä on palvelutehtävä, ei se saa palvella vain sitä, mikä on hetkellisesti tärkeää. Tieteen tulee katsoa eteen ja taaksepäin.[181] Tieteen tulee ennakoida ja ottaa kantaa muutoksiin sekä myös pyrkiä säilyttämään se, mikä vaikuttaa vähemmän arvokkaalta. Tämä tarkoittaa sitä, että tieteen kehitys ei ole eikä saakaan olla yhdenmukainen yhteiskunnan kehityksen kanssa. *Saarenpään* sanoin tieteessä tulee unohtaa hetkellinen myyvyys, ja keskittyä myös niihin asioihin, jotka eivät vaikuta niin tärkeiltä.[182]

Jotta tiede voi täysin toteuttaa palvelutehtävänsä, tulee sen olla vallasta, vallankäytöstä ja markkinoista vapaa ja riippumaton. Tieteen vapaus on juuri se ominaisuus, joka erottaa tieteen muista yhteiskunnallisista toiminnoista. Vapaana tieteen ei tule olla alistettuna hetkellisiin yhteiskunnallisiin, poliittisiin tai taloudellisiin pyyteisiin.[183]

Tiede yhteiskunnallisesti vaikuttavana ja jopa yhteiskuntaa järjestävänä ja ylläpitävänä tekijänä on vaikeasti määriteltävissä. Perinteisin tapa kuvata tiedettä on sanoa sen pyrkivän vain ja ainoastaan totuuteen.[184] Tiede ei dynaamisen luonteensa vuoksi kuitenkaan saavuta

---

181 Backman kuvaa tieteen luonnetta sanomalla tieteellisen tutkimuksen Janus-kasvoissa olevan kaksi silmää. Toinen katsoo eteenpäin, luo uutta, etsii teitä edessä olevien muurien ylittämiseksi tai särkemiseksi. Toinen silmä puolestaan katsoo tieteen historiallista kehitystä, arvioi itseään, tuloksiaan, metodiaan, paikkaa tieteen järjestelmässä. *Backman,* Oikeustiede yhteiskuntatieteenä, s. 1.

182 *Saarenpää,* Oikeusinformatiikka (2011), s. 412–413. Näin myös *Merton,* jonka mukaan tutkijan menetelmät tai tulokset pitää olla koko tiedeyhteisön käytössä ja arvioitavana. Katso tarkemmin *Merton,* Sociology of Science

183 *Häyhä,* Minun metodini, s. 27.

184 Pyrkiessään totuuteen tieteen tulee järjestää, pelkistää, paljastaa, tehdä näkymätön näkyväksi ja tarvittaessa kritisoida. Saarenpää Oikeusinformatiikka (2011), s. 412–413.

mitään lopullista totuutta.[185] Tarkemman määritelmän mukaan tieteellä tarkoitetaan toisaalta luontoa, ihmistä ja yhteiskuntaa koskevien tietojen systemaattista kokonaisuutta (tieteellisen tutkimuksen tulokset) ja toisaalta tällaisten tietojen tarkoituksellista ja järjestelmällistä tavoittelua (tieteellinen tutkimusprosessi).[186]

Auktoritatiiviset yritykset määritellä tiedettä ja tieteellisyyttä ovat tutkimuksen kannalta äärimmäisen vahingollisia. Tieteen käsite on dynaaminen ja sen merkitysisältö muuttuu koko ajan. Pelkästään tieteen määrittely on jo sinänsä tiedettä.[187] Tieteen dynaamisuutta tukee se, että yritykset määrittää tiedettä muuttavat tiedettä luomalla uutta. Ymmärtääksemme, mitä tiede on, meidän tulee tietää, mikä on sen tarkoitus.[188] Ymmärtämättä tieteen sisältämää tavoitteellista toimintaa nerokkaatkin kielelliset analyysit voivat olla merkityksettömiä ja jopa harhaanjohtavia.[189]

Tiede hahmottuu tarkoituksensa, ideaalisuutensa ja pyrkimystensä sekä aikakaudessa elävien ihmisten kokemusten kautta. Se kytkeytyy sekä sisäisin että ulkoisin sitein sosiaaliseen ympäristöönsä. Tiede on ilmausta aikakautensa hengestä, mutta se sisältää aikakauttaan ylittäviä luomuksia. Se ei sanalla sanoen tyhjene ympäristöönsä.

Oikeustiede yhtenä oikeuden, oikeudenmukaisuuden ja oikeuksien erityistieteenä ei ole staattinen vaan dynaaminen kokonaisuus.[190] Suhteessa muihin tieteisiin ja ennen kaikkea sisäisesti oikeustieteen

185 *Juti,* Tiedon filosofia antiikista nykyaikaan, s. 21. Hänen mukaansa tiede pyrkii aktiivisesti uuteen tulkinnalliseen järjestykseen

186 *Niiniluoto,* Johdatus tieteenfilosofiaan, s. 13. Vertaa *Salonen,* Tieteenfilosofia, s. 41.

187 *Niiniluoto,* Johdatus tieteenfilosofiaan, s. 15.

188 *Juntunen,* Edmund Hussrelin filosofia, s. 122–123.

189 *Salonen,* Tieteenfilosofia, s.11.

190 *Saarenpää,* Oikeusinformatiikka (2011) s. 412. Katso myös *Tuori,* Oikeustieteen ajattomuus, s. 401.

sekä sen eri osa-alueiden rajat ovat jatkuvassa muutoksessa. Oikeustieteitä on monia, ja tiede elää ja muuttaa muotoaan.

Oikeustiede on vain yksi oikeutta tutkivista tieteistä.[191] Oikeutta tutkimuskohteena ei ole varattu vain oikeustieteelle. Oikeutta tutkivat myös yhteiskuntatieteet.[192] Erona on se, että oikeustiede ymmärtää tutkimuskohteensa ennen kaikkea oikeudeksi normatiivisena ilmiönä.[193] Yhteiskuntatieteessä puolestaan oikeus nähdään yhteiskunnallisina käytäntöinä. Oikeustiede lähestyy oikeutta sisältäpäin, kun yhteiskuntatieteen näkökulma oikeuteen on ulkopuolisen tarkkailijan näkökulma.

Oikeustiede omaa kuitenkin varsin merkittävän etulyöntiaseman oikeuden tutkimuksessa. Se on ensinnäkin yksi vanhimmista tieteistä ja toisaalta se on perinteinen oikeudellisen profession kouluttaja. On varsin kiistatonta, että oikeustiede on ollut ja tulee olemaan oikeuden tutkimuksen johtava erityistiede.

Oikeustieteen aseman oikeuden tutkimuksen johtavana tieteenä vahvistuu entisestään. Syinä ovat tieteen laatuvaatimusten kasvu oikeudellistuvassa verkkoyhteiskunnassa ja oikeusvaltion asettamat lisääntyvät vaatimukset sääntelylle sekä oikeudellisen tiedon sisällölle

---

191 Täytyy kuitenkin huomauttaa Hartin tavoin siitä, että kysymykseen oikeustieteen tutkimuskohteesta ei ole annettu mitään yksiselitteistä vastausta oikeuskirjallisuudessa. *Hart,* The Concept of Law, s. 1-2.

192 Tosin on mahdollista nähdä myös oikeustiede yhteiskuntatieteenä, sillä se on yhteiskuntaa tutkiva tiede. Oikeustiede tutkii oikeutta yhteiskunnallisena järjestyksenä. *Kangas,* Minun metodini, s. 91–92.

193 Tuori on huomauttanut siitä, että oikeustieteeseen kuuluu myös deskriptiivinen ainesosa. Tästä hän käyttää nimitystä kätketty yhteiskuntateoria. Tällä hän tarkoittaa sitä, että oikeuskäsitteet, joita teoreettinen lainoppi kehittelee osana eri oikeudenalojen yleisiä oppeja, ilmentävät tiettyä kuvaa siitä yhteiskunnan osa-alueesta, jota kukin oikeudenala sääntelee. *Tuori,* EIF VII, s. 857–859.

ja sen käyttötavoille. Tämän vuoksi muiden tieteiden on entistä vaikeampi kilpailla oikeustieteen kanssa oikeuden syvällisessä tutkimuksessa, koska luotettavaa oikeudellista tietoa ja osaamista tarvitaan entistä enemmän.

Monimutkaistuvassa ja lisääntyvän sääntelyn yhteiskunnassa tarve tieteiden väliseen yhteistyöhön on varsin merkittävä. Tieteiden ja niiden puitteissa koulutetut professiot toimivat entistä enemmän yhdessä. Tämä on vaikuttanut tieteellisen yleissivistyksen tarpeen kasvuun muuttuvassa yhteiskunnassa.

Oikeustieteen rooliin kuuluu autoritaarisen vallankäytön tieteellinen kyseenalaistaminen ja vastustaminen. Kritiikki on olennainen osa oikeustieteen tehtäviä. Kritiikki ei voi kuitenkaan rajoittua vain oikeuden hahmossa tapahtuvan yhteiskunnallisen vallankäytön arvosteluun. Tieteen legitiimiys uuden tiedon tuottajana ja systemaattisena järjestäjänä perustuu olennaisesti myös tieteen omaan toimintaan ja tuottamaansa informaatioon kohdistamaan systemaattiseen kritiikkiin. Oikeudellisen systematiikan ylläpitäminen ja uudistaminen ovat oikeustieteen keskeisiä tehtäviä.[194]

Jotta oikeustiede voi toteuttaa yhteiskunnallista tehtäväänsä vallankäytön kyseenalaistajana ja vastustajana, tulee oikeustieteen perustua vallan paineista vapaaseen totuuden tavoitteluun. Tämän vuoksi oikeustieteen tulee osoittaa, että oikeudesta on mahdollista tietää jotakin enemmän kuin vain asetetun lain normit, lainvalmisteluaineisto ja oikeuskäytäntö. Tämä edellyttää ensinnäkin, että sen on kyettävä muuttumaan yhteiskunnan mukana. Toisaalta oikeustieteen tulee pystyä rakentamaan lähdeaineistosta mielekäs kokonaisuus eli tekemään käytetty aineisto paremmin ymmärrettäväksi. Tätä tarkoittaen on usein todettu oikeustieteen muokkaavan oikeusjärjestyksestä oikeusjärjestelmän.

194 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 37

Oikeustieteessä tulokset eivät edellä esitetyn vuoksi voi olla lopullisia tai yleispäteviä. Oikeustiede ei ensinnäkään voi toimia tyhjiössä, vailla yleistä viitekehystä. Toiseksi oikeusjärjestyksellä on vuorovaikutussuhteita useiden yhteiskunnallisten ilmiöiden kanssa.[195] Oikeustiede on väistämättä moniaineksinen ja metodisesti avoin tieteenala, kunhan se ymmärretään oikein. Oikeustiede on dynaaminen tiede, jonka tulee yhteiskunnan kehittyessä pystyä riittävän tehokkaasti havahtua muutokseen ja myös uusitutumaan.

2.2. Tunnistaminen valvonnan ja vallankäytön välineenä

Tunnistamisella tarkoitetaan toimenpidettä tai prosessia identiteetin luomiseksi tai esittämiseksi toiselle. Tietojärjestelmien käyttöön tällainen abstrakti määritelmä on kuitenkin riittämätön. Tietojärjestelmissä tunnistamisen tarkoitus on konkreettisempi, sillä sitä käytetään yhdistämään tietoja määrättyyn henkilöön.

Ihmisen tunnistaminen eli identifiointi on perustavaa laatua oleva yhteiskunnallinen asia. Jokaisen meistä täytyy tunnistaa eri yhteyksissä muita ihmisiä päivittäisten asioiden hoitamiseksi ja liiketoiminnan harjoittamiseksi. Nykyajan verkkoyhteiskunnassa tunnistamisen merkitys korostuu entisestään. Verkoissa toimittaessa yksilön tunnistaminen ja yksilöiden erottaminen toisistaan eli yksilöinti on oikeudellises-

195 Se on sidoksissa esimerkiksi yhteiskunnan taloudelliseen perustaan, politiikkaan, valtiovaltaan, valtiokoneistoon ym. *Backman,* Oikeustiede yhteiskuntatieteenä, s. 9-12.

ti erittäin tärkeää.[196] Tunnistamisen jälkeen henkilön on mahdollista käyttää oikeudellista identiteettiään.[197]

Tunnistamisen merkitys kasvaa yhteiskunnassa siksi, että yksilön, yhteisöjen, markkinoiden ja julkisen vallan kannalta on välttämätöntä tunnistaa yksilöt ja erottaa eri ihmiset luotettavasti toisistaan. Tunnistamisen avulla henkilön viestien ja toimenpiteiden oikeudellinen sidonnaisuus ja muu oikeudellinen arviointi myös kohdentuvat oikein. Tunnistaminen on aina ollut perusosa ihmisten välisessä kanssakäymisessä. Jotta voisi pyrkiä aitoon kanssakäymiseen toisten ihmisten kanssa, tulee pystyä tunnistamaan toinen henkilö. Toisaalta tunnistaminen nostaa välittömästi esille kysymykset tietosuojasta. Yksilöinä meillä on lähtökohtaisesti oikeus yksityisyyteen ja henkilötietojen suojaan.

Organisaatiot pyrkivät hallitsemaan ihmisiä kansalaisina, asiakkaina tai työntekijöinä.[198] Hallinta edellyttää ihmisen tunnistamista. Koska hallinnon ja työnantajien edustajat määräävät, milloin ihmiset joutuvat tunnistautumaan, on perusteltua puhua tunnistamisesta vallankäytön välineenä. Osana yleisempää yksityisyyden suojan menet-

196 Esimerkiksi perintätoiminnassa velallisen yksilöinti on tärkeää, jotta perintätoimet kohdistetaan oikeaan henkilöön. Velallisen oikea yksilöinti on olennainen tieto sekä perinnän onnistumisen että velallisen oikeussuojan kannalta. Velallisen yksilöinti on myös välttämätöntä oikeudellisen perinnän ja ulosottoperinnän toteuttamiseksi, sillä myös tuomioistuimet ja ulosottoviranomaiset edellyttävät toimissaan henkilön täsmällistä yksilöintiä. Tietosuojalautakunnan päätös 5/04. Diaarinumero 9/932/2004.

197 Identiteetin perustana voidaan pitää henkilön oikeus- ja oikeustoimikelpoisuutta sekä toimivaltaa. Näin myös *Pöysti,* Sähköinen identiteetti, s. 1113.

198 Esimerkiksi työsuhteen keskeisenä elementtinä on työn tekeminen työnantajan lukuun tämän johdon ja valvonnan alaisena (TSL 1:1).

teämisen tunnetta tämä johtaa siihen, että monet myös kokevat vastenmielisyyttä tunnistamiseen.

Vaikka organisaatioilla on ajoittainen tarve tunnistaa yksilöitä, saatetaan tunnistaminen tietyissä tilanteissa kokea ihmisarvoa loukkaavaksi. Mitä moninaisempia tunnistusratkaisut ovat, sitä enemmän ne auttavat kohdistamaan sosiaalista valvontaa yksilöihin.[199] Tehokkaita tunnistamisen ja valvonnan järjestelmiä ylläpitävät yhteiskunnat joutuvat vain hyväksymään niihin sisältyvät sosiaaliset riskit.

Eheimmät tunnistusratkaisut yhdistävät yksityisyyteen tunkeutuvan tietojen keruun potentiaalisesti kaikkialla olevaan vallan välineeseen. Tunnistamisen ratkaisujen tuleekin heijastaa osapuolten sosiaalisia arvostuksia. Tunnistusteknologioiden kehittyessä kasvaa tarve saavuttaa tasapaino yksilöllisten ja yhteisöllisten tarpeiden välillä.

Loppujen lopuksi on poliittinen kysymys, minkälainen tasapaino valitaan yksilöllisten ja yhteisöllisten intressien kesken. Yksityisyyden huomioiminen merkitsee kriittistä suhtautumista kaikkiin monikäyttöisiin tunnistusmuotoihin ja anonymiteetin ja pseudonyymin tunnistuskäytännön tukemista.[200]

---

199 Nagelin mielestä olemme sitä sidotumpia kollektiivisiin normeihin, mitä enemmän olemme alistettuja julkiselle tarkkailulle ja mitä enemmän olemme velvoitettuja paljastamaan elämämme sisimpiä asioita. *Nagel,* Concealment and Exposure, s. 4. Tunnistamisessa osana valvontaa on myös kysymys vallankäytöstä, kyvystä saada toinen toimimaan haluamallaan tavalla.. Palm onkin todennut: "The possibility of being seen and measured at all times is likely to affect the ways in which individuals conceive of, act and express themselves." *Palm,* Privacy Expectations at Work – What is Reasonable and Why?, s. 208. Vallankäytöstä tarkemmin katso esimerkiksi *Bentham,* The Panopticon Writings (1787), *Foucault,* Discipline and Punish (1975) sekä Williams, Shame and Necessity (1994).

200 *Heinonen,* Digitaalinen minä, s. 94.

Nykyaikaisen yhteiskunnan keskeisimpiä haasteita on tehokkaan tunnistamisratkaisun löytäminen. Ilman luotettavaa tunnistamisratkaisua julkisen vallan on hankala valvoa valtiossa asuvia ja suojella valtiota ulkoisilta ja sisäisiltä uhilta. Tämä on osoituksena siitä, että tunnistaminen on ymmärrettävissä vallankäytön välineeksi.

Perinteisesti yksilöiden yksilöimisessä ja tunnistamisessa on käytetty henkilötunnuksia. Henkilötunnukset eivät kuitenkaan vastaa riittävästi digitaalisen verkkoyhteiskunnan tunnistustarpeita. Tämän vuoksi on alettu kehittää vahvoja sähköisen tunnistamisen menetelmiä, joiden tarkoituksena on kehittää yksilölle sähköinen digitaaliseen toimintaympäristöön luotu identiteetti.

Ongelmana on se, miten tunnistaminen toteutetaan uudessa digitaalisessa ja tietoverkkoihin perustuvassa toimintaympäristössä. Ratkaisu ei ole helppo, sillä oikeudellisessa verkkoyhteiskunnassa muun muassa perusoikeudet vaikuttavat erilaisten oikeudellisten ilmiöiden ratkaisemiseen. Jo tunnistamisen toteutuksen alkuvaihessa tulee ennen kaikkea ratkaista, kuinka on mahdollista huomioida perusoikeuksien kunnioitaminen riittävällä tavalla.

2.3. Tunnistaminen fyysisessä ja digitaalisessa toimintaympäristössä

Verkkoyhteiskunnan keskeinen käsite on digitaalinen toimintaympäristö. Se on kehittynyt fyysisen toimintaympäristön rinnalle yhteiskunnan toimintojen siirtyessä entistä enemmän tietoverkoissa toimiviksi. Digitaalisen toimintaympäristön käsitteellä viitataan fyysisen toimintaympäristön rinnalle kehittyneeseen tietoverkoissa toimivaan digitaaliseen verkkoympäristöön.

Tässä uudessa toimintaympäristössä oikeudet ja velvollisuudet ovat samalla tavoin voimassa kuin fyysisessä toimintaympäristössä. Erona

fyysiseen toimintaympäristöön on kuitenkin se, että digitaalisessa toimintaympäristössä henkilön tunnistamisen merkitys saa korostuneen merkityksen. Luotettava toimiminen digitaalisessa toimintaympäristössä edellyttää luotettavaa tunnistamista.

Luotettavan henkilöntunnistuksen tarve on jaettavissa kahteen ryhmään: 1) fyysisen toimintaympäristön tunnistamiseen eli läsnä olevan henkilön tunnistamiseen ja 2) digitaalisessa toimintaympäristössä tapahtuvaan tunnistamiseen. Nämä eroavat siinä, mitä tunnistamisen menetelmiä on käytössä. Fyysisessä toimintaympäristössä läsnä oleva henkilö on mahdollista tunnistaa luotettavasti esimerkiksi tunnistamisasiakirjasta, mutta digitaalisen toimintaympäristön tunnistamisessa tämä on vielä rajoittunutta. Lisäksi digitaalisessa toimintaympäristössä käytettävät tunnistamisessa käytettävät identiteettitiedot saavat korostuneen merkityksen. Muutoin suurin osa tunnistamiseen liittyvistä riskeistä koskee kuitenkin yhteisesti kumpaakin toimintaympäristöä, kun kysymys on itse tunnistamistapahtumasta.

Henkilön tunnistaminen sekä kasvotusten että digitaalisessa toimintaympäristössä on olennaista turvallisen asioinnin ja yksilön oikeusturvan kannalta. Henkilöllisyyden ja tunnistamisen kannalta kansalaisen oikeusturvan tulee olla samalla tasolla toimintaympäristöstä riippumatta. Oikeustoimet ovat yhtä sitovia toimintaympäristöstä riippumatta.

Luotettava asiointi digitaalisessa toimintaympäristössä on mahdollista vain, jos digitaalisen toimintaympäristön tunnistautumisessa käytettävä tunniste on riittävän vahva. Fyysisen toimintaympäristön identiteetti ja digitaalisen toimintaympäristön identiteetti ovat sekä toisistaan erottamattomat että keskenään vuorovaikutuksessa. Digitaalisen toimintaympäristön identiteetti rakentuu pitkälti fyysisen toimintaympäristön identiteettien pohjalle.

Tulevaisuudessa vahvan sähköisen tunnistamisen merkitys kasvaa entisestään. Se myös lisää biometrisiin tunnisteisiin perustuvien

tunnistamisratkaisujen tuloa markkinoille. Yhteiskunnan toimintojen siirtyessä entistä enemmän verkoissa toimiviksi, kasvaa henkilön luotettavan tunnistamisen tarve. Tämä on myös yksi syy siihen, miksi biometrisen tunnistamisen sovellukset ovat yleistyneet. Yksilön tunnistaminen on saanut korostuneen oikeudellisen merkityksen digitaaliseen toimintaympäristöön perustuvassa verkkoyhteiskunnassa. On mahdollista jo puhua yksilön tunnistamisen oikeudellistumisesta osana verkkoyhteiskunnan oikeudellistumista.

Henkilön tunnistaminen digitaalisessa toimintaympäristössä ei ole kuitenkaan ongelmaton, koska tunnistustapahtuma tuo yhden lisäelementin asiointitapahtumaan. Digitaalisen toimintaympäristön palvelujen käyttö vaikeutuu, jos henkilöllä ei ole tarvittavaa tunnistusvälinettä käytössään. Sähköisen tunnistuksen ylikorostamisen riskinä on, että digitaalisen toimintaympäristön toimijat alkavat kontrolloida ja seurata toimintaa. Vaarana on, että siirrytään kohti valvontayhteiskuntaa.

Tunnistamista tarkasteltaessa esille nousevat seuraavat kysymykset: 1) missä tilanteissa henkilö on tarpeen tunnistaa sähköisessä asioinnissa, 2) mitä tunnistusmenetelmiä tulisi kussakin tilanteessa käyttää ja 3) onko asiakkaalla oikeus asioida sähköisissä asiointipalveluissa anonyymisti. Tunnistamisen oikeudellistuminen tuokin mukanaan uusia haasteita yksityisyyden suojan turvaamiseen.

2.4. Ihmisruumis informaatiolähteenä

Ihmisruumis on kiinnostanut tieteilijöitä tuhansia vuosia. Ihmisruumiin muotojen ja rakenteen tutkiminen avaakin uusia tutkimusalueita. Kiinnostuksesta huolimatta ihmisruumis on kuitenkin ollut enemmän tai vähemmän näkymätön tietosuojan näkökulmasta.

Tietosuojan keskiössä on ollut ennen kaikkea tietotekniikka ja sen vaikutus yksilön ykistyisyyteen, jonka lähtökohtana on fyysisen koskemattomuuden suojaaminen.[201] Näkökulma on viime aikoina noussut keskusteluun erityisesti tietotekniikan sovellusten yhdistyessä biotekniologiaan, josta esimerkkinä on biometrinen tunnistaminen.

Biometrisen tunnistamisen sovelluksissa on yksi yhteinen piirre: jokaisessa ihmisruumis on muunnettu digitaaliseksi koodiksi yksilön identifioimiseksi. Ihmisruumiin informationaalistuminen on myös se, mihin biometrinen tunnistaminen perustuu.[202] Yksilöitä on tämän vuoksi mahdollista myös kategorioida aiempaa tehokkaammin. Tämän kehityksen vuoksi onkin alettu puhua uudesta ruumiin ontologiasta, jossa ihmisruumis nähdään informaatiolähteenä tai jopa informaationa.

Ihmisruumiista saadaan informaatiota yksilön yksilöllisistä piirteistä, joiden kautta yksilö on tunnistettavissa. Esimerkiksi ruumiin rakenteesta ja muodoista on mahdollista tehdä johtopäätöksiä yksilön sukupuolesta ja iästä. Yksilö on siis mahdollista tunnistaa hänen ruumiinsa ominaispiirteiden perusteella.

Genetiikassa käytetty ruumiin ontologia lähtee ajatuksesta, että ihmisruumis on tärkeä informaatiolähde. Esimerkkinä toimii DNA, joka on koodina murrettavissa ja josta saadaan hyvinkin tarkkaa infor-

201 *Bygrave,* The body as data? Reflections on the relationship of data privacy law with the human body, s. 1–2.

202 *Ploeg,* Biometrics and the body as information, s. 44. Katso myös *Ploeg,* The Politics of Biometric Identification. Normative aspects of automated social categorization, s. 6, jossa Ploeg toteaa seuraavaa: "The informatization of the body entails that the question who you are, how you are, and how you are going to be treated in various situations, will increasingly be decided on the basis of information deriving from your own body… "

maatiota yksilöstä. Genetiikka on myös tyypillinen esimerkki ihmisruumiista informaatiolähteenä.[203]

Onko siis ihmisruumis itsessään informaatiota? Informatiikan ja tietotekniikan alalla käsitteellä ”tieto” on perinteisesti ymmärretty kaikenlaisia, jotakin asiaa todellisessa maailmassa kuvaavia merkkejä (toiminto tai kappale), jotka voivat viestiä informaatiota tästä asiasta.[204] Informaatiota on näin ollen tähän asiaan liitettävissä oleva tieto. Ihmisruumis on informaatiolähde, josta on mahdollista saada paljonkin yksilöön liittyvää informaatiota niin suoraan kuin välillisesti. Tämä ei automaattisesti tarkoita, että ihmisruumis itsessään on informaatiota. Ihmisruumis tulee kuitenkin perustellusti nähdä informaatiolähteenä.

Ihmisruumiin ja informaatioteknologian yhteenliittyminen tulee aiheuttamaan sekaannusta ja antaa aiheen epäilyille. Se myös luo tarpeen tarkastella aiemmin itsestään selviä asioita uudesta näkökulmasta. Ongelmana tällaisessa tilanteessa on perinteisten käsitteiden ja arvojen sijoittaminen uuteen ympäristöön, johon niitä ei alun perin ole suunniteltu.

Biometrinen tunnistaminen on nyky-yhteiskunnassa yleisin käytännön esimerkki tämän uuden ontologian omaksumisesta. Se perustuu ihmisruumiista joko suoraan tai välillisesti saatavaan informaatioon. On perusteltu tarve kiinnittää enemmän huomiota ihmisruumiin merkitykseen informaatiolähteenä myös tietosuojan näkökulmasta.

203 *Ploeg,* Genetics, biometrics and the informatization of the body, s. 44

204 *Bygrave,* The body as data? Reflections on the relationship of data privacy law with the human body, s. 2.

3. Tutkimuksen keskeiset oikeudelliset periaatteet ja käsitteet

3.1. Itsemääräämisoikeus

Persoonallisuusoikeudessa ihmisoikeuksilla on korostunut merkitys. Kansainvälisin ihmisoikeussopimuksin on pyritty yleisesti määrittelemään ne yksilön vapaudet ja oikeudet, joita nykyisen ihmiskäsityksen mukaan pidetään välttämättöminä oikeusvaltiossa. Persoonallisuusoikeuden pohjana on nimenomaan ihmiskäsitys; käsitys ihmisen vapauksista ja oikeuksista sekä vastaavasti velvollisuuksista oikeusvaltion puitteissa toimivassa demokratiassa.[205]

Persoonallisuusoikeuden yleisten oppien rakentamisen lähtökohtana pidetään yksilön itsemääräämisoikeutta. 2000-luvun ihmiskäsityksen mukaan yksilön liittymä yhteiskuntaan ja organisaatioihin[206] on ymmärrettävissä myös itsemääräämisoikeuden kautta. Yhteiskuntasopimusten tasolla ymmärrämme ihmisen vapaana yksilönä, joka käyttää itsemääräämisoikeuttaan demokratian asettamin välittömin rajoituksin.[207]

---

205 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 229.

206 Organisaatioista katso *Etzioni,* Modern Organisations. Etzionin ajattelun lähtökohta on teoksessa varsin yksinkertainen. Olemme sidoksissa organisaatioihin, ja organisaatiot kontrolloivat jäsentensä käyttäytymistä. Katso myös *Allardt,* Ihminen ja moraali hyvinvointivaltiossa. Allardt erottaa Etzionia mukaillen toisistaan hyöty- ja yhtenäisyysorganisaatiot.

207 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2009), s.276. Vertaa *Saarenpää,* Potilas, oikeus, ihminen, s. 269–270 sekä *Saarenpää,* Henkilöoikeus, joissa Saarenpää sanoo persoonallisuusoikeuden keskei-

Itsemääräämisoikeus on yleinen ajatusmalli, jota tarvitaan kuvattaessa yksilön liittymistä ympäröivään yhteiskuntaan. Se on tämän vuoksi yhteiskuntasopimuksen tasolle yltävä metaoikeus, jonka vaikutukset ja suoja ilmenevät eri tavoin eri oikeudenaloilla. [208]

Itsemääräämisoikeus on tullut uudella tavalla tärkeäksi asiaksi nyky- yhteiskunnassa. Oli kysymys sitten yksityisyyden suojasta, henkilötietojen käsittelystä, valvonnasta tai vaikkapa kulttuurisista tavoista tulee lähtökohtana olla oikeudellinen ihmiskäsitys. Näin siksi, että ihmisen oikeudet ja niiden suoja rakennetaan vallitsevan ihmiskäsityksen mukaisesti. Taustalla ovat ennen kaikkea uskonnolliset ja filosofiset ihmiskäsitykset, joiden avulla luodaan kuva ihmisen tarpeista ja niiden toteuttamiseen liittyvistä vapauksista.[209]

Oikeus itsemääräämiseen on mahdollista määritellä suppeasti tai laajasti. Suppean tulkinnan mukaan sillä tarkoitetaan kompetentin ja riittävän autenttisen henkilön oikeutta määrätä omista asioistaan.[210] Toisaalta laajemmasta näkökulmasta oikeus itsemääräämiseen on mahdollista määritellä vapaudeksi.[211] Henkilö on ymmärrettävissä vapaaksi, kun hän ohjaa itse omaa tahtoaan.[212] Juuri yksilön vapaus on pohjoismaisen oikeusajattelun perusajatuksia erityisesti oikeusvaltioajattelun näkökulmasta.

Yksilön vapaus ei kuitenkaan ole rajaton, sillä yksilön vapauksia rajoittavat toisten yksilöiden oikeudet ja vapaudet. Itsemääräämisoikeutta ei ole ilman velvollisuuksia, velvollisuuksia kunnioittaa toisten yksilöiden vapautta ja oikeuksia. Rawls onkin todennut, että jokaisella henkilöllä on yhtäläiset oikeudet laajimpaan mahdolliseen vapauteen

---

senä lähtökohtana olevan yksilön kunnioitus.

208 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2009), s.281.

209 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 222–223.

210 *Pietarinen,* Itsemääräämineen ja itsemääräämisoikeus, s. 25

211 *Schwartz,* Self-Determination: The Tyranny of Freedom, s. 80.

212 *Feinberg,* Social Philosophy, s. 15.

yhteen sovitettuna toisten henkilöiden samanlaiseen vapauteen.[213] Tällainen määritelmä antaa kuitenkin vain lähtökohdan itsemääräämisoikeuden arvioinnille. Itsemääräämisen käsitettä on tämän vuoksi tarpeen erotella tarkemmin.

Perusmerkitykseltään itsemääräämisoikeus on kykyä päätösten tekemiseen ja tehtyjen päätösten toteuttamiseen eli kykyä harkintaan, päättämiseen ja toimintaan eli kompetenssiin. Itsemääräämisen kohde on jokin sellainen asia, joka koskee henkilöä läheisesti, asia johon henkilöllä on valtaa.[214] Päätöksen kohteet tulee jakaa omia asioita koskeviin ja itseä koskeviin päätöksiin. Omia asioita koskevia päätöksiä ovat periaatteessa kaikki yksilön omaa toimintaa koskevat päätökset aina vähäpätöisestä jäätelön valinnasta omaa uraa koskeviin päätöksiin. Ne ovat usein myös niitä päätöksiä, joihin itsemääräämisoikeus useimmiten yhdistetään. Itseä koskevat päätökset puolestaan ovat olleet itsemääräämisoikeuden näkökulmasta vähemmän esillä. Ne liittyvät siihen, millainen yksilö on tai haluaa olla. Kysymys on toisin sanoen identiteettiä koskevista päätöksistä.[215]

Päätöksen lajista riippumatta itsemääräämisen muodostuu kahdesta osasta: henkilöstä, joka tekee ratkaisuja ja asiasta, joka on itsemääräämisen kohteena.[216] Jotta henkilö voisi itse määrätä, tulee hänellä olla sekä kompetenssi että valta käyttää kompetenssiaan asiaan. Tämä ei kuitenkaan vielä tarkoita, että henkilö olisi itsemääräävä. Henkilöä on mahdollista pitää itsemääräävänä vasta, kun hänen ratkaisunsa ovat autenttisia. Toisin sanoen, kun ratkaisut ovat itsenäisesti, riippumat-

213 *Rawls,* Theory of Justice, s. 60

214 *Pietarinen,* Itsemääräämisen ja itsemääräämisoikeus, s. 15–22.

215 *Schwartz,* Self-determination: The Tyranny of Freedom, s. 80.

216 *Pietarinen,* Itsemääräämisen periaate, s. 97.

tomasti tai omaehtoisesti tehtyjä.[217] Henkilön tulee siis määrätä itse itseään vapaana ulkoisten tekijöiden ohjauksesta ja olla vapaa kontrolloimaan itse itseään.[218] Lisäksi tärkeä osa itsemääräämistä on, että yksilöllä on henkisen kyvyn lisäksi fyysinen kyky ja vapaus toteuttaa päätöksensä.

Itsemääräämisoikeus ei kuitenkaan ole ehdoton. Yksilöinä olemme osa yhteiskuntaa, halusimme sitä tai emme. Toimiakseen yhteiskunta tarvitsee sääntöjä. Tästä seuraa, että myös ihmisten oikeudelliselle kelpoisuudelle ja itsemääräämisoikeudelle on asetettava tietyt rajat ja kriteerit.[219] Nämä rajoitukset ovat jaettavissa ulkoa tuleviin ja yksilön itsensä sisältä tuleviin. Ulkoisista rajoituksista esimerkkeinä toimivat lainsäädännössä tunnistetut vaihtoehdot eli pakottaminen ja oikeudeton vaikuttaminen. Sisäisesti vaikuttaviin tekijöihin kuuluu henkilön

217 *Pietarinen,* Itsemääräämisoikeus, s. 15–22 ja *Knee – Hadden – Porter – Rodriguez,* Self-Determination Theory and Romantic Relationship Processes, s.307.

218 *Santoro,* Autonomy, Freedom and Rights, s. 14–15 ja *Knee – Hadden – Porter – Rodriguez,* Self-Determination Theory and Romantic Relationship Processes, s.307. Katso myös *Habermas, Between Facts and Norms,* s.120, jossa Habermas puhuu yksityisautonomiasta. Tällä hän tarkoittaa oikeussubjektin kykyä toimia vapaasti ilman, että hänen täytyy tehdä tiliä muille tekemisistään tai antaa julkisesti hyväksyttäviä perusteluja toimintasuunnitelmilleen. Voidaan sanoa, että itsemääräämisoikeuteen liittyy ajatus vapaudesta olla oma herransa.

219 *Lohiniva-Kerkelä,* Verosalaisuus, s. 108 ja *Saarenpää,* Potilas, oikeus, ihminen, s. 269. Stalley jakaa tämän vuoksi itsemääräämisoikeuden positiiviseen ja negatiiviseen itsemääräämisoikeuteen. *Stalley,* Self-determination, s. 40.

oma käsitys omista kyvyistään tehdä valintoja ja päätöksiä.[220] Ollakseen itsemääräävä henkilön on oltava valintojensa lähde ja valintojen tulee myös olla aitoja.[221]

Ympäröivät olosuhteet tai toisten ihmisten teot eivät rajoita henkilön valinnan mahdollisuuksia täysin olemattomiin.[222] Henkilön tulee olla vapaa päättämään itse. Tällä tarkoitetaan vapautta henkilön itsensä sisäisiltä tai ulkopuolisilta tulevista ulkoisista voimista.[223]

Laajalta merkitykseltä itsemääräämisoikeuteen sisältyy omista asioistaan määrääminen sekä yksilön oikeus kompetenssiin ja autenttisuuteen. Oikeus kompetenssiin tarkoittaa ensinnäkin muiden velvollisuutta edistää henkilön kykyä itsenäiseen ajatteluun, päätöksentekoon ja toimintaan. Toisaalta se tarkoittaa myös muiden velvollisuutta pi-

220 *Appelbaum – Lidz – Meisel, Informed Consent,* s. 24. Katso myös, *Mäki-Petäjä-Leinonen – Juva – Pirttilä,* Dementoituvan ihmisen oikeudellinen toimintakyky ja sen lääketieteellinen arviointi, Lakimies 6/2006, s. 943, jossa oikeudelliselle kelpoisuudelle asetetaan ikä- ja toimintakykyvaatimus.

221 Rationaalisen valinnan –teoria lähtee ajatuksesta, että ihminen tekee valintansa rationaalisesti. Schwartz kritisoi tätä ajatusta, sillä yksilön valintoja ei ohjaa pelkästään hänen oma rationaalisuutensa. Myös opitut tavat ja kulttuuri vaikuttavat yksilön tekemiin valintoihin. *Schwartz,* Self-determination: The Tyranny of Freedom, s. 81–82.

222 Lagerspetz, Itsemääräämineen ja valta, s. 98. Vertaa *Berlin,* Vapaus, ihmisyys ja historia, s. 56.

223 *Feinberg,* Social Philosophy, s. 15. On mahdotonta elää täysin tyhjiössä vapaana vaikutteilta. Esimerkkinä voidaan mainita opetus ja kasvatus, jonka kautta yksilöön istutetaan tietyt tavat toimia. Nämä ovat puolestaan riippuvaisia muun muassa ajasta, paikasta ja kulttuurista. Näin ollen kysymys onkin enemmän toisten yksilöiden velvollisuudesta kunnioittaa toisen itsemääräämisoikeutta antamalla tilaa omaehtoiseen ja itsenäiseen ajatteluun ja harkintaan.

dättyä tekemästä mitään, mikä vähentää henkilön kykyä edellä mainittuihin toimintoihin. Oikeus kompetenssiin velvoittaa auttamaan henkilöä saamaan riittävästi päättämiseen ja toimintaan tarvittavaa tietoa.[224] Itsemääräämisoikeuteen kuuluu tiettyä toisten ihmisten vaikutusta erityisesti tiedollisesta näkökulmasta. Tätä kuvaa erityisesti velvollisuus edistää ihmisen mahdollisuutta ajatella ja päättää asioista itse sekä toimia toisen mahdollisuudet huomioiden.[225] Biometrisen tunnistamisen kohdalla tämä tarkoittaa sitä, että yksilölle on annettava riittävästi informaatiota tästä teknologiasta. Tällä tavoin yksilön on mahdollista tehdä autenttinen ja vapaaseen tahdonmuodostukseen perustuva päätös tämän teknologian käyttämisestä.

Oikeudellisessa kielessä oikeus kompetenssiin tarkoittaa oikeutta käyttää valtaa sillä kelpoisuudella, joka kullakin yksilöllä on. Oikeus valtaan tarkoittaa muun muassa oikeutta määrätä omasta ruumiista, terveydestä ja itseä koskevasta informaatiosta. Yksilöllä on valta itseä koskeviin asioihin, oikeus saada itseä koskevia tietoja sekä oikeus valvoa itseä koskevia tietoja.[226] Tämä osoittaa sen, että oikeus kompetenssiin sisältää oikeuden tietoon.

---

224 Schwartz tosin huomauttaa siitä, että yksilö ei voi koskaan saada riittävästi tietoa aidosti autenttisen ja vapaan päätöksen tekemiseen. *Schwartz,* Self-Determination: The Tyranny of Freedom, s. 82.

225 Tornbergin mukaan viranomaisten kannalta tähän liittyvät tiedottaminen ja neuvonta, joiden kautta ihmisillä on todellinen mahdollisuus muodostaa kuva asioista ja tehdä päätöksiä. *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 124–125 ja *Santoro,* Autonomy, Freedom and Rights, s. 14

226 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (1999), s. 309. Itsemääräämisoikeuden on myös määritelty tarkoittavan yksilön moraalista ja persoonallista autonomiaa. Toisaalta itsemääräämisoikeus voidaan jakaa yksityiseen ja julkiseen puoleen. Yksityinen itsemääräämisoikeus tarkoittaa yksilön oikeutta määrätä suhteistaan toisiin

Lyhyesti ilmaistuna itsemääräämisoikeudella tarkoitetaan yksilön oikeutta päättää itse itseään koskevista asioista, valvoa niiden toteutumista sekä saada oikeusturvaa yhteiskunnassa.[227] Se on tapana jakaa viiteen keskeiseen peruselementtiin. Nämä ovat 1) oikeus sisäiseen vapauteen, 2) oikeus ulkoiseen vapauteen, 3) oikeus kompetenssiin, 4) oikeus valtaan ja 5) oikeus tietoon.[228]

Oikeus sisäiseen vapauteen on mahdollista luonnehtia oikeudeksi henkiseen loukkaamattomuuteen. Yksilöllä on niin halutessaan oikeus olla yksin omine ajatuksineen ja käsityksineen tai vastaavasti oikeus edistää niitä yksin tai yhdessä muiden kanssa.[229]

Oikeus ulkoiseen vapauteen merkitsee ensi sijassa yksilön oikeutta olla fyysisesti yksin ja liikkua vapaasti. Digitaalisessa verkkoyhteiskunnassa ulkoinen vapaus merkitsee enenevässä määrin myös oikeutta

---

yksilöihin ja saada näissä suhteissa kunnioitusta ja suojaa. Julkinen itsemääräämisoikeus puolestaan kattaa ne oikeudet, joiden avulla yksilö osallistuu yhteiskunnan toimintaan ja erityisesti poliittiseen mielipiteen muodostukseen. Julkinen ja yksityinen itsemääräämisoikeus eivät ole toisensa poissulkevia, vaan ne edellyttävät toisiaan. *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 472.

227 Tornbergin mukaan itsemääräävä henkilö voidaan määritellä yksilöksi, jolla on kyky harkintaan, päättämiseen ja toimintaan ja että tämä toiminta tapahtuu hänen omien toimintatapojensa, arvojensa ja mieltymystensä mukaisesti. Puhutaan autenttisesta päätöksenteosta, jolloin henkilö pystyy näkemään myös päätösten mahdolliset seuraukset, pystyy tekemään päätöksensä ottaen huomioon nämä seuraukset ja kantamaan niistä vastuun. *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 123

228 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 218

229 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 218. Katso myös *Saarenpää,* Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan, s. 8

pysytellä erilaisen teknisen valvonnan ulkopuolella. Nyky-yhteiskunnassa erilaiset ihmisiin kohdistuvan teknisen valvonnan mahdollisuudet ovat moninkertaistuneet, jolloin henkilöllä tulee olla oikeus päättää olemisestaan valvonnan piirissä.[230] Tämän oikeuden käyttäminen edellyttää henkilön oikeutta tietää tällaisen valvonnan olemassaolosta, jotta päätöksenteko olisi ylipäätään mahdollista. Oikeus sisäiseen ja ulkoiseen vapauteen muodostavat yhdessä oikeuden integriteettiin eli koskemattomuuteen.[231]

Oikeus kompetenssiin eli kelpoisuuteen on itsemääräämisoikeuden yhteiskuntaan heijastuva osa. Lähtökohtana on ajatus ihmisestä toimimassa itse omassa asiassaan. Tätä oikeutta suojataan ensisijaisesti oikeustoimikelpoisuuden ja erilaisten muiden ihmisen ja hänen taitojensa arviointiin perustuvien kelpoisuuksien avulla.[232]

Oikeus valtaan tarkoittaa muun muassa oikeutta määrätä omasta ruumiista, terveydestä ja itseä koskevasta informaatiosta. Ihminen omistaa oikeudellisesti itsensä. [233] Tämä näkökulma on tullut entistä tärkeämmäksi käytettäessä esimerkiksi ihmisen informaatiota raaka-aineena eri markkinoilla. Kuitenkin yksilö itsemääräämisoikeutensa puitteissa itse ensisijaisesti määrää esimerkiksi omien tietojensa käytöstä vaihdannassa. Suhteessa yhteiskuntakoneistoon oikeus valtaan puolestaan merkitsee tiedollisen itsemääräämisoikeuden ohella viime kätistä oikeutta toteuttaa lailliset vaateet oikeudenmukaisella

230 *Saarenpää,* Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan, s. 8 Tämä on ollut yksi kansainvälisen yksityisyyden suojaa koskevan keskustelun painopisteistä jo usean vuoden ajan.

231 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 218–219.

232 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 219. Katso myös *Saarenpää,* Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan, s. 8

233 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 220

tavalla. Osana oikeusvaltion ajatusta yhteiskunnan on vastaavasti tarjottava tähän asianmukaiset ja tehokkaat koneistot.

Oikeus tietoon viittaa siihen, että voidakseen perustellusti päättää itseä ja yhteiskuntaa koskevista asioista tarvitaan enenevässä määrin asianmukaista tietoa itsestä, yhteiskunnasta, erilaisista yhteisöistä ja joskus myös muista kansalaisista.[234] *Tornbergin* mukaan oikeus valtaan ja oikeus tietoon ilmenevät lainsäädännössä informaatiota koskevan sääntelyn kautta. Siihen liittyy sekä henkilötietoja koskeva sääntely että viranomaisten velvollisuus julkisuusperiaatteen toteuttamiseen.[235]

Itsemääräämisoikeutta eri ulottuvuuksineen tulee nähdä välttämättömänä yhteiskunnallisena teoriana, joka kuvaa ihmiskäsitystä ja sen mukaisia oikeuksia. Itsemääräämisoikeus on ihmisoikeuksien ja perusoikeuksien säätämisen, niiden ymmärtämisen sekä noudattamisen välttämätön oikeuden yleisten oppien tason teoria.[236]

Perusoikeudet suojaavat itsemääräämisoikeuden toteutumista sekä sen välttämätöntä rajoittamista suhteessa toisten ihmisten itsemääräämisoikeuteen.[237] Itsemääräämisoikeus on liitettävissä perusoikeussäännöstön kokonaisuuteen ja sitä turvaavat erityisesti henkilökoh-

234 Yhteiskuntaa ja yhteisöjä ajatellen voidaan puhua läpinäkyvyyden vaatimuksesta. Läpinäkyvyyden vaatimus on tärkeä käsite siksi, että erilaisten yhteisöjen läpinäkyvyys huonosti toteutettuna tai väärin ymmärrettynä saattaa samalla kaventaa merkittävästikin yksilön vapauksia. *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 221.

235 *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s.126.

236 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 233. Katso myös Euroopan neuvoston suositus edunvalvontavaltuutuksista, jossa sanotaan:"self-determination is essential in respecting the human rights and dignity of each human being".

237 *Saarenpää,* Tieto, suoja ja byrokratia – näkökohtia suomalaisen tietosuojan kehityksestä ja tulkinnoista, s. 582.

taista koskemattomuutta, yksityiselämän suojaa ja vapausoikeuksia koskevat perustuslain säännökset. Toisaalta itsemääräämisoikeus on myös edellytys perusoikeuksien toteutumiselle. Itsemääräämisoikeus laaja-alaisena oikeutena on luonnehdittavissa eräänlaiseksi yleisperusoikeudeksi tai metaoikeudeksi, joka asettuu oikeusjärjestelmässä perusoikeuksien yläpuolelle ja jota edistetään perusoikeuksien avulla.[238]

Biometrisen tunnistamisen kohdalla itsemääräämisoikeudella on suuri merkitys. Itsemääräämisoikeutensa perusteella yksilöllä on oikeus itse päättää itseään koskevista asioista ja omista tiedoistaan sekä itseensä kohdistuvista toimenpiteistä. Biometrisessa tunnistamisessa oleellinen kysymys on juuri itsemääräämisoikeuden kunnioittaminen tätä teknologiaa käytettäessä ja käyttöönotettaessa.

3.2. Yksityisyys

3.2.1. Yksityisyys käsitteenä

Yksilöiden valvonta palvelee monia laillisia tarkoituksia. Elektronisen tiedonkeruun ja tallennuksen lisääntyminen on tuonut ihmisten tietoisuuteen sen riskit niin yksityisten kuin organisaatioidenkin yksityisyydelle. Yksityisyyttä koskevan lainsäädännön lisääntyminen on merkki siitä, että yhteiskunnassa on havahduttu yksityisyyden merkityksen kasvuun. Lisääntyvä lainsäädäntö merkitsee valvonnan lisääntymistä ja sen myötä yksityisyyden asteittaista niukkenemista.[239] Valvonta ja yksityisyys ovatkin keskenään vuorovaikutuksessa. Valvonnalla puu-

238 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2003), s. 310 ja *Ojanen,* T – *Scheinin,* M, Suomen valtiosäännön perusperiaatteet, s.223

239 *Saarenpää,* Yksityisyys, yksityiselämä ja yksilönsuoja, s. 336.

tutaan aina yksityisyyteen ja yksityisyyden suoja on puolustautumista valvontaa vastaan.[240]

Valvonnan kohdalla yksityisyyden suojan tehtävänä on suojata yksilön persoonaa. Jatkuva tarkkailu vaikuttaa kielteisesti tarkkailtavien luonteen ja persoonan kehitykseen. Yksilö toimii eri tavalla, jos uskoo olevansa tarkkailun kohteena. Jos yksilö ei voi koskaan olla varma katsellaanko tai kuunnellaanko häntä, se vaikuttaa yksilön käyttäytymiseen ja koko yksilön luonne muuttuu toisenlaiseksi. Tämä osoittaa samalla yksityisyyden suojan, itsemääräämisoikeuden ja ihmisarvon kunnioittamisen läheisen suhteen: tieto tai pelko ulkopuolisesta yksityiselämän tarkkailusta vaikuttaa yksilön käytökseen. Pitkään jatkuessaan seurauksena voi olla yksilön muuttuminen araksi, epäilyttäväksi, ilottomaksi ja epäileväksi.[241] Yksilöltä, joka joutuu elämänsä jokaisen hetken olemaan toisten seurassa ja jonka jokainen tarve, halu, ajatus, unelma tai mielihyvän kokemus on yleisen silmälläpidon alla, on riistetty hänen yksilöllisyytensä ja ihmisarvonsa.[242]

Yksilöllä on demokraattisessa oikeusvaltiossa aikaisempaa laajempi ja tehokkaampi oikeus yksityisyyteen eli oikeus olla yksin. Ensinnäkin yksilön itsemääräämisoikeuden voimistuessa yksityisyyden merkitys yhteiskunnassa kasvaa entisestään. Toisaalta teknologian kehittyessä sekä tietotekniikan käytön yleistyessä yksityisyyden loukkaamisen riskit lisääntyvät.[243]

---

240 *Heinonen – Hannula,* Valvonta tietoyhteiskunnassa, s. 10.

241 *Räikkä,* Yksityisyyden filosofia, s. 90 sekä Benn, Privacy, Freedom, and Respect for Persons, s. 41.

242 *Bloustein,* Privacy as an Aspect of Human Dignity, s. 188.

243 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 310. Tämä on Saarenpään mukaan johtanut yksityisyyden oikeudellistumiseen. Yksityisyyden oikeudellistuminen voidaan nähdä ongelmallisena, sil-

Periaatteena yksityisyys[244] liittyy läheisesti pohjoismaissa vahvaan julkisuusperiaatteeseen, jonka juuret ovat vapauden ajalla vuoden 1766 painovapausasetuksessa. Yksityisyyden oikeudellinen sääntely on julkisuusperiaatetta nuorempi, vaikka se kytketäänkin Ranskan vallankumouksen ihmisoikeusjulistuksiin. Vahvemmin yksityisyyden arvostuksen nousu kytkeytyy poliittiseen liberalismiin ja ajatukseen perusoikeuksien kunnioittamisesta.[245]

Yksityisyys on kunnian suojan tavoin sekä ajatuksena että oikeudellisen suojan kohteena erittäin vanha. Eurooppalaiseen oikeusajatteluun yksityisyys käsitteenä on kuitenkin vakiintunut vasta viime vuosikymmeninä. Osittain syynä on se, että Euroopan ihmisoikeussopimuksen terminologian mukaisesti yksityisyyden kanssa kilpailee käytännössä toisena käsitteenä yksityiselämän suoja, joka on otettu käyttöön myös perustuslaissa.[246]

Oikeudellisena käsitteenä yksityisyys on lähtöisin ennen kaikkea yhdysvaltalaisesta oikeustieteestä ja siellä oikeuskäytännössä synty-

---

lä se johtaa paitsi aihepiirin oikeudellisen tutkimuksen tärkeytymiseen myös tutkimuksen hajautumiseen. Riskinä tällöin on yhteyden katkeaminen yksityisyyden perusajatuksiin.

244 Yksityisyys osana itsemääräämisoikeutta on keskeinen käsite. Se voidaan laajentaa yleiseksi periaatteeksi eli oikeudeksi yksityisyyteen. Yksityisyys tulee näin ollen nähdä osana yksilön persoonallisuuden suojaa. Yksityisyyden ja persoonallisuuden suhteesta katso tarkemmin esimerkiksi: *Beverley-Smith – Ohly – Lucas-Schloetter,* Privacy, Property and Personality. Civil Law Perspectives on Commercial Appropriation. Cambridge University Press. New York 2005.

245 *Konstari,* Henkilörekisterilaki, s. 9–12.

246 Perustuslain 10.1 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.

neistä määritelmistä ja teorioista.[247] Yhteistä näille on se, että yksityisyyden ydin muodostuu oikeudesta olla rauhassa ja kontrolloida henkilökohtaisia tietojaan. Olennaisena osana yksityisyyteen kuuluu myös oikeus järjestää yksityiselämänsä ilman ulkopuolisten tahojen perusteetonta puuttumista. Perusteettomasta puuttumisesta esimerkkinä on yksilön valvonta hänen tietämättään. Yksilöllä tulee olla oikeus lainsäädännön rajoissa vapaasti päättää itseään koskevista asioista.[248] Kysymyksessä on yksityisyyden ja itsemääräämisoikeuden keskinäinen yhteys.

Yksityisyyden ja yksityisyyden suojan tarkastelun lähtökohtana tulee pitää itsemääräämisoikeutta. Se edellyttää oikeutta tietoon, on samalla sen käyttämisen kohde ja voimakkaasti sidoksissa informaatioon. Ensinnäkin rationaalisen päätöksenteon pohjaksi vaaditaan tietoa. Toisaalta itsemääräämisoikeutta ei ole, jos kaikki yksilöä koskeva informaatio on julkista. Näin ollen myös yksityisyys liittyy läheisesti itsemääräämisoikeuteen. Yksilöllisellä tasolla yksityisyys toimii myös yksilön terveen kehityksen edellytyksenä. Kehittyäkseen itsemääräävästi ja itsenäiseksi yksilö tarvitsee yksityisyyttä ja sen suojaa. Kunnioittamalla ja suojaamalla yksityisyyttä toteutetaan yksilön vapaata kehitystä ja itsemääräämisoikeutta. Tällä tavoin turvataan osaltaan myös yhteiskunnan kehitystä ja olemassaoloa Syynä on se, että yksityisyydellä on moraalinen arvo yhteiskunnassa, jota suojaamalla yhteiskunta suojelee yksilöiden lisäksi itseään.[249]

---

247 Yhdysvaltalaisesta yksityisyydestä ja sen historiasta katso tarkemmin *Frederick S. Lane,* American Privacy. The 400-Year History of Our Most Contested Right. Beacon Press. USA 2009. Käsitteenä yksityisyys omaksuttiin Suomen lainsäädäntöön henkilötietolainsäädännön myötä 1980-luvun lopulla henkilörekisterilain säätämisen yhteydessä. Suomalaisessa oikeuskielessä yksityisyys on siis varsin uusi käsite.

248 HE 49/1986 vp s. 21.

249 Stahl, Privacy and Security as Ideology, s. 286–287.

Huoli yksityisyyden suojaamisesta on noussut johtavaksi puheenaiheeksi valtion ja yritysten valvontamahdollisuuksien kasvaessa. Yksilöt haluavat elää elämäänsä rauhassa ja kontrolloida sitä, kuinka heitä koskevia tietoja hyödynnetään. Yksilön suojaa ja oikeuksia tietojen käsittelyssä on tapana kuvata käsitteellä yksityisyyden suoja. Tietotekniikan kehittymisen kärjistämä mahdollisuus tiedostojen väärinkäyttöön on perinteisesti ollut eräs keskeinen yksityisyyden suojaamisen ongelma.[250] Demokraattisessa oikeusvaltiossa oikeus yksityisyyteen on tämän vuoksi saanut kasvavan merkityksen ja tätä oikeutta suojataan myös aiempaa tehokkaammin. Syynä tähän on yksilön itsemääräämisoikeuden voimistuminen. Itsemääräämisoikeuden taustalla on tarve turvata tehokkaasti yksityiselämä sekä henkilökohtainen vapaus ja koskemattomuus informaatioyhteiskunnassa, jossa etenkin julkisen vallan on helppo kerätä kenestä tahansa valtavasti tietoa ja myös yhdistellä näitä tietoja keskenään.[251]

Vaikka yksityisyys on kansallisesti ja kansainvälisestikin tunnustettu ja suojattu perusoikeus, ei sitä ole tarkoin määritelty.[252] Syynä tähän on todennäköisesti se, että kaikista perusoikeuksista yksityisyys on vaikeimmin määriteltävissä.[253] Yksityisyyden määrittelemisen vaikeus

250 Tämän ongelman on suomalaisessa oikeustieteessä tuonut esiin muun muassa Heikki Karapuu vuonna 1972. Katso *Karapuu,* Oikeus yksityiselämän suojaan, s. 14.

251 Näin myös *Kulla,* Biometriset tunnisteet ja tiedollinen itsemääräämisoikeus, s. 37.

252 Ensimmäisiä määrittelyjä yksityisyydelle on Warren&Brandeisin lause ”the right to be left alone” 1800-luvun lopulta. Artikkeli löytyy osoitteesta: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

253 Tämän on myös suomalainen lainsäätäjä ymmärtänyt, sillä yksityisyyttä ei ole lainsäädännössä määritelty. Lainsäätäjä on ilmeisesti jättänyt tarkoituksella yksityisyyden käsitteen käytännössä määriteltäväksi. Saarenpää huomauttaakin osuvasti siitä, että lainsäätäjän

ei kuitenkaan saa johtaa siihen, että yksityisyyden merkitys katoaa.[254] Määrittelyn vaikeudesta huolimatta yksityisyys on merkittävä yhteiskunnallinen suhdekäsite[255], jonka oikeudellinen määrittely on tarpeetonta ja erheellistä. Oikeus yksityisyyteen pysyy kuitenkin ennallaan, mutta sen sisältö ja tehokkuus vaihtelevat yhteiskunnan muutoksen mukana.[256]

Yksityisyyden lainsäädännöllinen määritteleminen ei ole järkevää pelkästään senkään takia, että määrittelyä ja sen mukaista sääntelyä jouduttaisiin yhteiskunnan ja teknologian kehittyessä jatkuvasti uusimaan. Tällöin yksityisyyden suojan ulottuvuudet voisivat Saarenpään mukaan kärsiä ns. lainsäätäjäriskin mukanaan tuomista satunnaisista viiveistä ja virheistä lainvalmistelussa.[257]

Oikeustieteellisenä yläkäsitteenä yksityisyyden määritteleminen yksityiskohtaisesti lisäisi todennäköisesti epätietoisuutta yksityisyyden

---

tehtävänä ei edes ole yksityisyyden määritteleminen. *Saarenpää,* Yksityisyys, yksityiselämä, yksilön suoja, s.319. Katso myös *Saarenpää,* Preface, Teoksessa Legal Privacy (2008) toimittanut Ahti *Saarenpää,* s. 9–16. Katso myös *Leith,* Privacy as Slogan, s. 100.

254 Solove on ilmaissut asian seuraavasti: "Privacy seems to encompass everything, and therefore it appears to be nothing in itself." *Solove,* Understanding Privacy, s. 7.

255 Yksityisyyttä voidaan pitää yhteiskunnallisena käsitteenä jo pelkästään siitä syystä, että yksityisyyden laajuus antaa kuvan tärkeistä arvoista yhteiskunnassa. Etzioni on todennut asian seuraavasti: "Both the scope of privacy and the nature of the specific acts that are encompassed by definitions of privacy reflect a society´s particular values." *Etzioni,* The Limits of Privacy, s. 197.

256 *Saarenpää,* Yksityisyys, yksityiselämä, yksilönsuoja, s. 319.

257 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 311. Sääntelyriskeistä katso tarkemmin Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, s. 45–46.

roolista yhteiskunnassa. Yksityisyyttä ei kuitenkaan tule nähdä sellaisena pyhänä käsitteenä, jonka sisältöä ei voisi muuttaa, sillä yksilön oikeuksien tulee elää yhteiskunnan ja kulttuurin mukana.[258] Vaikka yksityisyys on haasteellinen käsite määritellä, ei määrittelyn vaikeus saa johtaa siihen, että *"yksityisyys, integriteetti ja yksityiselämän suoja vilistävät kilvan käsitteistössämme milloin saman sisältöisinä ja milloin erisisältöisinä"*.[259]

Dynaamisen luonteensa vuoksi yksityisyyttä kannattaa lähestyä ensisijassa asiakokonaisuuksittain.[260] Tällöin huomio kiinnittyy niihin ilmiöihin tai oikeussuhteisiin, joiden puitteissa yksityisyys voi vaarantua, se on jo säänneltyä tai sen suojaaminen edellyttää asioiden lainsäädännöllistä järjestämistä.[261] Yksityisyyteen on katsottu kuuluvan tiedollinen ja fyysinen tai alueellinen ulottuvuus.[262] Näiden lisäksi yksityisyydessä on myös sosiaalinen ulottuvuus (kuvio 2). [263]

---

258 *Etzioni,* The Limits of Privacy, s.188. Neuvonen on sanonut saman toteamalla yksityisyyden käsitteen olevan suhteessa ihmiskuvaan ja aikakauteen. *Neuvonen,* Yksityisyyden suoja Suomessa, s. 22. Katso myös *Blume,* The Importance of Information Privacy and its Future, s. 161-162.

259 *Saarenpää,* Yksityisyys, yksityiselämä, yksilönsuoja, s. 319.

260 Näin myös *Solove,* jonka mukaan yksityisyyttä tulee lähestyä niiden alueiden kautta, joita se suojelee. Katso tarkemmin *Solove,* Understanding Privacy, s. 171.

261 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 311.

262 *Palm,* Privacy Expectations at Work – What is Reasonable and Why?. s. 202. Vertaa *Westin,* joka erottaa yksityisyydessä sosiaalisen ja tiedollisen puolen.

263 *van Dijk,* The Network Society, s. 121. Muista tavoista jakaa yksityisyys katso esimerkiksi *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 311–318 ja *Saarenpää,* Perspectives on Privacy, s. 26–40.

Fyysisessä yksityisyydessä on kysymys valikoidusta intimiteetistä. Yksilöllä on oikeus itse päättää ruumiiseensa kohdistuvista toimenpiteistä ja siitä kenet lähelleen päästää. Siihen on yhdistettävissä oikeus ruumiilliseen koskemattomuuteen, oikeus olla alueellisesti yksin erilaisen valvonnan ulottumattomissa sekä geneettinen yksityisyys. Geneettinen yksityisyys eli oikeus pitää geneettiset tietonsa salassa. [264]

Tiedollisen yksityisyyden kohdalla kysymys on oikeudesta valikoivaan paljastamiseen. Siinä ei ole kysymys pelkästään henkilötietojen suojasta[265], vaan myös yksilön tiedollisesta omistusoikeudesta ja anonymiteetistä. Tärkeä osa tiedollista yksityisyyttä on myös oikeus tulla arvioiduksi oikeassa valossa, jolloin kysymys on oikeudesta kunniaan.

Sosiaalisessa yksityisyydessä puolestaan on kysymys yksilön oikeudesta itse päättää suhteistaan toisiin erilaisen valvonnan ulottumattomissa. Kysymys on niistä rajapinnoista, joita meillä on muihin

---

Neuvonen, Yksityisyyden suoja Suomessa, s. 28. Katso myös *Stefanova,* Privacy on the Web, s. 149-150 sekä *Kleve, P. – De Mulder,* R.: Privacy Concerns in the Information Society, s. 79.

264 Erityispiirteidensä vuoksi geneettisten tietojen käsittely edellyttää perustellusti erityistä oikeudellista suojelua. Kun otetaan huomioon tieteellisen tutkimuksen edistyminen, geneettisistä tiedoista saatetaan pystyä tulevaisuudessa selvittämään nykyistä enemmän informaatiota, ja yhä useammat tahot saattavat pystyä käyttämään niitä erilaisiin tarkoituksiin. 29 artiklan mukainen tietosuojaryhmä, Geneettisiä tietoja käsittelevä valmisteluasiakirja 12178/03/FI WP 91 (2004), s. 4–5. Katso myös *Laurie,* Genetic Privacy: a challenge to medico-legal norms.

265 Toisinaan henkilötietojen suojan tärkeyttä painottaen puhutaan myös tiedollisesta kotirauhasta. Aihetta on myös mahdollista lähestyä informaatioväkivallan näkökulmasta *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 315. Informaatioväkivallasta katso tarkemmin *Saarenpää,* Informaatioväkivalta (2006).

yksilöihin, yhteisöihin, markkinoihin ja yhteiskuntaan. Sosiaalisessa yksityisyydessä on samalla kysymys identiteettiemme suojasta. Esimerkkinä sosiaalisesta yksityisyydestä on työelämän yksityisyys ja muut (osittain) rajoitetut yksityiselämän tilanteet, joissa yksilöllä säilyy rajoitteista huolimatta oikeus päättää käyttäytymisestään ja suhteistaan muihin.

Nämä yksityisyyden muodot ovat usein myös limittäisiä tai päällekkäisiä keskenään, ja näin yhteydessä toisiinsa. Anonymiteetti esimerkiksi tulee nähdä oikeutena, joka sisältyy kaikkiin näihin yksityisyyden osa-alueisiin.[266]

Kuvio 2. Yksityisyyden kategoriat.

Yksityisyyden dynaamisesta luonteesta ja yksityisyys-käsitteen määrittelyn vaikeudesta huolimatta yksityisyys tulee ymmärtää vapaan toiminnan alueeksi, jonka sisällä yksilöllä on oikeus toimia olematta

266 *Saarenpää,* Perspectives on Privacy, s. 40–41. Vertaa *Neuvonen,* Yksityisyyden suoja Suomessa, s. 29.

vastuussa tekemisistään toisille. Yksityisyys tulee nähdä yhteiskunnallisena lupana toimia rauhassa yhteiskunnassa ilman aiheetonta puuttumista tähän vapauden piiriin.[267] Yksityisyydessä on kysymys niin oikeudesta, sosiaalisesta rakenteesta kuin tunteesta, että on rauhassa ulkopuolisilta ja että voi määrätä itse itsestään.[268] Tällaisena se kiinnittyy hyvin voimakkaasti yksilön ihmisarvoon, sillä se antaa yksilölle mahdollisuuden päättää ihmisarvoisesta elämästä. Perinnäinen syy yksityisyyden suojaamiselle onkin se, että yksityisyys ei itsessään ole päämäärä, vaan keino saavuttaa muita päämääriä. Suojaamalla yksityisyyttä yhteiskunta pyrkii suojaamaan myös muita tärkeinä pitämiään arvoja.[269]

Pöysti on katsonut, että yksityisyyden toimivin ja kattavin määritelmä on niin sanottu restricted access -teoria, jossa yksityisyys hahmotetaan rajoitettuna luoksepääsy- ja hyödyntämisoikeutena. Yksityisyyttä määrittävät tekijät ovat tässä teoriassa salaisuus, anonymiteetti ja yksinäisyys. Teoriaan on yhdistettävissä ajatus julkisuuden piiristä, jossa yksityisyys on rajoitetumpaa kuin muissa yksityisemmissä tilanteissa. Tällöin yksityisyyden voidaan ajatella muodostuvan henkilöä ympäröivistä kehistä. Henkilöä lähinnä olevista asioista muodostuu yksityisin piiri, johon kohdistuvaa viranomaisten ja toisten henkilöiden puuttu-

267 *Etzioni,* The Limits of Privacy, s. 196. Vertaa *Smith,* Privacy. How to Protect What´s Left of It, s. 313. Mahkonen puolestaan kuvaa yksityisyyttä valvonnaksi sen suhteen, milloin ja kuka voi havainnoida meitä. *Mahkonen,* Oikeus yksityisyyteen, s.21.Ethan Katsh on puolestaan määritellyt yksityisyyden tiedollisesta näkökulmasta. Hänen mukaansa yksityisyydellä tarkoitetaan valtaa siitä, mitä tietoja sivullisten on mahdollista saada yksilöstä selville. *M. Ethan Katsh,* Law in a Digital World, s. 228.

268 *Neuvonen,* Yksityisyyden suoja Suomessa, s. 22.

269 Näistä arvoista katso *Westin,* Privacy and Freedom. Atheneum. 1967.

mista on erityisesti rajoitettu. Tätä suojattavaa aluetta on mahdollista kutsua yksityisyyden tai yksityiselämän piiriksi.[270]

Yksityisyys tulee nähdä ennen kaikkea moniarvoisena käsitteenä, jonka avulla yhteiskunta suojelee yksilölle tärkeitä ja suojaamisen arvoisia oikeuksia. Näin tehdessään yhteiskunta luo yksilölle vapauden tilan, jota kutsutaan yksityisyydeksi. Yksityisyys tulee nähdä ennen kaikkea yhteiskunnallisena arvona tai hyvänä, joka ei niinkään rajoita yhteiskunnan toimintaa, vaan suojelee sitä.[271]

Historia, kulttuuri ja kulloinkin voimassa oleva oikeusjärjestelmä ovat perinteisesti vaikuttaneet siihen, miten yksityisyyttä suojataan. *Caten* mukaan itseavulla, yhteisymmärryksellä, teknisillä sovelluksilla ja vapaaehtoisilla toimintaohjeilla saavutetut ratkaisut ovat usein toimivampia yksityisyyden suojaamisessa kuin julkisen hallinnon väliintulo. Julkisella hallinnolla on myös merkittävä rooli yksityisyyden suojaamisessa. Sen rooli ulottuu lähinnä kuitenkin toimivien periaatteiden, keskustelun ja yhteistyön aikaansaamiseen.[272] Julkisen hallinnon roolin pienenemiseen on syynä se, että yksilön vastuu tekemisistään on yksityisyyden suojaamisessa tehokkaampi keino kuin lailla säätäminen.

Yksityisyyden taso riippuu siitä, kuinka paljon ja mitä tietoa yhteiskunta tarvitsee. Keskeistä on, minkälaisessa roolissa eri osapuolet esiintyvät ja minkälainen alistumisvelvollisuus asemansa vuoksi voi-

---

270 *Pöysti,* Tehokkuus, informaatio ja eurooppalainen oikeusalue, s. 487–488. Pöysti katsoo, että tällainen yksityisyyden piirien varaan rakentuva teoria on myös Suomen perustuslakiin otettujen yksityiselämän suojaa ja yksityisyyttä koskevien perusoikeussäännösten pohjana. Vertaa *Moor,* Towards a Theory of Privacy in the Information Age, s. 30–31, Katso myös Simmel, "Privacy", s. 480.

271 *Solove,* Understanding Privacy, s. 174. Katso myös *Goold,* How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy and the Political Value of Privacy.

272 *Cate,* Privacy in the Information Age, s. VIII.

daan tuossa tilanteessa katsoa olevan sillä, jonka yksityisyyteen halutaan puuttua. Yksityisyyden suojan toteutuminen on subjektiivista ja riippuu asiayhteydestä.[273]

Toisaalta yksityisyys ja sen suojaaminen ei myöskään ole sen enempää haitallista kuin hyödyllistä. Kuten Westin on asian ilmaissut: jokaisen tulee oman kulttuurinsa, asemansa ja henkilökohtaisen tilanteensa puitteissa tehdä jatkuvia valintoja eristäytyneisyyden ja kumppanuuden, intimiteetin ja sosiaalisen kanssakäymisen, anonymiteetin ja yhteiskunnallisen osallistumisen sekä pidättyvyyden ja julkiseksi tuomisen välillä.[274]

Vanha vastinpari yksityisyys / julkisuus ei ole menettänyt merkitystään, vaan pikemminkin sen merkitys on kasvanut. Olemme siirtyneet yhteiskuntaan, jossa avoimuus ja julkisuus ovat johtavia periaatteita. Nämä periaatteet ovat kuitenkin vaikeasti sovitettavissa yhteen yksityisyyden suojan kanssa. Tämä on myös yksi syy siihen, miksi yhä voimakkaammin käydään keskustelua yksityisyyden suojasta, sen tarkoituksesta ja merkityksestä niin yksilön kuin yhteiskunnan kannalta. Tähän keskusteluun teknologinen kehitys tuo mukanaan jatkuvasti uusia huomioonotettavia näkökohtia. Esimerkkinä toimii biometrinen tunnistaminen, jolla on omat vaikutuksensa yksityisyyden ja julkisuuden väliseen suhteeseen.

Kuten edellä on käynyt ilmi, yksityisyys on yksi haastavimpia ilmiöitä verkkoyhteiskunnassa. Ihmisoikeudet takaavat oikeuden yksityisyyteen, mutta tämän oikeuden toteuttaminen ja takaaminen digitaalisessa toimintaympäristössä on käymässä entistä vaikeammaksi. Uudet teknologiat tarjoavat laajat mahdollisuudet valvonnalle.

---

273 Eduskunnan oikeusasiamiehen ratkaisu, Valokuvaaminen Kelan toimistossa (Dnro 1140/4/11), s. 4.

274 *Westin,* Privacy and Freedom, s.42. Katso myös *Cate,* Privacy in the information age, s. 31.

Kysymys ei kuitenkaan ole pelkästään teknologinen. Tarvitaan laadukasta lainsäädäntöä ja järjestelmien suunnittelua. Lähtökohtana tulee olla ajankohtaiset oikeudelliset kysymykset. Yksityisyyden tyhjentävää määrittelyä tulee kuitenkin välttää, sillä yksityisyys on jatkuvasti kehittyvä käsite. Yhteiskunnallinen ja teknologinen kehitys nimittäin tuovat jatkuvasti mukanaan uusia haasteita yksityisyydelle ja samalla muokkavat vanhoja käsityksiä yksityisyyden sisällöstä.[275]

Teknologialla, erityisesti informaatioteknologialla, on oma merkityksensä siihen, miten yksityisyyteen ja sen eri näkökohtiin suhtaudutaan yhteiskunnassa.[276] Yksityisyyden asemaan yhteiskunnassa vaikuttaa hyvin voimakkaasti se, mikä näkökulma yhteiskunnassa halutaan ottaa teknologiaan. Tästä toisaalta aiheutuu yksityisyys-käsitteen heikkous ja vahvuus. Yksityisyyttä ei tule pitää itsestäänselvyytenä.

Biometrisen tunnistamisen kohdalla yksityisyyden ymmärtäminen edellyttää edellä esitetyn vuoksi laista ilmenemättömien sosiaalisten arvojen etsimistä ja jäljittämistä. Yksityisyys ei käy ilmi pelkästään sen lainsäädännöllisistä takeista. Yksityisyyden sosiaaliset arvot eivät välttämättä käy ilmi voimassa olevasta oikeudesta, sillä teknologiassa, tieteessä ja poliittisissa käytännöissä tapahtuvat muutokset eivät lainsäädännössä tule säännöllisesti huomioiduiksi.[277] Lainsäädännön tekstit ovat tämän vuoksi vain lähtökohta yksityisyyden arvojen ymmärtämi-

275 Näin myös *Solove,* Understanding Privacy, s. 188 ja 196–197.

276 *Minkkinen,* Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change, s. 49.

277 Minkkinen on viitannut tähän yksityisyyden suojan tulevaisuutta koskevassa artikkelissaan. Hänen mukaansa lainsäädäntö on vain yksi osa yksityisyyden suojaa ja tämän vuoksi yksityisyyden suojan ymmärtämisessä ei pitäisi katsoa pelkästään lainsäädäntöä. *Minkkinen,* Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change, s. 54–55.

sessä, koska jatkuvasti muuttuvien sosiaalisten arvojen välittäminen lainsäädännön kieleen on vaikeaa.

Luonteestaan huolimatta oikeus yksityisyyteen ei ole ehdoton eikä aukoton. Yhteiskunta ja demokratia olisivat tällöin mahdottomia. Oikeus yksityisyyteen on myös dynaaminen, jatkuvassa muutoksessa oleva oikeus. Tähän muutokseen vaikuttavat nykyään ennen kaikkea eurooppalaisen demokraattisen oikeusvaltion, yhteiskunnan sekä teknologian kehitys.[278]

Muuttuvasta luonteestaan huolimatta ihmiset tarvitsevat yksityisyyttä myös tulevaisuudessa. Teknologisen kehityksen seurauksena yksityisyyden merkitys hyvin suurella todennäköisyydellä korostuu. Tulee kuitenkin muistaa, että muutos on tarpeen yksityisyyden suojaamiseksi oikeudellisin keinoin.[279]

3.2.2. Yksityiselämän suoja

Arkielämässä yksityiselämän suojaa pidetään niin itsestään selvänä, että siihen kohdistuvaa loukkausta ei välttämättä edes huomata, ellei loukkaus kohdistu itseen tai läheiseen. Teknologian kehittyessä ei kuitenkaan enää hyväksytä kaikkia teknologisen kehityksen mukanaan tuomia kontrollimuotoja.

Yksityiselämää[280] koskevat normit ovat eräs keskeisimpiä kokonaisuuksia suomalaisessa oikeudessa. Jokaisella tulee olla yksityinen tila,

278 *Saarenpää,* Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan, s. 1.

279 *Blume,* The Importance of Information Privacy and its Future, s. 169.

280 Viljanen tulkitsee Euroopan ihmisoikeussopimuksen soveltamiskäytännön pohjalta perustuslain säännöksen yksityiselämän suojasta sisältävän ainakin henkilökohtaisen identiteetin suojan, moraalisen ja fyysisen koskemattomuuden, riittävän yksityisyyden turvaavan tilan, henkilötietojen keräämisen ja niiden käytön, sukupuolisen käyttäy-

jossa olla ja toimia itsenäisesti suhteessa toisiin ihmisiin ja yhteisöihin. Tarve yksityiselämän ja siihen liittyvän henkilökohtaisen koskemattomuuden suojaamiseen on ajatuksena ideologinen ja historiallinen. Sitä ei kuitenkaan löydy jokaisesta yhteiskunnasta, sillä sen toteuttaminen riippuu yhteiskunnassa kulloinkin voimassa olevista moraalisista ja poliittisista normeista.[281] Toisin sanoen, kukin yhteiskunta itse päättää, suojataanko ja miten tehokkaasti yksityiselämää.

Yksityisyyden tavoin myös yksityiselämän käsite on erittäin vaikeasti määriteltävissä. Selvää kuitenkin on, ettei yksityiselämän suojan merkitystä tule kiistää, vaikkei sitä tarkoin määriteltäisikään. Nyky-yhteiskunnassa kukaan ei voi elää täydellisessä yksityisyydessä. Jokaisen on hyväksyttävä se, että hänen yksityisyyttään ja yksityiselämää voidaan rajoittaa ja että siihen on mahdollista puuttua.

Olemme osa laajempaa kokonaisuutta, jonka toiminta häiriintyy yksityisyyden ollessa absoluuttinen ja ehdoton. Toisaalta kaikki toiminta ei voi myöskään olla täysin julkista, sillä siitä aiheutuu itsemääräämisoikeuden merkityksen vähentyminen. Tällainen ajatus täysimääräisestä paljastamisesta on sietämätön, sillä jokaisella tulee olla se henkilökohtainen tila, jossa olla rauhassa muilta ja yksin omien ajatustensa kanssa.

Tämä ”henkilökohtainen rauhan tila” on yksityisyyden ja yksityiselämän suojan ydin.[282] Tulee löytää tasapaino totaalisen yksityisyyden ja totaalisen julkisuuden välille. Tätä ei kuitenkaan ole mahdollista määrittää niin tarkasti, että se olisi toimiva. Oikeudelliset säännöt ja käytännön elämä vaihtelevat niin paljon, että tarkan rajan vetäminen

---

tymisen sekä oikeuden henkilökohtaisiin suhteisiin muiden ihmisten kanssa. *Viljanen,* Perusoikeusuudistus ja kansainväliset ihmisoikeussopimukset, s. 802.

281 *Blume,* Personregistrering (1996), s. 13–15

282 HE 84/1974 vp, s.3.

yksityisen ja julkisen välille on erittäin hankala tehtävä.[283] Yksityiselämän suojan tarkka määrittäminen ei ole järkevää, sillä määrittäminen voisi johtaa siihen, että sen alaa olisi vaikea myöhemmin esimerkiksi tulkinnan avulla muuttaa.

Yksilön suojaa ja oikeuksia tietojenkäsittelyssä on tapana kuvata käsitteellä yksityisyyden suoja. Tätä käsitettä käytetään toisinaan samassa merkityksessä kuin käsitettä yksityiselämän suoja.[284] Yksityisyyden suoja on kuitenkin käsitteistä laajempi, sillä yksityiselämän suoja on osa yksityisyyden suojaa. Yksityisyyden suojaan kuuluu myös yksilön oikeus tietää itseään koskevien tietojen käytöstä, kuten myös oikeus päättää näiden tietojen käytöstä.[285] Yksityisyyden suoja on käsitteistä laajempi jo senkin vuoksi, että yksityiselämän suoja omalta osaltaan turvaa yksityisyyden suojaa.[286]

Persoonallisuusoikeuden ja oikeusinformatiikan tutkimuksessa sekä eräissä laeissa yksityisyyden suoja on omaksuttu yleiskäsitteenä.[287] Vaikka käsitteiden käyttö on hiljalleen vakiintumassa, näitä käsitteitä – yksityiselämän suoja ja yksityisyyden suoja – käytetään suomalaisessa oikeustieteessä sekä oikeuskäytännössä epätarkasti myös rinnasteisina käsitteinä. Suomen perustuslakiin on kuitenkin valittu

283 *Blume,* Personregistrering, s. 14. Näin myös *Karapuu,* Oikeus yksityiselämän suojaan, s. 18.

284 Katso esim. *Karapuu,* Oikeus yksityiselämän suojaan, s. 1.

285 Saarenpään mukaan yksityisyyden keskeisiä osatekijöitä ovat yksityiselämän suoja, viestinnän luottamuksellisuus sekä henkilötietojen suoja. *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 240. Katso myös HE 75/2000vp., s. 13 sekä HE 96/1998 vp., s. 30. Katso myös KM 1997:9, s. 40.

286 Yksityisyyden ja yksityiselämän suojan hierarkkinen suhde nähdään kuitenkin hieman eri tavoin riippuen mm. oikeudenalasta.

287 Näistä laeista voidaan esimerkkinä mainita laki yksityisyyden suojasta työelämässä, luottotietolaki ja rikoslaki.

muoto yksityiselämän suoja. Lähtökohtana yksityiselämän suojaamisessa on yksilön oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä.

Biometrinen tunnistaminen ja yksityiselämän suoja ovat erittäin kiinteästi sidoksissa toisiinsa. Siinä puututaan yksityisyyden syvimpään kerrokseen. Sen ja yksityisyyden suojan välisen suhteen tasapainottamiseksi tarvitaan tunnistamisratkaisujen tarkoituksenmukaista kohdentamista sekä yksityisyyden suojan tarpeettomien loukkausten ehkäisemistä niin jälkikäteisesti kuin ennaltakin. Biometrinen tunnistaminen yleistyy ja tarve yksityisyyden ja yksityiselämän suojaamiselle on demokraattisessa oikeusvaltiossa entistä suurempi.

3.2.3. Henkilötietojen suoja

Oikeudellistuvassa valvontayhteiskunnassa henkilötietojen suojalla on korostunut merkitys. Se on myös entistä tärkeämpi osa oikeusjärjestelmää. Henkilötietojen suoja käsittää persoonallisuuden ja siihen on yhdistetty tiedollinen itsemääräämisoikeus. Taustalla vaikuttavat ajatus yksityiselämän suojasta ja toisen maailman sodan aikaiset kokemukset.

Henkilötietojen suoja on oikeudellinen peruskäsite. Sitä käytetään usein synonyyminä tietosuojan kanssa, vaikka nämä käsitteet eroavat toisistaan. Lakiteknisestä näkökulmasta henkilötietojen suoja on tietosuojalainsäädännön avulla toteutettavaa yksilön perusoikeuksien, usein yksityisyyden suojaa. Henkilötietojen suoja on ennen kaikkea yksilön suojaa, ei tietojen suojaa.[288] Tietosuojan taustalla on tai ainakin tulisi olla ihmiskäsitys. Kysymys on ihmistä koskevista tiedoista ja ihmisen oikeudesta yksityisyyteen.[289]

288 HE 125/2003 vp, s. 9.

289 *Saarenpää,* ATK ja yksilön suoja, s. 203.

Tietosuoja on kuitenkin vakiintunut kansainvälisesti käytetyksi ilmaisuksi puhuttaessa henkilötietojen suojan oikeudellisesta sääntelystä.[290] Ensisijaisesti tavoitteena on suojata luonnollisia henkilöitä ja heidän oikeuksiaan, ei vain tietoja. Käsite tietosuoja onkin osin harhaanjohtava. Tietosuojalainsäädäntö suojaa yksilöitä ja heidän perusoikeuksiaan henkilötietojen avulla toteutettavaa informaatioväkivaltaa vastaan.

Henkilötietojen suoja tai tietosuoja on käsitteenä sinänsä vaikeasti määriteltävissä ja rajattavissa. Esimerkiksi *Paul de Hertin ja Serge Gutwirthin* mukaan tietosuoja on luonteeltaan eräänlainen henkilötietojen käsittelyyn liittyvä yleiskäsite.[291]

Määrittelemättömyydestä huolimatta henkilötietojen suojan käsite on viime vuosikymmenien aikana vakiintunut osaksi eurooppalaista oikeuskäsitystä. Kehitys on alkanut 1970-luvun alkupuolella automaattisen tietojenkäsittelyn herättämästä huolesta, joka konkretisoitui useissa maissa vaatimuksiin tietosuojalakien aikaansaamisesta.[292]

Tietotekninen kehitys ei 1970-luvun jälkeen ole hidastunut. Tämän vuoksi henkilötietojen suojan tarpeellisuus on Nissenbaumin mukaan perusteltavissa seuraavilla tekijöillä: a) tallennettavissa olevien tietojen määrä on käytännössä loputon, b) tietojen pohjalta tehtävien

290 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 318–319.

291 *De Hert – Gutwirth*: Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, s. 3. Bygrave puolestaan puhuu tietosuojasta kahdessa merkityksessä: 1) henkilötietojen käsittelyä koskevana lainsäädäntönä ja 2) toimintana, johon saattaa kuulua tai olla kuulumatta lainsäädännöllisiä tekoja. *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 21.

292 *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s.93–95

analyysien laajuuden rajana on vain ihmisen kekseliäisyys ja c) tiedot on säilytettävissä käytännössä ikuisesti.[293]

Oman osansa henkilötietojen suojan tarpeellisuuteen on tuonut teknologisen kehityksen mahdollistamien uhkien realisoituminen 1980-luvulta alkaen ja viimeistään 2000-luvun ihmisiin kohdistuvassa valvonnassa ja kansainvälisessä tietojenvaihdossa.[294]

Yhteiskunnallisena peruslähtökohtana henkilötietojen suojaa tarkasteltaessa on perinteisesti ollut vallan ja vallankäytön näkökulma. Ihmisellä on demokraattisessa oikeusvaltiossa itsemääräämisoikeutensa nojalla ja siihen liittyen yksityisyytensä puitteissa oikeus pysytellä merkittävässä määrin yksin erilaisten valta- ja valvontajärjestelmien ulottumattomissa.[295] Henkilötietojen suoja on myös suojaa valvontaa vastaan.[296]

Henkilötiedot ovat kuitenkin tarpeellisia erityisesti hyvinvointivaltion palvelujen tarjoamiseen, väestön hallinnointiin kuin myös kaupallisiin tarkoituksiin. Yhteiskunnan toiminnan tehostaminen, palveluiden käyttäminen ja tehokas toiminta markkinoilla edellyttävät yksilön luopuvan osasta yksityisyyttään. Henkilötietojen suojan keskeinen tehtävä on niiden ehtojen järjestäminen, joiden puitteissa henkilötietoja on sallittua käsitellä. Henkilötietojen käsittely on jaettavissa hyvään ja huonoon byrokratiaan. Hyvän byrokratian edellyttämä henkilötietojen

293 *Nissenbaum,* Protecting Privacy in a Information Age: the Problem of Privacy in Public, s. 576

294 Näin myös *Koillinen,* Henkilötietojen suoja itsenäisenä perusoikeutena, s. 172 sekä *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 100–101.

295 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 321.

296 Schartumin ja BYgraven mukaan tietosuojaa voidaan lähestyä integriteetin, päätöksenteon ja vallankäytön näkökulmista. *Schartum–Bygrave,* Personvern i informasjonssamfunnet, s. 27–28. Katso myös NOU 1997:19, s. 21–24.

käsittely suoritetaan yksilön oikeuksien toteuttamiseksi hyvinvointivaltiossa (kysymys on toisin sanoen hyvän hallinnon toteuttamisesta yhteiskunnassa). Huonon byrokratian henkilötietojen käsittely puolestaan johtaa yksilön valvontaan vallan väärinkäytön välineenä. Yhtenä syynä tietosuojan kehittymiseen on tämän vuoksi ollut pelko siitä, että henkilötietojen lisääntyvä kerääminen ja käsittely uhkaavat demokraattisen yhteiskunnan perusteita mahdollistamalla yksilön valvonnan ja seuraamisen tämän henkilötietojen avulla.[297]

Yksilöön ja hänen yksityisyytensä kohdistuva laaja informaation kokoaminen sekä sen avulla tapahtuva valvonta vallan ja sen mahdollisen väärinkäytön välineinä ovat nyky-yhteiskunnassa vallitsevan ihmiskäsityksen vastaisia. Tarkkailuun sekä valvontaan on lupa ryhtyä vain lainsäädännön tämän erikseen perustellusti salliessa.[298]

Informaation käsittelyn merkitykseen vallankäytön kannalta on havahduttu eri maissa eri aikoina eri tavoin. Kansallisesti asenteiden myönteisyyteen henkilötietojen suojaa kohtaan riippuu teknologian kehityksestä sekä historiallisista ja kulttuurisista tekijöistä.[299]

Käsittelyn tehokkuutta tasapainottava henkilötietojen suoja on saanut positiivisoikeudellisen ilmiasunsa oikeusjärjestyksen perusteita määrittäviin eurooppalaisiin perus- ja ihmisoikeusnormistoihin sekä joihinkin kansallisiin valtiosääntöihin. Abstraktin tason perus- ja ihmisoikeussäännökset muodostavat henkilötietojen suojaa koskevien kansainvälisten sopimusten ja suositusten, EU-lainsäädännön ja kansallisten tietosuojalakien kanssa verraten laaja-alaisen ja peri-

297 *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 107.

298 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 321

299 Toisen maailmasodan konkreettiset kokemukset henkilötietojen käytöstä väkivallan välineinä Norjassa ja Saksassa ovat olleet omiaan nostamaan tietosuojan arvostusta näissä maissa. *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 321.

aateorientoituneen, mutta samalla myös tiheän ja yksityiskohtaisen oikeusnormiston.[300] Suomessa on voimassa henkilötietodirektiivin implementointina pidettävän henkilötietolain ohella suuri joukko laintasoisia erityissäänteleyitä. Henkilötietojen suoja koostuu yksityisen oikeusasemaa määrittävien perusratkaisujen lisäksi melko teknisestä sääntelystä.

Suomalaisittain henkilötietojen suojaa ja yksityisyyttä sekä tietosuojalainsäädännön merkitystä arvioitaessa tulee toisaalta ottaa erikseen huomioon julkisuusperiaatteen[301] yhteiskunnallinen merkitys. Julkisuusperiaatteen mukaisesti julkisina tarjolla olevien henkilötietojen käsittelyn avulla on perinteisesti luotu erilaisia kuvia ihmisistä, heidän identiteeteistään ja heidän yksityisyydestään. Rajoitettaessa henkilötietojen käsittelyä syntyy väistämättä jännitteitä henkilötietojen suojan ja julkisuuden välillä.[302] Henkilötietojen suojasta ja tietosuojalainsäädännöstä puhuttaessa on aina erityisen tärkeää muistaa kysymyksen olevan ihmisoikeusperusteisesta perusoikeuksien suojasta.[303]

---

300 *Koillinen,* Henkilötietojen suoja itsenäisenä perusoikeutena, s. 172.

301 Julkisuusperiaatteesta tarkemmin katso Mäenpää, Julkisuusperiaate.

302 Suhteessa julkisuusperiaatteeseen on toisaalta muistettava henkilötietojen suojan pääsääntöisesti sivuuttavan julkisuusperiaatteen siltä osin kuin kysymys on henkilötietojen käsittelystä. Tähän on syynä se, että ensisijaisesti suojataan ihmistä. Tämä on henkilötietodirektiivin yksiselitteinen lähtökohta ja tämä on vastaavasti henkilötietolain ja julkisuuslain keskinäisen suhteen järjestämistapa. *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 322–323.

303 Näin myös *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 235. Myös Eduskunnan perustuslakivaliokunnan käytäntö on osoittanut henkilötietojen suojan olevan korkeassa asemassa suomalaisessa yhteiskunnassa. Katso PeVL 14/2002 s. 2, PeVL 51/2002 s.2, PeVL 35/2004 s.2, PeVL 30/2005 s. 3 ja PeVL 19/2012 s. 3.

Henkilötietojen suojan merkityksen korostuminen on osoituksena siitä, että yksityisyyden tiedollinen puoli on saanut korostuneemman merkityksen. Henkilötietojen suoja on se osa oikeusjärjestelmää, jonka tehtävänä on tiedollisen yksityisyyden ja muidenkin luonnolliseen henkilöön liitettävissä olevien tietojen suojaaminen.[304]

3.3. Identiteetti

Identiteetistä on kirjoitettu paljon eri tieteissä. Psykologisessa mielessä identiteetti kuvataankin yleensä vastauksena kysymykseen ”Kuka minä olen?”. Tällöin identiteetti on kuvaus ihmisestä ja hänen mielestään. Mitä vaaditaan minuuden ja sen identiteetin luomiseksi? Ensimmäisenä tulee varmasti mieleen nimi. Nimi ei kuitenkaan ole vielä riittävän yksiselitteinen luomaan identiteettiä. Tarvitaan myös muuta, kuten sosiaaliset suhteet, suhteet omaisiin, ystäviin, työpaikkoihin ja viranomaisiin. Kaikilla näillä on oma tärkeä osuutensa identiteetin luomisessa.

Identiteetti on tämän tutkimuksen kannalta keskeinen käsite. Se toimii sosiaalisessa vuorovaikutuksessa perustavana rakenteena. Kasvokkain tapahtuva vuorovaikutus sisältää runsaasti luotettavuutta lisääviä merkkejä, jotka kertovat identiteetistä. Vaatteet, äänet, ulkomuoto ja keho lähettävät viestejä asemasta, vallasta ja roolista ryhmässä. Kyky tunnistaa muita riippuu paljon mahdollisuuksista havaita ja arvioida muiden toimia. Fyysisessä maailmassa ruumis itsessään tarjoaa käyttökelpoisen ja välttämättömänkin perustan identiteetille.

Identiteetti näyttelee avainroolia myös digitaalisessa maailmassa. Tällöin osapuolten identiteetin tietäminen on oleellista, jotta kyetään ymmärtämään vuorovaikutusta ja arvioimaan sen merkitystä. Digi-

304 *Pitkänen – Tiilikka – Varma,* Henkilötietojen suoja, s.1–2

taalisessa maailmassa identiteetti on myös hyvin ongelmallinen, sillä useimmat fyysisessä maailmassa ilmeiset persoonallisuuden ja sosiaalisen roolin peruspiirteet eivät ole käytettävissä. Digitaalinen maailma koostuu informaatiosta, jota ei kahlitse ruumiin yhtenäistävä ja vakauttava ankkuri. Todellisuudessa nämä kaksi maailmaa, fyysinen ja digituaalinen, eivät ole eronneet. Digitaalisen identiteetin takaa löytyy aina fyysinen toimija. [305]

Lähtökohtaisesti on ajateltavissa, että yhdessä ruumiissa on yksi identiteetti, vaikka minä voi olla hyvinkin monimutkainen, muuttuva ja epävakaa eri tilanteissa ja aikoina. Jokaisella yksilöllä on oma yksilöllinen ja ainutkertainen identiteetti, joka koostuu muun muassa mielikuvista, asenteista ja tunteista.[306] Tämän vuoksi identiteetti on mahdollista ymmärtää monella eri tavalla.

Allardt on kuvannut ihmisen identiteettiä seuraavasti: *”Ihmisen identiteetti rakentuu pääasiassa siitä, että hän kuuluu yhteen tiettyjen yksilöiden tai ryhmien kanssa: hän tarvitsee yhteisöjä ja ryhmiä, jotka määrittelevät, keiden kanssa hän kuuluu yhteen.*[307] ”*Lawrence Lessig* puolestaan kuvaa ihmisen identiteettiä tiedollisesta näkökulmasta. Hänen mukaansa identiteetissä ei ole kysymys vain siitä, kuka olet, vaan se kattaa myös kaikki sinusta saatavissa olevat todenmukaiset tiedot. Tällöin identiteetti kattaa nimen, sukupuolen, asuinpaikan, ajokortin numeron, henkilötunnuksen, ostokset Amazon.comista, ammattitiedot jne.[308]

---

305 *Heinonen,* Digitaalinen minä, s. 64

306 Identiteetin teoriassa yhtenä lähtökohtana on pidetty sitä, että identiteetin ytimessä on ajatus itsestä tietyn roolin haltijana. *Stets,* Justice, Emotion, and Identity Theory, s. 105.

307 *Allardt,* Ihminen ja moraali hyvinvointivaltiossa, s. 24. . Katso myös *Cast,* Identities and Behavior, s. 43. Identiteetistä sosiaalisena roolina katso myös *Stone, G.P.,* Appearance and the Self. s. 86–118.

308 *Lessig,* Code and Other Laws of Cyberspace (1999), s. 30–31.

Neethlingin näkemys identiteetistä tuo esiin sen, että identiteetin avulla jokainen yksilö on mahdollista erottaa toisistaan, identifioida. Hänen mukaansa identiteetillä tarkoitetaan ihmisen yksilöllisyyttä, joka määrittää tai yksilöi ihmisen erottaen hänet toisista.[309] Neethlingin määritelmä tuo havainnollisella tavalla esille sen tosiasian, että nyky-yhteiskunnassa identiteetti ei ole merkityksellinen vain yksilön, vaan myös yhteiskunnan kannalta. Neethlingin määritelmässä on kysymys kuitenkin vain yhdestä identiteetin ulottuvuudesta, oikeudellisesta tai hallinnollisesta identiteetistä. Esimerkkinä on henkilötunnus. Sen avulla jokainen kansalainen erotetaan yksiselitteisesti toisistaan. Henkilötunnus ei kuitenkaan ole keino varmistaa, että henkilö todella on se, keneksi tunnus hänet ilmoittaa. Perusteena on se, että henkilötunnus on vain koodipohjainen, osin satunnainen kyltti, jonka tietokone on antanut ihmiselle hänen syntyessään. [310]

Jokaisella on oma identiteettinsä, oma minä. Sillä on liittymäkohtia mitä erilaisimpiin asioihin yhteiskunnassa. Tämän lisäksi identiteetti on luonnollinen, filosofinen, psykologinen ja esimerkiksi kulttuurinen tutkimuskohde. Tämän vuoksi yksilön identiteettiä tulee tarkastella useamman eri tieteen näkökulmasta.

Identiteetin määritteleminen on haasteellista, sillä käsitteen luonteeseen kuuluu jatkuva kehittyminen[311]. Digitaalinen identiteetti on

309 *Neethling,* Personality rights: A comparative overview, s. 234. Vertaa *Brennan,* Conditions of Identity, s.5.

310 *Heinonen,* Digitaalinen minä, s. 16. Katso myös *Taylor,* Sources of the Self: The Making of the Modern Identity.

311 Nabeth Identity of Identity, s. 24. Katso myös *Hall,* joka teoksessaan Identiteetti esittää kysymyksen: Kuka tarvitsee identiteetin käsitettä? Eräänä vastauksena tuohon kysymykseen Hall tarjoaa seuraavaa: Identiteetin käsite on jotain, mitä ei voi ajatella vanhaan tapaan, mutta jota ilman tiettyjä kysymyksiä ei voi ajatella lainkaan. *Hall,* Identiteetti, s. 246.

hyvä osoitus siitä, kuinka käsitys ihmisen identiteetistä on laajentunut digitaalisella aikakaudella.

Digitaalista identiteettiä on mahdollista tarkastella ainakin kahdella tapaa. *Ezioni* kirjoittaa teoksessaan Modern Organizations ihmisen sidonnaisuudesta erilaisiin organisaatioihin, jotka kontrolloivat jäsentensä toimintaa.[312] Myös ihmisen identiteetti on mahdollista nähdä sen suhteen kautta, joka meillä on erilaisiin yhteiskunnallisiin organisaatioihin.[313]

Allardt on tarkastellut organisaatioita erottamalla toisistaan hyötyorganisaatiot ja yhteisyysorganisaatiot. *Saarenpää* on kehitellyt ajatusta eteenpäin erottamalla toisistaan hyötyorganisaatiot, valtaorganisaatiot, palveluorganisaatiot, yhteisyysorganisaatiot ja virtuaaliorganisaatiot. Saarenpään mukaan meillä on verkkoyhteiskunnassa erilaisia identiteettejä, jotka vaihtelevat merkittävästi suhteessa erilaisiin organisaatioihin.

Digitaalinen identiteetti on *Saarenpään* erottelussa osa virtuaaliorganisaatioita (cyber community), jotka ovat tietoverkkojen yhteydessä toimivia ja yleensä erityistä oikeudellista rakennetta vailla olevia tosiasiallisia organisaatioita.[314] Erilaiset organisaatiot siis määrittävät identiteettiä, ja identiteetti vaihtelee eri organisaatioiden myötä. Digitaalisesta identiteetistä puhutaan silloin, kun ihmisen identiteetti nähdään osana virtuaaliorganisaatiota, jolloin myös tuo organisaatio määrittää ihmisen digitaalista identiteettiä. Digitaalisella identiteetillä tarkoitetaan tunnistetietoja, jotka osoittavat luotettavalla tavalla tunnusten käyttäjän olevan niiden käyttöön oikeutettu henkilö. Identiteetti osoittaa tällöin oikean henkilön. [315]

---

312 *Etzioni,* Modern Organizations (1964), s. 1 ja 58.

313 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 242.

314 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 242.

315 *Saarenpää,* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 48 ja *Saarenpää,* Ihmiskäsitys ja laki, s. 465.

Kysymys digitaalisesta identiteetistä kuuluu niihin uuden verkkoyhteiskunnan ilmiöihin, joihin ei juuri ole oikeustieteessä syvällisemmin havahduttu, joihin ei ole yksinkertaisia lainsäädännöllisiä ratkaisuja ja joiden kehitykseen vaikuttavat varsin monenlaiset intressit. Tilanne on varsin ongelmallinen, sillä digitaalisesta identiteetistä on tulossa eräänlainen välttämättömyys verkkoyhteiskunnassa. Verkkoyhteiskunta ja sen elektronin hallinto rakentuvat verkkokommunikoinnin varaan. Lisäksi identiteetti on ajattelutapa ja siinä tarkatellaan yksilön oikeudellista liittymää yhteikuntaa.

Tämän vuoksi identiteettiä tulee oikeudellisestikin arvioida useasta eri näkökulmasta. Identiteetti ei oikeudellisestikaan ole yksiselitteinen asia. Kysymys ei ole ainoastaan ihmisen tarkasta tunnistamisesta, sillä identifiointi ja identiteetti ovat eri asioita. Tunnistamiseen riittää yleensä vähäisempi informaatio kuin kattavamman identiteetin muodostamiseen. Identiteetissä on kysymys monitasoisemmasta normatiivisesta ilmiöstä, joka on pääosin lailla sääntelemätön asia.[316]

Identiteettiä on mahdollista lähestyä oikeudellisesti tunnistetietojen, valvonnan, tietosuojan, markkinoiden, medioiden ja tietoturvallisuuden näkökulmasta.[317] Biometrisen tunnistamisen kohdalla näistä näkökulmista ovat merkityksellisiä erityisesti tunnistetietojen, valvonnan, tietosuojan ja tietoturvallisuuden näkökulmat.

Tunnistetietojen näkökulma. Peruslähtökohtana oikeudellisesta identiteetistä puhuttaessa on ihmisen tunnistaminen erilaisten tunnistetietojen ja niitä hyödyntävien asiakirjojen avulla. Tyypillisin tunnistetieto on ollut ja on ihmisen nimi. Sen rinnalle on eräissä maissa

316 *Saarenpää,* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 39 ja *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2012), s. 243. Näin myös *Sullivan,* Is Your Digital Identity Property?, s. 123.

317 Luettelo ei ole kattavaksi tarkoitettu. Sen tarkoituksena on vain valottaa oikeudellisen identiteetin monia kasvoja. *Saarenpää,* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 39–47.

syntynyt erilaisia henkilötunnuksia. Näiden ohella käytetään biometrisia tunnisteita, joista perinteisin on sormenjälki. Tietotekniikan kehittyessä biometristen tunnisteiden kirjo ja käyttötavat lisääntyvät. Huolena tällöin on biometristen tunnisteiden käytön lisääntyminen osana ihmisen valvontaa.

Valvonnan näkökulma. Tunnistetietojen käytöllä on pitkälti valvonnallinen tehtävä. Kysymys ei ole vain tunnistamisesta arkielämän perustilanteissa tai erilaisia oikeuksia vaadittaessa. Identiteetin näkökulmasta syyskuun 11. päivän terrori-isku on valitettava virstanpylväs. Sen vaikutukset heijastuvat juuri ihmisen identiteetin valvontaan. Terrorismin vastaisen taistelun nimissä valvontaa tunnistetietojen avulla on pyritty lisäämään kansallisesti ja kansainvälisesti. Esimerkiksi biometrisen passin käyttöönotto synnyttää jännitteen yksityisyyden ja henkilötietojen suojan sekä valvonnan välille.

Tietosuojan näkökulma. Perinteisillä tunnistetiedoilla pyritään täsmälliseen tunnistamiseen ihmisten erottamiseen yksilöinä toisistaan tai esimerkiksi heidän olinpaikkansa selvittämiseksi. Tietosuojalainsäädännöllä puolestaan pyritään rajoittamaan ihmisen tunnistamista niin täsmällisten kuin epätäsmällisten tietojen avulla. Tämän vuoksi tietosuojalainsäädäntö muodostaa kiistattoman kontrastin ihmisen valvonnalle tunnistetietojen avulla. Sen avulla pyritään sekä suojaamaan ihmisen yksityisyyttä, tekemään tunnistetietojen sallittu käyttö avoimeksi että yleisesti rajoittamaan henkilötietojen käsittelyä yhteiskunnassa.

Tietoturvallisuuden näkökulma. Verkkoyhteiskunnassa tietoturvallisuus on muodostumassa keskeiseksi tekijäksi ihmisten tunnistetietojen ja muiden henkilötietojen käsittelyssä. Tietoturvallisuudesta on tullut keskeinen verkkoyhteiskunnan oikeusperiaate: oikeus tietoturvallisuu-

teen. Oikeudellisessa katsannossa tietoturvallisuutta luonnehditaan perusoikeustasoiseksi oikeudeksi.[318]

Kuten edellä esitetyistä näkökulmista käy ilmi, identiteetti on oikeudellisessa katsannossa monitahoinen ilmiö.[319] Lähestyttäessä identiteettiä vain teknistyyppisenä ilmiönä pohtien, milloin ihminen on tai hänen tulee olla luotettavasti tunnistettavissa ja mikä tieto milloinkin on tarpeen, unohtuu ihmiskäsitys helposti. Oikeudellinen identiteetti on yksi ihmiskäsityksen keskeisiä kuvaajia. Saarenpää onkin sanonut: *"Se millaisen kuvan ihminen itse itsestään antaa ja millainen kuva ihmisestä annetaan ja sallitaan antaa häntä koskevan informaation avulla, on perustavaa laatua oleva ihmiskäsityksen mittapuu."*[320] Ihmiskäsitys on väistämättä sidoksissa sosiaaliseen identiteettiin, sillä demokratiassa yksilö on aina yhteisyysorganisaation jäsen.

Itsemääräämisoikeus on lähtökohta suhteessa eri organisaatioihin. Identiteetit puolestaan ovat liittymiä eri organisaatioihin sekä toisiin ihmisiin. Lähdettäessä säätämään yksilön oikeuksista ja velvollisuuk-

---

318 Saarenpää on esittänyt, että tietoturvallisuus on verkkoyhteiskunnassa eräänlainen metaperusoikeus. Kansalaisten perusoikeuksien toteutuminen verkkoyhteiskunnassa edellyttää tietoturvattua informationaalista toimintaympäristöä. Kysymys on informaatioinfrastruktuurin oikeudellisesta arvioinnista perusoikeuksien näkökulmasta. Verkkoyhteiskunnassa ihmisillä on oikeus tietoturvaan ja henkilötietojen käsittelijöillä on velvollisuus tietoturvan toteuttamiseen. *Saarenpää* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 47. Katso myös Tietoturvallisuus ja laki 1997.

319 Korhonen onkin nostanut erääksi oikeusinformatiikan kansainväliseksi haasteeksi yksilön identiteetin väärinkäytökset. Suurimpana esimerkkinä tästä on identiteettivarkaus. *Korhonen,* Oikeusinformatiikan kansainvälisiä haasteita tietoverkkojen yhdentyvässä maailmassa, s.185.

320 *Saarenpää,* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 52.

sista puututaan itsemääräämisoikeuteen ja vaikutetaan identiteetteihin.

Yksityisyys eri suojamuotoineen puolestaan on merkittävin väline identiteetin ulkoisen suojan järjestämisessä. Tämän merkitys korostuu verkkoyhteiskunnassa.[321] Itsemääräämisoikeutensa puitteissa ihmisellä itsellään on ensisijainen oikeus päättää siitä, millaisena hän näkyy organisaatioissa sen muille jäsenille. Vastaavasti ihmisellä itsellään tulee olla oikeus myötävaikuttaa siihen, millaisen kuvan organisaatiot luovat ja välittävät yksilöä koskevan informaation avulla. Moderniin ihmiskäsitykseen kuuluu oikeus yksityisyyden suojaan sekä muita yksilöitä että yksityisiä ja julkisia organisaatioita vastaan.[322] Kysymys ei ole vain suojasta sanan varsinaisessa merkityksessä, vaan myös oikeudesta identiteetin suojattuun hyödyntämiseen niin sosiaalisissa yhteyksissä kuin erilaisen kommunikaation puitteissa.

Tämän hetkisen tietosuojalainsäädännön valossa onkin kysyttävä: Vaatiiko sääntely joitain yksittäisiä tai periaatteellisia muutoksia identiteetin tullessa yhä enenevässä määrin digitaaliseen, sähköiseen muotoon? Henkilötietolakia valmisteltaessa tuohon kysymykseen vas-

321 Kuten Franko Aas on asian todennut: "Identity is not marked by its unique biography and a certain internal development, but is rather adjusted to the computer´s ontology: composed of items of information that like Lego bricks can be taken apart and clearly understood as well as fit with other items of information in new configurations." *Aas,* From Narrative to Database: Technological Change and Penal Culture, s. 386.

322 Yksilön oikeus yksityisyyden suojaan pitää sisällään myös yksilön oikeuden identiteettiin perus- ja ihmisoikeustasoisena oikeutena. Eduskunnan oikeusasiamiehen ratkaisu Dnrot 1242/4/07, 1447/2/07 ja 1223/2/08 (antopäivä 8.6.2009). Oikeus identiteettiin on alkanut muodostua omaksi erilliseksi perusoikeudekseen.

tattiin kielteisesti. Tuolloin tietoverkkojen aikakausi oli vasta aluillaan. Nyt verkkoyhteiskunnan aikana olisi aika kysyä uudelleen.

3.4. Kontrollisidonnaisuus

Demokratian näkökulmasta kontrollisidonnaisuus on henkilö- ja persoonallisuusoikeuden keskeisistä käsitteistä kiintoisin ja vaikein. Yksilön oikeuksien näkökulmasta katsottuna kontrolli jää helposti havaitsematta. Huomio kiinnittyy oikeuksiin ja vapauksiin eikä niinkään niiden vastakohtiin eli valvontaan ja tarkkailuun.

Valvonnalla on perinteisesti tarkoitettu epäluotettavien yksilöiden valvontaa, tarkkailua ja seuraamista.[323] Vaikka tällainen määritelmä kuulostaa vanhakantaiselta, osoittaa se kuitenkin yhden oleellisen asian valvonnasta. Valvontaa harjoitetaan epäluottamuksen poistamiseksi.

Lyon puolestaan on ottanut valvonnan määrittelemiseen modernimman näkökulman. Hän kuvaa valvontaa persoonattomaksi henkilötietojen käsittelyksi, jonka tarkoituksena on vaikuttaa tietojen kohteeseen ja hallita tätä.[324] Tämä osoittaa sen, että nykyajalle tyypillisessä valvonnassa pääroolissa ei enää ole kysymys pelkästään epäluottamuksen poistamisesta, vaan kysymys on yksilöiden hallitsemisesta ja kontrolloimisesta. Valvonta tulee nähdä modernin valvontayhteiskunnan vallan käyttönä, jossa myös tunnistamisella on oma merkittävä osansa.

Vaikka valvonnasta ja sen yhteiskunnallisista vaikutuksista on kirjoitettu jo reilut kaksi sataa vuotta, on valvonnan harjoittamisen his-

---

323 *Fowler,* H.W. – *Fowler,* F.G., The Concise Oxford Dictionary, s. 1302. Katso myös *Lyon,* Surveillance, Power, and Everyday Life, s. 449, jossa Lyon tarkoittaa valvonnalla kaikenlaista huomion kiinnittämistä yksilöllisiin tietoihin kontrolloimiseksi, hallitsemiseksi ja vaikuttamiseksi.

324 *Lyon,* Surveillance Society: Monitoring Everyday Life, s. 2.

toria kuitenkin lähes yhtä pitkä kuin ihmisen oma historia.[325] Pitkästä historiastaan huolimatta valvonta ja sen harjoittaminen saivat tarkemmat muotonsa vasta niin sanotussa modernissa maailmassa. Valvonnasta tuli enemmän rutiinia ja järjestelmällistä, kun 1900-luvun puolivälistä lähtien alettiin ymmärtää uuden teknologian esimerkiksi tietokoneen mahdollisuudet valvonnassa.[326]

Teknologinen kehitys on puolestaan johtanut siihen, että automaattisen tietojenkäsittelyn myötä tietokoneille on uskottu valvojan tehtävä. Tietokoneiden avulla on mahdollista rekisteröidä ja säilyttää tietoja tunnistettujen ihmisten päivittäisistä rutiineista. Ubiikkiyhteiskunta[327] on näiltä osin siirtynyt ajassa taaksepäin pikkukylän naapurivalvontaan. Valvojina eivät kuitenkaan enää ole naapurit, vaan

---

325 *Lyon,* Surveillance, Power, and Everyday Life, s. 449.

326 Valvonta ja erityisesti sen tutkiminen ovat nopeasti lisääntyneet viimeisten kahden vuosikymmenen aikana. Syynä tähän on ollut ensinnäkin hallinnon ja uusien teknologioiden nopea kehitys. Toisaalta valvonnan tutkimista on edesauttanut jatkuvasti uusiutuva valvonnan teoriapohja. *Lyon,* The search for surveillance theories, s. 3.

327 Ubiikkiyhteiskunta on yleisnimitys tietoyhteiskunnan seuraavalle vaiheelle, jossa tieto- ja viestintäteknologia tunkeutuu kaikkiin paikkoihin ja elämäntilanteisiin. Ihmiset, esineet ja paikat ovat yhteydessä toisiinsa elektronisten tunnisteiden avulla. Sana ubiikki tulee englannin kielen termistä ubiquitous computing eli sulautettu tietotekniikka. Sanasto ei ole vielä vakiintunut, sillä samasta asiasta käytetään myös termejä uusi arjen tietoyhteiskunta, ambient intelligence ("läsnä-äly") tai jokapaikan tietotekniikka. Korja, Kameravalvonnan oikeudellinen sääntely…, s. 12.Karhula huomauttaa siitä, että kansalainen on ubiikkiyhteiskunnassa haavoittuvaisempi. Tähän on syynä se, että arjen ja yhteiskunnan elintärkeät toimet ovat ubiikkiympäristössä yhä syvemmin tietojenkäsittelystä ja kansalaisiin liittyvistä tiedoista riippuvaisia. Tiedoilla voi olla myös kansalaisen oikeuksia

näkymättömät tietojärjestelmät ja niiden tuntemattomat isännät. Muutoksen seurauksena tulee olemaan anonymiteetin mureneminen ja asteittainen häviäminen.

Tietotekniikalla on kaksi puolta. Ensinnäkin se helpottaa päivittäisiä toimintojamme, mutta toisaalta se myös altistaa käyttäjän valvonnalle ja manipulaatiolle. Näitä kahta puolta ei ole mahdollista erottaa toisistaan, sillä ne mahdollistavat toistensa olemassaolon.[328]

Digitaalisen verkkoyhteiskunnan aikakaudella valvonnan tekninen järjestäminen on yksinkertaistunut. Jo langattomien laitteiden perusominaisuuksiin kuuluva paikantuminen avaa mahdollisuuksia erilaiseen seurantaan. Tämän lisäksi videovalvonta, tekninen valvonta, paikantaminen, sulautetun langattoman tietotekniikan eri sovellukset, biometrinen tunnistaminen ja tietojärjestelmien yhteiskäyttö tarjoavat yhdessä mahdollisuuksia yksilön ja hänen toiminnan lähes reaaliaikaiseen seurantaan. Vaikuttaa siltä, että on helppoa rakentaa tehokas ja samalla myös salaisen valvonnan yhteikunta.

Havainnollisen esimerkin tieteen ja teknologisen kehityksen avaamista mahdollisuuksista valvonnalle tarjoaa DNA-tietojen käyttö ihmisen tunnistamisessa. Nykyisin lainsäädäntö antaa mahdollisuuden tehdä niin sanottu henkilönkatsastus DNA-näytteiden ottamiseksi ja tallentaa tuo tieto poliisin henkilörekisteriin.

Yhteiskunta on organisaatio, jolle yksilöiden erilainen valvonta on sekä välttämätön työväline että myös houkutteleva mahdollisuus organisaation toiminnan tehostamiseen. Mitä kattavampaa valvonta on, sitä helpommaksi organisaation toiminta ja sen vallankäyttö käyvät. Teknologian kehittyessä vastaavasti erilainen valvonta on monissa ti-

---

kaventavia ja yhteiskunnan toimintamalleja merkittävästi muuttavia vaikutuksia. Karhula, Sähköpaimen – kansalainen ubiikkiyhteiskunnan varjossa, s. 47.

328 Näin myös *Whitaker,* The End of Privacy…, s. 101.

lanteissa myös muiden kuin julkisen vallan organisaatioiden toiminnan arkipäivää. Onkin aihetta puhua valvotusta vapaudesta vapauden negatiivisessa merkityksessä.[329] Kontrollista puhuttaessa on huomattava, että negatiivisen kontrollin ohella demokratiassa on ja siltä edellytetään merkittävää määrää sosiaalisen turvallisuuden takaavaa sosiaalista kontrollia.[330]

Kontrolli on osa yleisen järjestyksen ja turvallisuuden ylläpitoa ja se on yhteiskunnan keskeisimpiä tehtäviä yksilöiden oikeuksien turvaamiseksi. Yksilön vapauden rajoittamisen taustalla on näin ollen usein kollektiivinen etu.[331] Rajoittamalla jonkun yksittäisen oikeuksia varmistetaan monien muiden oikeuksien toteutuminen.

Yksilöllä on perinteisesti katsottu olevan yhteiskunnan kokonaisedusta riippumaton oikeus päättää omasta kehostaan. Biometriset ominaisuudet kuuluvat tämän itsemääräämisoikeuden piiriin. Voiko lainsäätäjä siten tunkeutua yksilön itsemääräämisoikeuden alueelle

---

329 Valvotussa vapaudessa on pohjimmiltaan kysymys kontrolloidusta vapaudesta. Yksilön vapaus on sidottu organisaation harjoittamaan kontrolliin. Yksilö on tietyin edellytyksin vapaa toimimaan haluamallaan tavalla.

330 Sosiaalisesta kontrollista katso tarkemmin *Segerstedt,* Social control as sociological concept. Hyvän esimerkin sosiaalisesta kontrollista tarjoaa holhoustoimi. Holhouksesta katso tarkemmin *Saarenpää – Mattila – Mikkola,* Holhous – yhteiskunnallinen ongelma, Helsinki 1972

331 Tällainen perustelu valvonnan lisäämiselle on kuitenkin huonolla pohjalla, sillä melkein mikä tahansa asia on mahdollista oikeuttaa tällä tavoin. Wickins on ottanut asiaan kantaa seuraavasti: “public interest must be judged by considering the balance between individuals, i.e. the rights of a single individual must be balanced against other single individuals.” Katso tarkemmin *Wickins,* The Ethics of Biometrics, s.52.

yhteiskunnallisen edun nimissä? Ajatus, jonka mukaan yksilöllä on autonominen valta päättää pelkästään itseään koskevista asioista, on eräs länsimaisen moraalisen ja oikeustieteellisen tradition kulmakivistä. Yksilön itsemääräämisoikeudella on perinteisesti ollut merkittävä asema esimerkiksi teorioissa oikeudenmukaisesta yhteiskunnasta. Tämän vuoksi yksilö on lähtökohtaisesti ensisijainen yhteiskunnan intresseihin nähden.[332]

Järjestäytynyt yhteiskunta merkitsee aina henkilökohtaista luopumista jostain vapaudesta. Tätä tarkoittaen on mahdollista ajatella demokratian aiheuttavan pahan olon tunnetta. Toisten oikeudet rajoittavat oikeuksiamme. Tämä johtaa itsemääräämisoikeutemme supistumiseen.

Kontrolli ja valvonta ovat luonteeltaan paradoksaalisia, sillä niiden pohjimmainen tarkoitus on perusoikeuksien turvaaminen. Samanaikaisesti niitä voidaan kuitenkin käyttää perusoikeuksia loukkaavalla tavalla yksilöiden tarkkailuun ja valvontaan.[333]

---

332 *Saarenpää,* Ihmiskäsitys ja laki, s.466. Keskustelua yksilön ensisijaisuudesta yhteiskunnan intresseihin nähden on käyty ennen kaikkea elinluovutusten kohdalla. Katso tarkemmin Kumlander, Ruumiin arvo? Kuolleen elinluovuttajan oikeusaseman tarkastelua perus- ja ihmisoikeuksien näkökulmasta sekä Pahlman, Potilaan itsemääräämisoikeus. Katso myös Nieminen, Ihmisarvon loukkaamattomuus perus- ja ihmisoikeussuojan lähtökohtana.

333 Katso valvonnan paradoksista tarkemmin esimerkiksi *Liberatore,* Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union, s. 113 sekä *Lyon,* Globalising Surveillance. Comparative and Sociological Perspectives.

Kansalaisten massamuotoinen valvonta ei kuitenkaan ole uusi eikä tuore ilmiö, sillä jo Benthamin ajatukset panoptikonista[334] loivat pohjan kansalaisten massamuotoiselle valvonnalle ja kontrollille.[335] Vaikka Benthamin suunnitelmaa ei toteutettu, käytetään panoptikonia täydellisen valvonnan vertauskuvana. Tällaisena se on erittäin ajankohtainen nykyajan ubiikissa valvontaympäristössä, sillä sähköisten jälkien tallentuminen lukemattomiin paikkoihin luo aidon panoptisen valvonnan mukaisesti epävarmuutta ihmisissä. He eivät tiedä näistä käytännöistä ja vaikka tietäisivätkin, he eivät kykene niihin vaikuttamaan. Kun nykyään puhutaan panoptikonista, tarkoitetaan sillä kuvitelmaa jatkuvasta valvonnasta. Tämä ei kuitenkaan tarkoita sitä, että ihmiset olisivat aina valvonnan alaisina. Heidän on kuitenkin perusteltua olettaa näin olevan. Kun ihmiset olettavat, että heitä seurataan jatkuvasti, he sisäistävät säännöt ja normit ja elävät kuuliaisesti ja toivotulla tavalla.

Max Weber ymmärsi valvonnan merkityksen ja loi ajatuksen siitä, että byrokratian kehityksen avain on tieto ja sen merkitys hallinnolle. Hänen mukaansa modernin byrokraattisen valtion kyky hallita ja

---

334 Panopticonista tarkemmin katso *Bentham,* The Panopticon Writings. Katso myös Mathiesen, jonka mukaan panoptikonin vastakohtana voidaan puhua synoptisesta valvonnasta. Tällöin kysymys on tilanteesta, jossa suuri joukko tarkkailee harvoja yhteenkoottuja (esimerkiksi tv-ohjelma Big Brother). Panoptisen ja synoptisen valtarakenteen kehitys on ollut yhdenmukaista ja niillä on yhdessä aivan keskeinen merkitys valvontatehtävälle nyky-yhteiskunnassa. Mathiesen, I Michel Foucault´s "Panopticon" – en gjenvisitt.

335 Solove on tähän liittyen todennut: "The Panopticon is a device of discipline; its goal is to ensure order, to prevent plots and riots, to mandate total obedience. The Panopticon achieves its power through ingenious technique of surveillance, one that is ruthlessly efficient." *Solove,* The Digital Person, s. 30.

valvoa perustuu sen kykyyn tietää yhteiskunnasta ja sen kansalaisista. Tässä tarkoituksessa valtion tehtävänä on sosiaalisen, taloudellisen ja teknisen infrastruktuurin tuottaminen kansalaisilleen sekä sääntöjen ja lakien asettaminen niiden käyttämiselle. Tietojen avulla hallinto kontrolloi sitä, miten palveluja tuotetaan, kuka mitäkin palvelua saa käyttää ja kenellä on pääsy mihinkin tietoon.[336]

Weberin malli ja teknologian kehitys ovat toimineet pohjana Clarken kehittämälle ajatukselle tietovalvonnasta. Käsitettä käytetään kuvamaan tapoja, joilla yhteiskunnat tekniikan avulla ottavat käyttöön tietoon perustuvia valvontamuotoja.[337] Tässä valvontamuodossa ihmisten tekemisiä valvotaan automaattisesti. Se on Clarken mukaan paljon halvempaa ja tehokkaampaa kuin tavallinen valvonta.[338] Clarken ajatus pitää tällä hetkellä erittäin hyvin paikkansa, sillä nykyään valvonta on pääasiassa tietovalvontaa.

Tietovalvonnassa korostuu yksi ominaisuus yli muiden. Tietokantojen tulee muodostaa toiminnallinen kokonaisuus, vaikka nämä olisikin hajautettu. Kasvava teknologinen konvergenssi eli yhdentyminen puolestaan tukee sitä, että tietojärjestelmät suunnitellaan ja rakennetaan keskenään yhteentoimiviksi. Järjestelmien yhteiskäyttö ja yk-

336 Katso tarkemmin *Weber,* The Theory of Social and Economic Organisations.

337 Clarke määrittelee tietovalvonnan seuraavasti: "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." Tietovalvonta, kuten valvonta ylipäätään, voidaan jakaa henkilölliseen ja massamuotoiseen valvontaan. *Clarke,* Information Technology and Dataveillance, s. 499. Katso myös *Solove,* The Digital Person: Technology and Privacy in the Information Age, s. 33 sekä Rubinstein et al. Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches.

338 *Clarke,* Information Technology and Dataveillance, s. 499.

silöön liittyvien tietojen helppo kokoaminen vaatii kuitenkin yleisen ja yhdenmukaisen avaimen onnistuakseen. Tällainen avain voisi olla esimerkiksi sähköinen identiteetti. Sähköinen identiteetti olisi omiaan lisäämään tietovalvonnan tehokkuutta eri tarkoituksissa esimerkiksi työpaikoilla, virastoissa, kaupoissa, pankeissa, rajan ylityksissä, liikennevälineissä jne. Jotta tietoja olisi mahdollista käyttää tehokkaasti palveluihin ja valvontaan, tulee tietojen olla yhdistettävissä ihmisiin ja heidän identiteetteihinsä.

Kontrolloivasta luonteestaan huolimatta valvontaa ei kuitenkaan harjoiteta arvotyhjiössä, sillä siinä puututaan lähes kaikkiin kansalaisoikeuksiin, kuten esimerkiksi yksityisyyteen ja vapauteen. Täydellisessä valvontayhteiskunnassa näitä arvoja ja oikeuksia ei ole, vaikka esimerkiksi lainmukainen tietosuoja toteutuisikin.

Valvonnan lisääntymisen vaikutukset yksityisyyteen ja vapauteen eivät ole vielä täysin selkiintyneet.[339] Huolena on, että lisääntyvä valvonta tarkoittaa yksityisyyden asteittaista rapautumista. Valvonnan lisääntymistä pidetään myös uhkana yksilön vapaalle kehittymiselle, sillä yksilö tarvitsee tietyn määrän yksityisyyttä kehittyäkseen vapaasti, toisten suorasta tai epäsuorasta vaikutuksesta vapaana. Valvonta uhkaa myös yksilön identiteetin vapaata kehitystä.

Valvontamahdollisuuksien kasvusta puhuttaessa on hyvä ottaa esille EU-tuomioistuimen ratkaisu C-293/12 ja 594/12, joka liittyy yksilöiden valvontaan. High Court (Irlannin ylin tuomioistuin) ja Verfassungsgerichtshof (Itävallan perustuslakituomioistuin) pyysivät unionin tuomioistuinta tutkimaan tietojen säilyttämisestä annetun direktiivin pätevyyden erityisesti kahden Euroopan unionin perusoikeuskirjassa taatun perusoikeuden, yksityiselämän suojan ja henkilötietojen suo-

339 Yksi valvonnan kehityssuunta on valvonnan käyttäminen sosiaalisen lajittelun eli syrjinnän välineenä. Tästä tarkemmin katso esim. *David Lyon* (ed.), Surveillance as Social Sorting.

jan, kannalta. Päätöksessään tuomioistuin katsoi EU:n tietojen säilyttämistä koskevan direktiivin pätemättömäksi. Tietojen säilyttämisestä annetussa direktiivissä eli niin sanotussa pakkotallennusdirektiivissä säädettiin, että sähköisten viestintäpalvelujen tarjoajien oli säilytettävä palvelujen käyttäjien liikenne- ja paikkatiedot sekä palvelun tilaajan tai käyttäjän tunnistamiseksi tarvittavat tarpeelliset tiedot.

Unionin tuomioistuin totesi, että kyseisellä direktiivillä puututtiin yksityiselämän suojaa ja henkilötietojen suojaa koskeviin perusoikeuksiin laajamittaisesti ja erityisen vakavasti. Tuomioistuin huomautti, että direktiivissä määriteltyjen tietojen avulla voitiin saada selville hyvinkin tarkkaa tietoa henkilön yksityiselämästä, eikä direktiivi sisältänyt minkäänlaista vakavan rikollisuuden ehkäisemisen tavoitteeseen perustuvaa erottelua, rajaamista tai poikkeusta. Tuomioistuin painotti, että perustavanlaatuinenkaan yleinen etu ei itsessään oikeuta direktiivissä määriteltyjä tallennustoimenpiteitä. Ratkaisu kuvaa sitä, kuinka kansalaisiin kohdistuva laajamittainen tiedonkeruu valvonnan mahdollistavalla tavalla ei ole demokraattisessa oikeusvaltiossa hyväksyttävää edes yleisen edun nimissä.

Tämä johtaakin kysymään, kuinka paljon valvontaa sallimme. Mikä määrä valvontaa on liikaa? Yksinkertainen vastaus on, että julkisen vallan tulee aina tiedostaa yksityisyyden olevan perus- ja ihmisoikeus, jota yksilö tarvitsee kehityksessään, omanarvon tunnossaan ja toimiakseen normaalisti yhteiskunnan jäsenenä. Meillä on Euroopan ihmisoikeussopimuksen nojalla oikeus yksityis- ja perhe-elämän suojaan, koska ilman näitä emme voi täysin kukoistaa yksilöinä.[340] Julkisen vallan tulee ymmärtää, että oikeus yksityisyyteen on myös tärkeä osa demokratiaa ja sen kehitystä.[341]

340 *Goold,* How Much Surveillance is Too Much?, s. 45.

341 Gooldin mukaan yksityisyys on myös tärkeä osa muiden ihmisoikeuksien toteuttamista. Katso tarkemmin *Goold,* How Much Surveillance is Too Much?, s. 45–46.

JAKSO II BIOMETRINEN TUNNISTAMINEN

4. Mitä on biometrinen tunnistaminen?

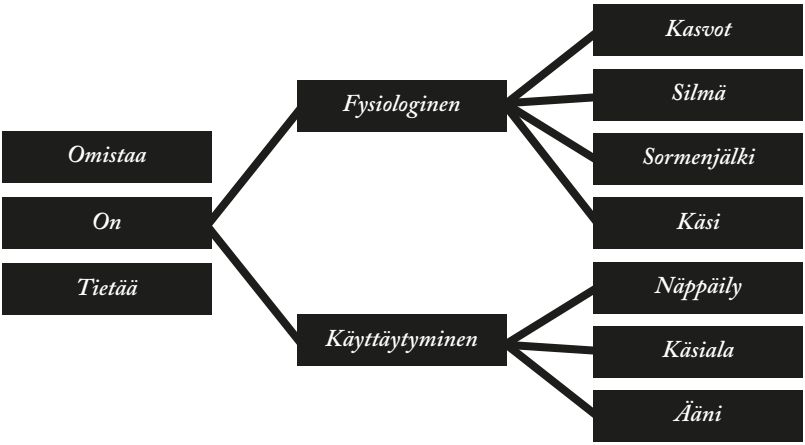
Tunnistusmenetelmät (kuvio 3) on mahdollista jakaa kolmeen luokkaan. Tunnistus perustuu siihen, että prosessissa on käytettävissä:

1. jotakin mitä käyttäjä tietää (knowledge);
2. jotakin mitä käyttäjä omistaa (possesses) tai
3. jotakin mitä käyttäjä on (characteristics).[342]

Ensimmäisessä luokassa ovat lähinnä salasanat ja tunnusluvut. Toiseen luokkaan kuuluvat perinteiset avaimet, kulkukortit ja muu vastaava materia, jolla pyritään henkilöiden tunnistukseen. Näiden kahden luokan eli ns. perinteisten henkilötunnistuskeinojen ei enää katsota riittävän tunnistamisessa. Biometriset tunnistusmenetelmät kuuluvat kolmanteen luokkaan.

342 *Miller,* Vital Signs of Identity, s. 22-23. Katso myös *Bolle – Connell – Pankanti – Ratha – Senior,* Guide to Biometrics, s. 4. Heidän mukaansa tavat voidaan jakaa kolmeen kategoriaan seuraavasti: 1) Tunnistamisvälineen (esim. avain, passi tai henkilökortti) halllussapito, 2) Tieto (esim. salasana tai tunnusluku) ja 3) biometrinen ominaisuus. Näitä tapoja voidaan yhdistellä, jolloin on kysymys vahvasta tunnistamisesta.

Kuvio 3. Tunnistusmenetelmät.



Perinteisessä tunnistuksessa ihminen tunnistaa ihmisen ja sähköisessä tunnistuksessa kone tunnistaa tunnusluvun/kortin. Biometrisessa tunnistuksessa kone tunnistaa ihmisen. Biometrian käyttö parantaa tunnistuksen luotettavuutta, koska siinä tunnistaminen tapahtuu suoraan ihmisen yksilöllisten fyysisten piirteiden avulla.[343]

Biometriaa käytetään henkilötunnistuksessa ja sen käyttökohteita ovat esimerkiksi biometriset passit, kulunvalvonta ja tietokoneen käyttäjätunnistus. Biometria ei ole vain keino korvata perinteisiä henkilöntunnistamisratkaisuja. Sovelluksesta riippuen biometriaa voidaan käyttää turvallisuuden parantamiseen, rikostorjuntaan ja jopa teknologian apuvälineenä. Koska biometrinen tunnistaminen viittaa laajaan eri teknologiat, järjestelmät ja sovellukset kattavaan joukkoon, on perusteltua käydä tarkemmin läpi biometrisen tunnistamisen terminologiaa ja luokitteluja.

343 *Nanavati – Thieme – Nanavati,* Biometrics, Identity Verification in a Networked World, s.4.

Biometrisella[344] tunnistamisella yleisesti tarkoitetaan ihmisen automatisoitua tunnistamista jonkin fysiologisen ominaisuuden tai käyttäytymispiirteen perusteella.[345] Tutuin esimerkki biometrisesta tunnistamisesta on sormenjälkitunnistus, jossa tietokone tunnistaa ihmisen hänen sormenjälkensä perusteella. Muita biometrisen tunnistuksen menetelmiä ovat esimerkiksi kasvontunnistus, äänentunnistus ja silmän iiriksen tunnistus. Määritelmä vaatii kuitenkin sen osien tarkempaa erittelyä.[346]

Automatisoitu. Tunnistuksen automatisointi tarkoittaa sitä, että tunnistus on mahdollista toteuttaa kokonaan ilman ihmistä. Tunnistuksen suorittaa tietokone erilaisten laitteiden ja ohjelmistojen avulla.

---

344 Termi biometria on peräisin kreikan kielen sanoista ”bios” (elämä) ja ”metron” (mitata). American Heritage Dictionaryn mukaan biometria on perinteisesti tarkoittanut biologisten ilmiöiden statistista tutkimusta. The American Heritage Dictionary. Saatavilla osoitteessa: http://www.ahdictionary.com/word/search.html?q=biometrics. Biometristen tunnisteiden hyväksikäyttäminen automaattisessa tunnistamisessa on kuitenkin johtanut siihen, että termin merkityssisältö on muuttunut.

345 *Nanavati, S. – Thieme, M. – Nanavati, R.,* Biometrics. Identity Verification in a Networked World, s. 9. Katso myös EU:n neuvoston sanasto (013) turva-asiakirjoista, turvatekijöistä ja muista teknisistä termeistä. Sanasto on saatavilla osoitteessa: http://prado.consilium.europa.eu/fi/glossarypopup.html ja National Science and Technology Council (NTSC), Privacy & Biometrics: Building a Conceptual Foundation, s. 120 sekä *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 148.

346 Käyttäytymispiirteeseen perustuvaa biometrista tunnistamista voidaan kutsua myös dynaamiseksi biometriseksi tunnistamiseksi. *Nanavati, S. – Thiemi, M. – Nanavati, R.,* Biometrics. Identity Verification in a Networked World, s. 9–11 sekä 29 artiklan mukainen tietosuojatyöryhmä, Valmisteluasiakirja biotunnisteista, s. 3.

Automatisoinnin ansiosta suuret ihmismäärät on mahdollista tunnistaa sujuvasti ja tehokkaasti.

Fysiologinen / käyttäytymispiirteeseen perustuva. Käytetyn tunnisteen perusteella syntyy jako fysiologiseen biometriseen tunnistamiseen ja käyttäytymispiirteeseen perustuvaan biometriseen tunnistamiseen.[347] Fysiologisessa biometrisessa tunnistamisessa tunnistaminen perustuu ihmisen fysiologisesta ominaispiirteestä saatavaan informaatioon. Käyttäytymispiirteeseen perustuvassa biometrisessa tunnistamisessa puolestaan tunnistaminen perustuu ihmisen käyttäytymispiirteestä saatavaan informaatioon, joka epäsuorasti perustuu myös ihmisen ruumiista saatavaan informaatioon.

Biometriseen tunnistukseen soveltuvan ominaispiirteen tulee olla yleinen (esiintyy kaikilla ihmisillä), yksilöllinen (esiintyy erilaisena eri ihmisillä) ja pysyvä (ei muutu ajan kuluessa). Lisäksi ominaispiirre pitää pystyä lukemaan ja analysoimaan koneellisesti. On myös toivottavaa, että tunniste on hyväksyttävä eli tunnisteeseen ei liity negatiivista sävyä.[348]

---

347 Vertaa *Russel,* D – Gangemi, G.T. Sr: Computer Security Basics. Kehitys on myös viemässä tätä jaottelua eteenpäin, sillä teknologisen kehityksen mukana on alettu puhua myös psykologisesta biometrisesta tunnistamisesta. Tällöin yksilö tunnistetaan tämän yksilöllisistä psykologisista ominaispiirteistä.

348 *Wayman,* J.L.: Fundamentals of Biometric Technologies. Saatavilla osoitteessa: http://www.engr.sjsu.edu/biometrics/publications_tech.html. Katso myös *Sethi,* I: Biometrics: Overview and Applications (2006) sekä Sisäasiainministeriön henkilöllisyyden luomista koskevan hankkeen loppuraportti. Katso myös *Huhanantti,* Itsepalvelujärjestelmän turvallisuus – esimerkkinä pankin itsepalvelujärjestelmät. Pro gradu –tutkielma. Oulun yliopisto, tietojenkäsittelyopin laitos. Oulu 1990.

Tunnistaminen. Tunnistaminen muodostuu kolmesta eri käsitteestä. Nämä ovat 1) tunnistaminen, 2) tunnistautuminen ja 3) todentaminen. *Tunnistamisessa (identification)* erotetaan kaksi merkitystä. *Viranomaistoiminnassa* tunnistamisella tarkoitetaan henkilöllisyyden toteamista eli henkilön yhdistämistä tiettyyn olemassa olevaan henkilöllisyyteen. Tämä voi tapahtua kahdella tavalla. Tapa numero 1: henkilö esittäytyy, ja tunnistaminen todennetaan tavalla tai toisella. Tapa numero 2: henkilöltä otetaan biometrinen tunniste, ja henkilöllisyys todetaan vertaamalla tunnistetta johonkin henkilörekisteriin tallennettuihin tunnisteisiin. *Yleisemmin* tunnistamisella kuitenkin tarkoitetaan toimijan yhdistämistä tiettyyn tunnukseen tai tunnisteeseen, jolla toimija esiintyy suhteessa toisiin toimijoihin.[349]

Tunnistaminen tulee erottaa *tunnistautumisesta (authentication)*, jolla tarkoitetaan omatoimista prosessia, jossa henkilö esittäytyy tunnistusjärjestelmälle ja todentaa esittäytymisensä jollakin keinolla. Tunnistautuminen on teko, jossa toimija on tunnistuksen kohde itse. Tunnistamisen puolestaan hoitaa joku, joka ei ole itse tunnistuksen kohteena.[350]

---

349 Käsitteiden tunnistaminen, tunnistautuminen ja todentaminen määrittelystä katso Sisäasiainministeriön henkilöllisyyden luomista koskevan hankkeen loppuraportti, s. 18. Vertaa HE 36/2009, s. 30. Katso myös *National Science and Technology Council,* Privacy & Biometrics: Building a Conceptual Foundation, s. 122–124.

350 Kysymys on aktiivisesta tunnistamisesta. Aktiivisessa tunnistuksessa useat välineet toteuttavat tunnistuksen ja todennuksen samaan aikaan. Esimerkiksi henkilötietoja tarkistettaessa henkilön tiedot todennetaan henkilökortista, passista taikka ajokortista ja samalla hänet tunnistetaan. Sähköisessä toimintaympäristössä tunnistus tehdään henkilön hallussa olevan välineen eli tunnisteen avulla ja todentaminen esimerkiksi henkilön tiedossa olevan salasanan avulla. *Voutilainen,* ICT-oikeus sähköisessä hallinnossa, s. 245.

Tunnistuksen yhteydessä henkilö todennetaan tietyksi henkilöksi. *Todentamisessa (verification)* on kysymys tiedon tai tahon aitouden varmistamisesta. Todentamisella tarkoitetaankin menettelyä, jossa toinen osapuoli varmistuu tunnistuksessa esitettyjen tietojen paikkansa pitävyydestä.[351] Eri yhteyksissä todennetaan esimerkiksi, onko järjestelmän käyttäjä tai viestikumppani se, joksi on esittäytynyt, tai onko viesti, passi tai muu asiakirja aito eli eheä ja alkuperäinen. Todentamiseen liittyy siis aina joku väite: henkilö on esittäytynyt herra X:ksi eli väittää olevansa herra X. Tällöin todentaminen on väitteen todenperäisyyden varmistamista.

4.1. Biometrisen tunnistamisen kehitys

Nykymuotoinen biometrinen tunnistaminen, jossa tunnistaminen on automatisoitua, on tullut osaksi verkkoyhteiskunnan elämää muutaman vuosikymmenen kuluessa tietoteknistymisen ansiosta. Se perustuu kuitenkin vuosituhansia vanhoihin ajatuksiin.[352] Kuten kaikella

---

351 *Voutilainen,* ICT-oikeus sähköisessä hallinnossa, s. 244. Katso myös VAHTI (12/2006), s. 37–38.

352 Ensimmäisenä merkkinä biometrisen tunnistamisen käytöstä voidaan mainita luolamaalaus n. 31 000 vuoden takaa, jossa esi-ihmiset merkitsivät luolamaalaustensa viereen kämmenenjälkensä. Tätä kämmenenjälkeä voidaan Janeen Renaghanin mukaan pitää tekijänsä unohtumattomana signeerauksena. Katso tarkemmin Renaghan, Etched in Stone, Zoogoer lehti, elokuu 1997. Katso myös *Clottes,* Chavet Cave (ca . 30 , 000 B . C), The Metropolitan Museum of Art. Saatavilla osoitteesa: http://www.metmuseum.org/toah/hd/chav/hd_chav.htm (käyty 16.7.2014). On myös esitetty, että kuningas Hammurab käytti kämmenen jälkeä vahvistaakseen antamansa lait. *Ashbourn,* The Social Implications of the Wide Scale Implemen-

teknologialla, myös biometrisella tunnistamisella on omat kehitysvaiheensa (niin sanotut sukupolvet), joiden kautta tämä teknologia on saavuttanut nykymuotonsa. Tällä hetkellä nykymuotoinen biometrinen tunnistaminen on vasta ottamassa ensimmäisiä varsinaisia harppauksiaan.

Kauan ennen tietokoneen keksimistä oli tapana tunnistaa yksilöt toisistaan kasvojen, äänen ja olemuksen perusteella.[353] Tunnistamisessa oli tapana luottaa omaan muistiin ja toisilta saatuihin tuntomerkkeihin. Perinteinen tapa kävi kuitenkin väkiluvun kasvaessa ja liikkuvuuden lisääntyessä erittäin vaikeaksi.

---

tation of Biometric and Related Technologies. Background paper for the Institute of Prospective Technological Studies, DG JRC – Seville, European Commission, January 2005, s. 4, (‘*Ashbourn,* Social Implications of Wide Scale Implementation of Biometrics, 2005’). Saatavilla osoitteessa: http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf Myös Kiinassa sormenjälkien ja jalanjälkien käytöllä on pitkä historia. Sormen- ja jalanjälkiä on käytetty Tang-dynastian aikaan sopimuksissa ja lasten erottamiseksi toisistaan. Katso tarkemmin *Farelo,* A History of Fingerprints, (saatavilla osoitteessa: http://www.interpol.int/Public/Forensic/fingerprints/History/BriefHistoricOutline.pdf) sekä *McMahon,* Biometrics: History.

353 Suurin osa myös nykyihmisistä hyödyntää päivittäin biometrista tunnistamista perinteisessä muodossaan eli tunnistaessaan yksilöitä näiden kasvojen tai äänen perusteella. Valokuvauksen keksiminen mahdollisti ulkomuodon tallettamisen paperille, mikä mahdollisti täysin tuntemattomien tunnistamisen. Nykyään kuvalliset henkilöllisyystodistukset ovat jo arkipäivää. Niitä käytetään rajavalvonnassa, kaupallisessa toiminnassa ja monissa muissa tilanteissa, joissa on oikeudellisesti tärkeää tunnistaa toinen. *Denning,* Information Warfare, s. 321.

Varsinainen biometrian hyödyntäminen tunnistamisessa eli biometrisen tunnistamisen ensimmäinen sukupolvi sai alkunsa, kun pariisilainen antropologi Alphonse Bertillon kehitti 1890-luvulla tavan tunnistaa rikolliset toisistaan hyödyntämällä yksilön fyysisiä yksilöllisiä piirteitä, kuten kallon ja hartioiden rakennetta ja muotoa.[354] Menetelmä ei kuitenkaan ollut ongelmaton. Suurin ongelma oli se, että tunnistamisessa käytettävät fyysiset piirteet eivät olleet muuttumattomia. Lisäksi ongelmia aiheutti se, että nämä piirteet eivät välttämättä olleetkaan yksilöllisiä. Tästä on esimerkkinä tapaus vuodelta 1903, jossa menetelmä ei erottanut kahta identtistä kaksosta toisistaan.[355]

1800-luvun lopulla nousi käyttöön Bertillonin menetelmän kaltainen menetelmä. Erona oli se, että uusi menetelmä pohjautui sormenjälkiin. Ensimmäinen sormenjälkeen pohjautuva järjestelmä kehitettiin Intiassa paikallisen poliisipäällikön, Sir Edward Henryn, toimesta. Järjestelmää alettiin kutsua Henryn menetelmäksi[356]. Menetelmää

---

354 *Garfinkel,* Database Nation: The Death of Privacy in the 21st Century, s. 39. Tätä ennen sormenjälkiä oli kuitenkin jä käytetty Intiassa William Herschelin toimesta sopimusten allekirjoituksena. Tätä voidaan pitää ensimmäisenä biometristen tunnisteiden järjestelmällisenä käyttönä. *McMahon,* Biometrics: History, s. 5.

355 Bertillonin menetelmä hylättiin sormenjälkitunnistamisen tullessa käyttöön. Syynä oli se, että sormenjälkitunnistus osoittautui nopeammaksi, tehokkaammaksi ja helpommaksi tavaksi tunnistaa yksilö.

356 Vertaa *Kindt,* joka kutsuu Henryn menetelmää Henry-Galton –menetelmäksi. Syynä on todennäköisesti se, että ennen Henryä sormenjälkiä oli luokitellut Francis Galton 1890-luvulla, johon Henry perusti tutkimuksensa. Galton julkaisi tutkimustuloksensa Nature-lehdessä vuonna 1902 artikkelissaan Finger print Evidence. Artikkeli on saatavilla osoitteessa: http://galton.org/essays/1900-1911/galton-1902-evidence.pdf. Ensimmäisten maiden joukossa sormenjälkitunnistusta hyödynnettiin Argentiinassa, jossa sitä alettiin viral-

pidetään nykyaikaisen sormenjälkitunnistamisen esivaiheena, jonka johdannaisia käytetään edelleen tänä päivänä.[357]

Varsinaisen, nykymuotoisena tunnetun biometrisen tunnistamisen ensimmäiset sovellukset tulivat laajempaan käyttöön vasta teknologisen kehityksen ottaessa suuria harppauksia 1900-luvun jälkipuoliskolla. Tämä merkitsi myös loppua niin sanotulle biometrisen tunnistamisen ensimmäiselle sukupolvelle. Ajalle ominaiset biometrisen tunnistamisen menetelmät eivät enää kyenneet vastaamaan teknologisesti kehittyvän yhteiskunnan tarpeisiin.

Teknologinen kehitys ja yhteiskunnan toimintojen siirtyminen verkoissa toimiviksi synnytti biometrisen tunnistamisen toisen sukupolven. Biometrisen tunnistamisen toisen sukupolven voidaan ajatella saaneen alkunsa 1980–1990 -luvuilla.[358] Ala on kasvanut räjähdysmäisesti 1990-luvulta lähtien, ja 2000-luvulle tultaessa biometrinen tunnistaminen on alkanut valtaamaan alaa jokapäiväisissä toiminnoissa.

Esimerkkejä toisen sukupolven menetelmistä ovat Yhdysvaltain US-VISIT –ohjelma, Amsterdamin Schipholin lentokentällä käy-

---

lisesti käyttää rikostutkinnassa vuonna 1902. Biometrics Institute, Biometrics: The Body and Soul of Security, s. 5. Artikkeli on saatavilla osoitteessa: http://www.biometricsinstitute.org/data/Press_Releases/2002_Body_and_souls.pdf

357 *Wayman,* Biometrics - Now and Then: The development of biometrics over the last 40 years.

358 Vuonna 1985 julkaistiin ajatus siitä, että silmän iiris on yksilöllinen ja muuttumaton, ja vuonna 1994 ensimmäinen silmän iirikseen perustuva tunnistamisratkaisu patentoitiin ja otettiin kaupalliseen käyttöön. Katso asiasta tarkemmin Daugman, How Iris Recognition Works. IEEE Transactions on circuits and systems forvideo technology , s. 21–30. Artikkeli saatavilla osoitteessa: http://www.cl.cam.ac.uk/~jgd1000/csvt.pdf

tettävä Privium –järjestelmä sekä Sydneyn lentokentällä käytettävä SmartGate –järjestelmä. Näissä järjestelmissä hyödynnetään sormenjälkiä, silmän iiristä tai kasvoja matkustajien tunnistamisessa.

Syynä biometrisen tunnistamisen lähes räjähdysmäiseen kasvuun ja yleistymiseen on myös 2000-luvun alun poliittinen ilmapiiri. Vuoden 2001 syyskuun tapahtumat johtivat tämän vanhan teknologian käyttömahdollisuuksien laajentumiseen etenkin Yhdysvalloissa, josta kehitys levisi myös Eurooppaan. Syyskuun 2001 tapahtumien valossa biometrisen tunnistamisen laajentuvaa käyttöönottoa on perusteltu turvallisuudella ja sen takaamisella.[359]

Poliittinen ilmapiiri ei yksinään olisi saanut liikkeelle yhä kehittyvää biometrisen tunnistamisen teknologiaa. Teknologisen kehityksen mukana biometrisen tunnistamisen kustannukset ovat laskeneet, laitteet ovat pienentyneet, tulleet helppokäyttöisemmiksi ja tarkemmiksi. Näiden syiden taustalla toki vaikuttaa poliittinen ilmapiiri, joka on kannustanut teknologian kehittämiseen. Oman lisänsä on tuonut yhteiskunnan vaatimukset helppokäyttöisestä, tehokkaasta ja entistä luotettavammasta tunnistamisesta uudessa digitaalisessa toimintaympäristössä.

Yhteiskunnan myötä teknologia kehittyy ja vastaavasti yksilöiden tunnistamisen mekitys myös lisääntyy. Esille on noussut niin oikeudellisia kuin teknologisia haasteita, joihin biometrisen tunnistamisen

359 *Lyon,* Surveillance after September 11, s. 4-5 ja *Nelson,* America Identified: Biometric Technology and Society, s. 59 – 80. Katso myös *Tranberg,* Biometric Data in Scandinavia, s. 387. Tranbergin mielestä myös EU:n passiasetuksen (Neuvoston asetus (EY) N:o 2252/2004 jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista) säätämisen taustalla on ollut yleinen terrorisminpelko.

kolmannen sukupolven on vastattava.[360] Toisaalta biometrisen tunnistamisen kohtaama julkinen keskustelu vaatii uudelta sukupolvelta entistä enemmän perusteluja teknologian käytölle ylipäänsä. Yhteiskunnan oikeudellistuessa ihmiset ovat entistä tietoisempia omista oikeuksistaan, mikä omalta osaltaan täytyy ottaa huomioon teknologiaa kehitettäessä.

4.2. Biometrisen tunnistamisen menetelmät ja niiden käyttömahdollisuudet

4.2.1. Yleistä

Biometrisen tunnistamisen menetelmät on mahdollista jakaa hyvin monella tavalla riippuen siitä, mikä näkökulma valitaan. Luokitteluvaihtoehdoista huolimatta, biometrisen tunnistamisen menetelmät jaetaan kahteen päätyyppiin: 1) fysiologiseen biometriseen tunnistamiseen ja 2) käyttäytymiseen perustuvaan biometriseen tunnistamiseen.[361]

Tämän tutkimuksen kannalta merkityksellistä ei ole jokaisen biometrisen tunnistamisen eri menetelmän läpikäyminen. Tutkimuksessa

360 Uutena ilmiönä voidaan mainita Applen patentoima yksilön pulssiin / sykkeeseen perustuva tunnistaminen, jonka Apple suunnittelee asentavansa iPhone-puhelimiinsa. Katso uutinen Apple Patents Integrated Heart Rate Monitor For Smartphones, Hover Touch Sensors osoitteesta: http://techcrunch.com/2013/12/24/apple-patents-integrated-heart-rate-monitor-for-smartphones-hover-touch-sensors/. Biometrisen tunnistamisen kolmannesta sukupolvesta on kysymys esimerkiksi psykologisessa biometrisessa tunnistamisessa.

361 Kehitys on viemässä myös kohti psykologista biometrista tunnistamista.

on aihepiirin kannalta valittu biometrisen tunnistamisen menetelmien jakaminen koviin ja pehmeisiin menetelmiin sen perusteella, miten menetelmä vaikuttaa yksilön yksityisyyteen ja muihin oikeuksiin.

Jakoon vaikuttaa se, että biometrisen tunnistamisen menetelmät koetaan usein loukkaavaksi sen vuoksi, että niiden avulla kerätään henkilökohtaisia tietoja.[362] Tärkeää on käyttää jaon perusteena menetelmän vaikutusta yksilön yksityisyydelle. Yksityisyys – etenkin fyysinen ja tiedollinen – on kuitenkin se oikeus, johon biometrisella tunnistamisella on kaikkein suurin vaikutus.

4.2.2. Kovat biometrisen tunnistamisen menetelmät

Kuten jäljempänä jaksossa 4.3.2. kuvataan, biometrisella tunnistamisella on vaikutuksia sekä tiedolliseen yksityisyyteen että fyysiseen yksityisyyteen. Koviin biometrisen tunnistamisen menetelmiin luetaan ne menetelmät, joilla on vaikutuksia yksilön fyysiseen koskemattomuuteen. Näistä esimerkkeinä toimivat sormenjälkitunnistus, verkkokalvotunnistus, silmän iirikseen pohjautuva biometrinen tunnistaminen ja ennen kaikkea DNA-tunnistus.

Koviin biometrisen tunnistamisen menetelmiin kuuluvat myös ne biometrisen tunnistamisen menetelmät, joiden käyttäminen ilman tunnistuksen kohteen tietoa tunnistamisesta vaikuttaa voimakkaasti yksilön yksityisyyteen sitä rajoittavasti. Esimerkkinä tällaisesta biometrisen tunnistamisen menetelmästä on kasvontunnistus

Fyysiseen koskemattomuuteen puuttuvat biometrisen tunnistamisen menetelmät on mahdollista lukea koviksi menetelmiksi senkin puolesta, että niiden avulla saadut tiedot yleensä ovat tavallisia henkilötietoja arkaluonteisempia. Yksilön fyysinen ja tiedollinen yksityisyys ovat kiinteässä yhteydessä toisiinsa. Biometrisen tunnistamisen

362 Perusteena on mahdollista käyttää myös sitä, minkälaisia henkilötietoja biometrisen tunnistamisen menetelmän kautta on saatavissa.

kohdalla yksilön ruumiilliset ominaispiirteet ovat koneella luettavaan muotoon muutettua informaatiota.

4.2.3. Pehmeät biometrisen tunnistamisen menetelmät

Pehmeät biometrisen tunnistamisen menetelmät ovat sellaisia, joiden vaikutus yksityisyydelle jää vähäisemmäksi. Pehmeän biometrisen tunnistamisen menetelmiin kuuluvat sellaiset menetelmät, jotka eivät puutu yksilön fyysiseen koskemattomuuteen. Menetelmät perustuvat fyysisten ominaispiirteiden sijaan käyttäytymispiirteisiin, eikä niillä olle niin suurta vaikutusta yksilön yksilöllisyydelle kuin kovilla menetelmillä. Esimerkkeinä pehmeistä biometrisen tunnistamisen menetelmistä voidaan mainita ääneen, allekirjoitukseen tai näppäilytekniikkaan perustuva tunnistaminen.

Pehmeät biometrisen tunnistamisen menetelmät ovat monesti kovia menetelmiä harvemmin käytettäviä, koska oviin menetelmiin perustuvat tunnistamisratkaisut ovat yleensä luotettavampia. Pehmeät biometrisen tunnistamisen menetelmät eivät kuitenkaan puutu yksilön yksityisyyteen yhtä voimakkaasti.

4.2.4. Biometrisen tunnistamisen käyttömahdollisuudet

Kuten teknologialla yleensä, myös biometrisen tunnistamisen sovelluksilla on omat käyttömahdollisuutensa. Pääasiallisia jaotteluita voidaan esittää kolme. Ensimmäinen tapa on jakaa biometrisen tunnistamisen käyttömahdollisuudet järjestelmien käyttötarkoitusten perusteella. Toinen tapa on jakaa biometrisen tunnistamisen käyttömahdollisuudet järjestelmän toteutustapojen perusteella. Kolmas jaottelu perustuu puolestaan siihen, millä yhteiskuntatoiminnan alueella biometrisen tunnistamisen sovelluksia on mahdollista hyödyntää. Kuvatut jaottelut eivät ole tyhjentäviä eikä niitä teknologian dynaamisen luonteen

vuoksi sellaisina voi esittääkään. Jaottelut ovat vain mahdollisia tapoja kuvata biometrisen tunnistamisen käyttömahdollisuuksia.

4.2.4.1. Käyttötarkoitus

Biometrisen tunnistamisen käyttömahdollisuudet ovat niiden käyttötarkoituksen perusteella jaettavissa kuuteen kategoriaan:[363]

Rikostutkinta. Biometrista tunnistamista on käytetty rikostutkinnassa jo yli sadan vuoden ajan. Automaattista biometrista tunnistamista on hyödynnetty jo yli 40 vuoden ajan rikostutkinnassa. Tunnistamisen muoto viittaa biometristen tunnisteiden käyttöön lainvalvonnassa epäillyn tai pidätetyn tunnistamiseksi.

Kauppa. Biometriset tunnisteet ovat hyödynnettävissä niin perinteisessä kaupankäynnissä kuin sähköisessä kaupassa. Niillä on mahdollista vahvistaa tai korvata perinteisiä tunnistamiskeinoja kuten PIN-koodeja ja allekirjoituksia. Sähköisessä kaupassa biometrisia tunnisteita voidaan käyttää yksilön tunnistamiseen ja henkilöllisyyden todentamiseen.

Kulunvalvonta. Kulunvalvonnassa biometristen tunnisteiden käyttö viittaa tietyille alueille määrättyyn aikaan pyrkivien henkilöiden tunnistamiseen. Tunnisteita hyödynnetään kulunvalvonnassa jo melko yleisesti. Esimerkkinä toimivat kuntosalit ja työpaikat, joissa perinteisen tunnistamisratkaisun on korvannut biometriseen tunnistamiseen pohjautuva kulunvalvontajärjestelmä.

Sisäänkirjautuminen. Biometristen tunnisteiden käyttö sisään kirjautumisessa viittaa verkkoa tai laitetta käyttävän henkilön tunnis-

363 Jaottelu perustuu kirjoittajien *Nanavati,* S – *Thieme,* M – *Nanavati,* R. hahmottelemaan jaotteluun, joka on julkaistu heidän teoksessaan Biometrics. Identity Verification in a Networked World. Katso tarkemmin. *Nanavati,* S – *Thieme,* M – *Nanavati,* R., Biometrics. Identity Verification in a Networked World, s. 209–233.

tamiseen tämän biometristen tunnisteiden avulla. Tällä hetkellä on käytössä monia sovelluksia, jotka tarjoavat tähän mahdollisuuden. Esimerkiksi monissa kannettavissa tietokoneissa ja mobiililaitteissa hyödynnetään biometrisia tunnisteita perinteisten käyttäjätunnusten ja salasanojen ohella ja sijasta.

Kansalaisten tunnistaminen. Biometriset tunnisteet ovat käytettävissä kansalaisten tunnistamisessa monissa eri viranomaistoiminnoissa aina passin myöntämisestä sosiaalitukien jakamiseen ja rajavalvontaan. Tunnisteita käytetään tällöin viranomaisen kanssa asioivan yksilön tunnistamiseksi.

Valvontatarkoitus. Biometristen tunnisteiden käyttö valvontatarkoituksiin aiheuttaa yhä eniten julkista keskustelua. Valvontatarkoituksessa tapahtuva biometrinen tunnistaminen eroaa kulunvavonnasta siinä, että se ei aina edellytä valvonnan kohteen tietoisuttaa valvonnasta. Tällaiseen käyttötarkoitukseen tulee oikeusvaltiossa suhtautua kriittisesti. Se myös vaatii vahvat perusteet, sillä lähtökohtaisesti yksilöllä on oikeus elää ilman aiheetonta puuttumista yksityiseen piiriin. Biometristen tunnisteiden käyttämisestä valvontatarkoituksessa tuleekin lähtökohtaisesti pidättyä.

4.2.4.2. Järjestelmien toteutustapa

Toinen tapa jakaa biometrisen tunnistamisen käyttömahdollisuuksia pohjautuu järjestelmien toteutustapoihin. Tämän jaottelun on kehittänyt Jim Wayman.[364] Toteutustavat ovat:

Avoin tai peitetty (overt / covert). Tämä viittaa siihen kerätäänkö biometrisia tunnisteita avoimesti vai peitellysti. Yleisin tapa on kerätä

364 *Wayman,* J.L., Fundamentals of Biometric Technologies. Saatavissa internetistä osoitteessa: http://www.engr.sjsu.edu/biometrics/publications_tech.html. Jaottelun tarkemmasta analyysista katso *Liu,* Bio-privacy, s. 53

tunniste avoimesti yksilön suostumuksella. Joitain biometrisen tunnistamisen järjestelmiä on kuitenkin mahdollista käyttää ilman yksilön tietoisuutta ja suostumusta. Esimerkkinä on kasvojen tunnistus, joka on liitettävissä osaksi kameravalvontajärjestelmää. Peitellyn järjestelmän käyttöä tulee kuitenkin välttää sen yksityisyyttä loukkaavan luonteen vuoksi.

Yhteistyöhön perustuva tai yhteistyöhön perustumaton (cooperative / non-cooperative). Erona näissä toteutustavoissa on se, miten järjestelmää on mahdollista huijata. Joutuuko järjestelmää huijaava toimimaan yhteistyössä järjestelmän kanssa vai välttääkö yhteistyötä.

Tuttu tai tuntematon (habituated / non-habituated). Tutussa järjestelmässä käyttäjät useasti käyttävät sitä eli se on käyttäjille tuttu. Tuntematon järjestelmä puolestaan on sellainen, johon käyttäjä vain harvoin törmää eikä sitä näin ollen tunneta.

Valvottu tai valvomaton (supervised / unsupervised). Valvotun ja valvomattoman järjestelmän erona on se, että valvotussa järjestelmässä järjestelmänvalvoja on paikalla valvomassa tunnistautumista. Valvomattomassa järjestelmässä kukaan ei valvo tunnistautumisprosessia. Tällaisen järjestelmän käytön kohdalla herää kysymys tunnistuksen kohteena olevan henkilön oikeusturvasta esimerkiksi tunnistuksen epäonnistuessa. Lähtökohtaisesti yksilön oikeuksiin vaikuttavaa päätöstä ei tule tehdä pelkästään koneen toimesta.

Avoin tai suljettu (closed / open). Erottelu viittaa siihen, miten biometrisia tunnisteita on tarkoitus käyttää. Suljetussa järjestelmässä biometrisia tunnisteita on tarkoitus käyttää vain yhteen tiettyyn tarkoitukseen. Avoimessa järjestelmässä puolestaan biometrisia tunnisteita on tarkoitus käyttää useampaan ennalta määräämättömään tarkoitukseen. Avoimen järjestelmän käyttäminen on suuri riski yksityisyyden suojan kannalta, sillä se tuo mukanaan mahdollisuuden järjestelmän ja sen tietojen väärinkäytölle. Henkilötietojen käyttötarkoituksen tulee

olla tarkkarajainen ja täsmällinen ja tämän tarkoituksen muuttamiseen tulee suhtatutua pidättyvästi.

Julkinen tai yksityinen (public / private). Tässä erottelussa huomiota kiinnitetään siihen suhteeseen, joka järjestelmää käyttävällä on järjestelmän haltijaan. Mikäli järjestelmän kohteena on esimerkiksi organisaation henkilökunta, on kysymyksessä yksityinen järjestelmä. Julkisessa järjestelmässä puolestaan järjestelmän kohteena ovat organisaation asiakkaat. Erona on siis se, missä roolissa järjestelmän kohtaa. Suljetulle henkilöpiirille suunniteltu järjestelmä on yksityinen ja avoimelle henkilöpiirille suunniteltu järjestelmä on julkinen.

Vakiintunut ympäristö tai vakiintumaton ympäristö (standard / non-standard environment). Erottelu vakiintuneeseen ja vakiintumattomaan käyttöympäristöön viittaa siihen ympäristöön, missä biometrista tunnistamista käytetään. Vakiintuneessa käyttöympäristössä on ympäristö aina hallittu ja kontrolloitu. Muussa tapauksessa kysymyksessä on vakiintumaton käyttöympäristö.

4.2.4.3. Järjestelmän käyttöalueet

Biometrisen tunnistamisen käyttömahdollisuudet ovat jaettavissa myös sen perusteella, millä sektorilla järjestelmää käytetään. Tällöin muodostuu seuraava jako viiteen sektoriin, joissa on mahdollista hyödyntää biometrista tunnistamista[365]:

Lainvalvonta. Lainvalvonnan sektori hyödyntää biometrista tunnistamista pidätettyjen, vangittujen ja epäiltyjen tunnistamiseen ja valvontaan. Tyypillisiä biometrisen tunnistamisen sovelluksia lainvalvonnan sektorilla ovat automaattinen sormenjälkitunnistus ja kasvontunnistus.

365 *Nanavati,* S. – *Thieme,* M. – *Nanavati,* R.: Biometrics. Identity Verification in a Networked World, s. 210.

Julkinen hallinto. Julkisen hallinnon sektorilla biometrista tunnistamista on mahdollista hyödyntää julkisen hallinnon asiakkaiden ja työntekijöiden tunnistamiseen. Tyypillisiä käyttötarkoituksia ovat esimerkiksi oleskelulupakortti, johon Suomessa otetaan kortinhaltijan biometriset tunnisteet.

Taloussektori. Taloussektorilla biometrisia tunnisteita käytetään niiden yksilöiden tunnistamiseen, jotka asioivat taloussektorin toimijoiden kanssa asiakkaana tai työntekijänä. Biometristen tunnisteiden käyttö taloussektorilla on yksi suurimmista tunnistamisen käyttöalueista. Jo vuoden 2001 alusta useat talousalueen toimijat ympäri maailman ovat käyttäneet toiminnoissaan sormenjälki-, kasvon- ja verkkokalvontunnistusta yksilöiden – niin asiakkaiden kuin työntekijöiden – tunnistamisessa.

Terveydenhuolto. Terveydenhuollon alueella biometrista tunnistamista voidaan hyödyntää terveydenhuollon asiakkaiden tai työntekijöiden tunnistamisessa. Käyttötarkoituksena voi olla esimerkiksi potilaan tunnistaminen.

Rajavalvonta. Rajavalvonnan alueella kysymys on maahantulon valvonnasta. Tällä alueella biometrista tunnistamista käytetään niiden yksilöiden tunnistamisessa, jotka ovat tekemisissä rajavalvontaviranomaisten kanssa. Tyypillinen esimerkki rajavalvonnan sovelluksesta on esimerkiksi biometristen tietojen tarkastaminen maahantulotarkastuksessa.

4.3. Biometrisen tunnistamisen riskit yksityisyyden suojalle

4.3.1. Riskin käsitteestä

Riskin käsitteellä viitataan johonkin tavoittelemisen arvoiseen asiaan liittyvään negatiivisen lopputuloksen mahdollisuuteen. Arkikielessä riskiä käytetään synonyymina uhan todennäköisyydelle. Riski on systemaattinen tapa kuvata vaaroja sekä epävarmuustekijöitä, jotka modernisaatio on itse tuottanut. Riskit ovat jaettavissa luonnon aiheuttamiin ja ihmisten itsensä tuottamiin riskeihin. Teknologian, kuten biometrisen tunnistamisen, aiheuttamat riskit kuuluvat jälkimmäiseen ryhmään. Riski on keino tulla toimeen modernin yhteiskunnan tuottamien epävarmuuksien kanssa.[366]

Riskejä osana modernin yhteiskunnan kehitystä on tutkinut esimerkiksi sosiologi Ulrich Beck. Hänen tarkastelukohteena on lähtökohtaisesti yhteiskunta kokonaisuudessaan. Hänen mukaansa modernista yhteiskunnasta on tullut riskiyhteiskunta, sillä modernisaatiokehitys on synnyttänyt yhteiskuntaan monenlaisia vaaroja ja epävarmuutta. Beck kutsuukin riskiyhteiskunniksi yhteiskuntia, jotka ensin peitetysti ja sitten yhä avoimemmin joutuvat vastatusten tietyn haasteen kanssa.[367]

Beckin mukaan nykyajan olennaisimpia riskejä ovat teknologian tuomat riskit. Jos vaara pystyttiin ennen havaitsemaan esimerkiksi näkemällä, nyt riskit eivät enää välttämättä ole aistein havaittavissa.[368] Riskejä ei voida enää myöskään rajata ajallisesti, paikallisesti eikä

366 *Beck,* Riskiyhteiskunnan vastamyrkyt, s. 21.

367 *Beck,* Risk Society: Towards a New Modernity, s. 19 ja Riskiyhteiskunnan vastamyrkyt: organisoitu vastuuttomuus, s. 102. Riskien toteutumisen todennäköisyyksistä katso tarkemmin *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 121–134.

368 *Beck,* Risk Society: Towards a New Modernity, s. 19–21

sosiaalisesti.[369] On siis syytä puhua globaalista riskiyhteiskunnasta. Riskien hallinta ja arvioiminen vaikeutuvat, kun niiden erilaisista tuntemattomista seurauksista tulee historian ja yhteiskunnan hallitseva voima.[370] Riskit ovat kontekstisidonnaisia ja henkilöiden riskiarviot muuttuvat ajan ja paikan suhteen.

Riski on siis mahdollista määritellä maltillisesti tai radikaalisti. Maltillisen

ymmärryksen mukaan riski on laskettavissa tilastollisesti ja saada selville onnistumisen ja epäonnistumisen todennäköisyys. Mitä pienempi on onnistumisen todennäköisyys, sitä suurempi on epäonnistumisen mahdollisuus. Radikaalin ymmärryksen mukaan ihmiset arvottavat ja valitsevat asioita epävarmuudessa pystymättä ennakoimaan valintojensa seurauksia.[371]

Nykyään modernin yhteiskunnan yhtenä tehtävänä on suojan tarjoaminen sen väestölle erilaisia riskejä ja vaaroja vastaan.[372]Samanaikaisesti monenlaiset pyrkimykset ja keinot arvioida, ehkäistä ja hallita riskejä ovat lisääntyneet. Yhteiskunnassa on esimerkiksi syntynyt erilaisia hallinnan ja kontrollin muotoja sekä kehitetty erilaisia valvontajärjestelmiä. Esimerkkinä ovat biometrisen tunnistamisen kaltaiset tekniset tunnistamis- ja valvontaratkaisut. Ihmisiä on alettu valvoa ja kontrolloida erilaisia apuvälineitä käyttämällä.

Riskien hallinnasta ja ehkäisemisestä muodotuvat omat riskinsä. Uuden teknologian kehitys on tuonut mukanaan biometriseen tunnistamiseen liittyen oikeudellisia huolenaiheita ja riskejä. Eräs biometrisen tunnistamisen mukanaan tuoma huolenaihe on valvontayh-

369 *Beck,* Riskiyhteiskunnan vastamyrkyt, s. 113

370 *Beck,* Risk Society: Towards a New Modernity, s. 21–23

371 *Harisalo,* Riskit yhteiskunnassa ja markkinoilla: itävaltalaisen teorian näkökulma, s. 57.

372 *Pratt,* Governing the Dangerous: dangerousness, law and social change, s. 1

teiskunnan luominen ja yksityisyyden väheneminen. Tämän vuoksi on erityisen tärkeää kiinnittää huomiota valvonnan ja biometrisen tunnistamisen esiin nostamiin eettisiin, sosiaalisiin ja oikeudellisiin näkökohtiin.

4.3.2. Biometrisen tunnistamisen riskit

Biometrisen tunnistamisen yleistyminen aiheuttaa yhä useammin huolta teknologian vaikutuksesta yksityisyyden suojaan. Tunnistamisen tarpeesta huolimatta kansalaisilla ja yksilöillä on yhteiskunnassa oikeus nauttia elämästään anonyymisti.[373]

Biometrinen tunnistaminen nostaa esille samat asiat kuin mikä tahansa henkilötietojen käsittely. Biometristen tunnisteiden erityspiirteiden vuoksi yksityisyyden suoja on uhattuna ja siihen kohdistuu riskejä. Tästä syystä on tärkeää tarkastella biometriseen tunnistamiseen liittyviä yksityisyyteen kohdistuvia riskejä. Biometriseen tunnistamiseen liittyvät yksityisyyden suojaan kohdistuvat riskit on mahdollista jakaa tiedolliseen yksityisyyteen ja fyysiseen yksityisyyteen kohdistuviin riskeihin.

4.3.2.1. Tiedollinen yksityisyys

Tämän päivän tietotekniikka antaa niin julkisen kuin yksityisen sektorin toimijoille mahdollisuuden kerätä, säilyttää ja verrata yksilöön liittyvää informaatiota, jota on mahdollista myös käyttää väärin. Henkilötietojen luvattomaan yhdistämiseen liittyvien riskien vuoksi tiedollinen yksityisyys on suurena huolenaiheena.

Biometrisen tiedon käyttöä ei itsessään kuitenkaan koeta uhaksi. Huolena on lähinnä tämän tiedon väärinkäyttö yhdistettynä rekisterin

373 Saman on sanonut myös Garfinkel. Katso tarkemmin *Garfinkel,* Database Nation: The Death of Privacy in the 21st Century.

muihin tietoihin. Biometrinen tunniste on tiedollisen yksityisyyden kannalta ongelmallinen sen muuttumattomuuden vuoksi. Muuttumattomana tunnisteena sitä on mahdollista käyttää yksilön seuraamiseen tietokannoissa ja niiden ulkopuolella. Biometriseen tunnistamiseen liittyvinä tiedollisen yksityisyyden uhkina ovat: [374]

1) *Oikeudeton käyttö*. Biometristen tunnisteiden oikeudeton käyttö voidaan nähdä suurimpana uhkana tiedolliselle yksityisyydelle. Biometrisen tunnisteen sisältävä rekisteri houkuttelee käyttämään rekisterin tietoja sen alkuperäisen tarkoituksen vastaisesti, josta esimerkkinä olisi biometrisen tunnisteen sisältävän passirekisterin tietojen hyväksikäyttäminen rikostutkinnassa. Oikeudettomaan käyttöön lukeutuvat seuraavat alakategoriat:

a) *Oikeudeton luovuttaminen*. Oikeudettoman käytön kohdalla huolena on se, että biometrista informaatiota luovutetaan ilman rekisteröidyn suostumusta tai tietoa. Biometrista tunnistetta ei saa luovuttaa kolmannelle osapuolelle ilman omistajansa lupaa. Mikäli biometrinen tunniste luovutetaan kolmannelle osapuolelle ilman lupaa, yksilöllä ei ole mahdollisuutta vaikuttaa tietojen käyttämiseen.

b) *Valvonta ja tarkkailu*. Tarkkailu viittaa eri tarkoituksiin kerättyjen tietojen yhdistämiseen profiilien luomista varten. Koska biometrinen tunniste on yhdistettävissä vain yhteen tiettyyn yksilöön, toimii se

374 Jaottelu perustuu *Nanavati – Thieme – Nanavati,* Biometrics. Identity Verification in a Networked World sekä *Liu,* Bio-privacy. Jaottelua on kuitenkin kehitelty eteenpäin. Katso *Nanavati,* S. – Thiemi, M. – *Nanavati,* R., Biometrics. Identity Verification in a Networked World, s.239, *Liu,* Bio-Privacy, s. 72–78 sekä Euroopan Neuvoston biometrista tunnistamista koskevaan raporttiin (Progress report on the application of the principles of convention 108 to the collection and processing of biometric data) vuodelta 2013. Katso myös *Kriikkula,* Biometriset tunnisteet ja tietosuoja erityisesti pankkialan sovelluksiin liittyen, s. 126–128.

yksilöllisenä tunnisteena, jonka avulla on mahdollista koota yhteen yksilöä koskevat tiedot. Biometristen tietojen avulla on mahdollista luoda kattavia profiileja yksilöistä, mikä edesauttaa yksilöiden tarkkailua yhteiskunnassa. Lisäksi biometrinen tunnistaminen voidaan toteuttaa salaisesti, mikä mahdollistaa yksilöiden salaisen seuraamisen. Tämä puolestaan johtaa erilaisten valvonnan ja kontrollin mahdollisuuksien lisääntymiseen.[375] Oma vaikutuksensa on myös sillä, että biometrinen tunnistaminen vaikuttaa yksilöiden välisiin (valta)suhteisiin. Manuaalisessa tunnistamisessa yksilö voi jossain määrin hallita itsensä tunnistamista, mutta automaattisessa (biometrisessa) tunnistamisessa yksilö itse ei enää pysty kontrolloimaan tunnistustapahtumaa, joka voi tapahtua myös ilmoittamatta. [376]

c) *Function creep*. Function creep käsiteenä tarkoittaa teknologian tai järjestelmän käytön laajentamista sen alkuperäistä tarkoitusta laajentavasti. Äärimmilleen vietynä välittämättömyys tiedollisesta yksityisyydestä biometrisen tunnistamisen kohdalla voi johtaa yksilöiden

375 Tämä riski on nostettu esiin myös Euroopan Neuvoston biometrista tunnistamista koskevassa raportissa. Katso myös *Goncalves – Gameiro,* Security, Privacy and Freedom and the EU Legal and Policy Framework for Biometrics.

376 *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 300. Katso myös *Ploeg,* The Politics of Biometric Identification, jossa Ploeg huomauttaa teknologioiden yhdistämisen vaikutuksesta valvonnan mahdollisuuksiin biometrisen tunnistamisen kohdalla. Ploegin mukaan biometriseen tunnistamiseen liittyvä valvonnan mahdollisuus kasvaa teknologioita yhdistämällä. *Ploeg,* The Politics of Biometric Identification, s. 4.

liikkeiden ja käyttäytymisen tarkkailuun. Biometrisia tunnisteita voitaisiin tällöin käyttää ihmisten sortamisen välineenä.[377]

2) *Oikeudeton kerääminen*. Kuten muitakin henkilötietoja, myös biometrisia tietoja on mahdollista kerätä ilman yksilön suostumusta. Vaikka moni nykyään käytössä olevista biometrisen tunnistamisen tekniikoista ei vielä tähän pystykään, on olemassa riski siitä, että tunnistetietoja kerätään ilman yksilön suostumusta. Esimerkiksi kasvokuvia voidaan jo nykyään käyttää ja kerätä ilman yksilön suostumusta.[378]

3) *Tarpeeton kerääminen*. Pääperiaatteena henkilötietojen käsittelylle on se, että henkilötietojen keräämisen on rajoituttava tietoihin, jotka ovat tarpeellisia ja yhteydessä laillisen tarkoituksen toteuttamiseen. Yksi suurimmista huolenaiheista on, että henkilötietoja kerätään, käytetään ja luovutetaan enemmän kuin on tarpeen. Biometrisen tunnistamisen käytölle tulee olla aito tarve, eikä sitä tule ottaa käyttöön vain sen helppouden ja nopeuden takia. Biometristen tunnisteiden hyödyntäminen paikoissa, joissa ne tuovat vain pinnallisen lisän, ei ole hyväksyttävää. Tällainen henkilötietojen kerääminen loukkaa yksilön tiedollista yksityisyyttä, sillä henkilötietoja tulee kerätä vain tiettyihin lainmukaisiin tarkoituksiin tietyin lain asettamin ehdoin.

4) *Identiteettivarkaus*. Biometrisella tunnistamisella pyritään estämään identiteettivarkauksia. Esimerkiksi Ranskassa identiteettivarkauksilta suojaamista on käytetty perusteluna sormenjälkien keräämiselle. EIT kuitenkin kumosi tällaisen perusteen sormenjälkitietojen keräämiseen ratkaisussaan M.K. v. Ranska (no.19522/09, 18.7.2013)

---

377 Myös Kindt näkee function creep –ilmiön liittyvän voimakkaasti biometriseen tunnistamiseen. Katso tarkemmin function creep –ilmiöstä biometristen tunnisteiden kohdalla *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 377-388.

378 Näin myös *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 302 –304. Kindtin mukaan tällainen menettely on yleensä myös vailla lainsäädännön tukea.

toteamalla sen mahdollistavan sormenjälkien keräämisen kaikista kansalaisista ilman hyväksyttävää syytä.

Biometristen tunnisteiden käyttöä identiteettivarkauksien estämisessä tulee välttää myös sen vuoksi, että näiden tietojen huolimaton käyttö edesauttaa ns. spoofingia eli tietojärjestelmän huijaamista. Pelkkää biometriaa käyttävä järjestelmä on hyvin haavoittuva identiteettivarkauksien suhteen. Varsinkin, jos useat toisistaan riippumattomat järjestelmät käyttävät samaa biometriaa, sen menettäminen identiteettivarkaalle on yksilön kannalta todella haitallista. Tällaisessa tapauksessa yksilöllä on kaksi vaihtoehtoa: 1) joko hän mitätöi biometrisen tunnisteensa kaikissa näissä järjestelmissä ja sulkee siten itsensä (osittain) niiden ulkopuolelle tai 2) hän ottaa riskin, että identiteetin varastanut taho voi milloin tahansa tunnistautua häneksi.[379]

5) *Anonymiteetin heikkeneminen*. Verkkoyhteiskunnassa anonymiteetti on erittäin keskeinen käsite. Pelkistetysti se on mahdollista jakaa anonymiteettiin ja pseudo-anonymiteettiin. Anonymiteetti on todellista tunnistamattomuutta. Pseudo-anonymiteetti puolestaan tarkoittaa sitä, että yksilön identiteetti ei ole suoraan selvitettävissä. Pseudo-anonymiteetistä voidaan esimerkkinä mainita nimimerkillä toimiminen. Yksilön oikea identiteetti on tällöin tunnistamaton, mutta saatavissa selville. [380]

---

379 Myös Kindt näkee biometristen tunnisteiden käytön tietyissä tilanteissa edesauttavan identiteettivarkautta. *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 346. Katso myös *Gripjink,* Trend report on biometrics: Some new insights, experiences and developments, s.262.

380 *Chawki,* Anonymity in Cyberspace: finding the balance between privacy and security, s. 141. Vertaa kuitenkin Roosendaalin näkemykseen, jossa anonymiteetti jaetaan neljään eri kerrokseen seuraavasti: anonymiteetti (anonymity), osa-anonymiteetti (semi-ano-

Kasvava tunnistamisen tarve on viemässä pohjan yksilön oikeudelta anonymiteettiin. Anonymiteetti oikeutena toimia ja vaikuttaa tuntemattomana yhteiskunnassa suhteessa julkiseen valtaan ja muihin organisaatioihin on harvemmin mainittu, mutta demokratiassa erinomaisen tärkeä yksityisyyden muoto.[381] Se on läheisessä yhteydessä itsemääräämisoikeuteen ja henkilökohtaiseen vapauteen. Se on myös yksilön identiteetin hallitsemisen välttämättömänä osana.[382]

Henkilötietojen keräämisen lisääntyminen on tehnyt yksilön valvonnasta ja profiloinnista entistä helpompaa. Yhtenä tällaisena muotona on biometrinen tunnistaminen uutena verkkoyhteiskunnan tunnistamisratkaisuna. Anonymiteetti on toimiva väline tällaista toimintaa vastaan. Yksilöllä on oikeus anonymiteettiin, mikäli tunnistamisella loukataan oikeutta yksityisyyteen tai muita perus- ja ihmisoikeuksia.[383]

Biometrisen tunnistamisen kohdalla eräs oleellinen kysymys on se, heikentääkö biometrisen tunnistamisen käyttöönotto anonymiteettia. Liun mukaan tätä mahdollisuutta ei voida kumota.[384] Biometrisen tunnistamisen tarkoitus on yksilöiden tunnistaminen. Koska biomet-

---

nymity), pseudonymiteetti (pseudonymity) ja osa-pseudonymiteetti (semi-pseudonymiteetti). *Roosendaal,* Elimination of Anonymity in regard to Liability for Unlawful Acts on the Internet, s. 215

381 *Nelson,* America Identified: Biometric Technology and Society, s. 105 sekä *Saarenpää,* Oikeusinformatiikka (2009), s. 370.

382 *EPIC,* Comments to the FTC. Face Facts, s 9. Katso myös *Kerr – Barrigan,* Privacy, Identity and Anonymity.

383 *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 296. Katso myös *Prins,* Making our body identify for us: Legal implications of biometric technologies, s. 163.

384 Liun mukaan olisi kuitenkin mahdollista semi-anonymiaan, mikäli biometrisen tunnistamisen järjestelmät suunnitellaan huolellisesti alusta alkaen. *Liu,* Bio-Privacy, s. 78–79.

rinen tunniste myös mahdollistaa muiden henkilötietojen yhdistämisen avulla, on biometrisella tunnistamisella voimakkaita vaikutuksia mahdollisuuteen pysyä anonyymina yhteiskunnassa.[385]

Biometrisen tunnistamisen laaja hyödyntäminen johtaa anonyymin toimimisen voimakkaaseen vähenemiseen, mihin on syynä jo pelkästään tämän teknologian perusluonne eli yksilön tunnistaminen. Anonymiteetin heikkeneminen on myös riski fyysisen yksityisyyden näkökulmasta, sillä anonymiteettiin kuuluu oleellisena osana oikeus liikkua tunnistamattomana yhteiskunnassa.

4.3.2.2. Fyysinen yksityisyys

Tiedollisen yksityisyyden uhkien lisäksi, biometriseen tunnistamiseen liittyy uhkia fyysisen yksityisyyden näkökulmasta. Yksilön kulttuuriset, uskonnolliset tai henkilökohtaiset uskomukset vaikuttavat usein niin, että biometrinen tunnistaminen satetaan kokea loukkaavaksi, tungettelevaksi tai häiritseväksi.[386]

Fyysisellä yksityisyydellä on perinteisesti tarkoitettu vapautta tarkoituksettomilta henkilöön kohdistuvilta tunkeutumisilta ja tutkimiselta. Fyysinen yksityisyys liittyy läheisesti ruumiilliseen koskemattomuuteen ja on yhteydessä ihmisarvon loukkaamattomuuteen. Biometrisen tunnisteen ottaminen edellyttää fyysiseen koskematto-

385 Näin myös *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 296. Katso myös *Nelson,* America Identified: Biometric Technology and Society, s. 106.

386 Katso esimerkiksi *Woodward, J.D, Jr – Webb, K – Newton, E – Bradley,* M – Rubenson, D, Army Biometric Applications: Identifying and Addressing Sociocultural Concerns, s. 21-32. (2001), saatavilla osoitteessa: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1237.pdf.

muuteen puuttumista, mikä aiheuttaa ongelmia fyysisen yksityisyyden näkökulmasta.

Fyysinen yksityisyys käsittää myös yksilön vapauden seuraamiselta ja tarkkailulta, johon kuuluu muun muassa videovalvonta ja vastaavanlainen tarkkailu. Yksilön identiteettiin liittyvän informaation kerääminen tunnistamistarkoituksessa on mahdollista nähdä fyysisen yksityisyyden loukkauksena. Yksilön seuraaminen ja tarkkailu on mahdollista uusien biometrisiin tunnteisiin perustuvien teknologioiden avulla ja siksi tunnistamisen käyttö on nähtävissä selkeänä riskinä fyysiselle yksityisyydelle.

4.3.3. Riskien ulottuvuudet

Maallikot ja asiantuntijat arvioivat teknologioiden riskejä hyvin erilaisin tavoin. Maallikot esimerkiksi näkevät teknologioissa uhkatekijöitä, joita asiantuntijat eivät välttämättä tunnista. Tämän vuoksi on oleellista katsoa riskien ulottuvuuksia erityisesti maallikoiden silmin. Maallikoiden kannalta riskien keskeisinä ulottuvuuksina ovat *kohdentuminen, hallinta, luottamus, tieto ja aika*. Riskin eri ulottuvuuksien tarkastelussa on kysymys vapaudesta valita eri vaihtoehtojen välillä sekä uskalluksesta tehdä päätöksiä ja ryhtyä tekoihin.[387]

Riskin *kohdentumisella* tarkoitetaan seuraavien kysymysten huomioimista riskiarvioissa: Kohdistuuko riski itseen, lähipiiriin vai jonnekin kauas? Jakautuvatko riskien hyödyt ja haitat oikeudenmukaisesti? Erityisen keskeisellä sijalla riskin kohdentumisessa on juuri se, kehen riski kohdistuu. Riskin kohdistuessa itseen riski näyttäytyy painavampina kuin kaukaiset asiat.[388] Merkitystä on myös sillä, miten oikeudenmukaisiksi riskit koetaan. Riskit, jotka kohdistuvat oikeudenmukaisesti,

387 *Kuusela – Ollikainen,* Riskit ja riskinhallinta-ajattelu, s. 16.

388 Kamppinen ilmaisee asian puhumalla egon painovoimalaista. *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 136.

ollaan todennäköisesti halukkaampia hyväksymään kuin epäoikeudenmukaisesti jakautuvat riskit.[389]

Ihmiset ja yritykset pyrkivät muun muassa etukäteissuunnittelulla parantamaan turvallisuuttaan ja tulevaisuutensa ennustettavuutta. *Riskienhallinta* on riskien järjestelmällistä määrittelyä ja niihin varautumista. Merkittäviä riskejä ovat ne, joista tietoisuus vaikuttaa tai vaikuttaisi päätöksentekoon. Riskien kanssa elämiseen ja niiden hallitsemiseen on tarjolla teoriassa monenlaisia keinoja. Esimerkkinä ovat riskialttiin toiminnan välttäminen, tietoinen riskinotto, riskin kanssa eläminen ja huolellinen suojautuminen riskiltä.[390]

Riskien hallinta on suorassa yhteydessä sen hyväksyttävyyteen. Riskien hallinnassa on erotettavissa oma hallinta ja ulkopuolinen hallinta. Riskit, joita voi itse hallita, näyttävät huomattavasti vaarattomammilta kuin riskit, joille altistuminen on toisten hallinnassa.[391] Riskienhallintaa varten luodaan järjestelmä, jossa ovat määriteltyinä riskienhallintapolitiikka, riskienhallinnassa ja sen kehittämisessä sovellettavat menettelyt, riskienhallinnan eri toimijoiden tehtäväjako, riskien tarkkailu- ja raportointimekanismit ja riskienhallinnan tuki.

Luottamus on kiinteässä yhteydessä riskien hallinnan kanssa. Riskien ollessa ulkopuolisen instituution hallinnassa luottamus tuohon ulkopuoliseen hallintaan vaikuttaa riskien hyväksyttävyyteen. Mitä vähemmän yksilö luottaa hallinnan instituutioon, sitä suuremmaksi uhaksi näiden hallintaan uskotut teknologiat koetaan.[392]

Beckin mukaan riskit ovat avoimia sosiaaliselle rakentumiselle ja määrittelylle, joten *tietoisuus* riskeistä liittyy tiedon valtaan ja auktoriteettiasemiin. Riskikäsityksiä on mahdollista muuttaa tai minimoida

389 *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 135–136.

390 *Kuusela – Ollikainen,* Riskit ja riskinhallinta-ajattelu, s. 16.

391 *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 136.

392 *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 136.

uuden tiedon avulla.[393] Riskien ulottuvuuksista tieto on keskeisessä asemassa, sillä se muovaa riskejä. Omakohtaiseen kokemukseen perustuvia riskihavaintoja on vaikea kumota teoreettisilla yleistyksillä. Teoreettinen tieto ei koskaan voi syrjäyttää havaintoon ja kokemukseen perustuvaa tietoa.[394] Esimerkiksi identiteettivarkauden uhria teoreettinen kuvaus teon haitattomuudesta ei vakuuta. Myös riskiviestintä vaikuttaa riskien kokemiseen, sillä kysymys ei ole pelkästään riskeistä sinänsä, vaan myös siitä, kuka niistä kertoo ja miten.

Riskeistä puhuttaessa *aika* on keskeinen ulottuvuus. Teknologian riskien ajallisiin ominaisuuksiin suhtautuminen on kaksijakoista.[395] Yhtäältä riskien arvioinnissa pätee hieman samansuuntainen ajatus kuin riskien kohdentumisen kohdalla: mitä lähempänä tapahtumat ovat ajallisesti, sitä painavampina ne näyttäytyvät. Toisaalta ajallisesti kaukaisia haittoja pelätään. Riskien ajallisen ulottuvuuden jäsentymistä vaikeuttaa lisäksi se, että monet prosessit ovat ajallisesti vaikea hahmottaa. Yksilö operoi omassa elämässään tyypillisesti korkeintaan muutaman vuosikymmenen aikavälillä ja poliittinen päätöksenteko yleensä vielä lyhyemmällä aikavälillä.[396]

Teknologiaa koskeva päätöksenteko huomioi tietyn määrän vaikutuksia, jotka harvemmin ulottuvat muutamaa vuosikymmentä pidemmälle. Maallikot eivät välttämättä ole tietämättömämpiä tai pelokkaampia kuin asiantuntijat. Yksilöt vain arvioivat riskejä useammilla

393 *Beck,* Risk Society: Towards a New modernity, s. 21-24

394 Modernissa yhteiskunnassa tieto omaa erityistä sosiaalista arvoa. Syynä on se, että uskomuksiin suhtaudutaan täysin eri tavalla, kun se muuttuu tiedoksi. Tässä tieteellisen tiedon tuottajilla on keskeinen asema, sillä he ovat todellisuuden mittareita, joihin pääsääntöisesti uskotaan. *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 136–137.

395 *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 137–138

396 *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 138. Katso myös *Kuusela – Ollikainen,* Riskit ja riskinhallinta-ajattelu, s. 37.

ulottuvuuksilla kuin asiantuntijat.[397] Monet maallikoiden kannalta tärkeistä ulottuvuuksista ovat kuitenkin sellaisia, ettei niitä voida saattaa yhteismitallisiksi tai arvioida luotettavalla asteikolla. Tästä huolimatta ne muistuttavat tärkeistä seikoista, kun tulevaisuutta koskevia päätöksiä ollaan tekemässä.

4.3.4. Riskien arviointi

Riski on pelottava kun se on hallitsematon, sisältää katastrofin ainekset ja katastrofilla on paljon uhreja ja seuraukset ovat kohtalokkaita. Riskin pelottavuutta lisää myös, että tapahtuma on riski tuleville sukupolville ja haitan vaikutukset ovat epäoikeudenmukaisia. Yhtä lailla riskin pelottavuutta lisää riskin lisääntyminen ajan myötä ja se, että riski ei ole vapaaehtoinen.

Olennainen riskiin liittyvä piirre on epävarmuus. Tulevia tapahtumia ei varmuudella voi tietää, vaikka tunnetaan tapahtumien todennäköisyyksiä. Riskin olemukseen liittyy aina myös, että tapahtumien hajonta vaihtelee ja riskien toteutuminen on yksilöllistä. Tapahtumien poikkeamista odotetusta tuloksesta tai tapahtumasta on arvioitavissa todennäköisyyksien avulla. Tämän vuoksi on kehitetty tapoja arvioida riskejä. Riskien välttämisessä yksilöllä, yrityksillä ja yhteiskunnalla on käytettävissään erilaisia varautumissuunnitelmia. Riskienhallinta on prosessi, jonka kautta tunnistetaan ja arvioidaan riskejä sekä valitaan ja toteutetaan toimenpiteitä, jotka vähentävät niiden seurauksia.[398]

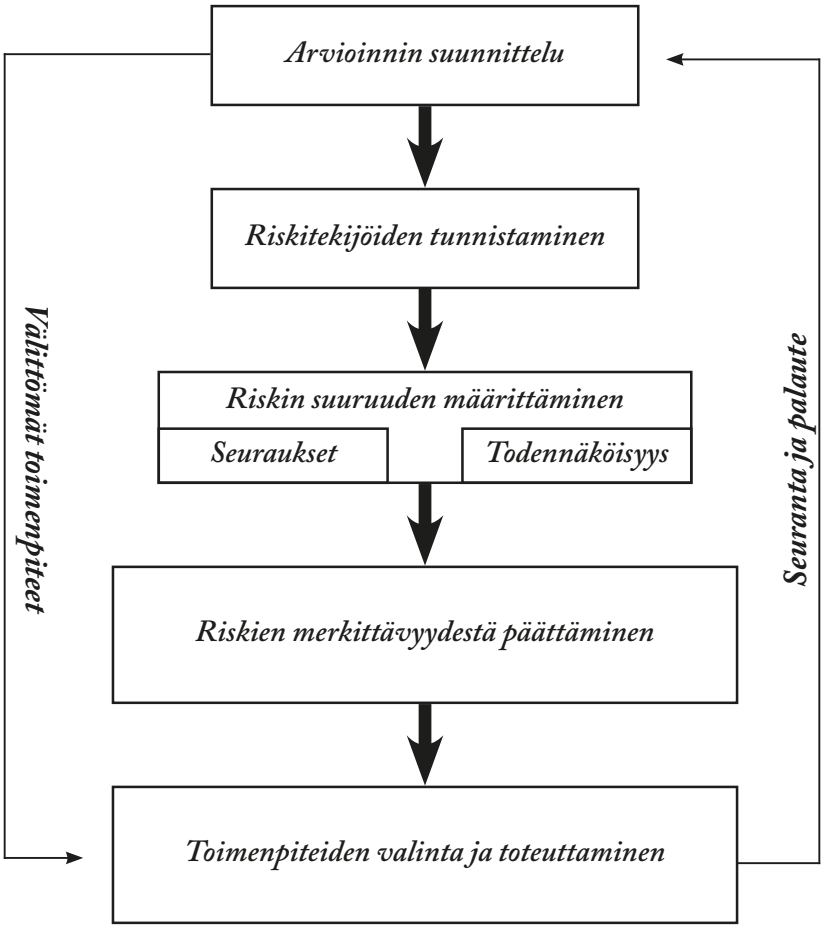
Tässä tutkimuksessa on käytetty neljään vaiheeseen jakautuvaa riskien arviointia. Malli on tarkoitettu biometrisen tunnistamisen järjestelmän ylläpitäjän käyttöön tekniikan käytöstä aihetutuvien riskien hallitsemiseksi. Vaiheet on taulukon (kuvio 4) muodossa esitettävissä seuraavasti:

---

397 *Kamppinen,* Teknologian riskit ja tulevaisuus, s. 138–139.

398 *Kuusela – Ollikainen,* Riskit ja riskinhallinta-ajattelu, s. 35

Kuvio 4. Riskienhallinnan vaiheet.



Riskien tunnistaminen. Riskinarviointi alkaa riskien tunnistamisesta. Se on riskinarvioinnin ensimmäinen ja tärkeä vaihe. Tavoitteena on löytää vastaus seuraaviin kysymyksiin:

- Mitä riskejä biometrisen tunnistamisen käytössä esiintyy?
- Mikä riskin aiheuttaa?
- Kuka tai ketkä ovat riskeille alttiina?
- Mitä vahinkoa riskin realisoitumisesta voi aiheutua?

Riskien tunnistaminen tarkoittaa kaikkien biometrisen tunnistamisen käytöstä riskejä aiheuttavien tekijöiden ja niiden syiden tunnistamista. Tunnistamisessa tulee ottaa huomioon aiemmin toteutuneet ja myös mahdolliset vielä toteutumattomat riskit. Riskien tunnistamisen lisäksi tulee tunnistaa vaaroille alttiiksi joutuvat henkilöt.

Riskin suuruuden arviointi. Riski on toiminnan aiheuttamien vahinkojen vakavuuden ja todennäköisyyden yhdistelmä. Yksinkertaisimmillaan riski määritellään vahingon mahdollisuudeksi, ja se osoitetaan kaavalla: riski = todennäköisyys x vahinko.[399] Riskissä on kaksi osaa: vahinko ja vahingon todennäköisyys.

Riskin suuruuden määrittämisen tarkoituksena on löytää riskeille niiden suuruutta kuvaava tunnusluku ja asettaa vaaratekijät riskin suuruuden mukaiseen järjestykseen. Määrittämällä riskin suuruus, tunnistetaan suurimmat riskit. Kohdistamalla toimenpiteitä suurimpien riskien pienentämiseksi, kohdistetaan toimenpiteet tehokkaasti juuri ongelmallisimmiksi koetuille alueille.

Riskin selvittäminen edellyttää sen aiheuttajan ja ratkaisusta aiheutuvien vahinkojen ja hyötyjen yksilöintiä sekä seurausten esiintymisen todennäköisyyden arviointia.[400] Näitä tekijöitä eri lailla painotettaessa

399 *Kamppinen – Raivola – Jokinen – Karlsson,* Riskit yhteiskunnassa. Maallikot ja asiantuntijat päätöksentekijöinä, s. 15.

400 *Kumpula,* Vaarojen varjoista nousevat riskit, s. 319

ihmiset päätyvät erilaisiin riskiarvioihin.[401] Riskimäärittelyt riippuvat myös arvoista ja arvostuksista. Riskit ovatkin osaksi yhteiskunnallisen kehityksen ja sosiaalisen määrittelyn tulosta.[402] Esimerkiksi yksityisyyden ja henkilötietojen suojan arvostus saattaa vaihdella käyttäjittäin tai käyttäjäryhmittäin. Myös käytettävällä tekniikalla on merkitystä. Tekniikan käyttämisen seuraukset arvioidaan todennäköisesti eri tavalla myös järjestelmän käyttäjän ja ylläpitäjän näkökulmista.

Riskin merkittävyydestä päättäminen. Riskin merkittävyydestä päättäminen tarkoittaa rajanvetoa sille, pienennetäänkö riskiä vai ei. Kaikkien riskien poistaminen ei aina ole mahdollista. Arvioinnissa tulee pohtia toimenpiderajoja: suurimpiin riskeihin keskitytään ensin ja toimenpiteet kannattaa ulottaa niin laajalle kuin mahdollista. Tavoitteena on poistaa tai pienentää kaikkia riskejä.

Toimenpiteiden valinta. Riskien arvioinnin tavoitteena on löytää tehokkaimmat toimenpiteet järjestelmän parantamiseksi. Ideana on käyttää riskin suuruutta toimenpiteiden kohdistamisperusteena. Suurimpien riskien pienentäminen tai poistaminen tulee olla etusijalla toimenpiteitä toteutettaessa.

Riskin pienentämiseksi tai poistamiseksi tehtävien toimenpiteiden toteuttaminen on riskienhallintaa, ja sen tavoitteena on vahinkojen ennaltaehkäisy ja vahinkokustannusten minimointi. Tavoitteena on löytää parhaita mahdollisia toimenpiteitä riskien pienentämiseksi.

401 *Kamppinen – Raivola – Jokinen – Karlsson,* Riskit yhteiskunnassa. Maallikot ja asiantuntijat päätöksentekijöinä, s. 15

402 *Kumpula,* Vaarojen varjoista nousevat riskit, s. 321

4.4. Biometrinen tunnistaminen ja yksilön identiteetti

4.4.1. Biometrinen tunnistaminen ja sähköinen identiteetti

Tutkimuksesssa on jo aijemmin käsitelty yksilön monia identiteejä suhteessa toisiinsa.[403] Tässä kappaleessa käsitellään tarkemmin verkkoyhteiskunnan identiteetin eli sähköisen identiteetin käsitettä.

Yhteiskunnan digitalisoituminen on johtanut siihen, että myös yksilön ominaispiirteet ja henkilökohtaiset tiedot digitalisoituvat, mikä puolestaan on vaikuttanut digitaalisessa muodossa olevan identiteetin merkityksen korostumiseen verkkojen varaan rakentuvassa yhteiskunnassa. Yksilön perinteisen, fyysisen identiteetin rinnalle on kehittynyt digitaalisen maailman identiteetti.[404]

Verkkoyhteiskunnan identiteetti muodostuu kolmesta osasta, joista jokainen on oma tärkeä kokonaisuutensa. Yläkäsitteenä on yksilön informationaalinen tai tiedollinen identiteetti. Yksilön informationaalinen identiteetti muodostuu yksilöstä eri lähteistä saatavissa olevasta informaatiosta, joiden pohjalta yksilö on tunnistettavissa.

Osana informationaalista identiteettiä on yksilön digitaalinen identiteetti.[405] Digitaalinen identiteetti muodostuu digitaalisessa

403 Huomautettava on kuitenkin siitä, että identiteetti ei ole vain luonnolliseen henkilöön, yksilöön, liittyvä käsite. Myös oikeushenkilöillä voidaan katsoa olevan identiteetti. Tässä tutkimuksessa kuitenkin kiinnitetään huomiota yksilön identiteettiin.

404 Digitaalisen identiteetin kohdalla on alettu puhua myös identiteetti 2.0 tai jopa identiteetti 3.0. –ilmiöistä. Nämä ilmiöt ovat syntyneet web 2.0 –ilmiön mukana.

405 Daniel Solove puhuu digitaalisesta persoonasta tai digitaalisesti henkilöstä. Tämän digitaalisen persoonan hän katsoo muodostuvan kaikesta yksilöön liittyvästä digitaalisesta datasta ja informaatiosta tallennuspaikasta riippumatta. *Solove,* Digital Person. Technology and

muodossa ja yksilöön liitettävissä olevasta informaatiosta.[406] Tämä informaatio jaetaan kolmeen osaan: 1) tunnistautumiseen tarvittava informaatio, kuten IP-osoite, sähköpostiosoite, käyttäjätunnukset ja aliakset; 2) data eli pankkitiedot ja sosiaalinen data[407] jne., 3) digitaaliset jäljet, kuten linkit, blogikommentit jne.[408]

Sähköinen identiteetti puolestaan muodostaa verkkoyhteiskunnan identiteetin syvimmän osan. Sähköisellä identiteetillä tarkoitetaan johonkin luonnolliseen henkilöön teknisesti ja oikeudellisesti luotettavalla tavalla liittyvää informaatiota, jonka perusteella henkilö on tunnistettavissa sähköisessä toimintaympäristössä.[409] Yksilöivän

---

Privacy in the Information Age, s. 1.

406 Näin myös *Sullivan,* Is Your Digital Identity Property?, s. 123.

407 Sosiaalisella datalla tarkoitetaan esimerkiksi henkilön perhettä kuvaavia tietoja, hänen toimintaansa kuvaavia tietoja, hänen yhteystietoja sekä erillisinä yksikköinä hänen rooliaan, asemaansa ja valtuuttaan kuvaavia tietoja tietyssä tilanteessa tai toiminnassa. Näitä tietoja on kirjattu muun muassa väestötietojärjestelmään, kaupparekisteriin, yhdistysrekisteriin, säätiörekisteriin, holhousasioiden rekisteriin sekä viranomaisten muihin yksittäisiin rekistereihin.

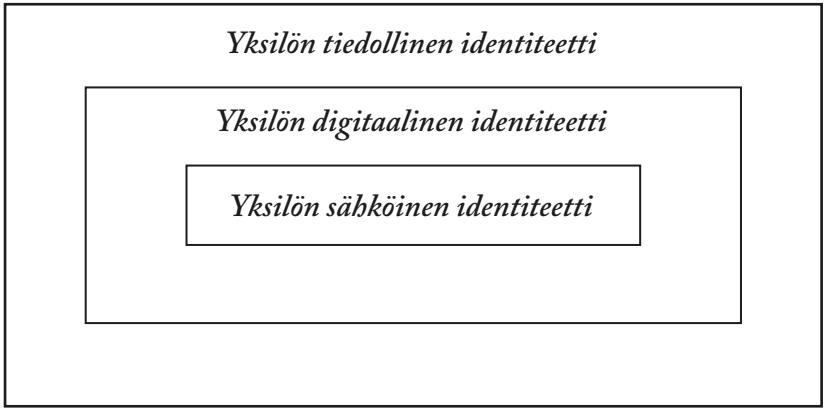
408 Koosel puolestaan kuvaa digitaalista identiteettiä seuraavasti: "Digital identities are who we say we are, when we are online. They can be a subtype of a public persona, an extension of our 'true'selves, or they can be completely fabricated and fantastical, to function as a mask to hide the identity of an Internet user from rest of the world. A digital identity can spin intricate, interconnected webs utilising creative, social and interactive platforms that enable them to share and perform to an open or closed audience." Kooselin kuvaus digitaalisesta identiteetista pohjaa osin Sean Cubittin näkemyksiin. Katso tarkemmin: *Koosel,* Exploring Digital Identity: Beyond the Private Public Paradox, s.1. Katso myös *Cubitt,* Digital Aesthetics. Vertaa *Voutilainen,* ICT-oikeus sähköisessä hallinnossa, s. 241.

409 *Pöysti,* Sähköinen identiteetti, s. 1112.

tiedon tai ominaisuuden on oltava ainutlaatuinen, vain tiettyyn henkilöön yhdistettävissä oleva tieto tai ominaisuus. Kysymys on yksilön tunnistamisen kannalta kaikkein kriittisimmästä informaatiosta, kuten henkilötunnuksesta tai biometrisesta tunnisteesta, joka on mahdollista liittää vain yhteen yksilöön. Sähköinen identiteetti on se osa yksilön identiteettiä, jonka avulla yksilön on mahdollista toimia tietoverkoissa oikeudellisesti luotettavalla tavalla.

Kuvion (kuvio 5) avulla verkkoyhteiskunnan identiteetti voidaan kuvata kerroksittain alla olevalla tavalla:

Kuvio 5. Identiteetti.



Sähköisen identiteetin käsitteeseen liittyy läheisesti sähköisen tunnistamisen käsite. Sähköisen tunnistamisen ja sähköisen identiteetin käsitteiden välille ei voida tehdä tarkkaa eroa. Nämä käsitteet ovat oikeuskirjallisuudessa ja säädösvalmistelussa rinnakkain käytettyjä käsitteitä. Erona näillä käsitteillä on kuitenkin se, että sähköisen identiteetin määritelmässä keskeisessä asemassa on henkilöön liittyvä informaatio, kun sähköinen tunnistaminen puolestaan viittaa tunnistamisessa käytettävään tekniseen menetelmään. Sähköisellä tunnista-

misella tarkoitetaan teknistä menetelmää, jolla tietojärjestelmän käyttäjän ja tietoliikenneviestin lähettäjän henkilöllisyys on luotettavasti selvitettävissä digitaalisessa toimintaympäristössä. Sähköinen tunnistaminen perustuu tunnistamisessa käytettävään, henkilön yksilöivään informaatioon. Sähköinen tunnistaminen perustuu siis yksilön sähköiseen identiteettiin.

Sähköinen viranomaisasiointi ja sähköinen kaupankäynti tarvitsevat fyysisen tunnistamisen sijasta jonkin muun menetelmän käyttäjän tunnistamiseen ja henkilöllisyyden määrittelyyn. Käytettäviä teknisiä menetelmiä kutsutaan sähköiseksi tunnistamiseksi, jonka avulla henkilön oikeudellinen identiteetti ja sen rajat eli henkilön sähköinen identiteetti voidaan luotettavasti määritellä.

Sähköisen tunnistamisen ja määrittelyn perustana olevan informaation on kuitenkin täytettävä tietyt edellytykset. Informaation on ensinnäkin oltava yksilöllistä, ainutlaatuista ja käsiteltävissä koneellisessa muodossa. Yksilöllisyys ja ainutlaatuisuus saavutetaan tunnistamisessa käytettävän informaation salaisuudella ja vaikealla väärennettävyydellä. Käyttökelpoista informaatiota ovat esimerkiksi salasana tai muu tieto, minkä henkilö tietää ja biometrinen tunniste. Sähköisen tunnistamisen kautta biometriset tunnisteet tullee tulevaisuudessa muotoutumaan kiinteäksi osaksi yksilön sähköistä identiteettiä.

Toisaalta biometriset tunnisteet ovat luonteeltaan muuttumattomia yksilön ominaispiirteitä. Biometristen tunnisteiden käyttöä osana sähköistä tunnistamista ei tulisi miettiä ensisijaisena vaihtoehtona. Biometrisen tunnisteen joutuessa vääriin käsiin yksilö saattaa joutua jättäytymään tällaisen tunnistautumismenetelmän ulkopuolelle. Laajassa käytössä tällainen aiheuttaa suuria ongelmia yksilön näkökulmasta.

Biometrisella tunnistamisella tulee olemaan suuri vaikutus yksilön sähköiseen identiteettiin. Biometristen tunnisteiden liittäminen osaksi yksilön sähköistä identiteettiä kasvattaa mahdollisuuksia seurata yksilöä ja hänen identiteettiään digitaalisessa toimintaympäristössä. Otet-

taessa biometrinen tunniste osaksi yksilön sähköistä identiteettiä on sitä mahdollista käyttää identiteetin avaimena. Biometrinen tunniste on lähes poikkeuksetta yksilöllinen ja näin liitettävissä vain yhteen tiettyyn yksilöön yhteiskunnassa. Yksilön tiedollisen identiteetin kaikkein syvin osa eli sähköinen identiteetti on sisäisessä vuorovaikutuksessa myös hänen muiden identiteettiensä kanssa. Yksilön identiteetti on aina myös ulospäin vuorovaikutuksellinen, jolloin sähköisen identiteetin kautta on mahdollista seurata myös muita yksilöitä.

Modernissa eurooppalaisessa oikeusvaltiossa yksilö ja yksilön kunnioitus ovat keskeisiä arvoja – oikeudellisesti ja muutenkin. Liitettäessä biometrinen tunniste tiukasti osaksi yksilön identiteetin käyttämistä on vaarana liiallinen puuttuminen yksilön oikeuksiin. Vähimmän puuttumisen periaatteen mukaisesti ihmisen tulee voida pitää tietyt osat identiteettiään salassa muilta. Biometristen tunnisteiden liittäminen osaksi yksilön oikeudellista ja sähköistä identiteettiä voi johtaa loppujen lopuksi myös yksityisyyden kaventumiseen ja asteittaiseen rapautumiseen.[410] Liiallinen ja liian syvälle menevä puuttuminen yksilön identiteettiin voi johtaa myös identiteetin asteittaiseen murene-

410 Tämä on todettu osaltaan myös sähköisistä allekirjoituksista annetussa EY-direktiivissä, jossa sisäistetyt tyypilliset uhkakuvat ja näitä vastaavat riskiasemat ovat erityisesti mm. seuraavat: 1) identiteettivarkaus, 2) sähköisen identiteetin kontrollin menettäminen ja identiteetin virheet, 3) varmennepalvelujen tarjoajien tietoturvallisuuden ja sen eri osa-alueiden pettäminen tai vaarantuminen, 4) käyttäjän mahdollisuuden anonymiteettiin vaarantuminen tietoverkoissa ja 5) henkilötietojen liian laaja tai epäasiallinen kerääminen ja käyttö palveluntarjoajien toiminnassa. Tässä esitetyt uhkakuvat perustuvat Tuomas Pöystin direktiivin pohjalta tekemään abstraktimpaan luetteloon. Katso tarkemmin *Pöysti,* Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin tietoturvallisuutta, s. 103–104.

miseen. Yksilöllä on oikeus identiteettiin eikä identiteetti voi kehittyä vapaasti, mikäli sitä on mahdollista seurata.

Sähköisen identiteetin käsitettä tulee nykyajan verkkoyhteiskunnassa pitää äärimmäisen tärkeänä, sillä sen avulla sähköisiä menetelmiä käyttämällä tehdyt toimet saadaan kohdistettua tiettyyn henkilöön ja tämän oikeudelliseen toimivaltaan ja kelpoisuuteen. Kysymys on siis henkilön oikeudellisesti luotettavasta tunnistamisesta digitaalisessa toimintaympäristössä toimittaessa.[411]

Yksilön oikeus identiteettiin asettaa julkiselle vallalle velvollisuuden huolehtia identiteetin turvallisesta kehittämisestä ja käyttämisestä. Koska julkisella vallalla on osana perusoikeuksien turvaamista velvollisuus huolehtia identiteetin kehittämisestä, on sillä velvollisuus huolehtia myös niiden edellytyksien luomisesta, joilla yksilön on mahdollista turvallisesti hyödyntää omaa identiteettiään myös digitaalisessa toimintaympäristössä. Yhtenä osoituksena tästä on identiteettivarkauden kriminalisointi.

Julkisen vallan velvoitteena on infrastruktuuria kehittämällä torjua identiteettivarkautta ja sähköisen identiteetin virheellistä kohdentamista. Erityisesti

lainsäätäjän ja hallinnon tehtävänä on tarjota luotettavat ja riittävän turvalliset henkilöllisyyden selvittämisen ja tunnistamisen välineet ja menettelytavat. Julkisen vallan tehtävänä on tarjota muun muassa sähköisen identiteetin käytön välineiden luomisessa käytettävät henkilöllisyyden tunnistamisvälineet. Globaalissa verkkoyhteiskunnassa tämä on korostetun tärkeä yhteiskunnan perusinfrastruktuurin ylläpitämi-

411 Esimerkiksi Virossa on käynnissä niin sanottu E-residency –hanke. Tarkoituksen on luoda e-virolaisuus, jonka voi saada myös ulkomaalaiset. E-virolainen saa id-kortin, jossa on henkilötiedot ja sormenjäljet. Katso tarkemmin https://e-estonia.com/e-residents/about/

seen kohdistuva lainsäädäntö- ja hallintotehtävä.[412] Kysymys on siis siitä, miten tehokkaasti yksilön identiteetti tunnustetaan yhteiskunnassa, jossa palvelut ovat siirtyneet suuressa määrin verkoissa hyödynnettäväksi. Näin ollen sähköistä tunnistamista ei voi luoda yksinomaan yksityisen sektorin rakanentaman välineen varaan. [413]

Digitaalisen aikakauden ominaispiirteet ovat muotoutuneet nopeasti. Tämä on johtanut yksilön identiteetin luomisen ja hallinnan nousemiseen yhdeksi digitaalisen aikakauden merkittävimmistä kysymyksistä. Syynä tähän voidaan nähdä kansalaisten tarve luottaa digitaalisen maailman toimijoihin ja tässä maailmassa käytettäviin teknologioihin ja palveluihin. Tämän luottamuksen aikaansaamiseksi sähköisen identiteetin luominen ja hallinta ovat keskeisiä kysymyksiä.[414] Tämä on saavutettavissa ainoastaan yksityisyyden huomioon ottavalla sähköisen identiteetin viitekehyksellä, joka mahdollistaa tunnistamisratkaisut, jotka suojaavat yksilön ihmisarvoa, tarjoaa suojaa väärinkäyttöä vastaan ja näin turvaa oikeusvaltioperiaatteen toteutumisen myös digitaalisessa toimintaympäristössä. Kysymys on kuitenkin yhteiskunnan kantavien periaatteiden siirtämisestä digitaaliseen elämään.

---

412 *Pöysti,* Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin tietoturvallisuutta, s. 104.

413 Digitaalisen identiteetin käyttötarkoitus voi vaihdella hyvinkin paljon. Digitaalinen identiteetti voidaan luoda esimerkiksi turvallisuussyistä, kaupallisessa tarkoituksessa tai vain huvin vuoksi. Näin myös *Rannenberg – Royer – Deuker,* Introduction, s. 1

414 Viviane Reding on huomauttanut siitä, että identiteettiriskeihin vastaamiseen ei ole olemassa mitään yhtä kaiken kattavaa ratkaisua. Paras tulos saavutetaan hänen mukaansa eri alojen välisellä yhteistyöllä, jonka kautta löydetään tasapainoinen kokonaisuus lailla sääntelemistä, menetelmiä ja teknologiaa. Redingin esipuhe teoksessa The Future of Identity in the Information Society, s. V

4.4.2. Biometrinen tunnistaminen ja identiteettivarkaus

Identiteettivarkaus ei ole uusi ilmiö. Tietoverkot ovat kuitenkin muuttaneet identiteettitiedon väärinkäyttöä ja sen mahdollisuuksia olennaisesti.[415] Tietoverkoissa identiteettitiedon väärinkäytön ominaispiirteenä on suuri hyöty suhteessa pieniin toteutuskustannuksiin sekä kiinnijäämisen riskiin. Koska tietoverkoissa identiteettivarkaus on mahdollista toteuttaa automaattisesti, tekijän on helppo käsitellä erittäin suurta määrää oikeudetta hankittuja identiteettitietoja pienin kustannuksin. Kiinnijäämisen riski on tietoverkoissa erittäin paljon pienempi reaalimaailmaan nähden. Verkko on myös täysin globaali toimintaympäristö, mikä vaikeuttaa identiteettivarkauden selvittämistä.[416]

Varsinainen syy ei ole kuitenkaan mikään näistä edellä mainituista yksin. Pohjimmiltaan kysymys on siitä, että identiteettitietojen merkitys verkkoyhteiskunnassa on olennaisesti korostunut.[417] Ihmisten ja palvelujen siirtyminen verkoissa toimiviksi on muuttanut tunnistamistarpeita yhteiskunnallisessa osallistumisessa. Tätä prosessia kutsutaan tunnistamisen välineistymiseksi ja siinä identiteetti muutetaan mitattavissa olevaksi informaatioksi. Kysymys on välineen avulla tapahtuvasta tunnistamisesta.[418]

Tunnistamisen välineistyminen viittaa siihen, että kasvokkainen tunnistaminen on muuttunut välinein toimivaksi tunnistamiseksi.

---

415 OECD huomautti jo vuonna 1998 turvallisen verkkoasioinnin tärkeydestä myös identiteettivarkauden näkökulmasta. Katso tarkemmin *OECD,* A Borderless World: Realising the Potential of Global Electronic Commerce.

416 *Sisäasiainministeriö,* Henkilöllisyyden luomista koskevan hankkeen loppuraportti, s. 53.

417 *OECD,* Online Identity *Theft,* s. 16.

418 *Caeton,* The Cultural Phenomenon of Identity Theft…, s. 20

Tunnistamisen välineistymisen on mahdollistanut yhteiskunnan digitalisoituminen ja verkkopalvelujen globalisoituminen. Suuri osa yksilöiden identiteettitiedoista on nykyään digitaalisessa muodossa, mikä on omalta osaltaan helpottanut myös identiteettitietojen väärinkäyttöä.

Identiteettivarkaudelle ei ole tarkkaa määritelmää.[419] Sillä viitataan laajaan joukkoon erilaisia tekokokonaisuuksia, joille on yhteistä identiteettitiedon kerääminen oikeudetta ja tämän tiedon käyttäminen joko rikoshyödyn hankkimiseksi tai muulla identiteetin haltijalle vahinkoa aiheuttavalla tavalla. Rikoslain 38 luvun 9a §:ssä identiteettivarkaus on seuraavan sisältöinen:[420] ” *Joka erehdyttääkseen kolmatta osapuolta*

419 Identiteettivarkaus voidaan määritellä myös seuraavasti: rikos, jossa oikeudettomasti hankittua toisen yksilön identiteettiä käytetään petoksen tekemiseen tai muuhun rikolliseen toimintaan, yleensä taloudellista hyötyä tavoitellen. (vapaa käännös). Määritelmän on esittänyt Belgian sisäministeri vuonna 2005. Katso Vragen en Antwoorden, Senaat 2004-05, 21.3.2005 (Vraag nr. 3-2371 van mevrouw Hermans d.d. 21 maart 2005). Saatavilla osoitteessa: http://www.senate.be/www/?MIval=/publications/viewPubDoc&TID=50344709&LANG=nl

420 Jo ennen identiteettivarkauden kriminalisointia rikoslakiin sisältyi eräitä pykäliä, jotka suojaavat henkilöllisyyttä joko suoraan tai välillisesti. Esimerkiksi toisena henkilönä esiintyminen viranomaiselle on RL 16 luvussa kattavasti kriminalisoitu: Kysymyksessä voi olla väärän henkilötiedon antaminen viranomaiselle, rekisterimerkintärikos sekä väärän todistuksen antaminen viranomaiselle. Huomattava kuitenkin on, että yksityiselle toisena henkilönä esiintymistä ei sellaisenaan ollut kriminalisoitu. Tämä koski esimerkiksi väärän henkilötiedon antamista pankissa, vakuutusyhtiössä, kaupassa, tai muussa vastaavassa paikassa, ellei kyseinen liikeyritys toimi julkista valtaa käyttävän viranomaisen apuna. HE 6/1997 vp, s.67 Oikean, mutta varastetun asiakirjan esittäminen yksityiselle palveluntarjoajalle ei ole

oikeudettomasti käyttää toisen henkilötietoja, tunnistetietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee."[421] Identiteettitietoja ovat varsinaisten henkilötietojen lisäksi erilaiset tunnisteet, joilla osoitetaan tunnisteen haltija tai tunnisteen haltijan oikeus päästä käsiksi tietoon tai palveluun. Esimerkkeinä ovat erilaiset korttien numerot, tilien ja palveluiden käyttäjätunnukset sekä biometriset tunnisteet.

Identiteettivarkaus on terminä kuitenkin harhaanjohtava, sillä identiteettivarkaudessa identiteettiä ei useimmiten oteta pois uhrin käytöstä. Identiteettiä – tai oikeammin identiteettiä koskevia tietoja – käytetään oikeudetta uhrin tietämättä. Oikeampaa olisikin käyttää termiä identiteettiin liittyvät rikokset tai identiteettirikokset. Tällainen termi on riittävän laaja ja kattaa kaikenlaiset teot liittyen identiteettiin, kuten identiteettivarkaudet ja henkilöllisyyden käytön.[422] Identiteet-

---

siis ennen identiteettivarkauden kriminalisointia ollut itsessään rangaistavaa. Tämä osoittaa sen, että Suomessa identiteettivarkauksien säädöstarve on ollut ilmeinen.

421 Myös Yhdysvalloissa identiteettivarkaus on kriminalisoitu liittovaltiotasolla (Identity Theft and Assumption Deterrence Act of 1998). Ratkaisussa Flores-Figueroa v. United States (556 U.S. 646 (2009)) identiteettivarkaus määriteltiin seuraavasti: "knowingly transfer[-ring], possess[ing], or us[ing], without lawful authority, a means of identification of another person." Katso myös ratkaisu U.S. v. Ozuna-Carbera (663 F.3d 496 (2011)).

422 Tämä on todettu EU:n OSA-neuvoston joulukuussa 2010 antamassa selvityksessä sekä YK:n identiteettiin liittyviä rikoksia koskevassa selvityksessä Handbook on Identity Related Crime. Kansainvälisellä tasolla yleisesti esiintyviä identiteettivarkauden termejä ovat mm. "identity theft" ja "identity fraud". Nämä termit esiintyvät ennen

tivarkaus on nimityksenä kuitenkin niin laajalti käytetty, että sen katsotaan heikkouksistaan huolimatta vakiintuneen.[423]

Identiteettivarkaudessa näyttäytyy kaksi elementtiä. Ensimmäinen on se, että identiteetin varastamiseen sisältyy toisen henkilön henkilöllisyyteen liittyvän tunnisteen tai muutoin hänelle yksin kuuluvan tunnisteen luvaton käyttöönotto ja hankinta. Toisena elementtinä on se, että hallussa tai tiedossa olevaa identiteettitietoa käytetään hyväksi. Tietojen käyttö voi tapahtua perinteisellä manuaalisella tavalla tai sähköisesti. Esimerkiksi toisen henkilöllisyystodistusta tai muuta identiteettiasiakirjaa käyttäen täytetään tilauslomakkeita palveluiden tai tavaroiden hankkimiseksi ilman henkilötietojen omistajan suostumusta. Toisaalta tiedon käyttö voi tapahtua sähköisesti erilaisia palveluja ja sitoumuksia tehden. Identiteettejä myös varastetaan eteenpäin myytäväksi rikollisiin tarkoituksiin.[424]

Tekotapojen vuoksi identiteettivarkaudet jaetaan perinteisiin reaalimaailmassa tapahtuviin identiteettivarkauksiin ja tietoverkoissa tapahtuviin identiteettivarkauksiin.[425] Perinteisissä identiteettivarkauksissa on hyvin pitkälti kysymys ns. henkilöllisyysvarkaudesta, jossa teko kohdistuu nimenomaan henkilöön ja jossa kerättävä tieto on henkilö-

---

kaikkea Yhdysvalloissa ja Iso-Britanniassa. Tosin muitakin ilmauksia käytetään. Katso *Gercke,* Legal Approaches to Criminalize Identity *Theft,* s. 25. Handbook on identity related crime

423 Yhtenäisen määritelmän puutetta voidaan pitää hidasteena identiteettivarkauden kansainvälisessä torjumisessa. *OECD,* Online Identity *Theft,* s. 9.

424 *Kangasniemi,* Identiteettivarkaudet – haasteita rikostutkinnalle ja – oikeudelle, paljon vaivaa ja harmia uhrille, s. 218-219. Katso myös *Gercke,* Legal Approaches to Criminalize Identity *Theft,* s. 19-20.

425 Perinteisillä identiteettivarkauksilla tarkoitetaan perinteisillä asiakirjoilla (esim. passi) reaalimaailmassa tehtäviä tekoja. Tietoverkoissa tapahtuvilla identiteettivarkauksilla puolestaan viitataan tietoverkoissa

tieto. Esimerkkinä mainittakoon lompakon varastaminen ja sitä kautta tietojen haltuunsaanti. Käyttäjän on mahdollista saada tiedot haltuunsa myös täysin laillisesti esimerkiksi pois heitetyn postin kautta.

Tietoverkoissa tapahtuvassa identiteettivarkaudessa identiteetti voi olla henkilötiedon lisäksi mikä tahansa tunniste, jota käytetään joko vain erottelemaan kokonaisuudet toisistaan tai osoittamaan, että tunnisteen haltija on se, joka hän väittää olevansa tai että tunnisteen haltijalla on oikeus päästä käsiksi tietoon tai palveluun, johon identiteetin todellisella haltijallakin on oikeus.[426] Tietoverkoissa tapahtuvissa identiteettivarkauksissa identiteettitieto hankitaan ja saadaan haltuun tietoverkoista.

Identiteettivarkaudet ovat teon tarkoituksen perusteella jaettavissa kolmeen kategoriaan:[427]

1) Taloudellista tai muuta hyötyä tavoittelevat identiteettivarkaudet.

Nykyajan informaatioyhteiskunnassa informaatiolla on todella suuri rahallinen arvo. Henkilötietoja myydään ja kerätään ammatti-

---

tapahtuviin identiteettitiedon väärinkäyttöihin. Sisäasiainministeriö, Henkilöllisyyden luomista koskevan hankkeen loppuraportti, s. 53. Katso myös *OECD,* Online Identity Theft.

426 *Sisäasiainministeriö,* Henkilöllisyyden luomista koskevan hankkeen loppuraportti, s. 47-48. Huomionarvoista on se, että identiteettivarkauksia tehdään yleensä oman identiteetin peittämiseksi. Esimerkiksi Yhdysvaltojen liitovaltion poliisi FBI huomauttaa siitä, että identiteettivarkaudet tehdään yleensä rikollisten ja terroristien henkilöllisyyden suojaamiseksi. Katso tarkemmin: http://www.fbi.gov/about-us/investigate/cyber/identity_theft

427 Jaottelu perustuu Sisäasiainministeriön Henkilöllisyyden luomista koskevan hankkeen loppuraporttiin ja YK:n julkaisemaan identiteettivarkauksia koskevaan käsikirjaan. Sisäasiainministeriö, Henkilöllisyyden luomista koskevan hankkeen loppuraportti, s. 53–58. sekä *Gercke,* Legal Approaches to Criminalize Identity *Theft,* s. 20.

maisesti yritysten välillä. Tämä on johtanut siihen, että myös identiteettivarkauksilla tavoitellaan yhä yleisemmin taloudellista hyötyä. Ammattimaisesti ja järjestäytyneellä tavalla toimivien rikoksentekijöiden tavoite on yksinkertainen: mahdollisimman suuren taloudellisen hyödyn saaminen mahdollisimman pienellä riskillä. Tavoitteena on hankkia rikoksen uhreilta mitä tahansa identiteettitietoa, joka on helposti muutettavissa rahaksi.[428] Identiteettitietoja varastetaan myös oman identiteetin piilottamiseksi.

Tietoverkon identiteettirikosten ansaintalogiikassa ratkaiseva tekijä on ennen kaikkea tietomassan valtava koko. Ansaintalogiikka ei siis perustu ensisijaisesti jonkin todella arvokkaan yksittäisen tiedon kaappaamiseen, vaan kysymys on nimenomaan massailmiöstä. Tarkoituksena on talousrikosten, kuten petoksen tekeminen varastetun identiteetin avulla, varastetun identiteettitiedon myyminen taloudellisen hyödyn toivossa tai oman identiteetin piilottaminen luomalla uusi identiteetti varastetun identiteettitiedon avulla.

2) Vahingontekotarkoituksessa toteutetut identiteettivarkaudet.

Identiteettivarkaus on myös yksi informaatioyhteiskunnan uusista kiusantekovälineistä. Tämä on johtanut siihen, että identiteettivarkauksia tehdään myös uhrin vahingoittamiseksi. Yhtenä identiteettivarkauden muotona ovatkin sellaiset koulu- ja työpaikkakiusaamiset, joissa ei synny taloudellisia tappioita eikä tavoitella taloudellista hyötyä. Motiivina tällaisessa identiteettivarkaudessa on kiusanteko. Se

428 Tyypillisiä kohteita ovat maksuvälinetunnisteet (esimerkiksi luottokorttinumerot, verkkopalveluiden asiointitunnukset sekä sähköpostiosoitteet). Huomautettava on kuitenkin siitä, että rikolliset keräävät kuitenkin entistä enemmän myös muuta henkilötietoa (kuten henkilöiden nimiä, katuosoitetietoja, henkilötunnuksia ym.). Näitä tietoja on mahdollista käyttää muun muassa törkeiden petosten, törkeiden maksuvälinepetosten sekä niihin liittyvän törkeän rahanpesun lisäksi laittoman maahantulon järjestämiseen.

muistuttaa reaalielämän perinteistä identiteettirikollisuutta yksittäistapauksellisuudellaan.

Tavoitteena tällaisessa identiteettivarkauden muodossa on jonkun henkilön tai tahon vahingoittaminen. Reaalimaailmaan verrattuna tietoverkossa kunniaa tai yksityisyyttä loukkaava tieto on mahdollista saada leviämään paljon suuremmalle joukolle. Erona on myös se, että loukkauksen välikappaleena käytetty tieto voi olla hyvin vaikeaa poistaa verkosta sen päästyä kerran leviämään riittävän laajalle. Tällöin teon vaikutukset voivat seurata rikoksen asianomistajaa vielä pitkään.

3) Muut identiteettivarkaudet.

Tähän kategoriaan lukeutuu suuri joukko erilaisia identiteettivarkauksia. Näiden tavoitteena ei ole taloudellisen hyödyn tavoittelu eikä vahingon aiheuttaminen identiteettivarkauden kohteelle. Sosiaalisessa mediassa luodaan esimerkiksi valeprofiileja jonkun julkisuuden henkilön nimissä ilman varsinaista vahingoittamistarkoitusta.

Identiteettivarkauksia ei ainakaan ensimmäisenä yhdistäisi biometriseen tunnistamiseen. Biometristen tunnisteiden liittäminen osaksi yksilön sähköistä identiteettiä on kuitenkin yleistymässä. Biometristen tunnisteiden käyttöä yksilön tunnistamisessa on perusteltu sillä, että käytettäessä biometrisia tunnisteita osana yksilön identiteettiä vaikeutetaan identiteettivarkauksia. Samalla kuitenkin saatetaan edesauttaa erittäin yksilöivän identiteettitiedon väärinkäyttöä.

On kuitenkin harhaanjohtavaa ajatella, että biometriset tunnisteet itsessään estäisivät identiteettivarkauksia. Näin siksi, että liitettäessä biometrinen tunniste osaksi yksilön sähköistä identiteettiä muutetaan fyysinen ominaispiirre digitaaliseen eli sähköiseen muotoon, joka on erittäin arkaluontoinen ja arvokas identiteettitieto. Tämän identiteettitiedon arvo perustuu nimenomaan tämän tiedon luonteeseen. Yksilön biometrinen tunniste on hyvin henkilökohtainen, sillä se on yhdistettävissä vain yhteen yksilöön yhteiskunnassa.

Kysymys on siis yksilön informationaalisen identiteetin kaikkein syvimmästä osasta, johon perustuvaa tunnistamista pidetään lähes täysin luotettavana. Tässä on myös tämän identiteettitiedon arvon perusta. Biometristen tunnisteiden ottaminen osaksi yksilön sähköistä identiteettiä saattaa osaltaan kääntyä tarkoitustaan vastaan, ja näin kannustaa toisen identiteetin luvattomaan hyväksikäyttöön.[429] Biometrisia tunnisteita ei tulisi käyttää identiteettivarkauksien ehkäisyssä pelkästään jo niiden yksilöllisen ja peruuttamattoman luonteensa vuoksi.[430]

429 *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 346. Katso myös *Gripjink,* Trend report on biometrics: Some new insights, experiences and developments, s. 262 sekä *Gripjink,* Two barriers to realizing the benefits of biometrics, s. 138–145.

430 Näin myös *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 348, jossa Kindt toteaa: "once the unique biometric data, whether the samples or the templates, are abused or stolen, it is in principle not possible for the data subject or for the controller to revoke the biometric data which will always remain based on the same biometric characteristics, let alone to revoke the biometric characteristics as such."

Nykyajan informaatioyhteiskunnassa identiteetti on suhteellisen helppo varastaa. Vielä helpompaa on kuitenkin identiteettivarkauden riskin vähentäminen. Identiteettivarkauksien torjunnassa oleellisin asia on niiltä suojautuminen ja ennaltaehkäisy. Tämä edellyttää sitä, että on tiedettävä omat identifioitavat tiedot, joita on käsiteltävä turvallisesti mukaan lukien myös tietojen säilyttäminen ja luovuttaminen.[431] Lisäksi henkilötietojen turvalliseen hävittämiseen tulee kiinnittää huomiota.[432]

431 Tosin on huomautettava siitä, että identiteettitietoja kerätään ja talletetaan niin monen eri tahon toimesta, että on käytännössä mahdotonta olla selvillä kaikista identiteettitiedoistaan. Tietyt identiteettitiedot, kuten henkilötunnukset ja biometriset tunnisteet, ovat kuitenkin sellaisia, joiden käyttöön ja luovuttamiseen tulee kiinnittää suurta huomiota niin tiedon kerääjän kuin tiedon luovuttajankin taholta.

432 OECD:n suosituksen mukaan identiteettivarkauden ehkäisyssä tulee eniten kiinnittää huomiota tietoisuuden lisäämiseen ja koulutukseen. Oleellinen osa identiteettivarkauksien ehkäisyssä on myös tietoturvallisuus ja sen parantaminen. *OECD,* Online Identity *Theft,* s. 105–111.

5. Biometrisen tunnistamisen sääntely

5.1. Yleistä

Biometristen tunnistusmenetelmien nopea kehitys ja viime vuosina yleistynyt soveltaminen edellyttävät niiden huolellista tarkastelua tietosuojan näkökulmasta. Tarkastelun tarpeeseen on syynä biometristen tunnisteiden luonne sekä se, että biometristen tunnisteiden laaja ja sääntelemätön käyttö aiheuttaa huolta erityisesti yksilön perusoikeuksien ja -vapauksien kunnioittamisesta. Tämän tyyppiset tiedot ovat luonteeltaan erityisiä, sillä ne kuvaavat yksilön käyttäytymistä ja fysiologisia ominaispiirteitä ja voivat näin mahdollistaa hänen yksilöllisen tunnistamisensa. Tämän vuoksi on erityisen tärkeää tarkastella biometriseen tunnistamiseen liittyvää sääntelyä.

5.2. Yksityisyys ja henkilötietojen suoja ihmisoikeuksina

Ihmisoikeudella tarkoitetaan kaikille kansainvälisesti tunnustettua arvoa tai arvoa, jolle on vaadittu kansainvälistä tunnustusta. Ihmisoikeuksien arvon tunnustaminen on tapahtunut lähinnä kansainvälisten sopimusten kautaa. Nämä sopimukset eivät velvoita kirjoittamaan sopimusvaltioiden perustuslakeja sopimusten sisällön mukaisiksi, vaan sitovat sopimusvaltiot toteuttamaan toiminnallaan sopimusten sisältämät velvoitteet oikeudenkäyttöpiirissään.[433]

433 *Jyränki,* Valta ja vapaus, s. 501–502. Jyrängin mukaan kysymys on eräänlaisesta lainsäädännön yhtenäistämispyrkimyksestä. Vertaa *Koskenniemi,* Ihmisoikeudet ja globalisaatio, s. 194, jonka mukaan yhtenäistämispyrkimyksestä on ainakin kansainvälisessä oikeudessa

Eurooppaa pidetään ihmis- ja perusoikeuksien suojaamisessa edelläkävijänä maailmassa. Oma vaikutuksensa on ollut toisen maailmansodan aikaisilla tapahtumilla, joiden vaikutuksesta havahduttiin perus- ja ihmisoikeuksien tarpeeseen. Näiden tarpeiden ja tapahtumien vuoksi Euroopassa alettiin valmistella kansainvälistä sopimusta ihmisoikeuksista. Kansainvälisten ihmisoikeussopimusten asema EU-oikeudessa on kuitenkin epäselvä ja osin kiistanalainen. Poikkeuksena on kuitenkin Euroopan ihmisoikeussopimus, jolla on jo pidempään ollut erityinen merkitys EU-oikeudessa.

Erityinen merkitys näkyy siinä, että Euroopan ihmisoikeussopimus asettaa vähimmäistason vastaavien perusoikeuksien suojalle EU-oikeudessa. EU:n perusoikeuskirjan 52 artiklan 3 kohta nimenomaisesti osoittaa, että perusoikeuskirjassa tunnustettujen oikeuksien merkitys on sama kuin vastaavilla oikeuksilla on Euroopan ihmisoikeussopimuksessa. Tämä ei kuitenkaan estä unionia määräämästä tätä laajemmasta suojasta.[434]

Euroopan ihmisoikeussopimuksen 8. artikla on yksityisyyden ja henkilötietojen suojan kannalta oleellisin artikla. Artikla on seuraavan sisältöinen:

1. Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.
2. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

---

luovuttu.

434 *Ojanen,* Perus- ja ihmisoikeudet – Eurooppalaisen konstitutionalismin Akilleen kantapää?, s. 1118

EIS 8 artiklan suoja käsittää neljä eri kohdetta: yksityiselämä, perhe-elämä, koti ja kirjeenvaihto. Nämä suojan kohteet ovat läheisessä yhteydessä toisiinsa ja ovat myös osittain päällekkäisiä. Näiden suojan kohteiden erottaminen ei ole aina mahdollista eikä tarpeellista.[435]

Artiklan tarkoitus on ennen kaikkea yksilön suojaaminen viranomaisten mielivaltaiselta puuttumiselta yksityis- ja perhe-elämään.[436] Tämä velvollisuuden negatiivinen puoli on oikeuskäytännössä saanut rinnalleen myös positiivisen puolen. Velvollisuuden positiivinen puoli asettaa valtiolle velvollisuuden ryhtyä toimenpiteisiin yksityis- ja perhe-elämän tehokkaaksi turvaamiseksi.[437]

Yksityiselämän suojaaminen velvoittaa valtion säätämään riittävät lainsäädännölliset takeet tämän oikeuden suojaamiseen myös yksityisten toiminnassa. Velvoitteen kohdalla valtiolla on kuitenkin katsottu olevan varsin paljon harkintavaltaa.[438] Valtio saa siis suhteellisen vapaasti valita, miten velvoitteen toteuttaa.

Euroopan ihmisoikeussopimuksen 8 artiklan kohdalla on erityisesti tullut ilmi EIT:n oikeuskäytännön dynaamisuus ja evolutiivisuus. EIS

---

435 *Hirvelä. – Heikkilä.,* Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön, s. 359.

436 Katso esimerkiksi Kroon ym. v. Alankomaat (no. 18535/91, 27.10.1994), Marckx v. Belgia (no. 6833/74, 13.6.1979) ja Airey v. Irlanti (no. 6289/73, 9.10.1979).

437 *Hirvelä – Heikkilä,* Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön, s. 360. Positiivisesta ja negatiivisesta velvoitteesta katso myös Pellonpää ym., Euroopan ihmisoikeussopimus. Katso myös tapaukset I. v. Suomi (no. 20511/03, 17.7.2008), Kroon ym. v. Alankomaat (no. 18535/91, 27.10.1994), Marckx v. Belgia (no. 6833/74, 13.6.1979) ja Airey v. Irlanti (no. 6289/73, 9.10.1979).

438 Katso tarkemmin Yourouw, The Margin of Appreciation Doctrine in the Dynamics of the European Court of Human Rights Jurisprudence.

onkin dynaaminen instrumentti, joka kykenee vastaamaan muuttuviin olosuhteisiin ja uudenlaisiin kysymyksiin. Nykyisin 8 artikla koskee mitä moninaisimpia elämänalueita poliisin käyttämistä tutkintakeinoista aina aborttiin asti.

EIS ei sisällä erityisesti henkilötietojen suojaa koskevia säännöksiä. Vaikka EIS 8 artikla ei suoranaisesti viittaa henkilötietojen suojaan, on oikeus henkilötietojen suojaan Euroopan ihmisoikeustuomioistuimen käytännössä katsottu vakiintuneeksi yksityisyyden suojan osaksi.[439]

EIS 8 artiklassa mainittu oikeus yksityisyyteen (yksityiselämän suojaan) on käsitteenä laaja. Se on usein myös yhteydessä ja osin päällekkäinen muiden artiklassa mainittujen suojan kohteiden kanssa. Käsitteen monialaisuutta oikeuskäytännössä voidaan kuvata parhaiten jakamalla se alakäsitteisiin. EIT:n ratkaisukäytännön perusteella yksityiselämän suojaan katsotaan kuuluvaksi ainakin seuraavat alaryhmät: 1) henkilökohtainen identiteetti, 2) henkinen ja fyysinen koskemattomuus, 3) yksilöä koskevan tiedon kerääminen ja käyttäminen, 4) seksuaalinen suuntautuminen ja toiminta sekä 5) sosiaalinen elämä ja henkilökohtaiset suhteet. Edellä luetelluista keskeisiä tämän tutkimuksen aihepiirin kannalta ovat henkilökohtainen identiteettu, henkinen ja fyysinen koskemattomuus sekä yksilöä koskevien tietojen kerääminen ja käyttäminen.

Henkilön identiteettiä koskevat kysymykset on katsottu kuuluvaksi yksityiselämän käsitteen keskeiseen ytimeen. Tämä on ymmärrettävää,

439 Muun muassa Leander-tapauksessa EIT katsoi, että viranomaisen toimesta ilman henkilön suostumusta ja tämän tietämättä tapahtuva henkilön yksityiselämää koskevien tietojen kerääminen, säilyttäminen ja luovuttaminen merkitsivät puuttumista EIS 8 artiklassa suojattuun henkilön yksityiselämään. Leander v. Ruotsi (no. 9248/81, 26.3.1987). Katso myös *Liu,* Bio-Privacy, s. 96 ja de Hert, P – Gutwirth, S, Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action.

sillä Euroopan ihmisoikeussopimus ei takaa oikeutta identiteettiin itsenäisenä ihmisoikeutena. Identiteettiin vaikuttava seikka on ensinnäkin oikeus nimeen. Identiteetistä on kysymys myös henkilön statuksen rekisteröinnissä, henkilön etnisessä alkuperässä sekä mahdollisuudessa tutustua itseään koskeviin viranomaisen asiakirjoihin.[440]

Henkilökohtaisessa identiteetissä on kysymys paljon muustakin kuin nimestä, statuksesta tai etnisestä alkuperästä. Pohjimmiltaan oikeudessa identiteettiin on kysymys yksilön oikeudesta tulla tunnustetuksi yksilönä yhteiskunnassa sekä suojan saaminen identiteetille ja persoonalle. Tällöin oikeus identiteettiin kiinnittyy hyvin voimakkaasti ihmisarvon kunnioittamiseen.

Yksilön näkökulmasta ja valvonnan kannalta tärkeä näkökulma identiteetin oikeuteen on kuitenkin unohtunut. Oikeus identiteettiin ei suojaa vain yksilön oikeutta tulla tunnustetuksi yksilönä ja oman identiteetin vapaata kehittämistä. Tärkeä osa tätä vapautta on vapaus tunnistamisesta ja tähän perustuvasta kontrollista. Oikeus identiteettiin sisältää yksilön oikeuden olla erilaisten tunnistusjärjestelmien ulkopuolella sekä oikeuden identiteetin vapaaseen ja turvalliseen käyttämiseen. Identiteetin vapaa käyttö edellyttää nimenomaan vapautta oman identiteettinsä käyttöön ja hallintaan ilman julkisten tai yksityisten toimijoiden puuttumista.[441] Biometrisella tunnistamisella puututaan tähän oikeuteen, sillä sen tarkoituksena on nimenomaan

---

440 Katso esimerkiksi Stjerna v. Suomi (no. 18131/91, 25.11.1994), B. v. Ranska (no. 13343/87, 25.3.1992), S. ja Marper v. Yhdistynyt Kuningaskunta (no. 30562/04 ja 30566/04, 4.12.2008) sekä Gaskin v. Yhdistynyt Kuningaskunta (no. 10454/83, 7.7.1989).

441 Kindt onkin todennut: "without a specific legal basis, not only police but also private actors are not entitled to identify or to control the identity of individuals or to keep identifying information without consent and plead for the ability to control our identities." *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s.

yksilön tunnistaminen, jonka kautta yksilöitä on myös mahdollista kontrolloida.

Yksityiselämän piiriin kuuluvat myös psyykkiseen ja fyysiseen koskemattomuuteen kohdistuvat loukkaukset. Tällaisia ovat ennen kaikkea henkilön fyysinen koskemattomuus ja itsemääräämisoikeus. Henkilökohtaiseen koskemattomuuteen kuuluu myös henkilöön, hänen vaatetukseensa tai esimerkiksi matkatavaroihin kohdistuva etsintä.[442] Biometrisen tunnisteen ottaminen edellyttää lähtökohtaisesti kajoamista yksilön fyysiseen koskemattomuuteen. Osana koskemattomuutta on yksilön oikeus olla fyysisesti yksin ja liikkua vapaasti. Tämä sisältää myös oikeuden pysytellä erilaisen teknisen valvonnan, kuten biometrisen tunnistamisen ulkopuolella.

Yksityiselämään puuttumisesta on kysymys myös henkilöä koskevien tietojen systemaattisessa keräämisessä rekistereihin ja tällaisten tietojen käyttämisessä. Esimerkkeinä tällaisista rekistereistä ovat esimerkiksi poliisin tai muiden tutkintaviranomaisten henkilötietoja sisältävät rekisterit sekä yksityisten toimijoiden rekisterit.[443] Nämä sisältävät enenevässä määrin myös biometrisia tunnisteita. Esimerkiksi

---

294. Mahdollisuudesta hallita omaa identiteettiään (ability to control identity) katso tarkemmin *EPIC,* Comments to the FTC. Face Facts, s. 8 sekä Kerr – Barrigar, Privacy, Identity and Anonymity.

442 Katso esimerkiksi EIT:n ratkaisut X ja Y v. Alankomaat (no. 8978/80,25.3.1985), M.C. v. Bulgaria (no. 39272/98, 4.3.2004), Pretty v. Yhdistynyt kuningaskunta (no. 2346/02, 29.7.2002) sekä Gillan ja Quinton v. Yhdistynyt kuningaskunta (no. 4158/05, 28.6.2010).

443 Rotaru v. Romania (no. 28341/95, 4.5.2000), Murray v. Yhdistynyt kuningaskunta (no. 14310/88, 28.8.1994), Leander v. Ruotsi (no. 9248/81, 26.3.1987) sekä S ja Marper v. Yhdistynyt kuningaskunta (no. 30562/04 ja 30566/04, 4.12.2008). Katso myös Peck v. Yhdistynyt kuningaskunta (no. 44647/98, 28.1.2003).

poliisin passirekisteriin talletetaan passinhaltijan sormenjäljet ja kasvokuva.

Biometrisen tunnistamisen käytöllä on suuri vaikutus yksityiselämän suojaan. Fysiologisten ominaispiirteiden kohdalla niiden kerääminen edellyttää puuttumista fyysiseen koskemattomuuteen. Niitä kerätään ja käsitellään erilaisissa rekistereissä poliisin ja yksityisten toimesta, minkä lisäksi biometrisella tunnistamisella on oma vaikutuksensa yksilön identiteettiin.[444] Biometrisen tunnistamisen avulla kerättävät tiedot ovat luonteeltaan erityisiä, sillä ne kuvaavat yksilön käyttäytymistä ja fysiologisia ominaispiirteitä ja voivat näin mahdollistaa hänen yksilöllisen tunnistamisensa. Kysymys on siis tiedoista, joiden kautta on mahdollista hyvin voimakkaasti vaikuttaa yksilön identiteettiin ja yksityiselämän suojaan. Esimerkiksi tapauksessa S ja Marper vs. Yhdistynyt kuningaskunta EIT katsoi, että DNAn ajaltaan rajaamaton tallentaminen loukkaa yksilön oikeutta yksityisyyteen. DNA on yksilön muuttumaton tunniste, jonka avulla yksilö on luotettavasti tunnistettavissa.[445]

Biometrisella tunnistamisella tavoitellaan ennen kaikkea turvallisuutta. Sopimuksen 5 artiklan turvaamalla oikeudella henkilökohtaiseen turvallisuuteen ei ole kuitenkaan kovin kattavaa sisältöä. Lähinnä sen tarkoituksena katsotaan olevan mielivallan kiellon korostami-

444 Kindtin mukaan yksilön tunnistaminen ja identiteetin hallinta ilman lainsäädännön tukea vaikuttaa yksilön oikeuteen nauttia yksityisyyden suojaa. Hänen mukaansa pelkkää rekisteröintiä itsessään voidaan pitää yksityisyyden loukkauksena, sillä se aiheuttaa vaaran tunnistamisesta. *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 299. Katso myös EIT:n ratkaisut asioissa Perry v. Yhdistynyt Kuningaskunta (no. 63737/00, 17.7.2003) ja Friedl v. Itävalta (no. 15225/89, 31.1.1995).

445 Tapauksen yksityiskohtaisemmasta tarkastelusta katso esimerkiksi *Liu,* Bio-Privacy, s. 109–115.

nen.[446] Yksityisyyden suojan näkökulmasta suurempi merkitys onkin rajoitusperusteena mainitulla kansallisen ja yleisen turvallisuuden suojelemisella.[447] Tämä johtaa siihen, että on suoritettava punninta yksityiselämän oikeuden ja sen rajoitusperusteen tarpeen välillä. Punninnassa ratkaisu tulee tehdä tapaus- ja tilannekohtaisesti.[448] Punninta tapahtuu ihmisoikeussopimusten sisäisenä operaationa, jossa suhteellisuusperiaatteella on oma paikkansa. Punninta ei tapahdu valmiiksi tulkittujen ihmisoikeusnormien ja kilpailevien oikeushyvien välillä, vaan vastapunnuksilla on oma legitiimi paikkansa ja painonsa ihmisoikeuksien sisältöä koskevassa arvioinnissa.[449]

Arvioitaessa mahdollista 8 artiklan loukkausta käytetään kolmivaiheista menettelyä. Lähtökohtana on sen arvioiminen, onko kysymyk-

446 *Hirvelä – Heikkilä,* Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön, s. 121.

447 Ojanen on huomauttanut siitä, että perus- ja ihmisoikeuksien yleisesti ottaen vahva asema EU:n oikeusjärjestyksessä ei sellaisenaan päde kuitenkaan perus- ja ihmisoikeuksien asemaan niin sanotulla oikeuden, vapauden ja turvallisuuden alueella. *Ojanen,* Perus- ja ihmisoikeudet terrorismin vastatoimissa Euroopan Unionissa, s. 1067.

448 Scheininin mukaan monet ihmisoikeudet, kuten yksityiselämän suojaa koskeva EIS 8 artikla, jättävät jo niitä koskevien kansainvälisten sopimusmääräysten mukaan sijaa punninnalle. Syynä tähän on se, että näihin sisältyvät rajoituslausekkeet viittaavat sallittuihin rajoitusperusteisiin, jotka tulee huomioida sikäli kuin se on välttämätöntä demokraattisessa yhteiskunnassa. *Scheinin,* Punninnasta ja ehdottomista ihmisoikeuksista terrorismia torjuttaessa, s. 204

449 *Scheinin,* Punninnasta ja ehdottomista ihmisoikeuksista terrorismia torjuttaessa, s. 204–205. Punninnassa noudatettavista periaatteista ja niiden kritiikistä katso tarkemmin esimerkiksi *Marshall,* Personal Freedom through Human Rights Law? : Autonomy, Identity and Integrity under the European Convention on Human Rights, s. 37-44.

sessä yksityis- ja perhe-elämä, koti tai kirjeenvaihto. Mikäli näin on, arvioidaan seuraavaksi se, onko kysymyksessä yksityiselämään puuttuminen. Jos puuttumisen olemassaolo todetaan, tulee arvioitavaksi, onko yksityisyyteen puuttuvalle toiminnalle jokin oikeutettu peruste.

Jotta yksityiselämään puuttuminen olisi oikeutettua, sen pitää olla kansallisen lain sallimaa eli puuttumiselle tulee olla oikeusperusta kansallisessa lainsäädännössä. Tämän lain tulee olla saatavilla ja oikeusvaltioperiaatteen mukainen sekä riittävän selvä ja täsmällinen. Laki ymmärretään materiaalisessa merkityksessä eli se kattaa myös oikeuskäytännön ja kirjoittamattoman oikeuden.[450]

Yksityiselämään puuttumisella tulee lisäksi olla oikeutettu päämäärä, joita ovat kansallinen ja yleinen turvallisuus, maan taloudellinen hyvinvointi, epäjärjestyksen ja rikollisuuden estäminen, terveyden ja moraalin suojaaminen sekä muiden henkilöiden oikeuksien ja vapauksien turvaaminen. Yksityiselämään puuttumisen oikeutettu tarkoitus on ollut olemassa esimerkiksi tilanteissa, joissa henkilöstä on salaa kerätty tietoja kansallisten turvallisuusintressien takia.[451]

Näiden kahden edellä mainitun rajoitusperusteen olemassaolo ei vielä kuitenkaan tee rajoitusta hyväksyttäväksi, vaan lisäksi rajoitukselta vaaditaan välttämättömyyttä demokraattisessa yhteiskunnassa. Käytännössä tämä tarkoittaa, että yksityiselämää ei rajoiteta suhteettomasti tavoiteltuun päämäärään nähden. Tällöin perusteltu arvioinnin lähtökohta on vähimmän puuttumisen periaate suhteellisuusperiaatteen osana. Yksityiselämän suojaa rajoitetaan toisin sanoen vain sen verran kuin on kyseisen tavoitteen saavuttamiseksi välttämätöntä.

Rikosten selvittämisen keinot eivät esimerkiksi aina täytä välttämättömyyskriteeriä. Vaikka tietojen kerääminen olisikin laillista, nii-

450 Kopp v. Sveitsi (no. 23224/94, 25.3.1998).

451 Leander v. Ruotsi (no. 9248/81, 26.3.1987). Vertaa kuitenkin M.K. v. Ranska (no. 19522/09, 18.4.2013).

den säilyttäminen yli tietyn ajan ei aina ole tavoiteltujen päämäärien vuoksi välttämätöntä. Tällaisia tietoja ovat muun muassa poliisin keräämät sormenjäljet ja DNA-profiilit.[452] Viranomaisten suorittaman henkilötietojen keräämisen ja rekisteröinnin sallittavuus riippuukin paljolti tiedon luonteesta ja keräämisyhteydestä, niiden käsittelystä sekä tietojen keräämistarkoituksesta.

Tapauksessa S ja Marper v. Yhdistynyt kuningaskunta EIT katsoi, että varsinkin DNAn kohdalla yksityisyyden suojaamiseen tulee kiinnittää erityistä huomiota. Sen kautta yksilöstä on mahdollista saada paljonkin yksityisyyden ydinalueeseen kuuluvaa informaatiota, kuten tietoa yksilön terveydentilasta ja perimästä.[453]

Yksityisten taholta tapahtuva henkilötietojen käsittely saattaa myös merkitä puuttumista yksityisyyden suojaan. Tällöin kysymys voi olla valtion positiivisesta velvollisuudesta suojata yksityishenkilön intressejä toista yksityishenkilöä vastaan.[454] Biometrisen tunnistamisen osalta tämä tarkoittaa sitä, että valtio saattaa olla velvollinen tarvittaessa ryhtymään lainsäädäntötoimiin suojellakseen yksilöitä yksityissektorin toimilta biometrisessa tunnistamisessa.

Valtioille on annettu harkintavaltaa sen suhteen, miten valtio arvioi omien toimiensa oikeutusta eli oikeuksien ja vapauksien käyttämisen rajoituksia demokraattisessa yhteiskunnassa.[455] Harkintavalta ei kui-

---

452 S ja Marper v. Yhdistynyt kuningaskunta ja M.K. v. Ranska.

453 S ja Marper v. Yhdistynyt kuningaskunta.

454 Costello-Roberts v. Yhdistynyt kuningaskunta (no. 13134/87, 25.3.1993) ja *Harris – O'Boyle – Warbrick,* Law of the European Convention of Human Rights, s. 24 Katso myös *Hirvelä – Heikkilä,* Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön, s. 385.

455 Oppi valtion harkintamarginaalista (margin of appreciation) liittyy kiinteästi subsidiariteettiperiaatteeseen. Subsidiariteetti periaate eli toissijaisuusperiaate koskee kansallisen lainkäytön ja EIT:n välistä suhdetta. Tämän mukaan ihmisoikeuksien tulee toteutua kansallisel-

tenkaan ole rajoittamaton, ja sen laajuus riippuu viime kädessä EIT:sta. Jos puuttuminen on marginaalin sisällä, ei loukkausta katsota olevan. Yleisesti ottaen valtion harkintavallan voi sanoa olevan verraten laaja valtion turvallisuuteen liittyvissä asioissa.

Vaikka yksityiselämän suojaa koskeva ihmisoikeusnormi sisältää rajoituslausekkeen, sisältää se kuitenkin myös loukkaamattoman ytimen. Ytimen alueella ihmisoikeusnormi vaikuttaa ehdottomana sääntönä. Punninnalle ei tämän vuoksi ole sijaa ytimessä vaikuttavan säännön soveltamisalueella. Kyseiset säännöt saattavat hyvinkin olla soveltamisalaltaan suppeita, mutta punninnan periaatteellinen torjunta niiden alueelle tultaessa on eräs ihmisoikeusajattelun kulmakivistä.

Valtion harkintavalta katsotaan suppeaksi etenkin silloin, kun kysymys on henkilön identiteetin tai yksityiselämän intiimeistä aspekteista.[456] Nämä ovat yleensä yksityiselämän ydinalueella. Oikeutta yksityisyyteen onkin yleensä katsottu loukatuksi, kun kysymys on henkilön persoonallisuutta koskevista tiedoista, tietoja käsitellään ilman henkilön suostumusta ja tämän tietämättä tai kun näiden tietojen käsittely vaarantaa yksilön oikeuden päättää vapaasti omista asioistaan.[457]

---

la tasolla ja EIT:n tehtävänä on valvoa, että sopimuksessa turvattua vähimmäistasoa ei loukata. *Hirvelä – Heikkilä,* Ihmisoikeudet – käsikirja EIT:n ratkaisukäytäntöön, s. 25.

456 *Hirvelä – Heikkilä,* Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön, s. 26 ja Odiere v. Ranska (no. 42326/98, 13.2.2003). Katso myös *Marshall,* Personal Freedom through Human Rights Law? : Autonomy, Identity and Integrity under the European Convention on Human Rights, s. 42.

457 Katso tarkemmin *Bygrave,* Data protection pursuant to the right to privacy in human rights treaties. Teoksessa International Journal of Law and Information Technology, nro 6, s. 247–284.

5.3. Biometrinen tunnistaminen perusoikeuksien näkökulmasta

Perusoikeudet ovat perustuslaissa ihmisille turvattuja yleisiä oikeuksia. Luonteeltaan nämä oikeudet ovat pysyviä, eikä niihin voida puuttua muuten kuin perustuslain säätämisen järjestyksessä.

Perusoikeudet ovat jaettavissa eksplisiittisiin ja implisiittisiin perusoikeuksiin. Eksplisiittiset perusoikeudet ovat niitä perusoikeuksia, jotka tunnistetaan suoraan perustuslain tekstistä. Implisiittisiä perusoikeuksia ovat puolestaan ne perusoikeudet, jotka eivät suoraan käy ilmi perustuslain tekstistä. Esimerkkeinä implisiittisistä perusoikeuksista ovat henkilötietojen suoja ja itsemääräämisoikeus. Itsemääräämisoikeutta pidetään merkittävimpänä implisiittisenä perusoikeutena. [458]

Pohjimmiltaan perusoikeuksien tarkoituksena on osoittaa, millaisessa oikeusvaltiossa elämme. Näin perusoikeuksista avautuu näkökulma koko oikeusjärjestykseen ja sen ymmärtämiseen. Perusoikeudet muodostavat pohjan koko lainsäädännölle, ja tästä syystä monet niistä ovat myös suoraan sovellettavia yhteiskunnassa toimittaessa.[459]

Luonteensa vuoksi perusoikeudet ovat oikeudellisen vallankäytön ytimessä olevia normeja, jotka viitoittavat oikeusjärjestyksen kehittämissuuntaa, rajoittavat valtion toimintamahdollisuuksia suhteessa sen oikeudenkäyttöpiirissä oleviin ihmisiin ja suojaavat yksilöiden välisissä oikeudellisissa kysymyksissä. Perusoikeuksien tärkeä tehtävä on myös

458 *Neuvonen – Rautiainen,* Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä, s. 32–34. Katso myös *Sinnot-Armstrong,* Two Ways to Derive Implied Constitutional Rights.

459 Katso He 1/1998 vp.

yhteiskunnan perusarvojen tiivistäminen oikeudellisiksi säännöiksi, jotka muodostavat koko oikeusjärjestyksen rungon.[460]

Luonteensa ja käyttötarkoituksensa vuoksi biometrisen tunnistamisen kannalta merkityksellisiä perusoikeuksia ovat oikeus henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen (PeL 7 §) sekä oikeus yksityiselämän ja henkilötietojen suojaan (PeL 10 §). Näiden oikeuksien käyttämisen edellytyksenä ja taustalla on yksilön itsemääräämisoikeus, joka perusoikeutena ei käy suoraan ilmi perustuslain perusoikeusluvusta. Merkityksellinen perus- ja ihmisoikeustasoinen oikeus, joka myöskään ei suoraan käy ilmi perustuslaista, on yksilön oikeus identiteettiin. Kysymyksessä on nyky-yhteiskunnassa usein unohdettu perusoikeus. Se ei kuitenkaan saisi jäädä vaille huomiota. Kaikkien perusoikeuksien taustalla puolestaan vaikuttaa ihmisarvon kunnioitus.

Lähtökohtana ihmisarvon kunnioitus. Ihmisarvolla tarkoitetaan käsitystä inhimillisyyteen ja inhimilliseen olemassaoloon välttämättä kuuluvista elementeistä. Dworkinin mukaan ihmisarvon käsite palautuu käsitykseemme oman elämämme sisäänrakennetusta arvosta ja siihen, kuinka muiden tulee sitä arvostaa.[461] Tämä kuvastaa hyvin ihmisarvon käsitteen luonnetta dynaamisena yhteiskunnallisena käsitteenä, joka muotoutuu ajan mittaan ihmiskäsityksen kehittyessä.[462]

---

460 *Neuvonen – Rautiainen,* Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä, s. 28.

461 *Dworkin,* Life´s Dominion. An Argument about Abortion and Euthanasia, s. 233–241

462 Joissain yhteyksissä on kuitenkin väitetty, että ihmisarvon käsitteellä ei olisi muuta arvoa kuin toimia ihmisen autonomisuuden välikappaleena. *Macklin,* Dignity is a useless concept, s. 1419–1420. Tällainen näkemys ei kuitenkaan voi pitää paikkansa, sillä itsemääräämisoikeus tulee nähdä osana laajempaa ihmisarvon käsitettä. Näin myös *Lötjönen,* Lääketieteellinen tutkimus ihmisillä, s. 85.

Perustuslain 1.2 §:n mukaan Suomen valtiosääntö turvaa jokaiselle ihmisarvon loukkaamattomuuden ja yksilön vapaudet ja oikeudet sekä edistää oikeudenmukaisuutta yhteiskunnassa. Ihmisarvon käsite esiintyy myös perustuslain 7.2 §: ssä, 9.4 §:ssä ja 19.1 §:ssä. Nämä säännökset ovat osoituksena perustuslain perustavan arvolähtökohdan yhteydestä yksilöllisiin perusoikeuksiin.[463] Valtiosäännön yhdeksi tehtäväksi on näin asetettu ihmisarvon loukkaamattomuuden turvaaminen.

Ihmisarvon loukkaamattomuuden vaatimus ilmaisee perustavanlaatuisten oikeuksien yleisinhimillisen perustan. Ihmisarvoa ei tule nähdä vain rajoittamattomien ihmisoikeuksien summana, vaan niiden ja kaikkien muidenkin perusoikeuksien taustalla vaikuttavana käsityksenä siitä, mitä ihmisyys on ja mitä siihen erottamattomasti kuuluu.[464] Tämän vuoksi ihmisarvon kunnioittamisen tärkein vaikutusmekanismi on periaatevaikutus, joka asettaa tavoitteen, mitä kohti pyrkiä.

Ainakin kaikkein perustavimmat ihmisyksilön oikeudet tulee nähdä perimmältään valtion tahdosta ja myös kulloisestakin oikeusjärjestyksestä riippumattomina. Ihmisarvon loukkaamattomuus osoittaa omalta osaltaan myös kaikkien ihmisyksilöiden olevan periaatteelli-

---

463 Ihmisarvon loukkaamattomuus on ollut esillä myös Korkeimman oikeuden ratkaisuissa KKO 1994:62 ja KKO 1993:12. Ratkaisussa KKO 1994:62 rikoksen tekijän maksettavaksi määrättyä vahingonkorvauksen määrää perusteltiin viittaamalla tekijän piittaamattomuuteen uhrin ihmisarvosta. Ratkaisussa KKO1993:12 ensikertalaiselle tuomittua ehdotonta vankeusrangaistusta perusteltiin sillä, että tekosarja oli loukannut uhrin ihmisarvoa. Katso myös ratkaisu KKO 1992:60.

464 *Marshall,* Personal Freedom through Human Rights Law?: Autonomy, Identity and Integrity under the European Convention on Human Rights, s. 23. Katso myös Lötjönen, Lääketieteellinen tutkimus ihmisillä, s. 83–84

sella tasolla yhdenvertaisia.[465] Ihmisarvoisen kohtelun periaate luo myös luontevan lähtökohdan persoonallisuuteen liittyvien oikeuksien laajalle turvaamiselle. Syynä on se, että perustuslain 1.2 § kattaa myös yksilön itsemääräämisoikeuden, joka on perustana muiden oikeuksien käyttöön nähden.[466]

Ihmisarvon loukkaamattomuus on yksi valtiosäännön perusperiaatteista, jotka sisältyvät perustuslain ensimmäiseen lukuun. Periaatteet eivät ole missään hierarkkisessa järjestyksessä, mutta ihmisarvon loukkaamattomuuteen on liitettävissä etusijakorostus. Yhdessä valtiosäännön demokraattisten perusteiden kanssa ihmisarvon loukkaamattomuus edustanee periaatteiden kärkeä.[467] Ihmisarvon merkitystä on korostettu perustuslain muiden säännösten tulkinnassa. Merkitystä ihmisarvon loukkaamattomuuden vaatimuksella olisi esimerkiksi sovellettaessa varsinaisia perusoikeuksia tai arvioitaessa perusoikeuksien rajoitusten sallittavuutta.[468]

Ihmisarvo liittyy kuitenkin useimpiin perusoikeuksiin, joten säännöksellä loukkaamattomuudesta ei ole vaikutusta perusoikeuskollisioiden tilanteessa. Ihmisarvoa on näin ollen vaikea käyttää punnintaperusteena kokonaisarviossa, jossa päätellään, onko tietylle perusoikeusrajoitukselle olemassa perusoikeuksien yleisten rajoitusperusteiden mukaista hyväksyttävää syytä. Säännöksen tulkintavaikutus

---

465 He 309/1993 vp, s. 24.

466 Näin myös *Karapuu,* Oikeus yksityiselämän suojaan, s. 10.

467 *Jyränki,* Uusi perustuslakimme, s. 52–53.

468 He 309/1993 vp, s. 42. Katso myös Ojanen – *Scheinin,* Suomen valtiosäännön perusperiaatteet, s. 223. Katso myös *Pajulammi,* Lapsi, oikeus ja osallisuus, s. 105, jossa Pajulammi esittää näkemyksen, että ihmisarvolla on kahtia jakautunut perustelutehtävä, kun sillä voidaan yhtäältä perustella ihmisen vapautta toimia ja toteuttaa itseään ja toisaalta sillä voidaan perustella noiden vapauksien rajoittamista. *Pajulammi,* Lapsi, oikeus ja osallisuus, s. 105.

aktivoituukin todennäköisimmin silloin, kun hallituksen lakiesityksessä tarkoitettua painavaa yhteiskuntapoliittista perustelua vastassa on perusoikeuden suojaamisintressi.[469]

Ihmisarvon loukkaamattomuuden vaatimuksella on kuitenkin myös kyky saada itsenäistä oikeudellista merkitystä.[470] Sen itsenäiseen oikeudelliseen sisältöön on kuitenkin toistaiseksi suhtauduttu varauksellisesti.[471] Tämän vuoksi ihmisarvon loukkaamattomuuden vaatimus on yhteiskunnan metaoikeus, joka kertoo ihmis- ja perusoikeuksien sisällöstä ja niiden edustamista arvoista.

Ihmisarvo tuleekin nähdä perus- ja ihmisoikeuksien taustalla vaikuttavana arvoperiaatteena ja metaoikeutena, jonka kautta yksilön perustavaa laatua olevat oikeudet ja vapaudet saavat oikeutuksensa. Samalla ihmisarvon vaatimus on kuitenkin noita oikeuksia ja vapauksia rajoittava tekijä yksilön tarvitessa suojelua muita tai omaa itseään vastaan. Ihmisarvon loukkaamattomuudella voidaan myös perustella sekä biometrisen tunnistamisen käytöä että sen kieltämistä. Vähimmän puuttumisen periaate vaikuttaa ihmisoikeutasoisena periaatteena myös ihmisarvon kunnoittamisen kohdalla: yksilön ihmisarvoon tulee puuttua vain sen verran kuin on välttämätöntä halutun tavoitteen saavuttamiseksi.

Oikeus itsemääräämiseen. Yksilön *itsemääräämisoikeus* on osa perusoikeusjärjestelmäämme, vaikkei sitä nimenomaisesti mainita perustuslaissa. Perusoikeusuudistusta koskevan hallituksen esityksen mukaan itsemääräämisoikeus merkitsee yksilön vapautta määrätä itsestään ja

469 *Saraviita,* Perustuslaki, s. 53.

470 Esimerkiksi hedelmöityshoitolaista antamassaan lausunnossa perustuslakivaliokunta totesi, että esimerkiksi sikiöön ja alkioon kohdistuvat ihmisarvoa loukkaavat lääketieteelliset ja tieteelliset kokeilut ovat perustuslain vastaisia. PeVL 59/2002 vp. Katso myös eduskunnan oikeusasiamiehen ratkaisu dnro 2893/2/11.

471 *Tuori,* Tuomarivaltio – uhka vai myytti?, s. 941–942.

toimistaan.[472] Näin ollen perustuslain 1 §:n maininta yksilön vapauden ja oikeuksien turvaamisesta korostaa perusoikeuksien keskeistä asemaa Suomen valtiosäännössä ja kattaa myös monien muiden oikeuksien käytön perustana olevan yksilön itsemääräämisoikeuden.[473]

Itsemääräämisoikeus on kiinteästi sidoksissa perustuslain 10 §:ssä säädettyyn yksityiselämän suojaan. Säännös turvaa osaltaan yksilön itsemääräämisoikeutta, sillä yksityiselämällä ei viitata pelkästään oikeuteen olla yksin rauhassa muilta, vaan siihen sisältyy myös oikeus vapaasti päättää suhteistaan muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään ja ruumiistaan.

Itsemääräämisoikeudelle löytyy 10 §:n ohella tukea muistakin perustuslain perusoikeussäännöksistä. Perustuslain 7 §:n säännös henkilökohtaisesta vapaudesta ymmärretään yleisperusoikeudeksi, joka suojaa ihmisen fyysisen vapauden lisäksi hänen tahdonvapauttaan ja itsemääräämisoikeuttaan. Yksilön itsemääräämisoikeutta turvaavat myös muut vapausoikeudet, kuten uskonnon ja omantunnon vapaus.[474]

Saarenpään mukaan perusoikeudet suojaavat itsemääräämisoikeuden toteutumista sekä sen välttämätöntä rajoittamista suhteessa toisten ihmisten itsemääräämisoikeuteen.[475] Itsemääräämisoikeus on liitettävissä perusoikeussäännöstön kokonaisuuteen ja sitä turvaavat

472 HE 309/1993 vp, s. 52–53.

473 HE 309/1993 vp, s. 42

474 Perustuslakivaliokunnan mukaan itsemääräämisoikeus kiinnittyy useisiin perusoikeuksiin, erityisesti perustuslain 7 §:n säännöksiin henkilökohtaisesta vapaudesta ja koskemattomuudesta sekä 10 §:n säännöksiin yksityiselämän suojasta. PeVL 10/2012. Katso myös PeVL 24/2010.

475 *Saarenpää,* Tieto, suoja ja byrokratia – näkökohtia suomalaisen tietosuojan kehityksestä ja tulkinnoista, s. 582.

erityisesti henkilökohtaista koskemattomuutta, yksityiselämän suojaa ja vapausoikeuksia koskevat perustuslain säännökset.

Näin itsemääräämisoikeus muodostuu oikeastaan kaikista sellaisista oikeuksista, jotka jollain tavalla antavat henkilölle tietyn vapauspiirin, jonka puitteissa yksilön on mahdollista toteuttaa vapauttaan oman harkintansa mukaan. Tämän perusteella itsemääräämisoikeus pohjautuu fyysiseen, henkiseen ja tiedolliseen suojaan sekä muihin oikeuksiin, jotka turvaavat eri tapoja toteuttaa itsemääräämisoikeutta. [476]

Toisaalta itsemääräämisoikeus on edellytys perusoikeuksien toteutumiselle. Itsemääräämisoikeus laaja-alaisena oikeutena on metaoikeus, joka asettuu oikeusjärjestelmässä perusoikeuksien yläpuolelle ja jota edistetään perusoikeuksien avulla. Vaatimus ihmisarvon loukkaamattomuudesta ilmaisee perustavanlaatuisten oikeuksien yleisinhimillisen perustan. Ainakin kaikkein perustavimmat ihmisyksilön oikeudet ovat perimmältään niin valtion tahdosta kuin kulloisestakin oikeusjärjestyksestä riippumattomia. Maininta yksilön oikeuksien ja vapauden turvaamisesta korostaa puolestaan perusoikeuksien keskeistä asemaa Suomen valtiosäännössä.[477]

Itsemääräämisoikeus koostuu näin useasta eksplisiittisestä perusoikeudesta varsinaisesti tyhjentymättä sellaisenaan yhteenkään niistä. Perusoikeutena itsemääräämisoikeus on sellainen, jonka eksplisiittisempi esiintuonti perustuslaissa turvaisi parhaiten perusoikeuden toteutumisen. [478]

---

476 *Neuvonen – Rautiainen,* Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä, s. 35.

477 HE 309/1993 vp, s. 42. Katso myös *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2003), s. 310 sekä *Scheinin,* Perusoikeudet (1999), s. 227.

478 *Neuvonen – Rautiainen,* Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä, s. 35.

Oikeus identiteettiin. Oikeus identiteettiin ei ole uusi oikeus. Sitä on suojattu useissa kansainvälisissä ihmisoikeussopimuksissa joko suoraan tai välillisesti muiden oikeuksien kautta.[479] Oikeus identiteettiin viittaa yksilön oikeuteen tulla tunnustetuksi yksilönä yhteiskunnassa ja tämän yksilöyden käyttämiseen, sillä se suojaa yksilön merkittäviä ja tiedettävissä olevia piirteitä ja sosiaalisia suhteita.[480]

Oikeus identiteettiin on läheisessä yhteydessä henkilön itsemääräämisoikeuteen. Pohjimmiltaan kysymys on siitä, millaisina liitymme yhteiskuntaan ja millaista suojaa yksilön persoonallisuus yhteiskunnassa saa.[481] Kysymys on itsemääräämisoikeuden tavoin yksilön persoonallisuuden suojasta yhteiskunnassa. Tämän vuoksi yksilön oikeuden identiteettiin tulee nauttia perusoikeustasoista suojaa, vaikkei se käykään suoraan ilmi perustuslaista.

Oikeudessa identiteettiin ei kuitenkaan ole kysymys vain yksilön oikeudesta itsemääräämiseen. Kysymys on sen tunnustamisesta, että yksilöllä on erottamaton oikeus tulla tunnustetuksi ainutlaatuisena yksilönä ja nauttia identiteetin ja persoonallisuuden suojaa yhteiskunnassa.

Koska oikeus identiteettiin on tiukasti sidoksissa yksilön itsemääräämisoikeuteen, on myös oikeus identiteettiin johdettavissa yksilön oikeudesta henkilökohtaiseen vapauteen. Perustuslain 7 §:n säännös

---

479 Oikeus identiteettiin on tunnustettu erillisenä oikeutena lapsen oikeuksien sopimuksen (SopS 59–60/1991) 8 artiklassa. Myös Yhdistyneiden Kansakuntien ihmisoikeusjulistuksessa tunnustetaan jokaiselle oikeus tulla tunnustetuksi yksilönä yhteiskunnassa. Euroopan ihmisoikeussopimus puolestaan takaa oikeuden identiteettiin välillisesti osana yksityisyyden suojaa. Katso esim. EIT:n ratkaisut Peck v. Yhdistynyt Kuningaskunta ja Schussel v. Austria (dec) Hakemusnumero 42409/98(julkaisematon) annettu 21.2.2002.

480 *McCombs – Gonzalez,* Right to Identity, s. 2.

481 *Neethling – Potgeiter – Visser,* Neethling's Law of Personality, s. 36

henkilökohtaisesta vapaudesta on yleisperusoikeus, joka suojaa yksilön tahdonvapautta. Tähän kuuluu myös yksilön oikeus vapaaseen identiteetin muodostukseen.[482]

Henkilökohtaisen vapauden oikeus kattaa näin ollen myös yksilön oikeuden muodostaa identiteettinsä haluamallaan tavalla ilman ulkopuolisten puuttumista siihen. Kysymys on toisin sanoen siitä, että yksilöllä on oikeus hahmottaa itsensä haluamallaan tavalla.[483] Oikeudessa identiteettiin on erotettavissa kaksi eri suojattavaa oikeushyvää: yksilön oikeus oman identiteettinsä vapaaseen kehitykseen ja oikeus identiteetin suojaan.[484]

Oikeutta identiteettiin turvaa osaltaan yksilön oikeus yksityiselämän suojaan, sillä yksityiselämän suojaan sisältyy yksilön oikeus vapaasti päättää suhteistaan muihin ihmisiin ja ympäristöön.[485] Oikeus yksityisyyteen omalta osaltaan myös tukee yksilön identiteetin vapaata kehitystä.[486] Tärkeänä osana tätä on se, että oikeus identiteettiin antaa suojaa liiallista tunnistamista vastaan.[487]

---

482 Yksilön identiteettiä turvaavat myös muut vapausoikeudet, kuten omantunnon vapaus.

483 *Marshall,* Personal Freedom through Human Rights Law? : Autonomy, Identity and Integrity under the European Convention on Human Rights, s. 97.

484 *McCombs – Gonzalez,* Right to Identity, s. 18

485 Näin myös *Reich,* The Individual Sector, s. 1409 sekä EIT ratkaisussaan P.G ja J.H v. Yhdistynyt Kuningaskunta (no. 44787/98, 25.12.2001). Katso myös EIT:n ratkaisu Burghartz v. Sveitsi (no. 16231/90, 22.2.1994).

486 Näin myös EIT ratkaisussaan Peck v. Yhdistynyt Kuningaskunta (no. 44647/98, 28.4.2003).

487 *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 297. Katso myös EIT:n ratkaisu S. ja Marper v. Yhdistynyt Kuningaskunta (no. 30562/04 ja 30566/04, 4.12.2008). Tunnistamisesta ja

> Oikeutta identiteettiin on sivuttu Korkeimman hallinto-oikeuden vuosikirjaratkaisussa KHO 2015:145. Kysymyksessä oli saamelaisena itseään pitävän henkilön oikeudesta tulla tunnustetuksi saamelaisena. Ratkaisussa KHO totesi seuraavaa: *”Henkilön itseidentifikaatiossa on kysymys henkilön perustuslailla turvatun perusoikeuden ydinalueen suojasta. Statukseton saamelainen menettää kaikki hänelle kuuluvat oikeudet ja ihmisarvon, jos häneltä evätään oikeus omaan identiteettiin.”*[488]

Ratkaisu osoittaa havainnollistavalla tavalla sen, että oikeudessa identiteettiin ei ole kysymys vain oikeudesta tulla tunnustetuksi henkilönä. Kysymys on pohjimmiltaan yksilön ihmisarvon kunnioittamisesta.[489] Yksilön oikeutta identiteettiin ei tämän vuoksi tulisi ymmärtää vain niiden oikeuksien, kuten yksityiselämän suojan kautta, joilla sitä perinteisesti on suojattu.[490]

Identiteetissä on kysymys yksilön olemassaoloon hyvin voimakkaasti liittyvästä erityisestä perustarpeesta. On hankala ajatella yksilöä ilman identiteettiä, sillä identiteetin avulla yksilö liittyy yhteiskuntaan ja saa persoonallisuuden suojaa. Samalla se toimii muiden perusoikeuksien pohjana.[491]

---

sen perusoikeuksia loukkaavasta luonteesta katso myös EIT:n ratkaisu Sciacca v. Italia (no. 50774/99, 11.1.2005) sekä von Hannover v. Saksa (no. 59320/00, 24.9.2004). Tapauksissa oli kysymys valokuvien julkaisemisesta ja sitä seuranneesta tunnistamisesta.

488 KHO: 2015:145 (antopäivä 30.9.2015)

489 Näin myös Inter-American Juridicial Committee, El alcance del derecho a la identidad, s. 3

490 *Sullivan,* Digital Identity: An Emergent Legal Concept, s. 72.

491 Amnesty International UK:n Nicky Parker on The Guardianin haastattelussa todennut: “From the moment we are born, we each have the human right to an identity. It's Article 8 of the Convention

Verkkojen varaan rakentuvassa ja suurelta osin verkoissa toimivassa yhteiskunnassa yksilön identiteetin merkitys korostuu entisestään. Yksilön oikeutta identiteettiin tulisikin laaja-alaisuutensa ja yhteiskunnallisen arvonsa vuoksi pitää itsemääräämisoikeuden kaltaisena itsenäisenä perusoikeutena, joka nauttii muita perusoikeuksia vahvempaa suojaa yhteiskunnassa. Perusteluna tälle on se, että yhteiskunta ei voi rajoittaa yksilöä käyttämästä identiteettiään, sen muodostamisesta puhumattakaan. [492]

Oikeus identiteettiin on itsemääräämisoikeuden kaltainen implisiittinen oikeus, joka koostuu useasta eksplisiittisestä perusoikeudesta varsinaisesti tyhjentymättä sellaisenaan yhteenkään niistä. Identiteetin oikeuden eksplisiittisempi esiintuonti perustuslaissa turvaisi parhaiten tämän oikeuden toteutumisen.

---

on the Rights of the Child, but it lasts for life. As an enabler for our other rights to function, it's the bedrock of a healthy and diverse society.… With a legally recorded identity we become citizens of society, able to enjoy essential social services such as health care, education and judicial protection. Without an identity we are invisible to the state and cannot flourish. In fact, without proper ID documents, the terminology that applies is that we are not people before the law." Haastattelu luettavissa osoitteessa: http://www.theguardian.com/childrens-books-site/2014/aug/20/amnesty-international-teen-takeover-2014-being-human

492 Myös McCombs ja Gonzalez katsovat oikeuden identiteettiin olevan itsenäinen oikeus. *McCombs – Gonzalez,* Right to Identity, s. 24. Sullivan pitää oikeutta identiteettiin ehdottomana oikeutena, jota ei voida rajoittaa perinteisillä perusoikeuksien rajoitusedellytyksillä. *Sullivan,* Digital Identity. An Emergent Legal Concept, s. 73 ja 85.

Oikeus henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen. Perustuslain 7 §:n mukaan jokaisella on *oikeus elämään, henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen.*[493]

Henkilökohtainen vapaus on luonteeltaan yleisperusoikeus, joka kattaa ihmisen fyysisen vapauden ja se koskee sekä ruumiillista että henkistä koskemattomuutta ja antaa suojaa myös yksityisten välisissä suhteissa.[494] Vapauden ja fyysisen koskemattomuuden suoja on edellytys muiden perusoikeuksien käyttämiselle. Näin se suojaa muun muassa henkilöön kohdistuvilta tarkastuksilta sekä pakolla toteutettavilta lääketieteellisiltä ja muilta toimenpiteiltä.[495] Henkilökohtaiseen koskemattomuuteen puuttumiseen edellytetään nimenomainen laissa säädetty peruste, joka ei saa olla mielivaltainen.

Oikeus turvallisuuteen on suhteellisen uusi perusoikeus, sillä se otettiin perusoikeudeksi vuoden 1995 hallitusmuodon uudistuksella. Oikeus henkilökohtaiseen turvallisuuteen on yhteydessä henkilökoh-

493 Hengen ja vapauden suoja ovat vanhimpia klassisia perusoikeuksia. Niillä on edeltäjänsä Ruotsin ajan kuninkaankaarissa ja Britannian Habeas Corpus Actissa. Vapauden ja fyysisen koskemattomuuden suoja ovat käytännössä edellytys muiden perusoikeuksien käyttämiselle.

494 Perustuslakivaliokunta on kehittänyt PeL 7 §:ään liittyvistä perusoikeuksista yläkäsitteen "henkilön itsemääräämisoikeus", jolla on vaikutusta esimerkiksi säädettäessä pakollisista terveystarkastuksista ja päihdetesteistä, annettaessa toimivaltuuksia järjestyksenvalvojille julkiseen tilaisuuteen saapuneiden turvaamiseksi, säänneltäessä ihmisten välisistä yhteyksistä ja yhteydenpito-oikeudesta, lapsen oikeusasemasta, sekä asevelvollisten terveystarkastuksista ja soveltuvuuskokeista. Näin muun muassa PeVL 39/2001, 13/2005, 17/2006, 5/2006 ja PeVL 26/2004. Katso myös *Saraviita,* Perustuslaki, s.154–155.

495 HE 162/2003 vp, s. 4–5.

taisen vapauden oikeuden kanssa. Oikeutta henkilökohtaiseen vapauteen suojataan henkilökohtaisen turvallisuuden kanssa, sillä oikeus henkilökohtaiseen turvallisuuteen suojaa yksilöä mielivaltaiselta puuttumiselta henkilökohtaiseen vapauteen. Oikeus henkilökohtaiseen turvallisuuteen on näin ollen epäitsenäinen ja yksilökohtainen oikeus, jota toteutetaan henkilökohtaisen vapauden oikeuden kautta. Kysymys ei siis ole turvallisuudesta yhteiskunnallisena tilana eli turvallisuuskäsitteestä siinä merkityksessä kuin se esiintyy ilmauksessa ”yleinen järjestys ja turvallisuus”.[496]

Edellä esitettyyn on mahdollista suhtautua myös toisella tavalla. Oikeus turvallisuuteen on tulkittavissa itsenäiseksi oikeudeksi, joka ei ole sidoksissa henkilökohtaisen vapauden oikeuteen. Oikeus turvallisuuteen on muuttunut kollektiiviseksi hyväksi, sillä *”turvallisuuden*

496 *Tuori,* Yleinen järjestys ja turvallisuus – perusoikeusko?, s. 93–94. Saraviidan mukaan oikeus turvallisuuteen on saanut käytännössä lisävahvistusta PeL 22 §:ssä säädetystä julkisen vallan velvollisuudesta turvata perusoikeuksien ja ihmisoikeuksien toteutuminen. Hän käyttää seuraavaa päättelyketjua: ”Kun julkisella vallalla on perusoikeuksien yleinen turvaamisvelvoite ja ihmisen turvallisuus on luonnehdittu perusoikeudeksi, viranomaisen toimivaltuuksista rajoittaa turvallisuusriskin aiheuttavien ihmisten vapautta, yksityisyyden suojaa, kotirauhaa ja fyysistä koskemattomuutta laajennetuin viranomaisvaltuuksin voidaan säätää tavallisessa lainsäätämisjärjestyksessä.” Tämä näyttää hänen mukaansa olevan 2000-luvun alkuvuosien yleisin perusoikeuskollisiotilanne. *Saraviita,* Perustuslaki, s. 159. Tämä on totta erityisesti biometrisen tunnistamisen kohdalla. Tilanteen voidaan sanoa kärjistyneen terrorismin vastaiseen sotaan liittyen, kun USA ja Euroopan unioni käynnistivät lukuisia hankkeita kansainvälisoikeudellisiksi sopimusjärjestelyiksi yhteistoiminnasta terrorismia vastaan, joista biometrisen tunnistamisen hyödyntäminen muun muassa rajavalvonnassa lisääntyi huomattavasti.

nimenomainen mainitseminen korostaa julkisen vallan positiivista toimintavelvoitetta yhteiskunnan jäsenten suojaamiseksi rikoksilta ja muilta heihin kohdistuvilta oikeudenvastaisilta teoilta, olivatpa niiden tekijät julkisen vallan käyttäjiä tai yksityisiä tahoja".[497] Biometrisen tunnistamisen kannalta perustuslain 7 § on merkityksellinen kahdesta syystä. Yksilön ominaispiirteisiin perustuvan biometrisen tunnisteen ottaminen merkitsee ensinnäkin puuttumista yksilön fyysiseen koskemattomuuteen. Toisekseen biometristä tunnistamista käytetään ennen kaikkea turvallisuuden parantamiseen. Esimerkiksi biometrisen passin käyttöönottoa on perusteltu sillä, että biometrinen passi turvaa paremmin yksilön oikeudet tunnistamisessa. Vaikka oikeuden turvallisuuteen ei enää nähtäisikään olevan sidoksissa henkilökohtaisen vapauden kanssa, ei tästä voida vetää johtopäätöstä, että turvallisuuden varjolla voitaisiin loukata henkilökohtaista vapautta ja koskemattomuutta mielivaltaisesti.

Turvallisuus ei tällöin ole sillä tavoin itsenäinen perusoikeus, että se menisi muiden perusoikeuksien edelle jonkinlaisena ylivertaisena oikeushyvänä. Turvallisuus tulee pikemminkin nähdä osana perusoikeusjärjestelmää.[498]

Oikeus turvallisuuteen on saanut lisävahvistusta PeL 22 §:ssä säädetyn julkisen vallan velvollisuudesta turvata perus- ja ihmisoikeuksien toteutuminen. Saraviita on käyttänyt seuraavaa karkeaa päättelyketjua: Koska ihmisten turvallisuus on luonnehdittu perusoikeudeksi ja julkisella vallalla on perusoikeuksien yleinen turvaamisvelvoite, voidaan turvallisuusriskin aiheuttavien ihmisten vapautta, yksityisyyden suojaa ja fyysistä koskemattomuutta rajoittavista laajennetuista viranomais-

497 HE 309/1993 vp, s. 47.

498 Näin myös *Jyränki – Husa,* Valtiosääntöoikeus, s. 413 sekä *Saraviita,* Perustuslaki, s. 157.

ten toimivaltuuksista säätää tavallisessa lainsäätämisjärjestyksessä.[499] Asetelma on kärjistynyt vuoden 2001 terrori-iskujen jälkeen. Asetelmaa voidaan perustellusti pitää 2000-luvun yleisimpänä perusoikeuskollisiotilanteena.

Positiivisesta toimintavelvoitteesta huolimatta oikeutta turvallisuuteen voidaan tuskin asettaa kollisioon henkilön vapausoikeuksien kanssa niin, että esimerkiksi rikostutkintavaltuuksia esteittä voitaisiin tavallisessa lainsäätämisjärjestyksessä laajentaa ruumiillisen koskemattomuuden suojauksen suhteen. Syynä on se, että oikeus henkilökohtaiseen koskemattomuuteen ja vapauteen ovat tarkoitettu ehdottomiksi oikeuksiksi. Oikeus turvallisuuteen on puolestaan lainsäätäjään kohdistuva toimintavelvoite.[500] Oikeus henkilökohtaiseen vapauteen on tämän vuoksi entistä merkityksellisempi ihmis- ja perusoikeuksia kunnioittavassa demokraattisessa oikeusvaltiossa. Oikeus henkilökohtaiseen turvallisuuteen edelleen suojaa myös mielivaltaiselta puuttumiselta henkilökohtaiseen vapauteen ja koskemattomuuteen. Tästä syystä se tulee myös huomioida turvallisuudesta puhuttaessa.

Liikkumisvapaus. EU:ssa liikkumisvapaudella on historiallisesti korostunut asema, koska se on yksi EU-oikeuden yleisiä periaatteita. Toisaalta se on myös yksi niin sanotusta neljästä perusvapaudesta tavaroiden, palvelujen ja pääomien vapaan liikkuvuuden ohella.

Perustuslain 9 §:ssä on turvattu kaikki nykyaikaisesti ymmärrettävän liikkumisvapauden osa-alueet. Yksilöllä on oikeus esimerkiksi liikkua maassa paikkakunnalta toiselle vapaasti ilman rajoituksia.

Yksilön liikkumisvapaus on perinteisesti katsottu kuuluvaksi klassisiin vapausoikeuksiin, jonka tarkoituksena on turvata yksilön ulkoista vapautta. Liikkumisvapaus suojaa yksilön vapautta päättää olinpaikastaan suhteessa julkiseen valtaan. Oikeus liikkua vapaasti tulee nähdä

499 *Saraviita,* Perustuslaki, s. 159.

500 *Saraviita,* Perustuslaki, s. 157.

myös yksilön autonomisuuden tärkeänä osana. Liikkumisvapaus ja henkilökohtainen vapaus ovatkin näin ollen sisällöllisesti lähellä toisiaan.[501]

Liikkumisvapaudessa on kysymys yksilön fyysisen vapauden yhdestä ulottuvuudesta. Liikkumisvapauden kohdalla herää seuraavat kysymykset: Onko sellaista viranomaistoimintaa olemassa, että olisi asiallisesti perusteltua seurata koko ajan, missä kansalaiset liikkuvat? Kellä viranomaisella on sellainen toimivalta?

Biometrisen tunnistamisen yleistyessä kasvaa myös riski sen avulla kerättyjen tietojen käytöstä valvonta- ja tarkkailutarkoituksiin. Tämä tuo mukanaan myös anonymiteetin murenemisen yhteiskunnassa. Liikkumisvapauden näkökulmasta ongelmia aiheutuu erityisesti siitä, miten biometrinen tunnistaminen kokonaisuutena vaikuttaa ihmisiin ja erityisesti heidän liikkumiseensa.[502] Yksilöllä tulee lähtökohtaisesti olla oikeus käyttää liikkumisvapauttaan ilman liiallisten fyysisten ja psykologisten rajoitusten – joita biometrisen tunnistamisen lisääntymisestä saattaa aiheutua – asettamista liikkumiselle ja käyttäytymiselle. Laaja-alaisesti käytettynä biometrinen tunnistaminen on miellettävissä valvonnan osaksi, jota voidaan pitää rajoituksena liikkumisvapauden käyttämiselle.

Oikeus yksityiselämän ja henkilötietojen suojaan. Suomen perustuslain 10 §:ssä taataan suoja jokaisen yksityiselämälle, kunnialle ja koti-

501 *Ojanen – Scheinin,* Liikkumisvapaus (PL 9 §), s. 317.

502 Esimerkkinä voidaan mainita uusi passilainsäädäntö, joka sallii biometristen tunnisteiden ottamisen passiin. Passin myöntämistä tai epäämistä tulee kuitenkin arvioida liikkumisvapauden rajoittamisen näkökulmasta, koska passi on maasta poistumisen pääsääntöinen edellytys. Näin ollen passin antamis- ja peruuttamisedellytykset ovat olennaisia liikkumisvapauden toteuttamisen näkökulmasta. Näin esimerkiksi perustuslakivaliokunta ratkaisuissaan PeVL 33/1997 vp ja 27/2005 vp.

rauhalle. Myös henkilötiedot nauttivat perustuslain suojaa. Perustuslain turvaaman suojan kohteina on neljä oikeushyvää: yksityiselämä, kunnia, kotirauha ja henkilötiedot. Ne muodostavat yhdessä suojatun alan, jonka kokonaisuutta mikään niistä ei yksinään kata, vaikka käsitteet menevät osittain päällekkäin.[503]

Perusoikeusuudistuksen esitöiden mukaan käsite ”yksityiselämä” tulee ymmärtää henkilön yksityistä piiriä koskevaksi yleiskäsitteeksi.[504] Syynä on se, että sitä ei voida selvästi erottaa esimerkiksi henkilökohtaisen koskemattomuuden, kunnian tai kotirauhan suojasta, sillä nämä oikeudet usein ilmenevät päällekkäisinä. Esimerkiksi puuttuminen henkilökohtaiseen koskemattomuuteen voi merkitä yksityiselämään puuttumista. Tällaisissa konkurenssitilanteissa on huolehdittava, että ehdotetut perusoikeusrajoitukset täyttävät perusoikeuksien yleisten rajoitusedellytysten lisäksi myös kaikkien kysymykseen tulevien perusoikeuksien erityiset rajoitusedellytykset.[505]

Perusoikeusuudistuksen yhteydessä yksityiselämän suojan piiriä ei pyritty täsmällisesti määrittelemään. Yksityiselämällä ei viitata pelkästään henkilön oikeuteen olla yksin rauhassa muilta, vaan siihen sisältyy selkeästi myös yhteisöllinen elementti: henkilön oikeus vapaasti päättää suhteistaan muihin ihmisiin ja ympäristöön. Säännös yksityiselämän suojasta näin ollen turvaa osaltaan yksilön itsemääräämisoikeutta.

Yksityiselämän käsite on tullut Suomen perustuslakiin lähinnä Euroopan ihmisoikeussopimuksen 8 artiklasta. Säännöksen tulkinnassa on tällaisessa tilanteessa perusteltua tukeutua tavanomaista enemmän vastaavan ihmisoikeusmääräyksen soveltamiskäytäntöön. Tällöin yksi-

503 *Jyränki,* Uusi perustuslakimme, s. 301.

504 HE 309/1993 vp, s. 53. Vertaa *Jyränki – Husa,* Valtiosääntöoikeus, s. 418.

505 *Viljanen,* Yksityiselämän suoja, s. 391.

tyiselämän suoja sisältää ainakin moraalisen ja fyysisen koskemattomuuden suojan sekä henkilötietojen suojan.[506]

Tieteen ja tekniikan kehitys luo yksityiselämän suojalle jatkuvasti uusia aikaisemmin tuntemattomia uhkia. Lainsäädäntö ei välttämättä pysty seuraamaan tätä kehitystä eikä ajoissa varautumaan yksityiselämään kohdistuviin uusiin uhkatekijöihin. Tämä ei kuitenkaan tarkoita sitä, että teknologinen ja yhteiskunnallinen kehitys tekisi yksityiselämän suojasta tyhjän oikeuden. Perustuslain yksityiselämän turvasäännös ulottaa vaikutuksensa myös sellaisiin puuttumisiin yksityiselämään, joita ei asianomaista säännöstä kirjoitettaessa vielä pystytty ennakoimaan.

Yksityiselämän perusoikeus nauttii suojaa toisaalta vertikaalisuhteessa estämällä lakivaraukset ylittävän puuttumisen yksityisyyteen lainsäädäntöteitse. Yksityisyyden kohdalla näin on siltä osin kuin valtio suojaa yksilöä tietojen tallentamiselta, seurannalta, tunkeutumiselta yksityiseen tilaan ja muutenkin valtio rajoittaa tiedollista ylivoimaansa.[507]

Yksityiselämää suojataan toisaalta myös horisontaalisuhteessa kriminalisoimalla yksityisyyden loukkaukset.[508] *Tällöin valtion tehtävänä on yksityisyyden turvaaminen suhteessa muihin ihmisiin. Yksityiselämän suojan kohdalla perusoikeuksien horisontaalivaikutuksella on erityinen merkitys. Syynä on se, että henkilön oikeutta yksityiselämään ei uhkaa niinkään julkisyhteisö, vaan uhka tulee yleisemmin toisen yksityisen toimijan taholta.*[509]

---

506 Näin myös *Viljanen,* Yksityiselämän suoja, s. 393

507 *Neuvonen,* Yksityisyyden suoja Suomessa, s. 29–30.

508 *Saraviita,* Perustuslaki, s. 180. Katso myös *Saraviita,* Suomalainen perusoikeusjärjestelmä.

509 Näin myös *Viljanen,* Yksityiselämän suoja, s. 394–395.

Yksityiselämän suoja on perusoikeutena säädetty PeL 10 §:ssä turvaamisvakuutuksena. Perustuslakivaliokunnan käytännössä on kuitenkin katsottu, että tätä perusoikeutta voidaan jonkin verran rajoittaa.[510]

Perustuslaissa säädetään yksilölle lähtökohtainen oikeus elää elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityisyyteensä. Yksityiselämän piiriin kuuluu muun muassa yksilön oikeus määrätä itsestään ja ruumiistaan.[511] Tähän kuuluu se, että yksilöllä on niin halutessaan oikeus olla sietämättä ulkopuolisten läheisyyttä, häirintää, katselua tai kuuntelua.

Perustuslain 10 §: ssä mainittu henkilötietojen suoja kuuluu lähtökohtaisesti yksityiselämän suojan piiriin. Henkilötietojen suoja on kehittynyt eräänlaisena yksityisyyden suojan sovellutuksena. Säännöksessä asetettu sääntelyvaraus edellyttää kuitenkin tarkempia lain tasoisia säännöksiä nimenomaan henkilötietojen suojasta.

Säännös kuitenkin osoittaa sen, että henkilötietojen suoja on perusoikeus, vaikka sen yksityiskohdista on mahdollista säätää lain tasolla, ja laki voi sisältää rajoituksia tähän suojaan. Perusteena voidaan mainita se, että yksityisyyden ja henkilötietojen suojan välisen kytköksen purkaminen auttaa paremmin jäsentämään nyt verraten avoimeksi jääneen konstitutionaalisen tietosuojaoikeuden alaa ja sisältöä.[512]

Perusoikeusuudistusta koskevan hallituksen esityksen mukaan säännös viittaa tarpeeseen lainsäädännöllisesti turvata yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä. Hallituksen esityksessä todetaan lisäksi, että tietyn tasovaatimuksen asettaa Euroopan neuvoston piirissä hyväksytty yk-

510 PeVL 18/2008 vp.

511 HE 309/1993 vp, s. 53

512 *Koillinen,* Henkilötietojen suoja itsenäisenä perusoikeutena, s. 171.

silöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä koskeva yleissopimus.[513]

Säännöksen lakiviittaus henkilötietojen suojasta edellyttää perusoikeusuudistuksen tarkoituksen mukaisesti lainsäätäjän säätävän tästä oikeudesta. Sääntelyn yksityiskohdat jäävät kuitenkin lainsäätäjän harkintaan. Lainsäätäjän liikkumavaraa rajoittaa kuitenkin henkilötietojen suojan kuuluminen yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata oikeus henkilötietojen suojaan tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa.[514]

Perustuslakivaliokunta on esittänyt henkilötietojen suojaa koskevat seuraavat lainsäädäntöä tarkoittavat edellytykset[515]:

1) Rekistereistä on yksityiskohdittain säädettävä lakitasossa. Esimerkiksi säilytysajasta ei voida säätää asetustasolla.

2) Rekisteriin merkityllä tulee olla oikeussuojakeino käytettävissään. Oikeussuojamenetelmä voi olla esimerkiksi oikeus tarkastaa itseään koskevat tiedot.

3) Julkisen vallan harjoittamalla rekisteröinnillä tulee olla hyväksyttävä tarkoitus, esimerkiksi rikosten selvittäminen.

4) Lailla säätämiseen liittyy tarkkuusvaatimus. Lakiin otettava ilmaisu ”erittäin painavat syyt” ei ole riittävän tarkka, jos se jää konkretisoitumatta lain tasolla. Tärkeinä sääntelykohteina ovat myös rekisteröinnin tavoite, rekisteröitävien henkilötietojen sisältö, niiden sallitut käyttötarkoitukset ja tietojen säilytysaika henkilörekisterissä sekä rekisteröidyn oikeusturva.[516]

---

513 HE 309/1993 vp, s. 53.

514 Katso esimerkiksi PeVL 51/2002 vp.

515 PeVL 7/1997 vp, PeVL 11/1997 sekä PeVL 27/1998 vp.

516 PeVL 14/1998 vp, PeVL 25/1998 vp, PeVL 11/2008 vp ja PeVL 32/2008 vp.

Yksityiselämän suoja saa näin ollen vahvistusta säännöksestä, jonka mukaan henkilötietojen suojasta säädetään tarkemmin lailla.[517] Henkilötietojen suojan pääasiallisena tarkoituksena on yksilön suojaaminen perusteettomalta henkilötietojen keräämiseltä, tallentamiselta, käytöltä ja luovuttamiselta. Yksityisyyden suoja puolestaan suojaa perusteettomalta puuttumiselta yksilön yksityiselämään. Näin ollen Perustuslain 10 § kuvaa hyvin yksityisyyden ja henkilötietojen suojan kiinteää yhteiseloa.

Suomalaisessa valtiosääntödoktriinissa henkilötietojen suoja on vakiintuneesti sijoitettu yksityiselämän suojan alakäsitteeksi.[518] Erillisen lakivarauksen on yleensä katsottu ilmentävän lainsäätäjän ainakin lähtökohtaisesti laajempaa harkintavaltaa henkilötietojen suojan alueella yksityisyyden suojaan verrattuna.[519]

Yksityisyyden suojan ja henkilötietojen suojan välisestä suhteesta käytävässä keskustelussa ei ole kysymys yksityisyyden suojan merkityksen kiistämisestä. Yksityisyyden suojan nähdään edelleen olevan kiinteässä vuorovaikutussuhteessa henkilötietojen suojan kanssa. Tulkinnan perusteena on se, että henkilötietojen kerääminen rekistereihin katsotaan yksityisyyden suojaan puuttumiseksi.[520]

Vaikka henkilötietojen suoja ja yksityisyyden suoja ovat kiinteässä vuorovaikutuksessa keskenään, tulee henkilötietojen suoja katsoa eril-

---

517 PeVL 19/2008 vp.

518 Katso esimerkiksi *Viljanen,* Yksityiselämän suoja, s. 396. On syytä huomauttaa siitä, että yhdysvaltalaisessa yksityisyyskeskustelussa henkilötietojen suoja katsotaan osaksi yksityisyyttä. Käytännössä oikeutta tiedolliseen yksityisyyteen ei kuitenkaan ole tunnustettu. Lähimmäksi tämän oikeuden olemassaolon tunnustamisessa on päästy ratkaisussa Whalen v. Roe.

519 *Kulla,* Biometriset tunnisteet ja tiedollinen itsemääräämisoikeus, s. 37.

520 Katso esimerkiksi PeVL 7/1997 vp.

liseksi perusoikeudeksi. Tulkintaa puoltaa myös se, että henkilötietojen suojan mainitseminen yksityiselämän suojaa koskevassa säännöksessä osoittaa henkilötietojen suojan olevan oma perusoikeutensa.[521]

Katsottaessa henkilötietojen suoja vain osaksi yksityisyyden suojaa kutistuisi suojattavien henkilötietojen ala. Henkilötietojen suoja kuitenkin ulottuu monille alueille, joita yksityiselämän suoja ei turvaa.[522] Tätä voidaan pitää uhkana henkilötietojen suojalle, jossa yksi suojaa puoltava argumentti on se, että kaikki henkilöön liitettävissä olevat tiedot ovat väärinkäytettävissä. Biometrisesta tunnistamisesta käy hyvin ilmi yksityisyyden ja henkilötietojen suojan välinen yhteys. Biometrisen tunnisteen ottamisessa puututaan yksilön fyysiseen yksityisyyteen ja tämän tiedon käyttäminen puolestaan vaikuttaa yksilön henkilötietojen suojaan. Kumpikaan oikeus itsessään ei riittävällä tavalla turvaa yksilön oikeutta yksityisyyteen ja henkilötietojen suojaan biometrisessa tunnistamisessa, vaan asiaa tulee arvioida kummankin oikeuden näkökulmasta.[523]

Henkilötietojen suojan ymmärtäminen itsenäisenä perusoikeutena tukee myös tiedollista itsemääräämisoikeutta.[524] Lisäksi voidaan katsoa, että toteamus siitä, että henkilötietojen suojasta säädetään tarkemmin lailla, tarkoittaa henkilötietojen suojan perusoikeudeksi, jonka

521 *Saraviita,* Perustuslaki, s. 184.

522 *Bygrave,* Place of Privacy in Data Protection Law. Artikkeli saatavilla osoitteessa: http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html

523 Schartumin ja Bygraven mukaan biometrinen tunnistaminen on yksi esimerkki siitä, miten informaatioteknologia vaikuttaa yksityisyyden ja henkilötietojen suojan suhteeseen. *Schartum – Bygrave,* Personvern i informasjonssamfunnet, s. 31–32.

524 *Pitkänen – Tiilikka – Warma,* Henkilötietojen suoja, s. 24. Katso myös *Koillinen,* Henkilötietojen suoja itsenäisenä perusoikeutena, s. 181. Vertaa Neuvonen, Yksityisyyden suoja Suomessa.

yksityiskohdista on mahdollista säätää lain tasolla.[525] Henkilötietojen suojan esittäminen itsenäisenä perusoikeutena lähtee näin ollen siitä, että nimenomaista henkilötietojen suojaa tarvitaan, jotta yksityisyyden suoja toteutuisi mahdollisimman tehokkaasti.[526]

Perusoikeuksien rajoittaminen. Luonteestaan huolimatta perusoikeudet eivät sinällään ole ehdottomia siten, ettei niitä voida missään tilanteissa rajoittaa. Useat perusoikeudet sisältävät tämän vuoksi lakivarauksen eli viittauksen siihen, että lailla voidaan säätää perusoikeuden rajoituksia tai antaa säännöksiä oikeuden käyttämisestä. Perusoikeudet eivät ole ehdottomia siinäkään tapauksessa, kun perusoikeussäännös ei sisällä mitään mainintaa rajoitusmahdollisuudesta.[527]

Perusoikeudet muodostavat kokonaisjärjestelmän, jolle on ominaista, että siihen sisältyvät ainesosat ovat usein jännitteisessä suhteessa keskenään. Useasti jännite liittyy siihen, että yhtäältä on kunnioitettava yksilöiden toimintavapautta ja samalla on huolehdittava toisten ihmisten turvallisuudesta. Yhden yksilön oikeudet ja vapaudet on sovitettava yhteen toisten yksilöiden oikeuksien ja vapauksien sekä koko yhteisön etujen kanssa. Kysymys on lähes aina jonkinlaisesta tasapainoilusta eri suuntiin käyvien näkökohtien välillä.

Olennaista onkin hahmottaa, mitä perusoikeuksia kulloinkin tarkasteltavana olevassa tilanteessa rajoitetaan, ja toisaalta mitä perusoikeuksia sillä mahdollisesti suojataan. Tämän jälkeen näitä perusoikeuksia tulee punnita keskenään ratkaisuntekohetkellä vallitsevien käsitysten pohjalta. Tämän tarkoituksena on kunkin yksilön perusoikeuksien toteutumisen turvaaminen mahdollisimman hyvin.[528]

---

525 *Korhonen,* Perusrekisterit ja tietosuoja, s. 92.

526 *Neuvonen – Rautiainen,* Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä, s. 34.

527 *Hallberg,* Perusoikeusjärjestelmä, s. 56 ja *Viljanen,* Perusoikeuksien rajoittaminen, s. 139.

528 *Viljanen,* Perusoikeuksien rajoittaminen, s. 139.

Perusoikeuksien välisiä kollisioita joudutaan ratkaisemaan sekä yleisellä tasolla lakeja säädettäessä että konkreettisessa lainsoveltamistilanteessa. Vastakkain voivat olla ensinnäkin kahden henkilön perusoikeudet. Punnintatilanteessa tulee jäljempänä mainituin perustein arvioida, mihin tasapaino kahden perusoikeuden välillä asetetaan. Eri perusoikeuksien lähtökohtainen asettaminen etusijajärjestykseen johtaa helposti käytännön tulkintoihin, jotka eivät perustu järkevälle harkinnalle.

Toiseksi perusoikeuskollisio voi ilmetä saman henkilön eri perusoikeuksien välisenä kollisiona. Saman henkilön eri perusoikeuksien kollisio aktualisoituu käytännössä vain silloin, kun hän syystä tai toisesta ei itse ole aktiivisesti ilmaissut omaa valintaansa. Kolmanneksi perusoikeuksia voidaan rajoittaa painavien yhteiskunnallisten intressien perusteella. Tällainen perusoikeuksien rajoittaminen vaatii tuekseen erittäin painavia perusteita juuri perusoikeuksien perustuslaintasoisuuden vuoksi. Mikä tahansa yhteiskunnallinen intressi ei kuitenkaan voi olla yksilön perusoikeuksien rajoittamisen perusteena.[529]

Perusoikeuden rajoittamisessa on kysymys perusoikeussäännöksen soveltamisalan piirissä olevan oikeuden kaventamisesta tai perusoikeussäännöksen suojaamaan yksilön oikeusasemaan puuttumisesta julkisen vallan toimenpitein. Yksilö on tällöin estynyt käyttämästä perusoikeuttaan täysimääräisesti siltä osin, kuin sitä on perustuslain edellyttämässä menettelyssä ja sallimalla tavalla rajoitettu.[530]

---

529 *Viljanen,* Perusoikeuksien rajoittaminen, s. 139–140.

530 Ennen kuin voidaan puhua perusoikeuden rajoittamisesta, joudutaan ratkaisemaan, onko kysymys ylipäätään perusoikeussäännöksen soveltamisalan piiriin kuuluvasta asiasta, eli onko perusoikeussäännöksellä merkitystä yksilön käyttäytymismahdollisuuksia rajoittavan tai yksilön oikeusasemaan muutoin puuttuvan sääntelyn kannalta. *Viljanen,* Perusoikeuksien rajoittaminen, s. 141.

Tulkinnallisena lähtökohtana on pidettävää perusoikeuden soveltamisalan tulkitsemista epäselvissä tapauksissa laajentavasti. Esimerkiksi sananvapauden piiri sinänsä kattaa kaikenlaiset ilmaisut niiden tarkoituksesta riippumatta. Näin ollen mainontaa ja muita kaupallisia ilmaisuja ei voida rajata pois sananvapauden suojan piiristä, vaan niihin kohdistuvaa sääntelyä on arvioitava sananvapauden rajoituksina, joiden sallittavuuden arvioinnissa on mahdollista antaa merkitystä sille, että elinkeinotoimintaan liittyvän viestinnän ei katsota normaalitilanteissa kuuluvan sananvapauden käyttämisen ydinalueelle.

Yleisen perusoikeuksien rajoitussäännöksen puuttumisen vuoksi perusoikeuksien rajoitusten sallittavuus määräytyy Suomessa lainsäädäntökäytännössä ja oikeustieteessä kehitettyjen perusoikeuksien yleisten rajoitusedellytysten täyttymisen perusteella.[531] Keskeisen aseman rajoitusten sallittavuuden arvioinnissa on saanut eduskunnan perustuslakivaliokunnan perusoikeusuudistusta koskevaan mietintöönsä kirjaama perusoikeuksien yleisten rajoitusperusteiden luettelo. Luettelo muodostaa perusoikeusrajoitusten sallittavuuden arvioinnissa käytettävän yleisen testin.[532] Rajoitusperusteet voidaan esittää tiivistetysti seuraavasti:

1) Rajoitusten tulee perustua eduskunnan säätämään lakiin. Tähän liittyy kielto delegoida perusoikeuksien rajoittamista koskevaa toimi-

531 Perusoikeusuudistusta valmisteltaessa oli esillä ajatus yleisen perusoikeuksien rajoittamista koskevan säännöksen sisällyttämisestä perusoikeuslukuun. Katso tarkemmin KM 1992:3, s. 378–388.

532 Luettelo otsikoitiin mietinnössä esimerkeiksi. PeVM 25/1994 vp, s. 4–5. Luettelosta on kuitenkin pidetty kiinni sellaisenaan ja laajennuksitta. Kielellisellä tasolla kriteerit ovat kuitenkin joustavia. *Saraviita,* Suomalainen perusoikeusjärjestelmä, s. 214. Katso myös *Viljanen,* Perusoikeuksien rajoitusedellytykset.

valtaa lakia alemmalle säädöstasolle.[533] Lailla säätämisen vaatimuksen tarkoituksena on suojata yksilön perusoikeuksia hallinnolliselta mielivallalta.

2) Rajoitusten on oltava tarkkarajaisia ja riittävän täsmällisesti määriteltyjä. Rajoitusten olennaisen sisällön tulee ilmetä laista.

3) Rajoitusperusteiden tulee olla perusoikeusjärjestelmän kannalta hyväksyttäviä ja painavan yhteiskunnallisen tarpeen vaatimia. Rajoitusperusteiden hyväksyttävyyttä tulee arvioida perusoikeusjärjestelmän kannalta. Hyväksyttävyyden arvioinnissa merkitystä voi olla esimerkiksi Euroopan ihmisoikeussopimuksen vastaavanlaista oikeutta koskevilla määräyksillä, ainakin siltä osin kuin niihin sisältyy tyhjentävä luettelo ihmisoikeuksien hyväksyttävistä rajoitusperusteista. Perusoikeussäännöksiä onkin perusteltua tulkita yhdenmukaisesti ihmisoikeussopimuksien kanssa.[534]

Perustuslakivaliokunta on arvioinut esimerkiksi perustuslain yksityiselämän ja henkilötietojen suojaa koskevien säännösten valossa ehdotuksia, joiden perusteella DNA-tunniste saadaan tallettaa poliisin henkilörekisteriin. Katsoessaan DNA-tunnisteen määrittämisen ja sitä kautta tapahtuvan vähäisen puuttumisen henkilökohtaiseen koskemattomuuteen perustuslain mukaiseksi perustuslakivaliokunta totesi toimenpiteen helpottavan törkeiden rikosten selvittämistä ja sitä kautta lisäävän jokaisen oikeutta turvallisuuteen.[535] Tällaiseen argumentointiin on kuitenkin syytä suhtautua varauksella, sillä se uhkaa hämärtää perusoikeuksien yksilökohtaista suojavaikutusta ja tehdä

533 *Saraviita,* Suomalainen perusoikeusjärjestelmä, s. 211. Saraviidan mukaan tätä velvollisuutta toteuttaa osaltaan PeL 80.1 §.

534 *Saraviita,* Suomalainen perusoikeusjärjestelmä, s. 211. Rajoituslausekkeista tarkemmin katso esim. *Viljanen,* The European Court of Human Rights as a Developer of the General Doctrines of Human Rights Law.

535 PeVL 7/1997 vp.

henkilökohtaisesta turvallisuudesta monien muiden oikeuksien yleisen rajoitusperusteen.[536]

4) Tavallisella lailla ei voida säätää perusoikeuden ytimeen ulottuvaa rajoitusta. Tämä on johtanut siihen, että ajatusta perusoikeuksien ydinalueesta on käytetty lähinnä käänteisesti: lainsäätäjän liikkumavaraa on pidetty normaalia suurempana, jos perusoikeusrajoitukset jäävät perusoikeussuojan reuna-alueelle.[537]

Perustuslakivaliokunnan lausunnoissa ei ole juurikaan pyritty määrittämään kulloinkin käsiteltävänä olevan perusoikeuden ydintä.[538] Tämä saattaa antaa vaikutelman, ettei rajoitusperusteilta ulottumattomissa olevaa aineellista ydintä olekaan. Esimerkkinä voidaan mainita se, että henkilötietojen suojaa koskevista perustuslakivaliokunnan lausunnoista on vaikea löytää ajatusta, että jokin arkaluontoisten tietojen laji olisi täysin suojattu käsittelyltä vertikaalisissa suhteissa. Kysymys on vain siitä, mitkä viranomaiset saavat henkilötietoja käsitellä, kuinka yksityiskohtaisin ehdoin ja millainen oikeusturva on taattava.[539]

Henkilötietojen kohdalla asiaa tulee kuitenkin ensisijaisesti arvioida yksityiselämän suojan kautta. Henkilötiedot ovat osa yksilön yksityisyyttä, jolloin niiden ydinaluetta tulee arvioida yksityisyyden suojan ydinalueen kautta. Määrittelyvaikeuksista huolimatta on selvää, että jokaisella perusoikeudella on sellainen ydinalue, jonka turvaamaa käyttäytymistä ei esimerkiksi saa säätää rangaistavaksi.[540]

---

536 Näin myös *Pellonpää,* Henkilökohtainen koskemattomuus (PL 7 §), s. 285.

537 PeVL 23/2006 vp, PeVL 29/2008 ja PeVL 17/1998 vp.

538 Katso esimerkiksi PeVL 25/1998 vp. ja PeVL 14/2002 vp.

539 *Jyränki – Husa,* Valtiosääntöoikeus, s. 407.

540 PeVM 25/1994 vp, s. 5. Perusoikeuden ydinalueen määrittely ei kuitenkaan ole yksiselitteinen tehtävä. PeVL 23/1997 vp. Viljasen mukaan ydinalueen koskemattomuuden vaatimuksella ei normaaleissa

5) Suhteellisuusvaatimus. Rajoitusten tulee olla välttämättömiä tavoitteen saavuttamiseksi sekä laajuudeltaan oikeassa suhteessa perusoikeuksien suojaamaan oikeushyvään ja rajoituksen taustalla olevan yhteiskunnallisen intressin painoarvoon.[541] Tämä osoittaa sen, että suhteellisuusvaatimuksen täyttymisen arviointi perustuu viime kädessä perusoikeuden takaamien intressien painoarvon keskinäiseen punnintaan.[542]

6) Perusoikeutta rajoitettaessa on huolehdittava riittävistä oikeusturvajärjestelyistä. Oikeusturvajärjestelyt tarkoittavat ennen kaikkea oikeutta muutoksenhakumahdollisuuteen, mutta myös muihin oi-

---

perusoikeuksien rajoitustilanteissa ole useinkaan itsenäistä merkitystä. Tähän on hänen mukaansa syynä se, että tällaiset ydinalueeseen kohdistuvat rajoitukset lienevät poikkeuksetta ainakin suhteellisuusvaatimuksen ja usein myös ihmisoikeusvelvoitteiden noudattamisen vaatimuksen vastaisia. *Viljanen,* Perusoikeuksien rajoittaminen, s. 161.

541 Perustuslakivaliokunta on mietinnössään kuvannut suhteellisuusvaatimusta seuraavasti: ”Rajoitusten on oltava välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi. Jokin perusoikeuden rajoitus on sallittu ainoastaan, jos tavoite ei ole saavutettavissa perusoikeuteen vähemmän puuttuvin keinoin. Rajoitus ei saa mennä pidemmälle kuin on perusteltua ottaen huomioon rajoituksen taustalla olevan yhteiskunnallisen intressin painavuus suhteessa rajoitettavaan oikeushyvään.” PeVM 25/1994 vp, s. 5. Perustuslakivaliokunnan lausunto kuvastaa hyvin vähimmän puuttumisen periaatetta ihmis- ja perusoikeuslähtöisenä periaatteena.

542 Viljasen mukaan punninnassa perusoikeuksiin kiinnittyvät intressit saavat korostuneen painoarvon. Tämän lisäksi punninnassa voivat vaikuttaa eri suuntiin menevinä argumentteina myös muut tekijät, kuten rajoituksen laajuuteen liittyvät yleiset näkökohdat, rajoitusten poikkeuksellisuus ja kohtuullisuus. *Viljanen,* Perusoikeuksien rajoittaminen, s. 157–158.

keusturvatakeisiin. Vaatimus on näin läheisessä yhteydessä perustuslain oikeudenmukaista oikeudenkäyntiä ja hyvää hallintoa koskevaan 21 §:ään. Esimerkiksi DNA-tunnisteen poliisin henkilörekisteriin tallettamisen kohdalla rekisteröidyn oikeusturvan kannalta on pidetty riittävänä, että tietosuojavaltuutettu voi hänen pyynnöstään tarkastaa rekisteritietojen lainmukaisuuden.[543]

7) Rajoitukset eivät saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa. Tämä tarkoittaa sitä, että perusoikeuden rajoitusta ei voida pitää perustuslainmukaisena, jos rajoitus loukkaa ihmisoikeussopimuksia.

Hyväksyttävät rajoitusperusteet ovat jaettavissa kolmeen ryhmään siten, että rajoitus oikeutetaan 1) muilla perusoikeuksilla, 2) muilla perustuslainsäännöksillä tai 3) perustuslain ulkoisilla perusteilla, kuten painavalla yhteiskunnallisella tarpeella.[544] Tähän liittyen keskustelua on herättänyt se, kuinka pitkälle perusoikeuksien rajoittamisessa voidaan mennä oikeuttamalla rajoitusta PeL 7.2 §:ssä mainitun turvallisuusperusoikeuden suojaamisella yksityisten välisissä suhteissa. Tuori on esittänyt huolen siitä, että tällaisessa tulkinta-asetelmassa murennetaan suojaa, jota yksilö nauttii julkisen vallan toimenpiteiltä.[545]

Rajoitusperusteiden toimivuuden kannalta on tärkeää huomata, että perusoikeusrajoituksen tulee täyttää samanaikaisesti kaikki luettelon asettamat vaatimukset. Luetteloa ei kuitenkaan ole tarkoitettu sillä tavalla tyhjentäväksi, ettei muilla seikoilla voisi olla merkitystä ar-

543 Katso tarkemmin PeVL 7/1997 vp.

544 *Viljanen,* Perusoikeuksien rajoitusedellytykset, s. 125–204. Katso myös *Jyränki,* Valta ja vapaus, s. 488.

545 *Tuori,* Yleinen järjestys ja turvallisuus – perusoikeusko?, s. 928

vioitaessa perusoikeusrajoituksen sallittavuutta. Luettelo sisältää kuitenkin arvioinnin kannalta tärkeimmät huomioon otettavat seikat.[546]

5.4. Henkilötietojen suojan periaatesääntely

5.4.1. Eurooppalainen periaatesääntely

Henkilötietojen suojan lainsäädännöllisen järjestämisen keskeisimmät periaatteet ovat vakiintuneet pitkälti kansainvälisen lainvalmistelun tuloksena. Merkittävimmät henkilötietojen suojaa koskevat kansainväliset sääntelyvälineet ovat Euroopan Neuvoston tietosuojasopimus, OECD:n henkilötietojen käsittelyä koskevat ohjeet sekä Euroopan Unionin henkilötietojen suojaa koskeva direktiivi.

Kaikkiin näistä sisältyy omat henkilötietojen käsittelyä koskevat periaatteet. Osa näistä sääntelyvälineistä ei kuitenkaan ole oikeudellisesti sitovia, mutta ovat silti vaikuttaneet merkittävästi niin kansalliseen kuin kansainväliseen henkilötietojen käsittelyn sääntelyyn ja sen kehittymiseen. Näitä sääntelyvälineitä on tarkoituksenmukaista käydä lyhyesti läpi kronologisessa järjestyksessä ennen kansalliseen sääntelyyn siirtymistä.

Euroopan Neuvoston tietosuojasopimus. Vuonna 1981 Euroopan neuvosto huomioi yksityiskohtaisesti henkilötietojen suojan laatimalla yleissopimuksen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. Sopimusta pidetään ensimmäisenä kansainvälise-

546 Viljasen mukaan rajoitusedellytysten luettelo soveltuu sellaisenaan oikeuden muotoon kirjoitettujen perusoikeuksien rajoittamisen arviointiin. Sen sijaan se ei koske hänen mukaansa ehdottomiksi ja täsmällisiksi kielloiksi kirjoitettuja perusoikeussäännöksiä. *Viljanen,* Perusoikeuksien rajoittaminen, s. 145–146.

nä oikeudellisesti sitovana instrumenttina henkilötietojen suojan alalla. Se on edelleen ainoa yksinomaan henkilötietojen suojaa koskeva kansainvälinen sopimus.[547]

Sopimuksen laatiminen katsottiin tarpeelliseksi, koska Euroopan ihmisoikeussopimuksen ei katsottu riittävällä tavalla turvaavan yksilön oikeuksia automaattisessa tietojenkäsittelyssä. Se ei kuitenkaan ole sellaisenaan sovellettavaa oikeutta, vaan sopimus ainoastaan velvoittaa jäsenvaltiot yhdenmukaistamaan kansallisen lainsäädännön sopimuksen periaatteiden kanssa.

Sopimusta sovelletaan ensisijaisesti automaattisen tietojenkäsittelyn avulla tapahtuvaan henkilötietojen käsittelyyn, mutta halutessaan jäsenvaltio voi soveltaa sen määräyksiä myös manuaalisesti tapahtuvaan henkilötietojen käsittelyyn. Sopimuksen sydämenä voidaan pitää sen II lukua, johon on otettu henkilötietojen käsittelyn perusperiaatteet. Sopimuspuolet sitoutuvat toteuttamaan nämä periaatteet kansallisessa lainsäädännössään yksityisyyden suojaamiseksi henkilötietojen käsittelyssä.

Nämä periaatteet ovat kootusti seuraavat[548]:

1.asianmukainen ja laillinen käsittely (fair and lawful processing). Käsiteltävien henkilötietojen tulee olla asianmukaisesti ja laillisesti hankittuja ja käsiteltyjä. (Artikla 5 a-kohta)

2. käyttötarkoitussidonnaisuus (purpose specification). Käsiteltävien henkilötietojen tulee olla määriteltyihin ja laillisiin tarkoituksiin talletettuja eikä niitä saa käyttää tavalla, joka on ristiriidassa mainittujen tarkoitusten kanssa. (Artikla 5 b-kohta)

3. minimointi (minimality). Käsiteltävien henkilötietojen tulee olla riittäviä, asiaan liittyviä, eivätkä liian laajoja niihin tarkoituksiin nähden, joita varten ne on talletettu. Tietojen tulee myös olla sellaisessa

547 *Liu,* Bio-Privacy, s. 97–98.

548 *Bygrave,* International agreements to protect personal data, s. 22-23.

muodossa säilytettyjä, ettei tiedon kohteen yksilöinti ole mahdollista kauemmin kuin mitä tietojen käyttötarkoitus vaatii. (Artikla 5 c- ja e-kohta)

4. laatuperiaate (adequate information quality). Käsiteltävien henkilötietojen tulee olla virheettömiä ja tarpeen mukaan ajan tasalla pidettyjä. (Artikla 5 d-kohta. katso myös artikla 5 c-kohta)

5. arkaluontoisten henkilötietojen erityisasema (sensitivity). Henkilötietoja, joista käy ilmi rotu, poliittiset mielipiteet tai uskonnollinen tai muu vakaumus, samoin kuin henkilötietoja, jotka koskevat terveyttä tai sukupuolielämää, ei saa käsitellä automaattisessa tietojenkäsittelyssä ilman kansallisen lainsäädännön takaamaa riittävää turvaa. Sama koskee henkilötietoja, jotka liittyvät rikosoikeudellisiin tuomioihin. Vuonna 2012 arkaluonteisiin tietoihin tehtiin biometrisia tunnisteita koskeva lisäys. Uudessa arkaluonteisia tietoja koskevassa sopimuksen artiklassa mainitaan biometriset tunnisteet arkaluonteisina tietoina. (Artikla 6)[549]

6. tietoturva (security). Rekisterinpitäjän on ryhdyttävä tarpeellisiin turvatoimiin automaattisesti käsiteltäviin rekistereihin talletettujen henkilötietojen suojelemiseksi vahingossa tapahtuvalta tai luvattomalta tuhoamiselta tai vahingossa tapahtuvalta katoamiselta samoin kuin luvattoman tiedostoon pääsyn, tiedoston muuttamisen tai levittämisen varalta. (Artikla 7)

7. läpinäkyvyys / tiedonsaantioikeus (transparency). Automaattisesti käsiteltävän henkilörekisterin olemassaolo, sen päätarkoitukset samoin kuin rekisterinpitäjän henkilöllisyys ja kotipaikka tai pääasiallinen toimipaikka on voitava selvittää. Tiedonsaantioikeuteen kuuluu myös yksilön oikeus saada kohtuullisin väliajoin ja ilman kohtuutonta

549 The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data – Propositions of Modernisation (annettu marraskuussa 2012).

viivytystä tai kustannuksia vahvistus siitä, onko häntä koskevia henkilötietoja talletettu automaattisesti käsiteltävään rekisteriin. Mikäli tällaisia tietoja on talletettu, yksilöllä on oikeus saada tiedot itselleen ymmärrettävässä muodossa. (Artikla 8 a- ja b-kohdat)

8. suojatoimet (rectification). Sopimuksen pääperiaatteiden mukaiset tiedot on saatava oikaistuiksi tai pyyhityiksi, jos niitä on käsitelty vastoin kansallisen lainsäädännön säännöksiä. Yksilön on myös voitava käyttää oikeuskeinoa, jos vahvistusta tai tiedonsaamista, oikaisua tai poistamista koskevaa pyyntöä ei noudateta. (Artikla 8 c- ja d –kohdat)

Mainitut periaatteet ovat henkilötietojen suojan keskeisiä periaatteita. Niiden funktio on tiedollisen asymmetrian poistaminen yksilölle epäedullisen epätasapainon lieventämiseksi.[550] Tiedollinen asymmetria viittaa tietojenkäsittelyn tehokkuuden ohella siihen, että ilman tietosuojalakien tuottamia oikeuksia henkilöllä on verraten vähäiset mahdollisuudet saada selville, mitä häntä koskevia tietoja käsitellään, kuka tietoja käsittelee, missä tarkoituksessa tietoja käsitellään, mitä uutta tietoa eri tietojen yhdistelemisellä tuotetaan sekä tietoa siitä, miten tietojen käsittely vaikuttaa häneen.[551]

Tämän vuoksi on myös puhuttu pienimmän mahdollisen asymmetrian periaatteesta. Henkilötietojen suojan tarkoituksena on henkilöiltä tiedon käsittelijöille kulkeutuvan tiedon määrän vähentäminen sekä tiedon käsittelijöiltä tiedon kohteena olevalle henkilölle kulkeutuvan tiedon määrän lisääminen.[552]

Kansallisen lainsäädännön ja erityisesti biometrisen tunnistamisen näkökulmasta merkityksellinen on sopimuksen 4. artikla, jonka mukaan jäsenvaltio sitoutuu ottamaan sopimuksen henkilötietojen kä-

550 *Brouwer,* Legality and Data Protection Law, s. 276

551 *Hildebrand,* Profiling and the Identity of the European Citizen, s. 308

552 *Jiang,* Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces, s. 4

sittelyä koskevat periaatteet huomioon kansallisessa lainsäädännössä. Suomen lainsäädäntö ei tältä osin täysin ota huomioon sopimuksen määräystä arkaluonteisten tietojen erityisasemasta, sillä biometristen tunnisteiden erityisasemaa ei ole lainsäädännössä huomioitu.

OECD:n tietosuojasuositus. Taloudellisen kehityksen ja yhteistyön järjestö OECD hyväksyi vuonna 1980 yksityisyyden suojaa ja kansainvälistä henkilötietojen siirtoa koskevan suosituksen (Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data).[553] Suositus sisältää muun muassa henkilötietojen keräämistä ja laatua, rekisteröidyn tarkastusoikeutta, tietoturvaa ja kansainvälistä tiedonsiirtoa koskevia yleisperiaatteita, jotka valtioiden tulisi järjestää lainsäädännössään. OECD:n tietosuojasuositus valmisteltiin samanaikaisesti ja yhteistyössä tietosuojasopimusta valmistelleen komitean kanssa.

OECD:n tietosuojasuositus sekä tietosuojasopimus sisältävät hyvin samansisältöiset henkilötietojen käsittelyä koskevat perusperiaatteet. Suosituksessa olevat periaatteet ovat kuitenkin tietosuojasopimusta osittain tarkemmat.

Suosituksessa asianmukaisen ja laillisen käsittelyn periaate (collection limitation principle) on täsmällisempi vaatimalla käsittelylle yksilön suostumuksen tai ainakin tämän tietoisuuden käsittelystä. Lisäksi suositus edellyttää, että tietojen käsittely on rajoitettua. Myös käyttötarkoituksen periaate (purpose specification principle) on täs-

553 Asiakirja on saatavilla osoitteessa: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. OECD:n periaatteet perustuvat U.S. Health, Education and Welfare Departmentin laatimiin Principles of Fair Information Practice –doktriiniin, joka julkaistiin vuonna 1973. OECD julkaisi uuden päivitetyn henkilötietojen suojaa koskevan asiakirjan vuonna 2013 (Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data)

mällisempi vaatimalla tietojen käyttötarkoituksen määrittelemistä viimeistään tietojen keräämistä aloitettaessa. Suositukseen on otettu myös avoimuuden periaate (openness principle), joka on muotoiltaan tietosuojasopimuksen muotoilua laaja-alaisempi.

Toisaalta suositus jää monilta osin tietosuojasopimusta rajallisemmaksi. Keskeisin puute on se, että suositus jättää arkaluonteisten tietojen aseman vain maininnan tasolle mitenkään erittelemättä näitä tietoja. Tarkkaa rajausta arkaluonteisten ja niin sanottujen tavallisten henkilötietojen välille ei todennäköisesti kuitenkaan ole haluttu tehdä, koska tietojen arkaluonteisuus tulee harkita tapaus- ja tilannekohtaisesti. Rajaamisen tekemättä jättämiseen on vaikuttanut myös se, ettei sopimuksen laatimisen yhteydessä ole löytynyt yksimielisyyttä arkaluonteisten tietojen kategorioista.[554]

Ongelmallista suosituksessa on, ettei siinä tietojen käsittelyyn edellytetä laillista tarkoitusta eikä tietojen poistamista tai tunnistamattomaksi tekemistä niiden käytyä tarpeettomiksi. Ongelmallista on myös se, että käyttötarkoitussidonnaisuus ei suosituksessa ole ehdoton. Siitä on mahdollista poiketa joko rekisteröidyn suostumuksella tai lainsäädännön nojalla.

Eroja tietosuojasopimuksen ja suosituksen välillä on myös rekisteröidyn tiedonsaantioikeuden (individual participation principle) toteuttamisen kohdalla. Suosituksessa kohtuullisen ajan ja kustannusten vaatimusta sovelletaan vain, kun tietoja annetaan rekisteröidylle. Tietosuojasopimuksessa kohtuullisen ajan ja kustannusten vaatimusta sovelletaan puolestaan sekä tietojen antamiseen rekisteröidylle että il-

554 Guideline's Explonatory Memorandum kappaleet 45 ja 51.

moitukseen siitä, onko rekisterinpitäjällä rekisteröityä koskevia tietoja rekisterissään.[555]

Vuonna 2013 tehdyn päivityksen jälkeen suositukseen otettiin erityiset vastuun toteuttamista koskevat toimenpiteet, joiden kautta toteutetaan suosituksen periaatteita. Näillä periaatteilla omalta osaltaan vahvistetaan suosituksen vastuun periaatetta (accountability principle).

Keskeinen periaatteita toteuttavista toimenpiteistä on ensinnäkin yksityisyyden hallintaohjelman laatiminen (privacy management programme), jonka tulee perustua yksityisyyden vaikutusten arviointiin. Toinen keskeinen toimenpide on tietoturvaloukkauksesta ilmoittaminen. Rekisterinpitäjän tulee ilmoittaa rekisteriin kohdistuneista tietoturvaloukkauksista tietosuojaviranomaisille sekä niille rekisteröidyille, joiden oikeuksiin loukkauksella on voimakas vaikutus.

EY:n henkilötietodirektiivi. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta säädettiin lähinnä henkilötietojen liikkuvuuden esteiden poistamiseksi ja EU:n jäsenvaltioiden tietosuojastandardien yhdenmukaistamiseksi. Direktiivin tarkoituksena ei kuitenkaan ole ainoastaan sisämarkkinoiden yhtenäistäminen, vaan myös yksityisyyden ja muiden perus- ja ihmisoikeuksien suojaaminen.

Direktiivin tavoitteena on yksilön perusoikeuksien ja –vapauksien suojaaminen henkilötietojen käsittelyssä. Erityisenä suojan kohteena mainitaan yksilön oikeus yksityisyyteen. Direktiiviä sovelletaan osittain tai kokonaan automatisoituun tietojenkäsittelyyn sekä sellaisten henkilötietojen manuaaliseen käsittelyyn, jotka muodostavat tai joiden

555 Bygrave kuitenkin tulkitsee suosituksen vaatimusta siten, että kohtuullisen ajan ja kustannusten vaatimusta sovelletaan sekä ilmoitukseen tietojen säilyttämisestä että tietojen antamiseen. Tästä ei kuitenkaan ole ollut yksimielisyyttä. *Bygrave,* Data Privacy Law. An International Perspective, s. 47.

tarkoituksena on muodostaa rekisterin osa. Direktiivi kattaa sekä yksityissektorin että julkisen sektorin henkilötietojen käsittelyn.

Direktiiviä ei kuitenkaan sovelleta kaikkeen henkilötietojen käsittelyyn. Soveltamisalan ulkopuolelle jäävät nimittäin yhteisön oikeuden soveltamisalan ulkopuolinen toiminta sekä yleinen turvallisuus, puolustus, valtion turvallisuus ja rikosoikeuden alalla tapahtuva valtion toiminta.

Direktiivin henkilötiedon käsite kattaa sekä objektiiviset että subjektiiviset tunnistettavissa olevaa henkilöä kuvaavat tiedot riippumatta toiminnan luonteesta, henkilön asemasta, tietojen tallennustavasta tai tietojen luonteesta.[556] Henkilötietojen käsittelyä ovat kaikki tietoihin kohdistetut toiminnot tai toimintojen kokonaisuudet tietojen käsittelyn tavasta riippumatta. Myös direktiivissä noudatetaan henkilötietojen käsittelyn periaatepohjaista sääntelyä. Direktiivistä löytyvät samat periaatteet kuin Euroopan neuvoston tietosuojasopimuksesta ja OECD:n tietosuojasuosituksesta.

Edellä mainittuja periaatteita on kuitenkin laajennettu ja tarkennettu. Esimerkiksi rekisterinpitäjän velvollisuuksia on laajennettu asettamalla vaatimus ilmoittaa rekisteröidylle henkilötietojen käsittelyn laajuudesta, riippumatta rekisteröidyn tarkastusoikeudesta (artiklat 10–11). Lisäksi rekiserinpitäjän tulee ilmoittaa henkilötietojen käsittelyn aloittamisesta tietosuojaviranomaiselle (artikla 18).

Näiden laajennusten ja tarkennusten lisäksi direktiivissä säädetään myös uusia yksilön asemaa parantavia oikeuksia. Direktiivissä säädetään yksilölle muun muassa oikeus saada tietää tietojen käsittelyssä noudatettavasta logiikasta (artikla 12(a)). Lisäksi yksilön oikeuksia on parannettu siten, että yksilön oikeusasemaan laajoja vaikutuksia omaavia päätöksiä ei saa tehdä pelkästään automaattisen tietojenkäsittelyn

556 *Kindt,* Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis, s. 94

avulla (artikla 15(1)). Poikkeavaa on myös se, että tietojen käsittelylle on asetettu tietyt sallitut rajat. Tietojen käsittely on sallittua vain tietyin edellytyksin (artiklat 7-8).

Oleellinen laajennus henkilötietojen käsittelyn periaatteisiin on myös sen yksityiskohtaiset säännökset henkilötietojen käsittelyn lainmukaisuuden valvonnasta. Direktiivi velvoittaa jäsenvaltiot perustamaan yhden tai useamman riippumattoman viranomaisen valvomaan henkilötietojen käsittelyn lainmukaisuutta. Näille tietosuojaviranomaisille on myös annettu runsaasti oikeuksia tehtävänsä tehokkaaksi suorittamiseksi (artikla 28).

Kuten edellä esitetystä käy ilmi, kansainvälisistä tietosuojan sääntelyvälineistä Euroopan henkilötietodirektiivi kertoo henkilötietojen käsittelyn periaatteista nykyään selkeimmin. Direktiivistä ne ovat myös siirtyneet osaksi kansallista lainsäädäntöä. Kansallista periaatesääntelyä käydään läpi seuraavassa kappaleessa.

5.4.2. Kansallinen periaatesääntely

Henkilötietojen suojan sääntely, ja esimerkiksi biometristen tunnisteiden sääntely sen osana, perustuu pääosin periaatesääntelyyn. Henkilötietojen suojan sääntely on toisin sanoen tarkoituksella haluttu jättää monilta osin periaatteiden tasolle. Syynä on se, että dynaamisen henkilötietojen käsittelymuotojen sääntely staattisella, yksityiskohtaisella ja tarkalla normistolla ei todennäköisesti johda toivottuun tulokseen.

Henkilötietojen suojan dynaamisuuteen on syynä muun muassa teknologinen ja yhteiskunnallinen kehitys sekä erilaisten henkilötietojen käsittelytapojen muutosherkkyys ja nopea kehitys. Esimerkkinä on henkilötietojen käsittely, jonka sääntelyn sitominen staattiseen ja tarkkaan normistoon hankaloittaisi näiden sääntöjen soveltamista teknologian kehittyessä. Tämän vuoksi on perusteltua, että henkilötietojen suojan sääntelytavat ovat dynaamisia. Tällainen sääntelytapa pystyy paremmin vastaamaan muuttuvan toimintaympäristön haasteisiin.

Periaatepohjaisen sääntelytavan taustalla on katsottu olevan sääntelyutopia. Tämän tunnuspiirteitä ovat muun muassa se, että 1) sääntely kohtaa hyvin sääntelyn kohteet, 2) sääntely toteutuu yhdenmukaisesti, 3) sääntelyn kohteille tarjotaan joustavuutta, 4) sääntely on tuloksellista ilman merkittäviä kustannuksia ja 5) sääntelyviranomaiset ymmärtävät toimialan ongelmia ja kohdentavat toimensa asioihin, joihin liittyvistä periaatteista ja tavoitteista vallitsee yhteisymmärrys.[557]

Henkilötietojen suojan sääntely perustuu Suomessa kansainvälisesti omaksutun sääntelymallin mukaisesti (pääosin) periaatesääntelyyn. Periaatesääntely on toteutettu henkilötietojen suojaa koskevassa lainsäädännössä pääasiassa yleissäännösten avulla. Yleissäännöksellä tarkoitetaan säännöstä, joka on kirjoitettu yleiseen muotoon ja joka ilmentää jotain yleistä periaatetta. Yleissäännöksen vastakohtana on konkreettinen oikeussääntö, joka sisältää nimenomaisen velvoitteen ja kiellon. Yleistä periaatetta ilmentävää säännöstä sovelletaan yksittäistapauksessa yhdessä muiden oikeussääntöjen kanssa sovittaen yleinen periaate yksittäistapaukseen. Periaatteen painoarvo ja konkreettinen sisältö riippuvat kunkin yksittäistapauksen tosiseikoista ja muista tilanteeseen sovellettavista konkreettisista oikeussäännöistä.[558]

Henkilötietojen käsittelyn osalta tulkinnassa on tärkeää tunnistaa kaikki asiaan vaikuttavat yleissäännöt sekä yksityiskohtaisemmat normit. Henkilötietojen suojan sääntelyn tulkinta muodostuu toisin sanoen sääntelykokonaisuudesta, jota on tullkittava sääntelykokonaisuuden monipuolisuus huomioon ottaen. Tulkintatilanteessa ratkaisun sisältöön vaikuttavat normit ja periaatteet on tasapainotettava niin, että ratkaisussa päädytään lainmukaiseen ratkaisuun, joka ei ole ristiriidassa keskeisten sääntelyn tavoitteiden tai niiden tausta-arvojen kanssa.

557 *Black,* The Rise, Fall and Fate of Principles Based Regulation, s. 12

558 HE 32/2012 vp., s. 73–74.

Henkilötietojen käsittelyn keskeiset periaatteet on mahdollista jakaa kolmeen kategoriaan: 1) yleiset periaatteet, 2) henkilötietojen käsittelijöitä koskevat periaatteet ja 3) yksilön oikeuksia koskevat periaatteet. Yleiset periaatteet koskevat kaikkia ja ovat tunnusomaisia modernille tietosuojalainsäädännölle. Henkilötietojen käsittelijöitä ja yksilön oikeuksia koskevat periaatteet ovat luonteeltaan myös yleisiä ja kaikkia koskevia, mutta kohdentuvat eri tavalla niihin, joilla on oikeuksia ja niihin joilla on velvollisuuksia. Nämä periaatteet liittyvät toisiinsa, mutta erottelu auttaa eri näkökulmista havaitsemaan, mikä on henkilötietojen käsittelyssä tärkeää.[559]

Periaatteiden avulla pyritään luomaan lainsäädäntöä ja vastaavasti ymmärtämään voimassa olevaa lainsäädäntöä ihmisen perusoikeuksien kunnioittamiseksi henkilötietojen käsittelyssä.[560] Periaatteiden taustalla on ihmisen itsemääräämisoikeus sekä sen suojaaminen perusoikeustasoisesti henkilötietojen käsittelyssä.

5.4.2.1. Yleiset periaatteet

Lakisääteisyys. Yleisistä sääntelyperiaatteista tärkein on lakisääteisyyden vaatimus. Henkilötietojen suojasta on säädettävä laissa ja henkilötietoja on lupa käsitellä vain lainmukaisesti. Periaate on selkeä viesti henkilötietojen suojan tärkeydestä.

Periaate osoittaa myös, että kysymys ei ole enää vain teknisluonteisesta asiasta. Tietosuojalainsäädäntö henkilötietojen suojaa koskevana lainsäädäntönä on jotain paljon enemmän. Kysymys on yksilön subjektiivisten oikeuksien perusoikeuspohjaisesta toteuttamisesta persoonallisuusoikeuden tasolla. Kysymys on yksiselitteisesti perusoikeuksien

559 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 342.

560 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 341–342.

suojasta.[561] Henkilötietojen suojan avulla toteutetaan yksilön ihmisarvon kunnioittamista henkilötietojen käsittelyssä.

Ennen EU:n tietosuojadirektiivin implementointia yleislaki, jolla tarkennettiin perustuslain 10.1 §:n mukaista henkilötietojen suojaa, oli henkilörekisterilaki. Henkilötietolaki korvasi henkilörekisterilain tullessaan voimaan vuonna 1999.[562] Tätä yleislakia täydentää laaja henkilötietojen suojaa koskeva erityislakien joukko, joista biometrisen tunnistamisen näkökulmasta merkityksellisiä ovat ennen kaikkea laki yksityisyyden suojasta työelämässä, laki henkilötietojen käsittelystä poliisitoimessa sekä passilaki. Nämä lait antavat mahdollisuuden biometristen tunnisteiden käsittelyyn erityislainsäädännön nojalla.[563]

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja

561 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 343

562 Henkilötietotoimikunta ehdotti alun perin henkilötietolain nimeksi lakia yksityisyyden suojasta henkilötietojen käsittelyssä (henkilötietolaki). Toimikunnan pyrkimyksenä oli, että lain keskeinen tavoite ja sääntelyn kohde, yksityisyyden suojaaminen ja henkilötietojen käsittely, ilmenisivät jo itse lain nimikkeestä. Nimike katsottiin kuitenkin liian vaikeaksi omaksua, joten nimikkeeksi tuli henkilötietolaki nimikkeen helppouden ja yksinkertaisuuden takia. HE 96/1998 vp., s. 30

563 Isyyden selvittämisessä voidaan käyttää hyväksi geneettistä tietoa. Laki oikeusgeneettisestä isyystutkimuksesta mahdollistaa DNA-tutkimuksen joko tutkittavan suostumuksella taikka tuomioistuimen määräyksestä. Kysymys on näin ollen biometrisesta tunnistamisesta yksilön DNA:ta ja muita geneettisiä ominaisuuksia hyväksi käyttäen. Laki näin ollen mahdollistaa biometrisen tunnistamisen käyttämisen osana isyyden selvittämistä. Laissa ei kuitenkaan säädetä biometristen tunnisteiden käsittelystä, vaan ainoastaan näytteen ottamisesta. Tämän vuoksi lakia ei tässä tutkimuksessa käsitellä.

käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Lailla myös pyritään turvaamaan, ettei yksityiselämän suojaa tai muita yksityisyyden suojaa turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta henkilötietoja kerättäessä, talletettaessa, käytettäessä, siirrettäessä, luovutettaessa tai muutoin käsiteltäessä.[564] Lain suojelukohteena eivät ole tiedot sinänsä, vaan yksilö sekä hänen oikeutensa ja turvallisuutensa.[565]

Henkilötietolakia sovelletaan sekä automaattiseen että manuaaliseen henkilötietojen käsittelyyn. Henkilötietolaissa ei kuitenkaan oteta kantaa syntymättömän lapsen tai kuolleen henkilön yksityisyyden suojaan. Vaille huomiota asia ei silti ole jäänyt. Syntymättömän lapsen kohdalla asia on ratkaistu niin, että hänen tietojaan pidetään lapsen äidin tietojen liitännäistietoina. Lapsen synnyttyä nämä tiedot tulevat lapsen henkilötiedoiksi. Henkilötietolaissa eikä lakia edeltäneessä henkilörekisterilaissa suoranaisesti säädetty kuolleenkaan henkilön henkilötietojen suojasta. Jo henkilörekisterilain soveltamiskäytännössä on kuitenkin katsottu, että laki koskee myös kuolleita henkilöitä.[566]

Yksilön tunnistettavuus. Henkilötietojen suojaa koskeva lainsäädäntö koskee lähtökohtaisesti vain kaikkea tiettyyn luonnolliseen henkilöön välillisesti tai välittömästi yhdistettävissä olevaa informaatiota.

564 HE 96/1998 vp., s. 30.

565 *Raatikainen,* Yksityisyyden suoja työelämässä, s. 18.

566 HE 96/1998 vp., s. 35. Samaan tulkintaan on päätynyt myös tietosuojalautakunta ratkaisussa 2/2009 (Dnro 1/933/2008). Katso myös *Tuori,* Lausunto (10.9.2008) perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle laiksi Jokelan koulukeskuksessa sattuneiden kuolemaan johtaneiden tapahtumien tutkinnasta (HE 51/2008). Vertaa *Kangas,* Digitaalinen jäämistövarallisuus, s.33, jonka mukaan henkilötietolain ajallinen soveltamisala päättyy kuolemaan. Katso myös PeVL 71/2002 vp.

Henkilötiedon käsite on tällöin olennainen peruskäsite, sillä henkilötietolaki koskee henkilötietojen käsittelyä.

Henkilötieto on aina tunnistetieto, sillä sen tulee olla liitettävissä tiettyyn henkilöön (HetiL 3 §). Eri tilanteissa erilainen informaatio voi kuitenkin johtaa eri tavoin yksilön tunnistettavuuteen. Myös sellainen välillinen informaatio, jonka avulla henkilö on tunnistettavissa, on henkilötietolain mukainen henkilötieto.[567] Henkilötietodirektiivissä on tarkennettu, milloin yksilö on tunnistettavissa. 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.

Teknologian kehittyminen on kuitenkin tuonut mukanaan tilanteita, joita lakia säädettäessä ei ole osattu eikä voitu ottaa huomioon. Tällaisissa tilanteissa on perusteltua tulkita henkilötiedon käsitettä laajentavasti. Tärkeää onkin huomata, että henkilötieto ei ole vain tekstitieto. Kaikenlaiset, tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot, kuten biometriset tunnisteet, ovat henkilötietoja.[568] Tässä tapauksessa tieto saa henkilötiedon luonteen, kun se yhdistelemisen kautta kuvaa yksilöä. [569]

---

567 Näin myös *Raatikainen,* Yksityisyyden suoja työelämässä, s. 42.

568 *Paavilainen,* Tietoturva, s. 99 sekä *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 343–345

569 Näin myös *Pesonen,* Viestintäoikeuden käsikirja, s.179. Neuvonen lähestyy asiaa teknologianeutraaliuden kautta toteamalla, että henkilötieto on teknologianeutraali ilmaisu, joka kattaa kaiken sormenjäljistä auton rekisteritunnukseen. Olennaista Neuvosen mukaan on, että tiedon perusteella tai tietoja yhdistelemällä on tietty luonnollinen henkilö yksilöitävissä. Neuvonen, Yksityisyyden suoja Suomessa, s. 74.

Tunnistettavuudella on kuitenkin rajansa. Henkilöä ei nimittäin pidetä tunnistettavissa olevana, jos tunnistaminen vaatii kohtuuttomasti aikaa, kustannuksia ja työtä.[570]

Rekisterinpidon avoimuus. Tietosuojalainsäädännön yksi perustavoitteista on henkilötietojen käsittelyn tekeminen lakisääteisenä avoimeksi. Henkilötietojen käsittelyn on tapahduttava niin, ettei se jää minkäänlaisen salaisen vallankäytön välineeksi.

Avoimuutta toteutetaan eri tavoin rekisteröityjen tiedonsaantioikeuksista aina tietosuojaviranomaisten tarkastusoikeuksiin.[571] Henkilötietodirektiivissä on pääsäännöksi asetettu myös rekisterinpitäjän velvollisuus ilmoittaa rekisterinpidosta tietosuojaviranomaisille. Direktiivi kuitenkin sallii tästä poikkeamisen. Suomessa vain eräistä keskeisimmistä rekistereistä sekä automatisoidun, ihmisen ominaisuuksia arvioivan päätöksentekojärjestelmän käyttöönotosta on rekisterinpitäjän aina ilmoitettava oma-aloitteisesti tietosuojavaltuutetulle (HetiL 36 §). Tavanomaiset hallinnon ja yritystoiminnan rekisterit sekä lakisääteiset rekisterit jäävät ilmoitusvelvollisuuden ulkopuolelle.

Sääntelyratkaisu on perusteltavissa sillä, että tietosuojaviranomaisten ylläpitämä rekisterien rekisteri on ennen kaikkea tietoturvallisuuden kannalta ongelmallinen kuten kaikki keskitetyt ja laajat rekisterit. Direktiivin mukainen ilmoitusvelvollisuus on myös liian byrokraattinen sisältäessään pelkästään saapuneiden ilmoitusten toteamista. Suomessa käytössä olevan sääntelyn lähtökohtana on ilmoituksen tarkoittaman tietojen käsittelyn yksityiskohtaisempi tarkastelu ja mahdollinen enempiin toimenpiteisiin ryhtyminen. Valittu rajoitetun

570 Euroopan neuvoston suositus, Protection of personal data used for employment purposes. Myös ILO:n ohjeistossa todetaan, että tunnistettavuuden käsitettä tulee tulkita kohtuullisesti.

571 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 345

ilmoitusvelvollisuuden malli on yhdenmukainen muutoinkin valitun kevyen byrokratian kanssa.

Omalta osaltaan rekisterinpidon avoimuutta toteutetaan rekisteröidyn osallistumisen periaatteella. Tiedollisen itsemääräämisoikeuden näkökulmasta on oleellista, että rekisteröity pystyy mahdollisimman tehokkaasti osallistumaan ja vaikuttamaan tietojensa käsittelyyn. Periaatetta toteutetaan rekisteröidyn suostumusta koskevien, tietojen keräämistä rekisteröidyltä itseltään koskevien ja rekisteröidyn tiedonsaantioikeuksia koskevien sääntöjen avulla.[572] Näitä sääntöjä käsitellään tässä tutkimuksessa myöhemmin kohdassa 5.3.2.3.

Tarpeellisuus. Keskeinen periaate tietosuojalainsäädännössä on tarpeellisuuden vaatimus. Henkilörekistereiden ja niissä olevien tietojen tulee olla tarpeellisia (HetiL 9 §). Tarpeellisuusvaatimus on sinänsä yksinkertainen asia rekisterinpitäjälle kohdistettuna käskynä. Henkilörekisterien pitäjien tulee pitää vain toimintansa kannalta tarpeellisia rekistereitä ja niissä tarpeellisia tietoja. Vaatimus tietojen tarpeellisuudesta on biometristen tunnisteiden kohdalla erityisen tärkeä. Biometrisen tunnistamisen kohdalla yhtenä uhkana on käyttötarkoitukseen nähden tarpeeton ja liiallinen tietojen kerääminen.

Tietoturvallisuus. Eri toimintojen lisääntyvä riippuvuus automaattisesta tietojenkäsittelystä ja tietoliikenteestä on nostanut tietoturvallisuuden tason yhdeksi yhteiskunnan keskeisistä rakennetekijöistä. Turvallista informaatioinfrastruktuuria ei saada aikaan ilman kehittynyttä tietoturvaa ja tietoturvakulttuuria. Perinteiset tietoturvallisuuden muodot ovatkin saaneet rinnalleen oikeudellisen tietoturvallisuuden. Kun verkkoyhteiskunnassa perusoikeuksien hyödyntäminen on siirtymässä enenevässä määrin tietoverkkoihin, on yksilöllä oikeus odottaa turvallista informaatioinfrastruktuuria. Verkkoyhteiskunnassa

572 *Bygrave,* Data Privacy Law. An International Perspective, s. 158.

tietoturvallisuus on tavanomaisten perusoikeuksien toimivuuden ja suojan tae: metaperusoikeus.[573]

Henkilötietojen käsittelyssä tietoturvallisuus on keskeisessä osassa. Henkilötietolaissa tietoturvallisuus on yksi keskeisiä ja välttämättömiä periaatteita. Henkilötiedot tulee suojata asianmukaisesti niiden luvatonta käyttöä vastaan.

Henkilötietolain tietoturvallisuussäännös on myös suhteellisuusperiaatteen ilmentymä. Täsmällistä tietoturvallisuuden tasoa ei ole laissa pyritty määrittelemään. Laissa puhutaan vain tarpeellisista toimista. Tietoturvallisuus onkin mitoitettava suojatarpeen mukaan. Tietojen laadun lisäksi myös taloudelliset tekijät ovat asiaan vaikuttavia.

Henkilötietolain tavoitteen ja yksilön oikeuksien näkökulmasta vaadittava tietoturvallisuuden taso ei voi olla vaatimaton. Sitä ei myöskään arvioida vain kannattavuuden tai helppouden näkökulmasta.[574] Biometristen tunnisteiden kohdalla tietoturvallisuudella voidaan tehokkaasti ehkäistä myös biometrisen tunnistamisen käytöstä aiheutuvia riskejä.

Hyvä tietojenkäsittelytapa. Henkilötietojen käsittelyn pohjan muodostaa asianmukaisuus ja lainmukainen käsittely. Onkin tarkoituksenmukaista puhua hyvästä tietojenkäsittelytavasta. Henkilötietolaissa hyvälle tietojenkäsittelytavalle on annettu näkyvä rooli. Se on otettu yhdeksi lain nimenomaisista tavoitteista. Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Hyvän tietojenkäsittelytavan ottaminen lain yhdeksi tavoitteeksi kuvastaa henkilötietolain abstraktisuutta. Täsmällisten sääntöjen pääosin puuttuessa on pyrittävä noudattamaan hyvää tapaa henkilötieto-

573 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 347

574 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 348

jen käsittelyssä. Itsekontrollin ja itseohjautuvuuden merkitys korostuu henkilötietojen suojan toteuttamisessa. Tällä tavoin toimittaessa painotetaan viranomaisten ohjaavaa roolia.

Hyvä tietojenkäsittelytapa ohjaa kunnioittamaan ihmistä jo ennakollisesti henkilötietojen käsittelyssä.[575] Oleellinen osa tätä kunnioitusta on rekisteröidyn ja rekisterinpitäjän intressien tasapainottaminen, mikä osaltaan käy ilmi erityisesti tietojen tarpeellisuuden vaatimuksesta, jota puolestaan tukee käyttötarkoitussidonnaisuuden vaatimus.[576] Tämä kuvaa osuvasti hyvän tietojenkäsittelytavan luonnetta henkilötietojen suojaa koskevana yleisenä periaatteena. Se ei tiivisty vain yhteen periaatteeseen, vaan vaikuttaa kaikkeen henkilötietojen käsittelyyn.

Laissa ei ole määritelty hyvää tietojenkäsittelytapaa. Siihen päästään optimoimalla lain eri säännösten soveltaminen sen tavoitteiden mukaisesti yksityisyyden ja muiden perusoikeuksien suojaamiseksi.[577] Henkilötietolain tavoitesäännöksen lisäksi hyvä tietojenkäsittelytapa ilmenee huolellisuusvelvoitetta koskevassa säännöksessä.

Hyvään tietojenkäsittelytapaan kuuluu ainakin rekisteröityjen oikeuksien kunnioittaminen. Rekisteröidyn oikeudet tulee huomioida kaikissa tietojen käsittelyn vaiheissa eikä rekisterinpitäjällä ole oikeutta jättää huomiotta rekisteröidyn kohtuullisia odotuksia yksityisyytensä kunnioittamiseen. Osana rekisteröidyn oikeuksien kunnioittamista on myös pidättyminen painostamasta rekisteröityä tietojensa antamiseen.[578]

Hyvään tietojenkäsittelytapaan kuuluu myös yksityisyyttä parantavan tekniikan käyttö, vaikka henkilötietolaki ei tähän ota kantaa.

---

575 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 349

576 *Bygrave,* Data Privacy Law. An International Perspective, s. 148.

577 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 349

578 *Bygrave,* Data Privacy Law. An International Perspective, s. 145–146.

Käsiteltävien tietojen määrä ja laatu kuitenkin korostavat yksityisyyttä parantavan tekniikan käyttöä osana hyvää tietojenkäsittelyä.[579]

Käsiteltävien tietojen suojaamisesta tulee huolehtia asianmukaisella tavalla jo ennakolta. Hyvä tietojenkäsittelytapa edellyttää myös, ettei kenenkään yksityisyyttä saa perusteettomasti loukata eikä vaarantaa. Esimerkiksi biometristen tunnisteiden keräämisen tarve ja vaihtoehtoisten yksilöintitietojen käyttömahdollisuudet tulee selvittää aina jo suunnitteluvaiheessa kaikkien käsittelyvaiheiden kannalta. Biometristen tunnisteiden kohdalla yksityisyyttä parantavan tekniikan käyttö saa korostuneen merkityksen näiden tietojen erityispiirteistä ja niihin liittyvistä yksityisyyteen kohdistuvien uhkien vuoksi. Yksityisyyttä parantavan tekniikan käyttö on suositeltavaa myös, jotta tietojen kerääminen voidaan minimoida ja niiden laiton käsittely estää.

Yksityisyyden suojaa parantavista tekniikoista ei ole yhtenäistä määritelmää. Yleisesti ottaen näillä tekniikoilla tarkoitetaan yhtenäistä tieto- ja viestintäteknisten toimenpiteiden järjestelmää, jolla suojataan yksityisyyttä poistamalla henkilötiedot kokonaan tai osittain tai ehkäisemällä tarpeeton ja / tai ei-toivottu henkilötietojen käsittely heikentämättä tietojärjestelmän toimivuutta.[580]

Erityisesti biometrisen tunnistamisen kohdalla yksityisyyttä parantavan tekniikan käyttö on suositeltavaa. Biometriset tunnisteet ovat luonteensa puolesta erityisen herkkä henkilötietojen ryhmä, joka vaatii vahvat suojatoimet. Koska laissa biometristen tunnisteiden käsittelylle ei ole säädetty erityisiä rajoituksia, rekisterinpitäjä voi vähentää biometrisiin tunnisteisiin kohdistuvia uhkia ja parantaa rekisteröidyn

579 HE 96/1998 vp, s. 31 sekä *Raatikainen,* Yksityisyyden suoja työelämässä, s. 81.

580 KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla KOM(2007) 228 lopullinen, s. 3

yksityisyyden suojaa käyttämällä yksityisyyttä parantavaa tekniikkaa. Tällä tavoin rekisterinpitäjä voi myös poistaa biometrisen tunnistamisen järjestelmiin kohdistuvaa epäluottamusta.

Tietosuojaviranomaisten palvelut. Tietosuojalainsäädäntöä kuvataan niin sanotuksi institutionaaliseksi lainsäädännöksi. Tällä tarkoitetaan sitä, että materiaalista lainsäädäntöä täydentää erityisesti sen toteutumisen ohjaukseen ja valvontaan tarkoitettu viranomaiskoneisto. Suomessa tietosuojavaltuutettu ja tietosuojalautakunta muodostavat tietosuojan varsinaisen viranomaiskoneiston. Työelämän tietosuojan alueella näitä viranomaisia täydentävät työsuojeluviranomaiset.

Tietosuojaviranomaisten tulee olla itsenäisiä ja riippumattomia viranomaisia. Tietosuojaviranomaiset eivät näin ollen ole tavanomaisia hallinnollisia viranomaisia. Avoimeksi on jäänyt se, minkälaista riippumattomuutta tietosuojaviranomaisilta edellytetään. Vähimmäisvaatimuksena on hallinnollinen riippumattomuus muista viranomaisista. Tällä tarkoitetaan tietosuojaviranomaisten riippumattomuutta muun muassa muiden hallinnollisten elinten, kuten ministeriön, budjetti- ja määräysvallasta. Erityisesti kysymys on sen takaamisesta, että tietosuojaviranomaiset ovat riippumattomia kaikenlaisesta suorasta ja välillisestä ulkopuolisesta vaikuttamisesta.[581] Tietosuojaviranomaisten riippumattomuus rinnastuukin paljossa tuomioistuinten riippumattomuuteen.

Kysymys on eräällä tavalla perinteisen valtiovallan kolmijako-opin vaihtumisesta uuteen vallan nelijako-oppiin. Tavanomaisten hallintoviranomaisten lisäksi tarvitaan riippumattomia ihmisten oikeuksia

581 EUT:n ratkaisu C-581/07, Euroopan komissio v. Saksa (2010) ECR I-1885. Katso myös *Bygrave,* Data Privacy Law. An International Perspective, s. 170.

turvaavia viranomaisia ennen kaikkea ihmisoikeusperusteisten oikeuksien toteutumisen valossa.[582]

Valvontaviranomaisten asema korostuu yksityisyyden suojan toteuttajana henkilötietojen käsittelyssä. Ensinnäkin henkilötietojen suojaa koskeva lainsäädäntö on luonteeltaan abstraktia ja periaatesuuntaista. Tällöin sitä avaavien hyvien käytäntöjen synnyttäminen eri sektoreille ei synny ilman viranomaistoimia.

Henkilötietojen suojaa koskevan lainsäädännön abstraktisuuden lisäksi tietosuojaviranomaisten korostunut asema on perusteltavissa tietosuojalainsäädännön hajanaisuudesta aiheutuvalla epätietoisuudella. Tietosuojaviranomaisten ohjaus ja valvonta vähentävät omalta osaltaan epätietoisuutta henkilötietojen käsittelyssä. Epätietoisuuden syntyessä rekisterinpitäjät ja rekisteröidyt voivat kääntyä tietosuojaviranomaisten puoleen saadakseen tietoa omista oikeuksistaan ja velvollisuuksistaan henkilötietojen käsittelyssä.

Automaattisen henkilöarvioinnin rajoittaminen. Henkilötietojen suojan ja tietosuojalainsäädännön kohdalla automaattisen päätöksenteon rajoittamisen periaate jää usein vaille huomiota. Osasyynä tähän on se, että se ei ilmene henkilötietolain alkuosan yleisistä säännöksistä.

Kysymys on merkittävästä ihmisoikeusperusteisesta metaperiaatteesta. Ihmisen ominaisuuksia koskevien arviointien tulee tapahtua pääsääntöisesti ihmisen toimesta.[583] Automaattisen päätöksenteon periaatteellinen ongelmallisuus henkilötietojen käsittelyssä on muuttunut käytännössä merkitykselliseksi siksi, että automaattisen päätöksenteon mahdollisuuksien lisääntyminen on tuonut erilaisia vaihtoehtoja automaattisten henkilöarviointien hyödyntämiseen jo arkipäivän toimistoautomaatiossa.

582 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 350–351

583 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 352.

Henkilötietolakiin automaattisen arvioinnin rajoittaminen on tullut Euroopan henkilötietodirektiivistä. Laki ei kuitenkaan täysin kiellä automaattista henkilöarviointia. Henkilötietolain 31 §:n mukaan sellaisen rekisteröidyn tiettyjen ominaisuuksien arviointiin tarkoitetun 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 rekisteröidyn sopimuksen tekemistä tai täytäntöönpanoa koskeva pyyntö.

Pääsääntönä siis on, että automatisoitu päätöksenteko on kielletty. Sallittua se on vain poikkeuksellisesti. Rajoituksen periaatteellisen merkityksen vuoksi automatisoitujen päätösjärjestelmien käyttöönotosta on ilmoitettava ennakolta tietosuojavaltuutetulle. Ilmoituksessa on samalla kuvattava järjestelmässä käytettävä logiikka (HetiL 36.2 §).

Automatisoidulla päätöksellä tarkoitetaan sellaista, rekisteröidyn tiettyjen ominaisuuksien arviointiin tarkoitettua päätöstä, joka tehdään ainoastaan automatisoidun tietojenkäsittelyn perusteella ja josta aiheutuu rekisteröidylle oikeudellisia vaikutuksia tai joka muuten vaikuttaa häneen merkittävällä tavalla. Automatisoitu päätös on kysymyksessä vain silloin, kun päätöksen sisältö ei perustu minkäänlaiseen inhimilliseen myötävaikutukseen.[584]

Päätöksen tarkoituksena on oltava rekisteröidyn ominaisuuksien, kuten käyttäytymisen, arvioiminen. Merkittävien oikeusvaikutusten aiheutuminen viittaa siihen, että pelkästään vähäiset oikeusvaikutuk-

584 HE 96/1998 vp, s. 65.

set eivät riitä (esimerkiksi suoramarkkinointi tietokoneen laatiman listan perusteella). Merkittäviä oikeusvaikutuksia ovat sellaiset, joilla on suurta merkitystä yksilön oikeusasemaan, esimerkiksi taloudellisiin tai sosiaalisiin oikeuksiin.

Biometrisen tunnistamisen käyttämisessä on aina kysymys automatisoidun päätöksen tekemisestä, jolla on vaikutuksia rekisteröidyn oikeuksiin.[585] Näin ollen henkilötietolain automatisoitua päätöstä koskevat säännökset tulee huomioida. Tällaisen järjestelmän käyttäminen on lähtökohtaisesti kielletty.

Käytännesäännöt. Abstraktina lainsäädäntönä tietosuojalainsäädäntö on vaikeasti ymmärrettävää.[586] Tämän vuoksi henkilötietolakiin on ratkaisumalliksi henkilötietodirektiivistä otettu käytännesäännöt. Henkilötietodirektiivi ja henkilötietolaki edellyttävät, että eri aloille pyritään laatimaan toimialakohtaisia käytännesääntöjä.

Käytännesäännöt ovat kertomus lain sisällöstä. Niiden avulla välitetään lakitekstiä yksityiskohtaisemmalla tavalla ohjeita ja tietoa hyvästä, yksilön oikeudet huomioon ottavasta henkilötietojen käsittelystä. Tämän vuoksi ne ovat tärkeitä välineitä paitsi lain tuntemisessa myös hyvän tietojenkäsittelytavan ymmärtämisessä ja kehittämisessä.

Suomi on yksi näkyvimmin tietosuojan käytännesääntöjä hyödyntävistä maista Euroopassa. Osin syynä on paikallisten tietosuojaviranomaisten puuttuminen. Loppujen lopuksi kysymys on kuitenkin ollut tietosuojavaltuutetun aktiivisuudesta käytännesääntöjen aikaansaamiseksi. Laki halutaan käytännesääntöjen avulla tuoda käyttäjien omin sanoin kuvattuna lähemmäksi käytäntöjä. Tällöin laki koetaan

585 Näin myös *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 376.

586 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 353

helpommin omaksi. Toisaalta käytännesääntöihin voi sisältyä myös virheellisiä käsityksiä.[587]

Sanktiojärjestelmä. Keskeinen rakenteellinen tekijä tietosuojalainsäädännössä ja myös osa yksilön oikeusturvaa on sanktiojärjestelmän olemassaolo. Henkilötietojen suojaa toteutetaan viime kädessä sanktioiden kautta. Tietosuojavaltuutetun ohjauksen ja valvonnan, hyvän tietojenkäsittelytavan sekä tietosuojalautakunnan päätöksenteon puitteissa pyritään ensisijaisesti tuomioistuintien välttämiseen. Toisaalta oikeusvaltioperiaate edellyttää, että kiistatilanteissa tulkinnat on mahdollista saattaa tuomioistuinten ratkaistavaksi.

Henkilötietojen käsittelyn kohdalla tuomioistuintie on kaksihaarainen. Tietosuojalautakunnan ratkaisuihin haetaan muutosta hallintotuomioistuimista. Rikosoikeudelliset asiat puolestaan kuuluvat yleisille tuomioistuimille.

Lainsäädäntöön on myös otettu kaksi erityistä sanktiolajia: henkilörekisteririkkomus ja –rikos. Henkilörekisteririkkomuksesta säädetään henkilötietolaissa, kun taas henkilötietorikoksesta rikoslaissa.

5.4.2.2. Rekisterinpitäjiä koskevat erityiset periaatteet

Henkilötietojen suojaa koskevalla lainsäädännöllä vaikutetaan merkittävästi niihin tapoihin, joilla eri toiminnoissa on lupa käsitellä henkilötietoja. Henkilötietoja on lupa käsitellä vain tietyin edellytyksin.

Henkilötietolaki koskee lähtökohtaisesti kaikenlaista henkilötietojen käsittelyä ja kaikkia käsittelijöitä, ellei laissa ole toisin säädetty. Henkilötietolaissa niitä, jotka käsittelevät henkilötietoja kutsutaan rekisterinpitäjiksi. Suurin osa henkilötietolain säännöksistä koskee juuri heitä. Rekisterinpitäjiä koskevat säännökset muokkaavat merkittävästi henkilötietojen käsittelyä käytännössä. Tämän vuoksi heitä koskevat

587 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 354

oikeusperiaatteet ovat tietosuojajärjestelmän toimivuuden kannalta erittäin tärkeitä.

Tarpeellisuus. Tarpeellisuusvaatimus on henkilötietojen käsittelyn yleinen ohjausperiaate. Erityisesti kysymys on kuitenkin tietojen käsittelijöiden toimintaa koskevasta periaatteesta, joka on myös rekisterinpitäjien toiminnan keskeinen mittapuu.

Tarpeellisuusvaatimus käy ilmi henkilötietolain 9 §:stä, jonka mukaan käsiteltävien henkilötietojen tulee olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia.[588] Tarpeellisuusvaatimus ei kuitenkaan poista suostumuksen edellyttämistä.

Tarpeellisuusvaatimus täyttyy, kun käsiteltävät henkilötiedot ovat asianmukaisia ja olennaisia eivätkä liian laajoja käyttötarkoitukseensa nähden.[589] Arvioinnin lähtökohtana on se, ovatko tiedot rekisterinpitäjän toiminnan järjestämiseksi objektiivisesti arvioiden asiallisesti perusteltuja.[590] Tarpeellisuusvaatimukseen liittyy keskeisesti suunnitelmallisuus, sillä tietojärjestelmät ja niiden käyttö on suunniteltava tarpeellisten henkilötietojen käsittelyä varten. Tarpeellisuusvaatimuksella on kiinteä yhteys myös tietojen hävittämisvelvollisuuteen, sillä se

588 Bygraven mukaan tästä velvollisuudesta voidaan käyttää myös nimitystä suhteellisuusperiaate tai minimaliteettiperiaate. *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 60 ja Data Privacy Law. An International Perspective, s. 151

589 *Bygrave,* Data Privacy Law. An International Perspective, s. 148.

590 Tämä arviointitapa merkitsee muun muassa sitä, että rekisterinpitäjän toimintaa verrataan muihin vastaaviin rekisterinpitäjien omaksumiin käytäntöihin. Käytäntöön tulee kuitenkin liittää yleisen hyväksyttävyyden vaatimus ennen kuin sen voidaan katsoa olevan hyväksytty toimintatapa. HE 49/1986 vp, s. 28.

omalta osaltaan asettaa velvollisuuden hävittää määritellyn käyttötarkoituksen kannalta tarpeettomaksi käyneet tiedot.[591]

Tarpeellisuusvaatimus koskee kuitenkin myös sitä, kuinka pitkälle henkilön yksityisyyteen henkilötietojen käsittelyssä mennään. Esimerkiksi biometristen tietojen kokoamista tulee välttää, jos käytettävissä on muita vähemmän yksityisyyteen puuttuvia menetelmiä. Tämä tarkoittaa sitä, että ensin on määriteltävä selvästi se tarkoitus, jota varten biometriset tiedot kerätään ja käsitellään. Lisäksi on tarpeen arvioida tietojen suhteellisuus ja laillisuus yksilön perusoikeuksien ja –vapauksien kunnioittamiseen kohdistuvat riskit huomioon ottaen. Vähimmän puuttumisen periaatteen mukaisesti on erityisesti selvitettävä muiden vähemmän yksilön oikeuksiin ja vapauksiin vaikuttavien tapojen käyttömahdollisuudet. Biometrisen tunnistamisen käyttöä ei tule pitää ensisijaisena vaihtoehtona. Huomioitava myös on, että biometrinen tunniste voidaan erityislainsäädännön puuttuessa ottaa käyttöön vain käyttäjien suostumuksella.

Biometrisia tunnisteita saa käyttää vain, jos se on asianmukaista, olennaista eikä liian laajaa. Tämä asettaa rekisterinpitäjälle velvollisuuden arvioida tarkkaan käsiteltävien tietojen tarpeellisuutta ja suhteellisuutta. Mitä arkaluonteisemmasta tiedosta on kysymys, sitä tarpeellisempia näiden tietojen tulee olla käsittelyn tarkoituksen kannalta. Biometristen tietojen kokoamista tulee välttää, jos käytettävissä on muita menetelmiä. Kysymys on ennen kaikkea vähimmän sallitun puuttumisen periaatteesta henkilötietojen käsittelyyn sovellettuna.[592]

Tietosuojavaltuutettu on ottanut biometristen tunnisteiden tarpeellisuuteen kantaa henkilötietojen käsittelyä opiskelijoiden läsnä-

591 Näin myös *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 60.

592 Näin myös *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 357.

olon kirjaamista koskeneessa ratkaisussaan (Dnro 236/41/2006). Ratkaisussa tietosuojavaltuutettu katsoi, että biometrinen tunniste ei ollut tarpeellinen tieto opiskelijoiden poissaolojen seurannassa. Tietosuojavaltuutettu ei pitänyt myöskään tällaista tunnistusta hyvänä vaihtoehtona biometrisen tunnisteen luonne huomioon ottaen.[593]

Tarpeellisuusvaatimukseen liittyy myös aiemmin esillä ollut EIT:n ratkaisu M.K. vastaan Ranska (no.19522/09, 18.4.2013), jossa EIT totesi sormenjälkien tarpeettoman säilyttämisen olevan yksityisyyttä loukkaavaa ja haittaa henkilön mahdollisuutta päättää toiminnastaan. Ratkaisu osoittaa sen, että osana tarpeellisuusvaatimusta rekisterinpitäjällä on velvollisuus hävittää tarpeettomaksi käynyt henkilörekisteri. Vain siinä tapauksessa, että siihen talletetut tiedot on erikseen säädetty tai määrätty säilytettäväksi tai että rekisteri siirretään arkistoon, voidaan hävittämisvelvollisuudesta poiketa. Tarpeellisuusvaatimus on näin voimassa koko henkilötietojen elinkaaren ajan.

Tarpeellisuusvaatimus asettaa rekisterinpitäjälle velvollisuuden säännölliseen henkilötietojen käsittelyn arviointiin. Tarpeellisuusvaatimuksen mukaan tietojen tarpeellisuutta täytyy arvioida rekisterinpitäjän sen hetkisen tarpeen mukaan. Mahdollisia tulevia tarpeita ei tule arvioinnissa ottaa huomioon, sillä henkilörekisterien säilyttäminen

593 Vertaa Kammarrätt i Stockholm, joka vuonna 2006 antamassaan ratkaisussa katsoi lukiolla olevan oikeus käyttää sormenjälkeen perustuvaa tunnistusta kouluruokailun valvonnassa (Kammarrättens i Stockholm dom 2005-11-01 i mål nr 1982-05). Regeringsrätten vahvisti tuomion joulukuussa 2008. Ruotsin tietosuojaviranomainen (Datainspektion) on ottanut päivastaisen kannan. Näinkin myönteistä kantaa biometristen tunnisteiden käyttöön ja intressivertailu oppilaitoksen rutiinien hyväksi ovat paljossa vakiintuneiden tietosuojaperiaatteiden vastaisia.

vain varmuuden vuoksi ei ole hyvän tietojenkäsittelytavan mukaista. [594]

Jos henkilötiedot muutetaan sellaiseen muotoon, ettei niistä voida tunnistaa yksityistä henkilöä, tiedot eivät ole enää henkilötietolain sääntelyn piirissä. Tällaiset anonyymit tiedot voidaan arkistoida tai niiden hyödyntämistä on mahdollista jatkaa. Tällainen tietojen anonymisointi on tehtävä niin, että henkilö ei ole tunnistettavissa edes muita tietoja yhdistelemällä.[595]

Biometristen tunnisteiden kohdalla rekisterinpitäjälle säädetty velvollisuus hävittää tarpeettomaksi käynyt henkilörekisteri toteuttaa yksilön oikeutta yksityisyyteen henkilötietojen käsittelyssä. Tarpeettomaksi käynyt biometrisia tunnisteita sisältävä henkilörekisteri tulee hävittää, jotta yksilön biometriset tunnisteet eivät joudu niihin valtuuttamattomien käsiin. Tällä olisi suuri vaikutus yksilön perusoikeuksiin ja –vapauksiin. Koska biometriset tunnisteet ovat luonteensa vuoksi erityinen henkilötietojen ryhmä, tulee niiden hävittämisessä noudattaa erityistä huolellisuutta.

Suunnitelmallisuus. Suunnitelmallisuus on keskeinen perusvaatimus henkilötietojen sallitussa käsittelyssä. Henkilötietojen käsittelyn tulee olla perusteltua ja tiettyä käyttötarkoitusta varten rajattua. Tällaista henkilötietojen käsittely voi olla vain suunnitelmallisena. Kysymys on myös menettelyn avoimuudesta.

Suunnitelmallisuus ulottuu tiedon koko elinkaareen sillä, suunnitelmallisuuden vaatimus edellyttää sellaista ennen sallitun käsittelyn aloittamista tapahtuvaa suunnittelua, missä huomioidaan tietojen hankintatavat, erilaiset käsittelytavat, käyttötarkoitukset, mahdolliset luo-

---

594 Näin myös *Vanto,* Henkilötietolaki käytännössä, s. 155. Katso myös Voutilainen, jonka mukaan tietojen säilyttäminen ja hävittäminen on suunniteltava jo rekisteriä perustettaessa. Voutilainen, Oikeus tietoon, s. 321.

595 *Pitkänen – Tiilikka – Warma,* Henkilötietojen suoja, s. 231.

vutukset sekä säilyttäminen, arkistointi ja tuhoaminen.[596] Keskeistä roolia suunnitelmallisuuden toteuttamisessa ja sen muille osoittamisessa näyttelee rekisteriseloste, jonka jokaisen rekisterinpitäjän tulee laatia. Rekisteriselosteessa tulee kuvata muun muassa rekisterin sisältö, tietolähteet, tietojen käyttötarkoitus sekä tietojen käsittely- ja luovutustavat.

Suunnitelmallisuus pitää sisällään kaksi erillistä vaatimusta. Ensinnäkin henkilötietojen käsittelyn tulee olla asianmukaista. Toiseksi suunnitelmallisuuden osana on tietojen käsittelyn tarkoitusten sekä hankinta- ja luovutuskohteiden määrittely ennen käsittelyn aloittamista.

Asianmukaisuudessa oleellista on se, että rekisterinpitäjä kykenee osoittamaan, miksi henkilötietojen käsittely on rekisterinpitäjän toiminnassa tarpeellista ja asiallista. Asiallisuus arvioidaan tapauskohtaisesti ja asianmukaisuutta arvioitaessa huomioon otetaan se, millaisiin rekisterinpitäjän tehtäviin henkilötietoja aiotaan käsitellä ja onko käsittely yleisesti hyväksyttävää. Tärkeä osa asianmukaisuutta on myös henkilötietojen käsittelyn avoimuuden vaatimus. Henkilötietojen käsittely ei ole avointa, jos yleisöllä ei ole oikeutta saada tietoja rekisterinpidosta. Tärkeä osa avoimuutta on myös rekisteröidyn oikeus saada ennakolta tieto siitä, mihin hänen tietojaan aiotaan käyttää.[597]

Esimerkiksi sormenjälkitunnistuksen käyttö kuntosalin sisäänkirjautumisessa väärinkäytön ehkäisemisessä ei täytä asianmukaisuusvaatimusta eikä tarpeellisuusvaatimusta. Tähän tarkoitukseen on käytettävissä vähemmän rekisteröidyn yksityisyyteen puuttuvia keinoja.[598]

---

596 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 357.

597 *Wallin,* Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnustettuina perusoikeuksina s. 378

598 Saman on todennut Norjan tietosuojaviranomainen (PVN) ratkaisuissaan PVN-2006-09 ja PVN-2006-08.

Hyvää tietojenkäsittelytapaa noudattaen biometristen tunnisteiden käyttö tällaisessa tilanteessa ei ole perusteltua.

Henkilötietojen käsittelyn perusteluvaatimus tarkoittaa sitä, että rekisterinpitäjän rekisterinpitoon on löydyttävä asianmukaiset perusteet ja toiminnan on muutoinkin oltava asiallista.[599] Kysymys on toisin sanoen hyvän tietojenkäsittelyn yhdestä osasta. Henkilötietojen määrittelemätön käsittely ei ole hyvän tietojenkäsittelytavan mukaista.

Käyttötarkoituksen määrittely puolestaan asettaa rekisterinpitäjälle velvollisuuden arvioida toimintaansa kokonaisvaltaisesti. Arvioinnissa tulee ottaa huomioon rekisterinpitäjän toiminnan kaikki osa-alueet sekä henkilötietojen käsittelyn tarve ja käyttötarkoitukset näillä osa-alueilla.[600]

Henkilötietojen käsittely pelkästään helppouden ja tehokkuuden nimissä ei täytä asianmukaisuuden vaatimusta. Nykyajan informaatioyhteiskunnassa teknologisen imperatiivin ajatuksen mukaisesti sekä hallinnon eri sektoreilla että myös yksityissektorilla erilaiset biologisen tunnistamisen toteutustavat kuuluvat usein välineisiin, joiden avulla tavoitellaan varmuutta, tehokkuutta ja hallintotaakkojen vähentämistä eri toiminnoissa.

Yksilön oikeuksin näkökulmasta varsin vaarallisen esimerkin biometrisen tunnistamisen käytöstä löytyy säteilylain muuttamista koskeneesta hallituksen esityksestä. Siinä ehdotettiin biometrisen tunnistamisen käyttöä itsepalvelusolariumin ikärajan valvomiseksi. [601] Nykytiedon mukaan biometrisesta tunnisteesta, kuten sormenjäljestä,

---

599 *Voutilainen,* Oikeus tietoon, s. 303. Henkilörekisterilain mukaan henkilörekisterin käyttötarkoitus oli määriteltävä ennen rekisteriin talletettaviksi aiottujen henkilötietojen keräämistä (HenkRekL 4 §). Säännös ilmensi myös periaatetta, jonka mukaan rekisteritoiminnan tulee perustua suunnitelmallisuuteen. HE 49/1986 vp, s. 27.

600 *Vanto,* Henkilötietolaki käytännössä, s.41.

601 HE 146/2011 vp, s. 6

ei ole mahdollista päätellä mitään yksilön iästä. Biometrisen tunnistamisen käyttäminen tällaiseen tarkoitukseen ei täytä henkilötietolain asianmukaisuus- eikä tarpeellisuusvaatimusta.

Lainsäädännön näkökulmasta arvioiden ei tällaisessa yhteydessä tule luoda erityislainsäädäntöä suhteessa henkilötietolakiin biometristen tunnisteiden osalta. Tunnistamista ja kulunvalvontaa koskevan lainsäädännön tulee olla myös teknologianeutraalia, eikä niitä tulee sitoa tiettyyn tekniseen ratkaisuun.

Käyttötarkoitussidonnaisuus. Käyttötarkoitussidonnaisuuden periaate on yksi tietosuojalainsäädännön varhaisimpia ja tärkeimpiä perusajatuksia.[602] Lainsäädännöllä pyritään vain ennalta määriteltyyn tarkoitukseen tapahtuvaan henkilötietojen käsittelyyn. Henkilötietojen käsittelyoikeus on vain tiettyjä osoitettuja tarkoituksia varten.

Jos rekisteröidyillä on oikeuksia tai velvollisuuksia suhteessa tietojen käsittelijään, yksityisyyden suojan riskiä voidaan pitää suhteellisen pienenä, kun tiedot rajataan vain tuossa käyttötilanteessa tarpeellisiin. Tällaisen yhteyden puuttuessa lainsäätäjän on määriteltävä tietojen käytön rajat (muun muassa mitä tietoja saa käsitellä, minne tietoja saa luovuttaa ja kuinka kauan tietoja saa säilyttää).

Käyttötarkoitussidonnaisuuden periaate vaikuttaa lähtökohtaisesti kaikissa eri tilanteissa. Se ilmenee erilaisten rekistereiden perustamisen yhteydessä, rajoittaa ja ohjaa henkilötietojen tavanomaista käsittelyä ja rajoittaa henkilötietojen vapaata luovuttamista.[603] Lisäksi periaate rajaa myös henkilötietojen käsittelyyn organisaatiossa oikeutettujen henkilöiden joukkoa.

---

602 *Bygrave,* Data Privacy Law. An International Perspective, s. 153.

603 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 358. Katso myös *Wallin,* Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnustettuina perusoikeuksina

Henkilötietojen suoja tietojenkäsittelyssä on voimakkaasti käyttöyhteyssidonnaista. Tämän vuoksi henkilötietolaissa on säädetty, että henkilötietojen käsittelyn on tapahduttava siihen käyttötarkoitukseen, johon henkilötiedot on kerättykin.[604] Henkilötietoja saa käyttää tai muutoin käsitellä vain tavalla, joka ei ole yhteensopimaton ennen henkilötietojen käsittelyä määriteltyjen käyttötarkoitusten kanssa.

Tietojen alkuperäinen käyttötarkoitus sitoo merkittävällä tavalla henkilötietojen ja rekistereiden myöhempää käyttöä. Henkilötietojen käsittelyn tarkoitus sekä säännönmukaiset tietojensiirrot on kuitenkin mahdollista määritellä myöhemmin uudelleen, jos se on muuttuneiden olosuhteiden vuoksi tarpeen. Näin määritelty tarkoitus ei kuitenkaan saa olla yhteensopimaton henkilötietojen alkuperäisen käsittelyn tarkoituksen kanssa.[605]

Henkilörekisterin käyttötarkoitukseen on siis mahdollista tehdä pieniä muutoksia, jotka eivät ole ristiriidassa käsittelyn alkuperäisen tarkoituksen kanssa. Muutosten vaikutusten arvioinnin tulee tapahtua rekisteröidyn näkökulmasta eli muutoksesta tulee ilmoittaa rekisteröidylle. Tällöin rekisteröity voi itse arvioida sen, haluaako hän enää sallia tietojensa käsittelyä tähän muuttuneeseen tarkoitukseen. Yksilöllä on itsemääräämisoikeutensa puitteissa oltava oikeus vastustaa tietojensa käsittelyä, mikäli rekisterin käyttötarkoitus muuttuu.

---

604 Suoramarkkinointia koskevassa tietosuojavaltuutetun ohjeistuksessa on kuluttajien profiloinnin kohdalla todettu, että henkilörekisterin tietoja ei tule käsitellä niille ennalta määritellyn käyttötarkoituksen vastaisesti, ja tätä periaatetta on noudatettava myös profiloinnissa. Jos esimerkiksi yrityksen asiakasrekisterin käyttötarkoitukseksi on määritelty asiakassuhteen hoitaminen ja kehittäminen, profilointia ei voi suorittaa tämän käyttötarkoituksen vastaisesti. Tietosuojavaltuutetun toimisto, Tietosuoja suoramarkkinoinnissa, s. 11.

605 HE 96/1998 vp, s. 38 ja *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 358.

Käyttötarkoitussidonnaisuuden periaate on näin kiinteässä yhteydessä tarpeellisuusvaatimukseen. Käyttötarkoitussidonnaisuuden periaate ja tarpeellisuusvaatimus muodostavat parin. Käyttötarkoitussidonnaisuus sitoo tietojen käsittelyn tiettyyn ennalta määriteltyyn tarkoitukseen. Tarpeellisuusvaatimus rajaa tietojen käsittelyä tarpeelliseen ja käyttötarkoituksen mukaiseen tietojen käsittelyyn.

Myös suunnitelmallisuuden periaate on läheisessä yhteydessä käyttötarkoitussidonnaisuuden kanssa. Käyttötarkoitussidonnaisuuden pohjana on määrittelyvelvollisuus, joka luo henkilörekisterin käyttämisen lähtökohdan.[606] Tiedollisen itsemääräämisoikeuden ja informointivelvollisuuden lisäksi käyttötarkoitussidonnaisuuden periaate on olennainen osa sitä, että henkilö tietää suostumusta antaessaan, mihin henkilötietoja tullaan käyttämään ja luovuttamaan.[607]

Käyttötarkoitussidonnaisuuden ja myös tarpeellisuusvaatimuksen keskeinen kysymys viime vuosina on ollut passia varten otetut sormenjäljet. Syynä biometristen tunnisteiden passiin ottamiselle on perusteltu lentomatkustamisen turvallisuudella, mutta näitä tietoja on pyritty käyttämään myös muissa tarkoituksissa, erityisesti rikostutkinnassa. Perustuslakivaliokunta ei pitänyt sormenjälkien keräämistä täysin tarpeellisena, koska hallituksen esityksen mukaan siihen sisältyi huomattavia riskejä. Erityisesti perustuslakivaliokunta vastusti sormenjälkien

606 Bygrave katsoo käyttötarkoitussidonnaisuuden koostuvan kolmesta kokonaisuudesta tai periaatteesta: 1) henkilötietojen keräämisen käyttötarkoitus tulee määritellä, 2) käyttötarkoitusten tulee olla lainmukaisia ja 3) henkilötietojen käsittely ei saa olla ristiriidassa määritellyn käyttötarkoituksen kanssa. *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 61. Katso myös *Bygrave,* Data Privacy Law. An International Perspective, s. 155.

607 *Neuvonen,* Yksityisyyden suoja Suomessa, s. 63.

käyttöä muuhun tarkoitukseen kuin passien varmistamiseen.[608] Näin ollen passirekisterin sormenjälkitietoja ei ole mahdollista käyttää rikostutkinnassa.[609]

Huolellisuusvelvollisuus. Henkilötiedoilla on suurta merkitystä yksittäisen kansalaisen yksityisyyteen ja myös jokapäiväiseen elämään, minkä vuoksi henkilötietojen käsittelyssä on noudatettava erityistä huolellisuutta. Tämän vuoksi henkilötietolain 5 §:ssä rekisterinpitäjälle asetetaan huolellisuusvelvoite.

Huolellisuusvelvoitteen mukaan rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta. Huolellisuusvelvoite koskee myös rekisterinpitäjän lukuun toimivia. Huolellisuuteen kuuluu siis ennen kaikkea oman toiminnan kannalta henkilötietojen käsittelyä koskevan lainsäädännön riittävä tunteminen ja noudattaminen.[610]

Henkilötietolain mukainen huolellisuusvelvollisuus on kuitenkin jotain enemmän kuin tavanomainen huolellisuusvelvollisuus. Se liittyy hyvään tietojenkäsittelytapaan ja velvoittaa toimimaan huolellisesti

608 PeVL 14/2009 vp. sekä HE 234/2008 vp. s. 63. Pohjana perustuslakivaliokunnan ratkaisussa on ollut EIT:n päätös tapauksessa S. ja Marper vastaan Yhdistynyt kuningaskunta. Katso myös HaVM 9/2009 vp. Heikki Karapuu on vuonna 1972 esittänyt näkemyksen siitä, että perusoikeussäännöksellä voidaan kieltää kansalaisten kortistointi sillä perusteella, että he uskaltautuvat käyttämään hallitusmuodon (nyk. perustuslain) heille takaamia perusoikeuksia. *Karapuu,* Oikeus yksityiselämän suojaan, s. 22.

609 Samaan johtopäätökseen päädyttiin myös Sisäministeriön selvityksessä passin sormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa. Sisäministeriön julkaisuja 20/2014.

610 *Pitkänen – Tiilikka – Warma,* Henkilötietojen suoja, s. 72.

yksityisyyttä ja muita perusoikeuksia kunnioittavalla tavalla. Huolellisuusvelvoitteessa on tietyllä tavalla kysymys tietojen käsittelyn sosiaalisesta hyväksyttävyydestä. Henkilötietojen käsittelyn ei tule olla vastoin yleisiä sosiaalisia normeja.[611]

Huolellisuusvelvoite tarkoittaa käytännössä sitä, että henkilötietojen käsittelyssä ja rekisterinpitoa suunniteltaessa rekisterinpitäjän tulee valita tietojenkäsittelyn vaihtoehdoista se, joka vähiten rajaa rekisteröidyn oikeuksia yksityisyyden suojaan. Tällainen ajatus kuvaa osuvasti vähimmän puuttumisen periaatetta henkilötietojen käsittelyssä. Tarkoituksena on suojata rekisteröityä liialliselta henkilötietojen keräämiseltä ja näin yksilön oikeutta yksityisyyteen. Pohdittaessa esimerkiksi tarpeellisten tietojen määrää huolellisuusvelvoite yhdessä vähimmän puuttumisen periaatteen kanssa ohjaavat ensisijaisesti minimoimaan käsiteltävien tietojen määrän rekisteröitävien yksityisyyden ja muiden perusoikeuksien suojaamiseksi. Huolellisuusvelvoitetta voidaankin pitää eräänlaisena optimointikäskynä, sillä henkilötietoja on käsiteltävä niin, että huolellinen henkilötietojen käsittelijä varoo avoimissa tulkintatilanteissa toimimasta yksityisyyttä loukkaavalla tavalla.[612] Huolellisuusvelvoitetta korostaa omalta osaltaan henkilötietolain 9.2 §:ssä säädetty virheettömyysvaatimus.

---

611 *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 61. Myös henkilörekisterilakiin sisältyi rekisterinpitäjän huolellisuusvelvoite (HenkRekL 3 §). Huolellisuusvelvoite tuli huomioida kaikessa henkilörekisterilain alaan kuuluvassa toiminnassa. Sillä oli yleistä rekisterinpitoa ohjaava ja muotoileva tehtävä. *Konstari,* Henkilörekisterilaki (1992), s. 88–89.

612 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 359. Voutilaisen mukaan lainsäädäntö lähtee siitä oletuksesta, että muun kuin rekisteröidyn itsensä tekemä henkilötietojen käsittely on yksilön yksityisyyden suojaan puuttumista *Voutilainen,* Oikeus tietoon, s. 301.

Huolellisuusvelvollisuuteen sisältyvä intressivertailu rekistrinpitäjän tarpeiden ja rekisteröidyn oikeuksien kanssa käy ilmi esimerkiksi Ruotsin tietosuojaviranomaisen vuonna 2006 antamasta ratkaisusta, jossa oli kysymys sormenjäljen käyttämisestä lennon lähtöselvityksessä. Ratkaisussaan viranomainen antoi lentoyhtiölle luvan sormenjälkeen perustuvalle matkustajan tunnistamiselle, koska lentoyhtiöllä oli perustltu tarve menetelmälle. Ratkaisuun vaikutti suuresti se, että sormenjälkitunnistuksen ohella käytössä oli vähemmän rekisteröidyn yksityisyyteen puuttuva keino.[613] Intressivertailussa päädyttiin siis rekisteröidyn kannalle, sillä sormenjälkitunnistamisen käytön katsottiin olevan mahdollinen vain käyttäjän suostumuksella.

Tietoturvallisuus. Henkilötietojen suojan oleellinen osa on henkilötietojen turvallinen käsittely.[614] Sen ohella, että tietoturvallisuus on yksi tietoturvalainsäädännön yleisperiaatteista, sen merkitys tulee erityisesti esille rekisterinpitäjän toiminnassa.

Henkilötietolain 32 §:n mukaan rekisterinpitäjä on velvollinen huolehtimaan henkilötietojen suojasta tarpeellisilla tietoturvatoimenpiteillä. Lainkohdan mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

---

613 Datainspektionen, Samråd enligt personuppgiftslagen (1998:204, dnr. 84-2006). Katso myös Tanskan tietosuojaviranomaisen (Datatilsynet) ratkaisu 2006-219-0370.

614 Lessigin mukaan henkilötietojen käsittelyyn vaikuttaa neljä eri mekanismia: 1) lainsäädäntö (law), 2) sosiaaliset normit (norms), 3) markkinavoimat (market)ja 4) teknologia (architecture). *Lessig,* Code and other laws of cyberspace, s. 85–99. Tietosuojaa ja tietoturvaa koskeva lainsäädäntö on näin ollen vain yksi väline henkilötietojen suojaamisessa.

Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.[615]

Henkilötietodirektiivi (17 artikla 1 kohta) sisältää henkilötietojen käsittelyyn kohdistuviin riskeihin liittyvän arviointikriteerin. Tämä ei käy ilmi henkilötietolaista, mutta se on syytä ottaa huomioon suojaustoimien vaatimustasoa arvioitaessa. Suojaamistoimenpiteitä ja niistä aiheutuvia kustannuksia on arvioitava suhteessa niillä saavutettuun suojaustasoon ja suhteessa henkilötietojen käsittelyyn organisaation sisältä ja ulkoa käsin kohdistuviin riskeihin. Tämä edellyttää, että riskit on pyrittävä tunnistamaan, arvioimaan ja hallitsemaan. Arvioimalla henkilötietoihin kohdistuvat uhat ja niiden toteutumisen riskit pystytään parhaiten suunnittelemaan ja toteuttamaan asianmukaiset turvatoimet.[616]

Edellä mainitun henkilötietodirektiivistä ilmenevän suhteellisuusperiaatteen mukaan toimittaessa rekisterinpitäjän tietoturvaratkaisut on yksilöidysti perusteltava. Tällöin tietoturvallisuus on nähtävä kokonaisuutena, joka ulottuu järjestelmäsuunnittelusta yksittäisten tietovälineiden käyttöön.[617] Tämä osoittaa sen, että tietoturvatoimenpiteillä

615 Direktiivi 95/46/EY, johdanto-osan kohta 46 ja 17 artikla sekä *Pitkänen – Tiilikka – Warma,* Henkilötietojen suoja, s. 222. Näin myös *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 68. Katso myös *Vanto,* joka on lähestynyt tietoturvatoimenpiteitä jakamalla tietoturvatoimenpiteet seitsemään osaan: 1) Tietoturvatoimintaperiaatteet, 2) Organisatoriset toimenpiteet, 3)Fyysinen tietoturva, 4) Verkkoturvallisuus, 5) Työntekijät, 6) Ajoittainen päivitys ja 7) Toimeenpano. *Vanto,* Henkilötietolaki käytännössä, s. 138–139.

616 Näin myös *Raatikainen,* Yksityisyyden suoja työelämässä, s. 349.

617 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 360.

voidaan pyrkiä suojaamaan sekä tietojen luottamuksellisuutta että yleisemminkin kansalaisten yksityisyyden suojaa.

Henkilötietolaissa säädettyyn suojaamisvelvollisuuteen sisältyy vaatimus valvoa henkilörekisteriin pääsyä. Pääsynvalvontaan sisältyy olennaisena osana kunkin käyttäjän tunnistaminen ennen tietojärjestelmään pääsyä. Tässä olennaisena osana puolestaan on kunkin käyttäjän tunnistaminen ennen tietojärjestelmään pääsyä sekä pääsynvalvonnan ajantasaisuudesta huolehtiminen.

Henkilötietodirektiivin ja -lain tietoturvasäännös jättää avoimeksi sen, minkälaisiin konkreettisiin toimenpiteisiin rekisterinpitäjän on ryhdyttävä. Tällainen neutraali ja abstrakti säätämistapa antaa mahdollisuuden uusille tulkinnoille yhteiskunnan ja teknologian kehittyessä. Toimenpiteitä pohdittaessa merkitystä tulee antaa ennen kaikkea tietojen laadulle. Esimerkiksi biometriset tunnisteet erityisenä henkilötietojen ryhmänä nostavat vaadittavaa tietoturvan tasoa.

Biometrisia tunnisteita käsiteltäessä turvatoimien tehokkuuteen tulee kiinnittää erityistä huomiota, etenkin silloin, jos tietoja siirretään internetin välityksellä. Turvatoimet tulee ottaa käyttöön prosessin alusta alkaen. Erityisen tärkeä vaihe on tietojen rekisteröintivaihe.[618]

Turvatoimia suunnitellessaan rekisterinpitäjän tulee olla selvillä siitä, että tietokantojen loukkaamattomuuteen, luottamuksellisuuteen ja käyttöoikeuksiin liittyvien ominaisuuksien mahdollinen menetys estää kyseiseen tietokantaan perustuvien kaikkien sovellusten myöhemmän käytön ja aiheuttaa rekisteröidylle peruuttamatonta vahinkoa. Esimerkkinä voidaan mainita tilanne, jossa valtuutetun henkilön sormenjäljet liitetään valtuuttamattoman henkilön henkilöllisyyteen. Tällöin valtuuttamaton henkilö saisi oikeudettomasti käyttöönsä sormenjälki-

618 Esimerkiksi henkilötietojen käsittelystä poliisitoimessa annettuun lakiin on otettu erilliset säädökset koskien henkilön fyysisiin ominaisuuksiin perustuvien tunnistetietojen tietoturvasta (10a §).

en omistajalle kuuluvat palvelut. Tällainen tilanne johtaisi henkilöllisyyden varastamiseen, mikä tekee uhrin sormenjäljistä käyttökelvottomat tulevia sovelluksia varten ja näin rajoittaa yksilön vapautta.

Laatuperiaate. Laatuperiaate liittyy henkilötietojen käsittelyyn kolmella tavalla. Periaate ilmenee ensinnäkin lakisääteisyyden vaatimuksena siten, että käsiteltävän informaation laadusta on säädettävä laissa eikä sitä siten ole lupa jättää vain byrokraattisten käytäntöjen tai alemman asteisen ohjeistuksen varaan. Toiseksi laatuperiaate merkitsee vaatimusta informaation tilannekohtaisesta oikeellisuudesta huolehtimisesta, mihin rekisterinpitäjällä on velvollisuus sekä oma-aloitteisesti että rekisteröidyn vaatimuksesta. Laatuperiaatteen kolmantena osana voidaan nähdä myös käsiteltävien tietojen tarpeellisuuden vaatimus.

Henkilötietolakiin sisältyy erityinen laatuperiaatetta kuvaava säännös (HetiL 9§). Säännöksen mukaan rekisterinpitäjän on huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä. HetiL 9 §:stä ja lainkohdan perusteluista ei kuitenkaan käy ilmi, milloin tieto on virheellinen. Luulot, olettamukset, uskomukset ja todennäköisyydet eivät ainakaan täytä virheettömälle tiedolle asetettavia kohtuullisiakaan vaatimuksia.[619] Ytimekkäästi asia voidaan ilmaista seuraavasti: henkilötieto on virheellinen, jos se ei anna oikeaa informaatiota seikasta, jota sillä on haluttu kuvata tai jos sen käyttämistä ei kyseisessä tilanteessa voi pitää asianmukaisena.[620]

Henkilötieto on puolestaan epätäydellinen sen ollessa osin puutteellinen. Tällaiset tiedot voivat johtaa toiseen tulokseen kuin jos käytettävissä olisivat täydelliset tiedot. Tiedon puutteellisuudella voi olla rekisteröidylle yhtä haitallisia seurauksia kuin tiedon virheellisyydelläkin. Henkilötietojen automaattiseen käsittelyyn ja erilaisten tunnistus-

619 *Raatikainen,* Yksityisyyden suoja työelämässä, s. 138.

620 *Wallin–Nurmi,* Tietosuojalainsäädäntö – henkilörekisterilaki ja siihen liittyvät säädökset, s. 95.

välineiden käyttöön liittyy vaara epätäydellisten tietojen käyttämisestä päätöksenteossa.[621]

HetiL:ssa ei ole säädetty erityistä aikarajaa sille, milloin jokin henkilötieto on vanhentunut. Tiedon vanhentumisaika riippuu henkilötietojen käsittelylle määritellystä tarkoituksesta. Selvästi vanhentuneeksi tiedoksi voidaan katsoa henkilötieto, joka ei ole enää olemassa. Yleisesti ottaen tieto on vanhentunut, kun se on käynyt merkityksettömäksi käsittelyn tarkoituksen kannalta.

Kuten edellä esitetystä käy ilmi, laatuperiaate asettaa velvollisuuden informaation tilannekohtaisesta oikeellisuudesta huolehtimiseen. Käsiteltävien tietojen tulee olla niiden käyttötarpeen ja käyttötilanteiden näkökulmasta arvioituna tarpeellisia ja virheettömiä.[622]

Virheettömyysvaatimuksen tarkoituksena on, että yksilöitä arvioidaan oikeiden tietojen valossa. Tämä tarkoittaa sitä, että erityisesti tietojen, joilla on välitön ja merkittävä vaikutus rekisteröityyn ja tämän oikeuksiin, on oltava virheettömiä.[623] Tällaisia tietoja on käsiteltävä siten, että rekisteröityä koskevat tiedot tallennetaan rekistereihin huolellisesti ja asiallisesti oikeina.

Virheettömyysvaatimusta arvioitaessa on otettava huomioon sekä henkilötietojen käsittelyn tarkoitus että käsittelyn merkitys rekisteröidyn yksityisyyden suojalle. Rekisterinpitäjän on noudatettava erityistä huolellisuutta sellaisten tietojen kohdalla, joita käytetään yksityistä henkilöä koskevaan päätöksentekoon.[624]

Biometristen tunnisteiden käsittelyssä virheettömyysvaatimus tarkoittaa sitä, että kerättävien tietojen on oltava ajan tasalla. Velvollisuus

621 *Raatikainen,* Yksityisyyden suoja työelämässä, s. 141.

622 Raatikainen on sanonut tämän siten, että mahdollista virheellisyyttä tulee verrata henkilötietojen käsittelylle määriteltyyn tarkoitukseen. *Raatikainen,* Yksityisyyden suoja työelämässä, s. 138.

623 HE 96/1998 vp, s. 42.

624 *Pitkänen – Tiilikka – Warma,* Henkilötietojen suoja, s. 105.

saa biometristen tunnisteiden kohdalla korostuneen merkityksen niiden luonteen vuoksi. Biometrisilla tunnisteilla on suuri merkitys yksilön yksityisyyden suojalle. Tämä tarkoittaa sitä, että niillä on myös suuri vaikutus rekisteröityyn ja tämän oikeuksiin. Lisäksi biometrisiin järjestelmiin liittyvillä virheillä voi olla vakavia seurauksia yksilölle.

Valtuutettujen henkilöiden oikeudeton torjuminen ja valtuuttamattomien henkilöiden oikeudeton hyväksyminen voi erityisesti aiheuttaa vakavia ongelmia. Biometristen tietojen käytön tulee ennen kaikkea vähentää tällaisten virheiden riskiä. Ne voivat kuitenkin myös luoda illuusion, että rekisteröidyn tunnistaminen tai todentaminen / varmentaminen tapahtuu aina oikein. Rekisteröidyn voi olla vaikea tai jopa mahdoton todistaa päinvastaista. Järjestelmä voi esimerkiksi virheellisten tietojen perusteella tunnistaa rekisteröidyn henkilöksi, jolle ei tulisi sallia lentokoneessa matkustamista tai jolta tulisi kieltää pääsy tiettyyn maahan. Tällaisten ongelmien ratkaiseminen on vaikeaa henkilölle, jota vastaan on olemassa tällaisia "kiistattomia" todisteita. Tällaisten tilanteiden välttämiseksi biometristen tunnisteiden kohdalla tietojen oikeellisuuteen ja ajantasaisuuteen tulee kiinnittää normaalia enemmän huomiota.

Tiedottamisvelvollisuus. Demokraattiseen oikeusvaltioon kuuluu johtavana oikeusperiaatteena avoimuus. Avoimuus on huomioitu myös rekisterinpidossa, sillä henkilötietolaki velvoittaa rekisterinpitäjän ilmoittamaan rekisteröidylle, kun tietoja kerätään ja tallennetaan ensimmäistä kertaa henkilörekisteriin. Salainen henkilötietojen kerääminen rekisteriin ei täytä henkilötietolaissa asetettua asianmukaisuusvaatimusta. Sitä ei voida pitää laillisena eikä se ole myöskään hyvän tietojenkäsittelytavan mukaista. Henkilötietojen käsittelyn lähtökohtaisena pääsääntönä on tämän vuoksi rekisterinpitäjien *informointi- tai tiedottamisvelvollisuus (HetiL 24 §)*.

Tiedottamisvelvollisuus on erittäin laaja. Se koskee kaikkea lain soveltamisalaan kuuluvaa henkilötietojen käsittelyä. Kerättiinpä hen-

kilötietoja millä tavalla tai keneltä tahansa, on tiedottamisesta huolehdittava. Myöskään sillä, mihin tarkoitukseen henkilötietoja kerätään, ei lähtökohtaisesti ole merkitystä.

Rekisteröidylle annettavaan informaatioon sisältyvät tieto siitä, mihin rekisteröidyn yhteystietoja tai muita henkilötietoja luovutetaan sekä tiedot siitä, jos rekisteröidyn henkilötietoja tullaan päivittämään toisen rekisterinpitäjän henkilörekisteristä. Tämän lisäksi tiedottamisvelvollisuuden piiriin kuuluu kaikki tilanteet, joissa henkilötietoja kerätään esimerkiksi jonkin valvonta-, tarkkailu- tai seurantamenetelmän tai –välineen kautta.[625]

Käytännössä rekisterinpitäjä toteuttaa velvoitteen laatimalla rekisteriselosteen. Rekisteriseloste sisältää samoja tietoja, joista rekisterinpitäjä on velvollinen informoimaan rekisteröityä. Selostetta voidaan hyödyntää linkittämällä se verkkopalvelun yhteyteen, jossa henkilötietoja kerätään, pitämällä se saatavilla toimipaikassa tai muutoin toimittaa se rekisteröityjen käyttöön.[626] Omalta osaltaan tätä velvollisuutta tukee myös rekisteröidylle kuuluva omien tietojen tarkastusoikeus.[627]

Rekisterinpitäjälle säädettyyn ilmoittamisvelvollisuuteen kuuluu, että rekisterinpitäjä huolehtii henkilötietoja kerätessään siitä, että

---

625 *Raatikainen,* Yksityisyyden suoja työelämässä, s. 240.

626 Tietosuojavaltuutetun toimisto, Rekisterinpitäjän yleinen informointivelvollisuus, s. 3 ja *Raatikainen,* Yksityisyyden suoja työelämässä, s. 241.

627 Bygrave käyttää tästä kolmen periaatteen kokonaisuudesta nimitystä rekisteröidyn osallistumisen ja hallinnan periaate (data subject participation and control). Bygrave jakaa tämän periaatteen kolmeen kokonaisuuteen, jotka siis ovat rekisterinpitäjän velvollisuus informoida rekisteröityä henkilötietojen käsittelystä, ilmoittaa henkilötietojen käsittelystä tietosuojaviranomaiselle ja rekisteröidyn oikeus tarkastaa itseään koskevat tiedot. *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 63–64.

rekisteröity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta sekä henkilötietojen käsittelyn tarkoituksesta. Informoinnissa on ilmettävä ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien toteuttamiseksi asianomaisessa henkilötietojen käsittelyssä. Tämä toteuttaa osaltaan rekisteröidyn tiedollisia oikeuksia, sillä saadun informaation avulla rekisteröidyn on mahdollista arvioida käsittelyn laillisuutta ja asianmukaisuutta. Ilmoittamisvelvollisuuden keskeisenä tavoitteena on myös pitää henkilö ajan tasalla siitä, miten, milloin ja missä hänen henkilötietojaan käsitellään.[628] Ilmoittamisvelvollisuuden sisältö määräytyy viime kädessä tapauskohtaisesti.

Tiedottamisvelvollisuus ei ole kuitenkaan ehdoton. Siitä on mahdollista poiketa joko tietojen laadun vuoksi – esimerkiksi rikosten selvittämiseksi – tai tarkoituksenmukaisuusperustein kerättäessä tietoja muilta kuin rekisteröidyltä. Viimeksi mainitussa tapauksessa kohtuuton vaiva tai haitta antaa oikeuden ilmoittamatta jättämiseen, kun kysymys ei ole rekisteröityä koskevasta päätöksenteosta. Poikkeuksista voidaan säätää myös laissa (HetiL 24.2 §).

Biometristen tunnisteiden kohdalla informointivelvollisuus tarkoittaa sitä, että rekisterinpitäjän tulee informoida rekisteröityä tietojen keräämisestä. Informointiin kuuluu erityisesti tietojen tarkoituksen

628 Saarenpää Henkilö- ja persoonallisuusoikeus (2012), s. 349. Katso myös Pesonen Viestintäoikeuden käsikirja (2011), s. 173 ja 182–183. Ruotsin henkilötietolaki eroaa suomalaisesta laista koskien sääntelyä rekisteröidyn informoinnista tietojenkäsittelystä. Ruotsin henkilötietolaissa informointivelvollisuus on jaettu kahteen osaan: vapaaehtoisesti tapahtuvaan informointiin ja hakemuksesta tapahtuvaan informointiin. Vapaaehtoisesti tapahtuva informointi vastaa Suomen henkilötietolain informointivelvollisuutta, kun hakemuksesta tapahtuva informointi vastaa rekisteröidyn tarkastusoikeutta. Katso tarkemmin SOU 2002:110, s. 69 – 70 sekä *Öman – Lindblom,* Personuppgiftslagen. En kommentar, s. 307–345.

tarkka määrittely ja rekisterinpitäjän henkilöllisyyden ilmoittaminen. Huomiota tulee kiinnittää siihen, että rekisteröidyn tietämättä tietoja keräämiä järjestelmiä vältetään. Rekisteriselosteen laatimiseen tulee biometristen tietojen kohdalla myös kiinnittää erityistä huomiota, sillä rekisteriseloste toimii käytännössä ilmoitusvelvollisuuden julkisena osana.

Ankara vastuu. Huolellisuusvelvoitetta korostetaan vahingonkorvausvelvollisuudella. Rekisterinpitäjä on velvollinen korvaamaan taloudellisen ja muun vahingon, joka aiheutuu henkilötietojen lainvastaisesta käsittelystä.

Henkilötietolaissa säädetty vahingonkorvausvelvollisuus perustuu ankaran vastuun periaatteelle, sillä vahingonkorvausvelvollisuuden syntyminen ei edellytä rekisterinpitäjältä tahallisuutta tai tuottamusta. Jo henkilötietojen lainvastainen käsittely johtaa korvausvelvollisuuteen. Syy ankaralle vastuulle on yksiselitteinen: lainvastainen henkilötietojen käsittely loukkaa yksityisyyttä tai muita perusoikeuksia. Vahingonkorvausoikeudelliselta kannalta katsottuna lainvastainen henkilötietojen käsittely aiheuttaa rekisteröidylle kärsimystä.[629]

Sääntely on selvä osoitus yksilön persoonallisuuden suojan korostetusta merkityksestä yhteiskunnassa. Erityisesti biometristen tietojen kohdalla ankaran vastuun periaate on perusteltu lähtökohta. Näiden tietojen lainvastainen ja varomaton käsittely aiheuttaa vakavaa vaaraa rekisteröidyn oikeuksille. Pahimmassa tapauksessa lainvastainen käsittely estää rekisteröityä identiteettinsä täysimääräiseen (oikeudelliseen) hyödyntämiseen.

629 Katso esimerkiksi KKO: 1998:85, joka koski henkilörekisterilain mukaista samanlaista korvausvelvollisuutta.

5.4.2.3. Yksilön oikeudet

Kolmantena näkökulmana henkilötietojen suojan lainsäädännöllisiin periaatteisiin on yksilön näkökulma. Tietosuojalainsäädäntö palvelee yksilöitä ja heidän perusoikeuksiaan. Henkilötietolaissa yksilön oikeudet on asetettu etusijalle, sillä yksilöllä on oikeus edellyttää laillista, hyvän tietojenkäsittelytavan mukaista henkilötietojen käsittelyä.[630] Biometrisen tunnistamisen näkökulmasta merkitykselliset yksilön oikeudet ovat suostumuksen ensisijaisuus, arkaluonteisten tietojen erityisasema, tarkastus- ja oikaisuoikeus sekä oikeus tietosuojaviranomaisten palveluihin. Kaikki edellä mainitut yleiset ja rekisterinpitäjää koskevat erityiset periaatteet ovat yhtä lailla yksilön oikeuksiin liittyviä. Niitä on tulkittava rekisteröidyn eduksi hyvän tietojenkäsittelytavan puitteissa.

Suostumuksen ensisijaisuus. Keskeisin yksilön oikeuksia ilmaiseva periaate henkilötietojen käsittelyssä on suostumuksen ensisijaisuus. Tietosuojalainsäädäntö rajoittaa informaation vapauden ja sen vapaan kulun periaatteita ensisijaisesti niin, että henkilötietoja on lupa käsitellä vain henkilön itsensä antaman suostumuksen perusteella. Henkilötiedot eivät ole muiden vapaasti käytettävissä olevaa informaatiota, vaan yksilöllä on oikeus omiin tietoihinsa ja oikeus ohjata ja valvoa niiden käsittelyä.[631]

Suostumuksen ensisijaisuus on nimenomaisesti ilmaistu henkilötietolaissa henkilötietojen käsittelyn edellytykseksi. Suostumukseen perustuvassa käsittelyssä toteutuu parhaiten henkilön tiedollinen it-

630 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 364

631 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 364

semääräämisoikeus ja rekisterinpidon avoimuus.[632] Lähtökohtaisesti henkilötietoja saa käsitellä rekisteröidyn antamalla suullisella, kirjallisella tai sähköisessä muodossa olevalla yksiselitteisellä suostumuksella. Biometristen tietojen kohdalla suostumuksella on korostunut merkitys, sillä sen ottaminen edellyttää lähtökohtaisesti puuttumista fyysieen koskemattomuuteen, joka edellyttää joko laissa säädettyä oikeutusta tai yksilön suostumusta.[633]

Suostumuksen tulee olla selkeästi annettu tahdonilmaus ja sen tulee olla nimenomaan suostumuksen muodossa annettu rekisterinpitäjälle.[634] Suostumuksen tulee olla myös sillä tavoin yksilöity, että suostumusta annettaessa rekisteröity saa tietää suostumuksensa laajuuden. Suostumus ei ole pätevä esimerkiksi silloin, jos maininta suostumuksesta on sisällytetty palvelun käyttöehtoihin. Pätevään suostumukseen

---

632 HE 96/1998 vp, s. 38–39. Katso myös Tietosuojatyöryhmän lausunto 5/2005 sijaintitietojen käytöstä lisäarvopalvelujen tarjoamisen yhteydessä sekä *Pitkänen – Tiilikka – Warma,* Henkilötietojen suoja, s. 83.

633 Vertaa *Tranberg,* jonka mukaan henkilötietoja saa käsitellä myös ilman suostumusta, jos rekisterinpitäjän tarve henkilötietojen käsittelyyn on suurempi kuin rekisteröidyn tarve olla luovuttamatta tietojaan. *Tranberg,* Biometric Data in Scandinavia, s. 394.

634 Neuvonen huomauttaa siitä, että henkilötietojen kokonaisuudessa kysymys on julkisoikeudessa perinteisestä suostumuksesta, jolla mahdollistetaan tietyt toimenpiteet. Tällainen suostumus eroaa yksityisoikeudellisesta suostumuksesta, jolla oikeus tietoihin siirtyisi. Neuvonen, Yksityisyyden suoja Suomessa, s. 66. Vertaa Voutilainen, Oikeus tietoon, s. 245. Tietojen omistuksesta katso myös *Pitkänen – Tiilikka – Warma,* Henkilötietojen suoja, s.10–12 sekä *Purtova,* Property Rights in Personal Data: Learning from the American Discourse. Amerikkalaisesta näkökulmasta erityisesti katso Posner, The Economics of Justice.

kuuluu myös tiedon kohteen todellinen mahdollisuus suostumuksen antamisesta kieltäytymiseen ilman sanktioita.

Lisäksi suostumukselta edellytetään tietoisuutta, joka perustuu asian oikeudellisen merkityksen tuntemukseen. Tietoisuus edellyttää tällöin sitä, että henkilölle ei ole epäselvää, mihin suostumuksensa antaa. Henkilölle tulee toisin sanoen olla riittävästi tietoa, johon perustaa päätöksensä. Häntä tulee tarvittaessa myös informoida suostumuksen seuraamuksista. Mitä merkityksellisemmästä ja seurauksiltaan vaikeaselkoisemmasta asiasta on kysymys, sitä enemmän henkilölle on annettava etukäteen informaatiota, jotta hän pystyy antamaan tietoisen suostumuksen.[635] Oleellisena osana suostumusta on myös se, että suostumus on aina peruutettavissa.

Suostumukselle asetettujen edellytysten täyttyminen määräytyy kuitenkin viime kädessä tapauskohtaisesti, jolloin merkitystä on annettava muun muassa kerättävien tietojen laadulle.

Suostumus sinänsä ei kuitenkaan oikeuta rekisterinpitäjää laista poikkeavaan toimintaan. Yksilön itsemääräämisoikeus ja rekisterinpitäjän velvollisuudet ovat eri asioita. Rekisterinpitäjän tulee lisäksi muistaa asiallisesti perustellun käsittelyn vaatimus sekä henkilötietojen käyttötarkoitussidonnaisuus. Suostumuksen olemassaolo ei oikeuta rekisterinpitäjää käsittelemään henkilötietoja ilman asiallista perustetta ja keräämään ennalta määriteltyihin käyttötarkoituksiin sopimattomia henkilötietoja taikka käyttämään henkilötietoja ennalta määrittelemättömiin tarkoituksiin.[636] Suostumuksellakaan ei siis ole lupa käsitellä käyttötarkoituksen kannalta tarpeettomia henkilötietoja.

Suostumuksella tapahtuvasta henkilötietojen käsittelystä on kysymys myös rekisteröidyn toimeksiannosta tapahtuvassa henkilötietojen käsittelyssä. Esimerkkinä voidaan mainita tilanne, jossa henkilö tekee

---

635 *Raatikainen,* Yksityisyyden suoja työelämässä, s. 62.

636 *Vanto,* Henkilötietolaki käytännössä, s.44.

palveluntarjoajan kanssa sopimuksen geneettisen tutkimuksen tekemisestä. Tällöin henkilötietojen käsittelyn perusteena on sopimuksen täytäntöönpaneminen, jossa rekisteröity on osallisena. Tällaisessa tilanteessa käsittely perustuu suostumukseen rekisteröidyn aktiivisuuden vuoksi.

Lisäksi henkilötietolaki antaa oikeuden käsitellä henkilötietoja, jos käsittely on yksittäistapauksessa tarpeen rekisteröidyn elintärkeän edun suojaamiseksi. Keskeistä tämän edellytyksen kannalta on se, että edun tulee olla elintärkeä, esimerkiksi ensiavun tarjoaminen onnettomuustilanteessa. Tämä edellytys ei täyty silloin, kun henkilötietojen käsittely on tarpeen elintärkeän edun suojaamiseksi muussa kuin yksittäistapauksessa.[637] Tällaiseen henkilötietojen käsittelyyn vaaditaan tietosuojalautakunnan lupa.

Vasta edellä kuvattujen jälkeen tulevat sovellettavaksi poikkeukset suostumuksen periaatteeseen. Ensimmäisenä tällaisena poikkeuksena on henkilötietojen käsittely, josta on erikseen laissa säädetty. Suostumus on siis korvattavissa ensisijaisesti lainsäädännöllä.[638] Tämä tarkoittaa sitä, että käsittely ei voi perustua asetukseen eikä asetuksen nojalla määrättyyn tehtävään, vaan käsittelyn tulee perustua laintasoiseen säännökseen.[639] Säännös mahdollistaa henkilötietojen käsittelyn, mutta se ei suoraan anna siihen oikeutta. Käsittelystä tulee säätää erikseen erityislainsäädännössä.

Erityislainsäädännön nojalla tapahtuvasta biometristen tunnisteiden käsittelystä on kysymys yksityisyyden suojasta työelämässä an-

637 HE 96/1998 vp, s. 39. Katso myös *Vanto,* Henkilötietolaki käytännössä, s. 46.

638 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 364

639 HE 96/1998 vp, s. 39. Katso myös *Vanto,* Henkilötietolaki käytännössä, s. 47, jossa Vanto muistuttaa siitä, että henkilötietolaki soveltuu myös sellaiseen henkilötietojen käsittelyyn, josta on säädetty muussa laissa, ellei erityislaissa toisin säädetä.

netun lain, passilain sekä henkilötietojen käsittelystä poliisitoimessa annetun lain nojalla tapahtuvasta biometristen tietojen käsittelystä. Vaikka biometristen tunnisteiden käsittelyä ei mainita yksityisyyden suojasta työelämässä annetussa laissa, sallii laki kuitenkin biometristen tunnisteiden käsittelyn. Syynä on se, että laki nojaa sääntelyssä hyvin pitkälti henkilötietolakiin, joka henkilötietojen käsittelyn yleislakina sallii biometristen tunnisteiden käsittelyn.

Lakisääteisen käsittelyn lisäksi poikkeuksia suostumuksen ensisijaisuuteen on yhteysvaatimukseen perustuva henkilötietojen käsittely, joka mahdollistaa henkilötietojen joustavan käsittelyn tavanomaisissa asiakas- ja jäsenyyssuhteissa sekä konserneissa tai muissa taloudellisissa yhteenliittymissä. Lisäksi yhteysvaatimuksesta on kysymys, kun henkilötietoja käsitellään rekisterinpitäjän toimeksiannosta. Tällöin toimeksiannon saajalla on välillinen oikeus henkilötietojen käsittelyyn, sillä hänen oikeutensa perustuu rekisterinpitäjän oikeuteen käsitellä henkilötietoja. Näin ollen toimeksisaajan toiminta ei ole toimeksisaajan itsenäistä toimintaa.[640] Lähtökohtana on tietojen kerääminen rekisteröidyltä itseltään asiallisen yhteyden syntyessä. Tämä tarkoittaa hiljaisen suostumuksen syntymistä rekisteröidyn aktiivisten toimenpiteiden seurauksena.[641]

Poikkeusperusteena suostumuksesta toimii myös tietosuojalautakunnan lupa henkilötietojen käsittelylle. Lupaa henkilötietojen käsittelylle tulee hakea, jos mikään edellä mainituista henkilötietojen käsittelyn edellytyksistä ei täyty. Tietosuojalautakunta voi antaa lupia vain

640 Voutilainen, Oikeus tietoon, s. 280. Katso myös *Vanto,* jonka mukaan toimeksisaajalla ei ole itsenäistä oikeutta käsitellä henkilötietoja omiin tarkoituksiinsa. *Vanto,* Henkilötietolaki käytännössä, s. 50.

641 Vaikka asiallinen yhteys olisikin laissa tarkoitetulla tavalla olemassa, rekisterinpitäjän tulee pystyä asiallisesti perustelemaan henkilötietojen käsittely yleensä ja tiettyjen henkilötietojen käsittely erityisesti. *Vanto,* Henkilötietolaki käytännössä, s. 47–48.

erittäin rajoitetusti intressipunninnan jälkeen. Käytännössä merkittävä osa tietosuojalautakunnan luvista on koskenut muun muassa erilaisia ns. mustia listoja väärinkäytöstilanteista eri aloilla. Esimerkiksi vakuutusyhtiöt ovat saaneet luvan luovuttaa toisilleen ja käsitellä näin saatuja vahinkotietoja vakuutusrikollisuuden ehkäisemiseksi (TSL 14.12.2009).

Arkaluonteisten tietojen erityisasema. Tietyt erityisen henkilökohtaiset ja arkaluonteiset tiedot on katsottu sellaisiksi, että ne vaativat erityistä suojaa.[642] Arkaluonteiset tiedot myös muodostavat yksilön perusoikeuksien ankarimmin suojatun tiedollisen alueen. Tämän vuoksi niiden käsittely on lähtökohtaisesti kiellettyä ilman asianomaisen suostumusta tai erityistä lakisääteistä perustetta. Lähtökohtana arkaluonteistenkin tietojen kohdalla on suostumuksen ensisijaisuus, mutta arkaluonteisten tietojen erityissääntely tekee näistä tiedoista muita tietoja suojatumpia. Vastaavasti arkaluonteisten tietojen tietoturvan tulee olla tavallista parempaa.

Arkaluonteisten tietojen luettelo henkilötietolaissa kuvastaa yleistä käsitystä siitä, mitkä henkilötiedot eivät kuulu julkisuuteen eivätkä vaihdantaan. Syynä on se, että arkaluonteiset tiedot ovat sellaisia, joiden avulla yksilön identiteettiä ja yksilöllisyyttä on mahdollista helposti käyttää väärin.[643]

---

642 Tämä on todettu myös EIT:n ratkaisussa Z v. Suomi (antopäivä 25.2.1997), jossa tuomioistuin totesi seuraavaa: ”highly intimate and sensitive nature of information…call for the most careful scrutiny… as do the safeguards designed to secure an effective protection.” Katso myös *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 68.

643 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 368.

Arkaluonteisten tietojen luettelo on seuraava:

1. rotu tai etninen alkuperä;
2. henkilön yhteiskunnallinen, poliittinen tai uskonnollinen vakaumus tai ammattiliittoon kuuluminen
3. rikollinen teko, rangaistus tai muu rikoksen seuraamus;
4. henkilön terveydentila, sairaus tai vammaisuus taikka häneen kohdistetut hoitotoimenpiteet tai niihin verrattavat toimenpiteet;
5. henkilön seksuaalinen suuntautuminen tai käyttäytyminen; taikka
6. henkilön sosiaalihuollon tarve tai hänen saamat sosiaalihuollon palvelut ja muut sosiaalihuollon etuudet.

Arkaluonteisten tietojen käsittely on eri tilanteissa kuitenkin yhteiskunnassa myös välttämätöntä. Tämän vuoksi henkilötietolaissa on erikseen lueteltu joukko tehtäviä, joissa muutoin kielletty käsittely on sallittua. Ne ulottuvat henkilöiden itsensä julkistamien arkaluonteisten tietojen käsittelystä sosiaali- ja terveydenhuollon toimijoiden oikeuteen saada käsitellä niiden toiminnassa tarpeellisia tietoja. Viime kädessä tietosuojalautakunta voi rajoitetusti myöntää lupia arkaluonteisten tietojen käsittelyyn. Lisäksi erityislainsäädäntö sisältää arkaluonteisten tietojen käsittelykieltoon poikkeuksia. Tällöinkin käsittelyn on kuitenkin oltava perusteltua ja sen on rajauduttava vain henkilön etujen, oikeuksien ja velvollisuuksien hoitamisen kannalta välttämättömiin tietoihin.

Käsittelykieltoon otetut varsin laaja-alaiset poikkeukset tekevät arkaluonteisten tietojen käsittelystä enemmän periaatteellisen kuin kattavan käytännön realiteetin. Tästä huolimatta näihin tietoihin on suhtauduttava erityisellä huolellisuudella.

Arkaluonteisten henkilötietojen kohdalla nousee esille kysymys siitä, onko laissa mainittu luettelo tyhjentävä vai tuleeko sitä tulkita

henkilötiedon käsitteen tavoin laveasti.[644] Kysymys nousee esille myös biometristen tunnisteiden kohdalla. Biometrisia tunnisteita ei henkilötietolaissa mainita arkaluonteisten tietojen luettelossa. Voidaanko biometriset tunnisteet tästä huolimatta nähdä henkilötietolaissa tarkoitettuina arkaluonteisina henkilötietoina? Vastaus kysymykseen ei ole helppo, sillä asiasta ei ole yhtenäistä näkemystä.

Tukea väitteelle, että biometriset tunnisteet tulee nähdä yleisesti arkaluonteisina henkilötietoina, ei juuri ole. Biometrisia tunnisteita ei ole pidetty arkaluonteisina henkilötietoina sen vuoksi, että ne eivät suoraan paljasta arkaluonteista tietoa (esimerkiksi terveystietoja), vaan arkaluonteisen tiedon esiin saaminen biometrisesta tunnisteesta vaatii erityisiä toimenpiteitä.[645]

Tämän ajatustavan mukaan vain tiettyjä biometrisia tietoja on ehdottomasti pidettävä arkaluonteisina tietoina. Tietosuojatyöryhmä mainitsee esimerkkinä kasvojen tunnistamiseen perustuvat biometriset järjestelmät, joissa on mahdollista käsitellä tietoja, jotka koskevat

644 Esimerkiksi Raatikainen katsoo, että arkaluonteisia tietoja käsittelevä luettelo on tyhjentävä. Raatikainen, Yksityisyyden suoja työelämässä, s. 185. Vertaa *OECD,* Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Guideline's Explonatory Memorandum kappaleet 45 ja 51.

645 *Prins,* Biometric technology law, making our body identify for us: legal implications of biometric technologies, s. 162 ja 29 artiklan mukainen tietosuojatyöryhmä, Working Document on Biometrics 2003 (WP80), s. 10. Katso myös Belgian tietosuojaviranomaisen (Commissie voor de Bescherming van de Persoonlikje Levensfeer) lausunto CBPL, Avis n° 17 /2008 du 9 avril 2008, s. 8–9, jossa hän on ottanut sen näkökannan, että biometriset tunnisteet itsessään eivät ole arkaluonteisia henkilötietoja. Ne ovat arkaluonteisia henkilötietoja, jos ne esimerkiksi kuvaavat yksilön terveydentilaa tai etnistä alkuperää.

henkilön rotua tai etnistä alkuperää.[646] Muita esimerkkejä ovat silmän iirikseen perustuva tunnistaminen sekä DNA-tunnistus, joiden avulla voidaan saada tietoja yksilön terveydestä.

Asia ei kuitenkaan ole näin yksiselitteinen, sillä arkaluonteisuutta on mahdollista lähestyä niin sanotun avaintiedon käsitteen (kuten henkilötunnuksen) kautta. Tällöin tiettyjä avaintietoja ei itsessään pidetä arkaluonteisina. Niiden arkaluonteisuus johdetaan siitä, mitä tietoa tämän avaintiedon kautta saadaan. Avaintiedon arkaluonteisuutta arvioitaessa ei tule pelkästään kiinnittää huomiota tämän tiedon elementin luokitukseen. Huomiota tulee lisäksi kiinnittää siihen, mitä tietoa tämän tiedon avulla on yhdistettävissä.[647] Tätä pelkkää avaintietoa tulee arvioida arkaluonteisena, ei niinkään itsestään, vaan tämän avaintiedon tietoja yhdistävän luonteen vuoksi. Tätä ajatusta kuvaa henkilötietodirektiivin 7 artiklan 8-kohdan vaatimus antaa lainsäädännöllistä suojaa yksilöllisille tunnisteille.

Biometriset tunnisteet eroavat yksilöivän luonteensa vuoksi niin sanotuista tavallisista henkilötiedoista. Yksilöivän luonteensa vuoksi biometrista tunnistetta voidaan pitää niin sanottuna ”avaintietona”, jonka avulla yksilöä koskevia tietoja on mahdollista yhdistää.[648] Ne ovat myös sellaisia henkilötietoja, jotka mahdollistavat yksilön identiteetin ja yksilöllisyyden väärinkäytön. Biometriset tunnisteet ovat ainutlaatuinen ja arkaluontoinen henkilötietojen ryhmä, joilla on vaiku-

646 29 artiklan mukainen tietosuojatyöryhmä, Working Document on Biometrics 12168/02/FI WP 80, s.9.

647 *Bing,* Classification of personal information, with respect to the sensitivity aspect, s. 107–108.

648 Katso *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 305, jossa Kindt esittää näkemyksen siitä, että biometrisia tunnisteita tulee pitää arkaluonteisina niiden identifioivan luonteen vuoksi.

tuksia anonymiteettiin ja joiden väärinkäyttö loukkaa yksilön oikeutta yksityisyyteen.

Biometristen tunnisteiden asemaa arkaluonteisena tietona puoltaa myös näkemys siitä, että tietojen arkaluonteisuus riippuu tietojen käsittelyn asiayhteydestä.[649] Henkilötietojen arkaluonteisuutta ei pidä nähdä ennalta-annettuna, vaan tietojen arkaluonteisuus tulee johtaa tietojen käyttötarkoituksesta ja –yhteydestä.[650]

Nämä seikat yhdessä henkilötietolain tarkoituksen kanssa puoltavat näkemystä siitä, että biometriset tunnisteet tulee tulkita arkaluonteisiksi henkilötiedoiksi, joita koskevat tiukemmat käsittelyedellytykset. Tälle kannalle on päätynyt myös hallintovaliokunta, joka on ulkomaalaislakia koskeneen hallituksen esityksen yhteydessä antamassaan mietinnössä todennut biometristen tunnisteiden rinnastuvan arkaluonteisiin tietoihin.[651]

Biometrisia tunnisteita tulee pitää arkaluonteisina henkilötietoina kolmesta syystä: 1) ne sisältävät tietoja, joita on perinteisesti pidetty

649 Tiettyjen henkilötietojen luokitteleminen asiayhteydestä riippumatta arkaluonteiseksi on varsin kiistanalaista. Katso tähän liittyvästä kritiikistä esimerkiksi. Simitis, Sensitive Daten – Zur Geschichte und Wirkung einer Fiktion, s. 469–493. Katso myös *Bygrave,* Data Privacy Law. An International Perspective, s. 165-167.

650 *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 69. Näin myös *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 369.

651 HaVM 36/2010 vp. Katso myös PeVL 55/2010 vp. ja PeVL 14/2009 vp. Myös esimerkiksi Tsekin tasavallan henkilötietolaissa biometriset tunnisteet nimenomaisesti mainitaan arkaluonteisia henkilötietoja koskevassa lainkohdassa. Article 4 (b) of the Personal Data Protection Act N° 101/2000 of 4 April 2000 on the Protection of Personal Data and on Amendment to Some Acts, 4 April 2000("Czech Republic Personal Data Protection Act N° 101/2000 of 4 April 2000")

arkaluonteisina, 2) niistä saadaan terveyttä ja perinnöllisyyttä koskevia tietoja ja 3) niitä voidaan käyttää yksilöllisinä tunnisteina.[652]

Arkaluonteiset henkilötiedot ovat yksilön yksityisyyden suojan ydinalueella. Biometriset tunnisteet ovat pysyvä, muuttumaton ja peruuttamaton osa yksilöä. Ne myös sisältävät yksilöstä sellaista informaatiota, joka mahdollistaa hänen tarkan tunnistamisensa hyvin erilaisissa yhteyksissä.

Tästä syystä on perusteltua pitää biometrisia tunnisteita henkilötietoina, jotka tarvitsevat erityistä suojaa yksilön yksityisyyden suojan turvaamiseksi henkilötietojen käsittelyssä.[653] Biometrisissa tunnisteissa on kuitenkin kysymys yksilön fyysisiä ominaispiirteitä koskevista hyvin yksilöivistä tiedoista, joiden kerääminen vaatii puuttumista yksilön ulkoiseen vapauteen. Näiden tietojen avulla yksilön identiteettiä on myös mahdollista väärinkäyttää. Tällaisina tietoina biometriset tunnisteet tarvitsevat erityistä lainsäädännöllistä suojaa tavallisiin henkilötietoihin verrattuna.[654]

Lain englanninkielinen versio on saatavilla osoitteessa: http://ec.europa.eu/justice/policies/privacy/docs/implementation/czech_republic_act_101_en.pdf.

652 *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 747.

653 *Liu,* Bio-privacy, s. 100.

654 Kuten Kindt on Asian ilmaissut: "Biometric data shall be considered as a category of personal data for which appropriate attention is needed as well as a regulation for the processing of such data." *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 228. Biometristen tunnisteiden erityistä luonnetta on varsin osuvasti kuvattu Kalifornian osavaltion korkeimman oikeuden toimesta ratkaisussa Perkey v. Department of Motor Vehicles (42 Cal.3d 185 (1986)), jossa oikeus totesi seuraavaa:"… a fingerprint is a much more private matter than a name or address and its disclosure can

Biometristen tunnisteiden asemaa arkaluonteisina tietoina puoltaa omalta osaltaan myös se, että Euroopan Neuvoston tietosuojasopimuksen päivitetyssä 6 artiklassa biometriset tunnisteet on rinnastettu arkaluonteisiin tietoihin. Voimassa olevassa kansallisessa lainsäädännössä biometriset tunnisteet on kuitenkin katsottu henkilötiedoiksi. Vain tietyissä tapauksissa biometriset tunnisteet ovat arkaluonteisia tietoja. Ne ovat kuitenkin monin tavoin rinnastettavissa arkaluonteiseen tietoon.

Tarkastus- ja oikaisuoikeus. Henkilötietojen käsittelyn tulee perustua avoimuuteen, sillä avoimuuden avulla toteutetaan rekisteröidyn oikeutta valvoa omien tietojensa käsittelyä. Sen ohella, että yksilöllä on pääsääntöisesti oltava mahdollisuus tietää, missä ja miten hänen tietojaan käsitellään, yksilöllä on myös mahdollisuus vaikuttaa niiden sisältöön.

Tässä tarkoituksessa henkilötietolain 26 §:ssä säädetään rekisteröidylle omien tietojen tarkastusoikeus[655], joka on osa yksilön oikeutta tulla arvioiduksi oikeassa valossa. Tarkastusoikeuden kautta toteutuu myös yksilön oikeus puolustaa omaa identiteettiään.[656] Yksilöllä on tiedollisen itsemääräämisoikeuden nimissä oikeus tarkastaa omat tietonsa ilman, että hänen tarvitsee tätä erikseen perustella. Tarkastusoikeus ei myöskään ole riippuvainen siitä, tietääkö rekisteröity, että hänestä on rekisterissä tietoja.

---

lead to much greater intrusions on privacy than the simple disclosure of an individual´s name." Oikeus kuvasi yksilön sormenjälkeä avaimeksi arkaluonteisiin ja mahdollisesti vaarallisiin yksilöstä saataviin tietoihin.

655 Raatikaisen mielestä "tarkastaminen" ei ole täysin onnistunut ilmaus, sillä kysymys on henkilön oikeudesta saada tietää ja saada haltuunsa itseään koskevat henkilötiedot, jotka on tallennettu henkilörekisteriin. *Raatikainen,* Yksityisyyden suoja työelämässä, s. 248.

656 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 371.

Tarkastusoikeus yleensä myös ohittaa rekisterinpitäjän mahdollisen salassapitovelvollisuuden. Toisaalta tarkastusoikeutta on katsottu yhteiskunnan edun nimissä parhaaksi rajoittaa esimerkiksi sen vuoksi, että tiedot kuuluvat maan turvallisuuden, yleisen järjestyksenpidon tai rikostutkinnan kannalta tärkeisiin tietoihin. Kaikkiin rekistereihin tarkastusoikeus ei siis päde. Avoimuus ei saa vaarantaa yhteiskunnan kriittisiä toimintoja. Tällaisessa tapauksessa tietosuojavaltuutetulla on oikeus tarkastaa rekisterin tiedot niiden lainmukaisuuden varmistamiseksi ja rekisteröidyn oikeusturvan vuoksi.

Tarkastusoikeuden käyttämiseksi on esitettävä tätä tarkoittava pyyntö rekisterinpitäjälle kirjallisesti tai henkilökohtaisesti rekisterinpitäjän luona. Tarkastusoikeutta ei näin ollen voi toteuttaa asiamiehen välityksellä.[657] Eduskunnan oikeusasiamiehen potilastietojen tarkastamista koskevassa ratkaisussa kuitenkin valtakirjan käyttö katsottiin perustuslain nojalla hyvän hallinnon mukaiseksi menettelyksi.[658] Aiemmin vakiintuneesti henkilökohtainen oikeus on hiljalleen muuttumassa myös valtuutuksella käytettäväksi.

Tietojen tarkastusoikeuden käyttämisen yhteydessä saattaa ilmetä henkilörekisterin tietojen olevan virheellisiä, tarpeettomia, puutteellisia tai vanhentuneita tietoja. Tällaisessa tilanteessa rekisteröidyllä on oikeus saada tietonsa oikaistuksi (HetiL 29 §). Rekisteröidyn havaitessaan jonkun tiedon virheelliseksi, tarpeettomaksi, harhaanjohtavaksi

657 Tietosuojavaltuutetun toimisto, Henkilörekisteriin talletettujen tietojen tarkastaminen, s. 4. Ohjeessa todetaan se, että tarkastusoikeus kuuluu myös alle 18-vuotiaalle. Katso myös *Raatikainen,* Yksityisyyden suoja työelämässä, s.253.

658 Eduskunnan oikeusasiamiehen potilastietojen tarkastamista koskeva ratkaisu 2022/4/04. Tätä puoltaa myös ILOn näkemys. ILOn mukaan työntekijöillä tulisi olla oikeus nimittää työntekijöidensä edustaja tai valitsemansa työtoveri avustamaan heitä tarkastusoikeutta. ILO, Työntekijöiden henkilötietojen suojaaminen.

tai vanhentuneeksi, rekisterinpitäjä on velvollinen korjaamaan tiedon. Mikäli rekisterinpitäjä ei korjaa tietoja, rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi.

Oikaisemista koskevalle vaatimukselle ei ole asetettu mitään tiettyä muotoa. Oleellista on se, että rekisterinpitäjä voi varmistua oikaisemisvaatimuksen esittäjän henkilöllisyydestä.[659] Tietojen oikaisuoikeus ulottuu myös muihin kuin rekisterinpitäjän omiin rekistereihin. Rekisterinpitäjän on nimittäin myös estettävä tällaisen tiedon leviäminen, jos tieto voi vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan. Henkilötietojen tulee näin ollen olla oikeita koko tiedon elämänkaaren ajan.[660]

Rekisteripitäjä on velvoitettu myös oma-aloitteisesti oikaisemaan virheelliseksi havaitsemansa tiedot. Laissa esitetty vaatimus oma-aloitteiseen oikaisemiseen kuvaa hyvin sitä, että rekisterinpitäjälle on laissa asetettu aktiivinen vaatimus pitää rekisterinsä ajan tasalla. Kysymys on näin ollen hyvän tietojenkäsittelytavan noudattamisesta. Hyvään tietojenkäsittelytapaan ei kuulu virheellisten, puutteellisten, tarpeettomien tai vanhentuneiden henkilötietojen käsittely. Esimerkiksi rekisteröidyn kuolema on sellainen tilanne, jonka seurauksena rekisterinpitäjän tulee oma-aloitteisesti poistaa kaikki sellaiset kuollutta henkilöä koskevat tiedot, joille ei ole asianmukaista ja laillista perustetta. Tämä tarkoittaa esimerkiksi kuolleen henkilön sormenjälkitietojen poistamista.

Oikeus saada tietonsa korjatuksi on läheisessä yhteydessä rekisterinpitäjälle asetettuun virheettömyysvaatimukseen.[661] Oikeus kuvaa myös sitä yksityisyyteen liittyvää periaatetta, jonka mukaan jokaisella on oikeus tulla arvioiduksi oikeassa valossa. Periaate on erityisen mer-

659 *Voutilainen,* Oikeus tietoon, s. 270.

660 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 371.

661 Näin myös *Vanto,* jonka mukaan oikeus saada tietonsa korjatuksi voidaan nähdä rekisterinpitäjälle säädetyn virheettömyysvaatimuksen peilikuvana. *Vanto,* Henkilötietolaki käytännössä, s. 132.

kityksellinen nimenomaan henkilötietojen käsittelyssä, sillä tiedollisen itsemääräämisoikeuden nojalla yksilöllä tulee olla oikeus myös saada virheelliset henkilötietonsa korjatuksi.

Tietosuojaviranomaisten palvelut. Oikeus tietosuojaviranomaisten palveluihin on sekä yleinen tietosuojajärjestelmän tunnusmerkki että erityinen rekisteröityjen oikeuksiin vaikuttava tekijä. Rekisterinpitäjän ja rekisteröidyn välisessä suhteessa vallitsevan epätasapainon vuoksi erityinen riippumaton viranomaiskoneisto on valjastettu paitsi ohjaamaan henkilötietojen käsittelyä yleisellä tasolla myös palvelemaan yksilöitä. Viranomaistoiminnassa ja erityisesti tietosuojavaltuutetun toiminnassa lähtökohtina ovat ohjaus ja neuvonta. Tietosuojavaltuutettu antaa henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa sekä valvoo henkilötietojen käsittelyä henkilötietolain tavoitteiden toteuttamiseksi.

Tietosuojavaltuutetulla on tehtävässään kuitenkin myös rajoitettu päätösvalta. Hän voi antaa rekisterinpitäjälle määräyksen rekisteröidyn tarkastusoikeuden toteuttamisesta tai tiedon korjaamisesta. Pääsääntönä on kuitenkin se, että varsinainen päätöksentekoelin on tietosuojalautakunta. Keskeisiä työvälineitä toiminnan tehokkuutta ajatellen ovat tietosuojavaltuutetulle annetut tiedonsaanti- ja tarkastusoikeudet. Niiden avulla tietosuojavaltuutettu voi rekisteröityjä paremmin selvittää yksittäistapauksissa henkilötietojen käsittelyn laillisuus.

Tietosuojalautakunnan toimivalta painottuu lainvastaisen henkilötietojen käsittelyn kieltämiseen ja oikaisemiseen sekä lupien myöntämiseen. Tyypillisesti asiat tulevat esille joko tietosuojavaltuutetun aloitteesta tai lupahakemuksina. Lisäksi tietosuojalautakunnalla on oikeus käsitellä henkilötietolain soveltamisalan kannalta tärkeitä kysymyksiä. Tätä toimivaltaa lautakunta on kuitenkin varsin niukasti käyttänyt.

5.4.3. Henkilötietojen suojan muutokset Euroopan Unionissa

EU:n nykyisen tietosuojalainsäädännön keskeisellä säädöksellä eli henkilötietodirektiivillä[662] oli antohetkellään kaksi tavoitetta: tietosuojaa koskevan perusoikeuden suojaaminen ja henkilötietojen vapaan liikkuvuuden takaaminen jäsenvaltioiden välillä. Teknologiset ja yhteiskunnalliset muutokset yhdessä toimintaympäristön muutoksen kanssa ovat kuitenkin aiheuttaneet sen, että olemassa oleva tietosuojakehys on koettu riittämättömäksi nykyisessä informaatioyhteiskunnassa niin yksilön oikeuksien ja vapauksien kuin taloudenkin näkökulmasta.

Nykyisen tietosuojakehyksen tavoitteet ja periaatteet eivät ole menettäneet merkitystään. Siinä esitetyt tavoitteet ja periaatteet eivät kuitenkaan ole pystyneet estämään henkilötietojen suojan täytäntöönpanon hajanaisuutta. Ongelmana ovat olleet sekä oikeudellinen epävarmuus että verkkoympäristössä toimimiseen liittyvät huomattavat riskit. Tämän vuoksi katsottiin tarpeelliseksi laatia EU:lle vahvempi ja johdonmukaisempi tietosuojakehys. Kehystä on tarkoitus tukea tehokkaalla täytäntöönpanolla informaatiotalouden kehittymisen turvalliseksi edistämiseksi sekä yksilöiden omien tietojen valvonnan mahdollistamiseksi. Tällä tavoin voidaan vahvistaa oikeusvarmuutta ja luottamusta käytännön toiminnan sujuvuuteen kaikkien informaatiotalouden toimijoiden kannalta.[663] Uuden tietosuoja-asetuksen tarkoi-

662 Direktiiviä täydennettiin puitepäätöksellä 2008/977/YOS. Se on unionin tasolla sovellettava yleinen väline, joka koskee henkilötietojen suojaa poliisiyhteistyön ja rikosasioissa tehtävän oikeudellisen yhteistyön alalla.

663 Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus). COM(2012) 11 final, s. 1–2.

tuksena on varmistaa, että tietojen käsittelyä koskevat säännöt kestävät ajan saatossa ja ovat digitaaliselle aikakaudelle sopivia.

Pohjimmiltaan muutoksessa on kysymys yksilöiden oikeuksien ja vapauksien turvaamisesta henkilötietojen käsittelyssä entistä enemmän informaation käsittelyyn ja verkoissa toimimiseen perustuvassa yhteiskunnassa. Henkilötietojen suoja saa asetuksen myötä entistä korostuneemman merkityksen niin oikeudellisesti kuin muutenkin. Edellä mainittujen syiden vuoksi Euroopan komissio antoi ehdotuksen yleisestä tietosuoja-asetuksesta tammikuussa 2012.

Yleisen tietosuoja-asetuksen tavoitteina ovat yksilön oikeuksien vahvistaminen, sisämarkkinaulottuvuuden lujittaminen, tietosuojan globaalin ulottuvuuden huomioiminen sekä tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen. Asetuksen tavoitteena on myös luoda Euroopan Unionille ajanmukainen, vahva, yhtenäinen ja kattava tietosuojakehys, jolla parannetaan luottamusta verkkopalveluihin ja näin edistetään digitaalisten sisämarkkinoiden kehittämistä. Asetus tulee korvaamaan vuonna 1995 annetun henkilötietodirektiivin. Sillä päivitetään ja nykyaikaistetaan tietosuojadirektiiviin sisältyvät henkilötietojen käsittelyn periaatteet.

Miten asetus muuttaa henkilötietojen käsittelyä? Asetuksessa luetellaan rekisteröidyn eli henkilötietojen käsittelyn kohteena olevan henkilön oikeudet, kuten omia tietoja koskeva tiedonsaantioikeus, oikeus saada tiedot oikaistua, oikeus tulla unohdetuksi sekä oikeus tietojen poistamiseen ja tietojenkäsittelyn vastustamiseen. Ehdotus sisältää täsmennyksiä voimassaolevaan sääntelyyn sekä merkittäviä uusia velvoitteita ja sanktioita.

Asetuksessa on sääntelyn lähtökohdaksi otettu niin sanottu riskipohjainen lähestymistapa. Tarkoituksena on ottaa sääntelyssä huomioon henkilötietojen käsittelyyn kulloinkin liittyvät riskit ja yhtäältä välttää vähäriskisten toimien ylisääntelyä. Toisaalta halutaan varmistaa rekisteröidyn suoja korkean riskin toiminnassa. Tällöin arvioitavina

ovat muun muassa tietojen laatu, luonne, käsittelytarkoitus ja laajuus. Rekisterinpitäjä ja henkilötietojen käsittelijä velvoitetaan ryhtymään toimiin, jotka vastaavat henkilötietojen käsittelyyn kulloinkin kohdistuvaa riskiä.

Keskeisenä periaatteena asetuksessa on rekisterinpitäjän tilivelvollisuus. Tällä tarkoitetaan sitä, että rekisterinpitäjän vastuulla olisi koko henkilötietojen käsittelyprosessin ajan säädösten noudattamisen seuraaminen. Uutena asiana asetuksessa säädetään myös, että yli 250 työntekijän yritysten tulisi asettaa tietosuojavastaava. Lisäksi uutta olisi myös se, että komission valta hyväksyä menettelyitä henkilötietojen siirrossa EU:n ulkopuolelle kasvaisi.

Rekisteröidyn kannalta merkittävin muutos asetuksessa on periaate oikeudesta tulla unohdetuksi. Yksilöllä tulee olla oikeus tulla poistetuksi rekistereistä. Asetuksessa on myös lähdetty direktiiviä laajemmin erottelemaan täysivaltaisten aikuisten ja lasten mahdollisuuksia suostumuksen antamiseen. Tämä sisältää oikeuden vastustaa henkilötietojen käsittelyä, joka tällöin muuntaisi oikeuden kieltää henkilötietojen käsittely suoramarkkinoinnissa oikeudeksi kieltää muunkinlainen käsittely. Vastustaminen täyttäisi myös yhden edellytyksen oikeudesta tulla unohdetuksi. Asetuksen myötä rekisteröity saisi myös laajemman oikeuden omien tietojensa tarkastamiseen ja oikeuden siirrättää tietonsa järjestelmästä toiseen.

Näiden suurempien periaatteellisten ja oikeudellisten muutosten lisäksi asetukseen sisältyy myös muun muassa seuraavat muutokset:

Uudet määritelmät: asetukseen sisältyy uusina määritelminä muun muassa biometriset tiedot, henkilötietojen tietoturvaloukkaus, geneettiset tiedot ja terveystiedot. Myös suostumuksen määritelmää on tarkennettu.

Arkaluonteisten tietojen alaa laajennetaan kattamaan myös geneettiset tiedot.

Elinkaariajattelu: tekniikoita valitessa tulee huomioida myös tietosuojan ja henkilötietojen suojan vaatimukset.

Ilmoitusvelvollisuuden laajentuminen: velvollisuus ilmoittaa tietovuodoista paitsi rekisteröidylle ja tietosuojaviranomaisille myös tietyissä tilanteissa julkisesti.

Laajennus henkilötietojen alaan: asetus koskisi myös tietoja, joista yhdistelyn kautta saisi henkilötietoja.

Tietosuojaviranomaisen aseman muutos: asetuksessa ehdotetaan EU:n tietosuojaneuvoston perustamista. Lisäksi kansalliset tietosuojaviranomaiset saisivat tietosuojarikkomuksissa kanneoikeuden.

Tuleva henkilötietojen suojaa Euroopan Unionissa koskeva asetus parantaa yksilön oikeuksia ja asemaa henkilötietojen, ja erityisesti biometristen tunnisteiden käsittelyssä Unionin alueella. Biometriset tunnisteet on otettu asetuksen soveltamisalan piiriin ottamalla niitä koskeva erillinen määritelmä asetukseen. Tällä tavoin ne myös erottuvat niin sanotuista tavallisista henkilötiedoista. Lisäksi biometriset tunnisteet mainitaan tietosuojan vaikutusten arviointia koskevassa 33 artiklassa.

Biometriset tunnisteet jäävät kuitenkin vähälle huomiolle. Ne mainitaan vain kahdessa asetuksen artiklassa. Artiklaan 4 on otettu biometrisia tunnisteita koskeva määritelmä, jonka lisäksi ne mainitaan tietosuojan vaikutusten arviointia koskevassa 33 artiklassa. Uudistuksessa biometrisille tunnisteille ei myöskään ole annettu nimenomaista asemaa erityistä suojaa vaativana henkilötietojen ryhmänä, joista säädetään artiklassa 9.[664]

664 Samoihin asioihin on kiinnittänyt huomiota myös Euroopan Neuvosto vuonna 2013 antamassaan biometrista tunnistamista koskevassa raportissa. Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data, s. 17

Esityksen yksityiskohdista on käyty eri tasoilla runsastakin keskustelua ja säännöksen voimaantulo voi tapahtua nopeasti tai hitaasti. Lopullinen päätös asetuksen hyväksymisestä saatiin vuoden 2015 lopussa Euroopan parlamentin, komission ja ministerineuvoston kolmikantaneuvotteluissa.[665] Asetuksen sisältö voi vielä jossain määrin muuttua kolmikantaneuvottelujen yhteydessä. Asetusta ryhdytään soveltamaan kahden vuoden siirtymäajan jälkeen eli vuoden 2018 alusta lukien.

5.5. Biometristen tunnisteiden käsittely kansallisen erityislainsäädännön nojallla

5.5.1. Laki yksityisyyden suojasta työelämässä

5.5.1.1. Yleistä

Työnantajan oikeus valvoa työntekijöitä perustuu työsopimuslain työnjohto- ja valvontaoikeuteen[666], joka toimii Paanetojan mukaan työnantajan vallankäytön oikeutuksena. Hänen mukaansa työsuhteessa vallalla tarkoitetaan oikeutta tai mahdollisuutta määrätä tai päättää

665 Asetuksen lopullista tekstiä ei ollut vielä julkaistu ennen tämän tutkimuksen valmistumista.

666 Tämän on todennut työtuomioistuin antamissaan ratkaisuissa TT 2001-60 ja T:1999-31. Työsopimuksen olennaisiin tunnusmerkkeihin kuuluu työnantajan työnjohto- ja valvontaoikeus, jota kutsutaan oikeuskirjallisuudessa ja työmarkkinakäytännössä myös työnantajan direktio-oikeudeksi. Sitä koskevat säännökset ovat työsopimuslain 1:1, 1:7, 1:9 sekä 3:1:ssä. Oikeustieteessä on katsottu, että työnjohto-oikeus on jouduttu päättelemään käänteisesti TSL 3:1:sestä ja TSL 1:1:stä. Tämän vuoksi on pidetty suotavana, että työnjohto-

toiseen vaikuttavista asioista.[667] Työsuhteessa valta on hänen mukaansa näin ollen ymmärrettävissä työnantajan voimana ja kykynä vaikuttaa päätöksillään työn teon sisältöön ja laatuun sekä työolosuhteisiin.[668]

Tarkemmin kuvattuna kysymys ei kuitenkaan ole niinkään vallasta ja vallankäytöstä, vaan sosiaalisesta kontrollista.[669] Syynä on se, että työnantajan työnjohto- ja valvontaoikeus kuuluu niihin työnantajan mekanismeihin, joilla ohjataan yhteisön jäsen toimimaan normien mukaisesti. Sosiaalinen kontrolli kohdistuu sellaiseen käyttäytymiseen, joka poikkeaa normeista. Sosiaalisen kontrollin avulla työntekijöitä ohjataan sisäistämään työpaikan normit ja käyttäytymään niiden mukaisesti. Tällä tavoin sosiaalisen kontrollin avulla pyritään takaamaan jatkuvuuden kannalta riittävän yhdenmukainen toiminta. Sosiaalinen kontrolli ja valvonta sen osana ovat nähtävissä perinteisenä osana työelämää[670], sillä erityisesti työelämän valvonnassa on kysymys ihmisten

---

ja valvontaoikeuskirjattaisiin selkeästi työsopimuslakiin. *Engblom,* Työnjohto-oikeus erityisesti työtuomioistuimen käytännön valossa, s. 126–127.

667 *Paanetoja,* Vallankäytöstä työsuhteessa, s. 129. Vertaa Kielitoimiston sanakirjan määritelmään, jossa valta määritellään jonkun tai jonkin oikeudeksi tai mahdollisuudeksi hallita jotakuta, määrätä tai päättää jostakin.

668 *Paanetoja,* Vallankäytöstä työsuhteessa, s. 129–130. Katso myös *Saarinen,* Työsuhdeasioiden käsikirja I, s. 976.

669 Näin myös Julkunen, Työprosessi ja pitkät aallot. Työn uusien organisaatiomuotojen synty ja yleistyminen, s. 145–149. Katso myös *Kidwell,* R.E. – *Kidwell,* B.N., Employee reactions to electronic control systems, the role of procedural fairness.

670 Fredrick Taylorin (1911/1967) kirjoituksiin perustunut tieteellinen liikkeenjohto eli taylorismi perustui työvaiheiden osittamiseen, yksityiskohtaiseen työnjakoon, työtehtäviin kuluvan ajan mittaamiseen, suoritusperusteiseen palkkaukseen ja työn valvontaan. Taylor ja muut

suostuttelusta hyväksymään vallitseva sosiaalinen järjestys.[671] Työelämässä sosiaaliseen kontrolliin ja valvontaan sen osana on yhdistettävissä niin positiivisia kuin negatiivisiakin painotuksia riippuen näkökulmasta ja asiayhteydestä. Toisaalta valvonta on monissa tehtävissä hyödyllistä tai tarpeellista esimerkiksi tuotannonohjauksen, työsuojelun ja työturvallisuuden kannalta.[672] Tietyt valvonnan tehtävät, kuten työajan ja työturvallisuuden valvonta, kuuluvat työnantajan lakisääteisiin velvollisuuksiin. Toisaalta valvonta voi vaikuttaa negatiivisesti työhyvinvointiin.[673]

Valvonnan kohdalla suurimpana ristiriitana on erityisesti työntekijän oikeus yksityisyyteen ja työnantajan oikeus valvoa työn tekemistä ja laatua. Työntekijällä on intressi sen kontrollointiin, mitä yksityisiä asioita muut hänestä tietävät. Työnantajan on kuitenkin kaikessa toiminnassaan, etenkin teknisin menetelmin toteutetussa valvonnassa ja työntekijän henkilötietojen käsittelyssä, huomioitava työntekijöiden yksityisyyden suoja. Suomalaisessa oikeusjärjestelmässä työsuhde ei itsessään anna työnantajalle yleisvaltuutta puuttua työntekijän perusoikeuksiin. Työntekijän velvoittaminen alistumaan yksityiselämään,

---

tieteellisen liikkeenjohdon kehittäjät uskoivat, että tieteellisin menetelmin työ oli mahdollista suunnitella mahdollisimman tehokkaaksi. *Taylor,* Principles of Scientific Management, s.9.

671 Monahanin mukaan valvonta on ihmisten tai ryhmien systemaattista seurantaa, jonka tarkoituksena on säädellä ja hallita näiden käyttäytymistä. Monahan, Surveillance as Cultural Practice, s. 498. The Sociological Quarterly 2011, s. 495–508.

672 *Saarinen,* Työsuhdeasioiden käsikirja I, s. 994.

673 *Kuokkanen – Alvesalo-Kuusi,* Työn elektroninen valvonta osana työntekijän hallinnan jatkumoa ja turvallistamista, s. 35 sekä *Mamia – Alvesalo-Kuusi – Kuokkanen – Virtanen,* Työn elektroninen valvonta Suomessa, s. 16.

henkilökohtaiseen vapauteen tai koskemattomuuteen puuttuviin toimenpiteisiin on mahdollista vain laissa säädetyin tavoin.[674]

Työelämässä yksilöllä ei ole ollut mahdollisuutta päättää, kenen kanssa hän on vuorovaikutuksessa. Työntekijälle on tärkeää sen kontrollointi, millaisena hän työyhteisössä näyttäytyy ja minkälaisten tietojen pohjalta häntä arvioidaan. Tämä pohjautuu hyvin pitkälti perusajatukseen itsemääräämisoikeudesta yksityisyyden perusarvona.[675] Yksityisyyttä suojataan työelämässä sen vuoksi, että työntekijällä on oikeus vapaasti muodostaa suhteita ja kehittyä työyhteisön täysiarvoisena jäsenenä. Tämä on myös tärkeä osa yksilön kunnioitusta. Henkilötietojen suojan näkökulmasta yksityisyyden suurin merkitys työelämässä on kuitenkin siinä, että se tasoittaa työnantajan ja työntekijän välistä tiedollista epätasapainoa.[676]

Työnantajan suorittaman valvonnan ja työntekijän alisteisen aseman vuoksi työntekijän yksityisyyden ja henkilötietojen suoja on ja tulee edelleen olemaan työelämässä runsaasti keskustelua herättävä aihe. Ajankohtaisuudesta kertoo myös biometristen tunnisteiden käytön yleistyminen työelämässä, esimerkiksi kulunvalvonnassa.[677] Näissä tilanteissa voi ilmetä perusoikeuksien ristiriitatilanteita.

---

674 *Kuokkanen – Alvesalo-Kuusi,* Elektroninen valvonta osana työntekijän hallinnan jatkumoa ja turvallistamista, s. 45.

675 Näin myös *Palm,* Privacy Expectations at Work – What is Reasonable and Why?, s.207.

676 Näin myös *Palm,* Privacy Expectations at Work – What is Reasonable and Why?, s. 209.

677 Biometristen tunnisteiden käyttö työelämässä on ollut kansainvälisesti esillä ILOn vuonna 2006 laatiman Seafarers´ Identity Documents Conventionin myötä. Doumbia-Henryn mukaan sopimus oli ensimmäinen kansainvälinen biometrisen tunnistamisen ohjelma. *Doumbia-Henry,* How biometrics helps the seafarers and world trade, s. 35–36.

Esimerkiksi biometrisen tunnistamisen avulla pyritään suojaamaan henkilökohtaisen vapauden ja koskemattomuuden piiriin kuuluvia perusoikeuksia. Samalla sillä kuitenkin puututaan voimakkaasti yksityisyyden suojaan kuuluviin perusoikeuksiin. Rajoitusten luonnetta on punnittava siten, että ne ovat hyväksyttäviä ja suhteellisia ja ettei niillä tehdä tyhjäksi perusoikeuksien ydinsisältöä. Yksityisyys ja henkilötietojen suoja ovat keskeinen osa myös työntekijän oikeuksia. Tästä syystä tässä jaksossa selvitetään, miten yksityisyyttä ja henkilötietoja suojataan työnantajan suorittamassa elektronisessa valvonnassa ja tämän käsitellessä työntekijän henkilötietoja, kuten biometrisia tunnisteita.

Laki yksityisyyden suojasta työelämässä (YksTL) tuli voimaan 1.10.2001.[678] Sitä on tämän jälkeen uudistettu, sillä ensimmäinen laki yksityisyyden suojasta työelämässä ei sisältänyt säännöksiä alkoholi- ja huumetestien käytöstä eikä teknisestä valvonnasta ja sähköpostin valvonnasta työpaikoilla. Näitä koskevat säännökset otettiin uuteen vuonna 2004 voimaan tulleeseen lakiin yksityisyyden suojasta työelämässä.

Työelämän osapuolille on tärkeää tietää, miten henkilötietojen käsittelyyn liittyviä kysymyksiä ratkaistaan työelämässä. Tämän vuoksi

678 Ruotsissa työelämän tietosuoja-asioita koskee yleislaki eli henkilötietolaki (Personuppgiftslag 1998:204), jota täydentää työelämän henkilötietojen käsittelyä koskevat erityissäännökset. Ruotsin lainsäädäntöön ei toistaiseksi sisälly erillistä lakia työelämän yksityisyydestä. Ruotsin hallitus asetti komitean valmistelemaan lainsäädäntöä yksityisyyden suojaan työelämässä vuonna 1999. Komitean mietintö Personlig integritet i arbetslivet (SOU 2002:18) valmistui vuonna 2002. Lain tarpeellisuudesta on uudestaan käyty keskustelua vuonna 2009, kun annettiin uusi komitean mietintö Integritetsskydd i arbetslivet (SOU 2009:44). Toistaiseksi erityiselle työelämän tietosuojalaille ei kuitenkaan ole nähty tarvetta.

tarvitaan erityislainsäädäntöä nimenomaan työelämän alueelta. Lain tarkoituksena on turvata toisaalta työnhakijoiden ja työntekijöiden yksityisyyden suojaa sekä toisaalta ottaa huomioon työnantajan toimintaan liittyvä tarve kerätä henkilötietoja.

Yksityisyyden suojasta työelämässä annetun lain säätämisen taustalla vaikuttaa näkemys siitä, että henkilötietolaki ei riittävästi vastaa kaikkiin työelämän erityispiirteistä aiheutuviin yksityisyyden suojaa koskeviin ongelmiin. Henkilötietolain mukaiset henkilötietojen käsittelyn edellytykset ovat monelta osin varsin yleisiä ottaen huomioon ne tarpeet, joita toisaalta työntekijän yksityisyyden suojaaminen ja toisaalta työelämän tarpeet edellyttävät.[679]

Lain tavoitteena on mahdollisimman hyvän yksityisyyden suojan turvaaminen työnhakijoille, työntekijöille ja virkamiehille ottaen huomioon työelämän erityistarpeet ja -piirteet. Lain tarkoituksena on myös yksityisyyden suojaa koskevien perusoikeuksien toteuttaminen ja menettelytapojen säänteleminen kerättäessä henkilötietoja työelämässä.

5.5.1.2. Lain tarkoitus ja soveltamisala

Lain tarkoituksena on yksityiselämän suojan ja muiden yksityisyyden suojaa turvaavien perusoikeuksien toteuttaminen työelämässä. Lisäksi lain tarkoituksena on edistää hyvän tietojenkäsittelytavan noudattamista ja kehittämistä käsiteltäessä sekä työnhakijoiden että työntekijöiden henkilötietoja työelämässä. Lakia sovelletaan työntekijää koskevien henkilötietojen käsittelyyn. Tämän lisäksi laissa säädetään muun muassa teknisestä valvonnasta työpaikalla.

679 Työntekijän alisteinen asema suhteessa työnantajaan oli yksi sellainen seikka, joka tuli huomioida. Normaalitilanteessa rekisteröity ja rekisterinpitäjä toimivat yleensä toisiinsa nähden tasavertaisemmassa asemassa kuin työntekijä ja työnantaja. HE 75/2000 vp, s. 3.

Laki täydentää henkilötietolakia, joka on henkilötietojen käsittelyn yleislaki.[680] Yleislakina henkilötietolaki ei kuitenkaan ratkaise kaikkia henkilötietojen käsittelyyn eri aloilla liittyviä yksittäisiä kysymyksiä. Työelämän osapuolille, työnantajille ja työntekijöille, on tärkeää tietää, miten henkilötietojen käsittelyyn liittyviä kysymyksiä ratkaistaan nimenomaan työelämässä. Lain tarkoituksena on turvata toisaalta työnhakijoiden ja työntekijöiden yksityisyyden suojaa sekä toisaalta ottaa huomioon työnantajan toimintaan liittyvä tarve kerätä henkilötietoja.

Yksityisyyden suojasta työelämässä annetussa laissa säädetään työelämän tilanteista henkilötietolakia täsmällisemmin. Henkilötietolaki sisältää kuitenkin yleisiä tietosuojaan liittyviä säännöksiä, jotka ovat sovellettavissa myös työelämään. Näitä säännöksiä ei ole katsottu tarpeelliseksi sisällyttää erityislainsäädäntöön.[681] Syynä on se, että henkilötietolaissa säädetyistä seikoista ei ole tarpeen eikä asianmukaista ottaa säännöksiä erityislakeihin.[682] Tämän vuoksi laissa käytetään muun muassa henkilötietojen käsittelyyn liittyvää käsitteistöä merkityssisällöltään samana kuin henkilötietolaissa. Biometriset tunnisteet ovat henkilötietolaissa tarkoitettuja henkilötietoja. Niiden hyödyntämisessä työelämässä tulee tämän vuoksi huomioida sekä henkilötietolain että yksityisyyden suojasta työelämässä annetun lain säännökset.

680 Raatikainen on sanonut asian seuraavasti: HetiL koskee jokaisen Suomessa toimipaikan omaavan työnantajan toimintaa, sillä siinä ei ole mitään rajoituksia esimerkiksi henkilöstön määrän tai toimialan suhteen. *Raatikainen,* Yksityisyyden suoja työelämässä, s. 19.

681 HE 75/2000 vp, s. 14.

682 *Oikeusministeriö,* Lainkirjoittajan opas (2013), s. 233.

5.5.1.3. Henkilötietojen käsittelyn yleiset edellytykset YksTL:n mukaan

Tarpeellisuusvaatimus. Henkilötietojen suojaa koskevan lainsäädännön pyrkimyksenä on mahdollisimman avoimen tietojen käsittelyn toteuttaminen, mutta toisaalta myös se, että vain tarpeellisia tietoja kerätään.[683] Jokaisella on lähtökohtaisesti oikeus määrätä itse omien henkilötietojensa käytöstä ja luovuttamisesta. Tämä on osa yksilön tiedollista itsemääräämisoikeutta. Tarpeettoman aineiston luovuttamisen ja kokoamisen ristiriita on erityisen hyvin esillä työelämässä. Työntekijä ei kuitenkaan alisteisen asemansa vuoksi voi käyttää itsemääräämisoikeuttaan täysin vapaasti. Tällöin kysymyksessä ei toisin sanoen ole vapaasti annettu tietoinen suostumus, sillä riittävää tasapainoa osapuolten välillä ei ole. Tämä on myös yksi syy siihen, miksi on ollut tarpeen säätää erillinen tarpeellisuusvaatimus työelämän henkilötietojen käsittelyä varten. Se on osa heikomman ja vahvemman välisen suhteen tasapainottamista.

Pelkistetysti asia voidaan sanoa siten, että työnantajan ja työntekijän välisessä suhteessa tietyt asiat ja tiedot ovat työntekijän yksityisasioita, jotka eivät kuulu työnantajalle, ellei siihen ole erityistä perustetta. Tämän vuoksi työnantaja saa käsitellä vain välittömästi työn kannalta tarpeellisia henkilötietoja. Näiden tietojen tulee lisäksi liittyä osapuolten oikeuksien tai velvollisuuksien hoitamiseen, työntekijöille tarjottaviin etuuksiin tai johtua erityislainsäädännöstä. Tarpeellisuusvaatimus on ehdoton, sillä siitä ei voida poiketa edes työntekijän suostumuksella.[684] Sen on toisin sanoen aina toteuduttava työnhakijan ja työnteki-

683 *Koskinen,* Yksityisyyden suoja työelämässä, s. 352

684 Tarpeellisuusvaatimus sisältyi jo vuoden 2001 lakiin. Lain uudistamisen yhteydessä tarpeellisuusvaatimusta koskeva säännös säilyi asiasisällöltään ja sanamuodoltaan samana, mutta se erotettiin omaksi momentikseen. Tällä haluttiin korostaa tarpeellisuusvaatimuksen ehdottomuutta. TyVM 8/2004, s. 5.

jän henkilötietoja käsiteltäessä. Työnantaja saa rekisterinpitäjänä pitää yllä vain tarpeellisia rekistereitä ja niissä tarpeellisia tietoja.[685] Työntekijän suostumus ei siis voi syrjäyttää tarpeellisuusvaatimusta, koska suostumukselle ei työntekijän alisteisen aseman vuoksi voida antaa täysin vapaaseen tahdonmuodostukseen perustuvaa merkitystä.[686]

Tarpeellisuusvaatimus rajoittaa työnantajan oikeutta käsitellä henkilötietoja. Työnantajan on henkilötietolain velvoitteiden mukaisesti ennalta määriteltävä ne tarkoitukset, joihin tietoja kerätään. Näiden tarkoitusten on myös oltava nimenomaisia ja laillisia. Lisäksi käsittelyn tarkoituksesta tulee ilmetä, minkälaisten tehtävien hoitamiseksi henkilötietoja kerätään.[687]

Työelämässä esiintyvät tilanteet ovat kuitenkin erilaisia ja kerättävien henkilötietojen määrä ja laatu vaihtelevat riippuen työstä ja työtehtävistä. Tarve henkilötietojen keräämiselle voi johtua muun muassa viranomaisista, asiakkaista, työympäristöstä, henkilöstöhallinnosta ja organisaation kehittämisestä.[688] Tietojen tarpeellisuus määrittyy tämän vuoksi tapaus- ja työntekijäkohtaisesti. Työnantajan tulee itsenäisesti ratkaista tiedon tarpeellisuus ja myös pystyttävä perustelemaan se lain edellyttämällä tavalla.[689] Työnantajan on joka tapauksessa voitava perustella kerättävien henkilötietojen tarpeellisuus välittömästi työ-

685 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2003), s. 357

686 *Raatikainen,* Yksityisyyden suoja työelämässä, s. 125.

687 Näin myös *Raatikainen,* Yksityisyyden suoja työelämässä, s. 126.

688 *Koskinen – Alapuranen – Heino – Salli,* Henkilötietojen käsittely työelämässä, s. 105.

689 Tarpeellisuusvaatimuksella on liittymä myös työnhakijoiden ja työntekijöiden syrjintäsuojaan, koska työsuhteen kannalta tarpeettomien tietojen kerääminen voi johtaa joissakin tilanteissa syrjintään. HE 75/2000 vp, s. 17.

suhteen kannalta. Harkittaessa keräämistä on syytä ”testata”, pystyykö tarpeellisuuden perustelemaan.[690]

Välittömästi työsuhteen kannalta tarpeellisina tietoina pidetään työtehtävien suorittamisen, työntekijän valinnan, työolosuhteiden, työ- ja virkaehtosopimusten tiettyjen määräysten toteuttamisen sekä lainsäädännön edellyttämiä tietoja.[691] Tarpeellisuusvaatimuksen sanamuodolla korostetaan sitä, että käsiteltävien henkilötietojen tulee liittyä osapuolten oikeuksien ja velvollisuuksien hoitamiseen.[692] Tarpeellisuusvaatimus tuleekin nähdä henkilötietojen käsittelyn punaisena lankana, joka kulkee lain läpi. Tarpeellisuusvaatimus vaikuttaa siihen, millaisia henkilötietoja on lupa kerätä ja muutoin käsitellä.[693] Tässä tapauksessa käyttötarkoitus on työsuhde eli työnantajan tulee perustella kerättävien henkilötietojen tarpeellisuus juuri työsuhteen kannalta.

Tarpeellisuusvaatimuksen tulkinta YksTL:n osalta on HetiL:n tulkintaan nähden tiukempaa.[694] Syynä tiukempaan sanamuotoon on työntekijän alisteinen asema suhteessa työnantajaan. Työsuhteessa työnantaja on vahvemmassa asemassa työntekijään nähden, minkä

690 HE 75/2000 vp, s. 15 ja *Raatikainen,* Yksityisyyden suoja työelämässä, s. 125.

691 Työelämän monimuotoisuuden vuoksi on mahdotonta luetella välittömästi työsuhteeseen liittyviä tarpeellisia henkilötietoja tyhjentävästi. Tämä on todettu myös YksTL:a koskevassa hallituksen esityksessä sekä ILOn työntekijöiden henkilötietojen suojaamista koskevan ohjeiston selostusosassa. Katso HE 75/2000 vp., s. 15 sekä Kansainvälisen työjärjestön (ILO:n) ohjeistus, Työntekijöiden henkilötietojen suojaaminen.

692 HE 75/2000, s. 15

693 HaVL 2/2001, s. 3.

694 *Koskinen – Alapuranen – Heino – Salli,* Henkilötietojen käsittely työelämässä, s. 106

vuoksi henkilötietojen käsittelyn edellytystenkin tulee olla tiukemmat.[695]

Tarpeellisuusvaatimus on asetettu henkilötietojen käsittelyn edellytykseksi jo henkilötietolaissa. Henkilötietolain mukaiset henkilötietojen käsittelyn edellytykset ovat monilta osin kuitenkin varsin yleisiä ottaen huomioon ne tarpeet, joita toisaalta työntekijän yksityisyyden suojaaminen ja toisaalta työelämän tarpeet edellyttävät. Työntekijöitä koskevien välittömästi työsuhteeseen liittyvien henkilötietojen tarpeellisuusvaatimuksella varmistetaan työntekijöiden yksityisyyden suojan riittävä taso.[696] Samalla sillä on pyritty sovittamaan yhteen työnantajan tarve käsitellä työntekijän henkilötietoja ja työntekijän tarve näiden tietojen suojaamiseen. Työsuhde edellyttää toimiakseen kuitenkin tietojen luovuttamista tietyssä määrin työnantajan käyttöön.[697]

Tarpeellisuusvaatimus on niin keskeinen henkilön yksityisyyden suojan kannalta, että sitä on tämän vuoksi tarpeen korostaa henkilötietolaissa säädetyn vaatimuksen lisäksi.[698] Työelämän henkilötietojen käsittelyn erityislakina YksTL:n tarpeellisuusvaatimus syrjäyttää henkilötietolain säännöksen tarpeellisuusvaatimuksesta ja tulee sovellettavaksi työnantajan ja työntekijän välisessä suhteessa henkilötietolain tarpeellisuusvaatimuksen sijaan.

Biometrisen tunnistamisen käytön tulee olla nimenomaan työsuhteen kannalta tarpeellista eikä tästä vaatimuksesta voida poiketa edes työntekijän suostumuksella. Biometrisen tunnisteen antamatta jättäminen ei saa johtaa työntekijän kannalta haitallisiin seuraamuksiin.

---

695 HE 75/2000 vp, s. 17.

696 HE 75/2000 vp, s. 3.

697 HE 75/2000, s. 15 sekä *Koskinen – Alapuranen – Heino – Salli,* Henkilötietojen käsittely työelämässä (2005), s. 103. Katso myös *Raatikainen,* Yksityisyyden suoja työelämässä, s. 127.

698 HE 75/2000 vp, s. 15 ja *Raatikainen,* Yksityisyyden suoja työelämässä, s. 127.

Työntekijä voi jättää antamatta sellaisia tietoja, jotka eivät ole työsuhteen osapuolten oikeuksien ja velvollisuuksien kannalta tarpeellisia.

Tarpeellisuusvaatimuksen kohdalla tulee myös huomioida vähimmän puuttumisen periaate. Henkilötietoja käsiteltäessä työnantajan ei tule puuttua työntekijän yksityisyyteen enempää kuin on välttämätöntä toimenpiteiden tarkoituksen saavuttamiseksi. Tämä käy erityisen hyvin ilmi Euroopan neuvoston työelämää koskevasta suosituksesta. Suosituksen mukaan työnantajien palvelussuhteen hoitamiseksi keräämien henkilötietojen on oltava asiaan liittyviä eivätkä ne saa olla liian laajoja, kun otetaan huomioon työsuhteen laatu sekä työnantajan kehittyvät tiedontarpeet.[699] Vähimmän puuttumisen periaatteen mukaisesti biometristen tunnisteiden käsittely edellyttää siten työnantajalta painavampia perusteita kuin niin sanottujen tavallisten henkilötietojen käsittely.

Esimerkiksi Norjan tietosuojaviranomainen on ratkaisukäytännössään katsonut, ettei biometrisen tunnistamisen käyttäminen työajan- ja kulunvalvonnassa täytä tarpeellisuusvaatimusta. Syynä tähän on se, että sama tavoite on saavutettavissa vähemmän työntekijän yksityisyyteen puuttuvin keinoin. Pelkästään se, että biometrinen tunnistaminen on helpompaa ja tehokkaampaa, ei riitä oikeuttamaan sen käyttöä.[700]

Työntekijä ensisijainen tietolähde. Henkilötietojen keräämisen lähtökohtana on se, että tiedot tulee hankkia rekisteröidyltä itseltään. Vain rekisteröidyn suostumuksella tietoja on lupa kerätä muualta. Tämä on voimassa myös työelämän henkilötietojen käsittelyssä.[701]

---

699 Euroopan Neuvosto, Protection of personal data used for employment purposes.

700 PVN-2006-11 REMA 1000 - fingeravtrykk ved registrering av timer.

701 Henkilötietolakia vastaavasti tietojen keräämisellä työelämässä tarkoitetaan sellaista järjestelmällistä toimintaa, jonka tarkoituksena on manuaalisen käsittelyn avulla muodostaa työnhakijoista ja työnteki-

Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, työntekijältä on hankittava suostumus tietojen keräämiseen. Vain poikkeuksellisesti, kuten viranomaisten luovuttaessa tietoja työnantajalle tämän laissa säädetyn tehtävän suorittamiseksi, suostumus voidaan jättää hankkimatta (YksTL 4 §). Ulkopuolisilta hankittavat henkilötiedot tarkoittavat kaikkia HetiL:ssa määriteltyjä henkilötietoja niiden keräämistavasta riippumatta. Siten ne koskevat myös tietoja, joita kerätään muun muassa tietoverkosta.[702]

Tarkoituksena on sen takaaminen, että työntekijä on selvillä henkilötietojensa käsittelystä.[703] Tällä tavoin taataan myös työntekijän oikeus tulla arvioiduksi oikeiden tietojen perusteella. Vaatimus on läheisessä yhteydessä tarpeellisuusvaatimukseen, sillä kerättävien henkilötietojen tulee aina olla välittömästi työsuhteen kannalta tarpeellisia. Suostumuksellakaan ei voida kerätä tarpeettomia tietoja.

Vaatimus tietojen keräämisestä ensisijaisesti työntekijältä itseltään kuvaa sitä, että tiedollinen itsemääräämisoikeus on voimassa myös työelämässä. Työelämän yksityisyyteen kuuluu työntekijän mahdollisimman suuri oikeus tietää ja päättää omiin henkilötietoihinsa liittyvästä

---

jöistä henkilörekisteri tai sen osa tai käsitellä tietoja automaattisen tietojenkäsittelyn avulla. HE 75/2000 vp, s. 17.

702 *Raatikainen,* Yksityisyyden suoja työelämässä, s. 213. Katso myös HE 75/2000 vp. Tietosuojavaltuutettu on ratkaisussaan katsonut, että niin sanotusti googlaamalla tapahtuvaa henkilötietojen keräämistä ja tallettamista voidaan pitää työelämän tietosuojalain 4 §:n ja henkilötietolain 5 §:n, 6 §:n ja 9 §:n vastaisena menettelynä. Tietosuojavaltuutettu, Henkilötietojen kerääminen internetistä hakukoneen avulla ns. Googlaamalla työnantajan toimesta ja tietojen poistaminen google-hakukoneesta.

703 HE 75/2000 vp, s. 17

käsittelystä, tietää omien henkilötietojensa sisällöstä ja oikeus tulla arvioiduksi oikeiden henkilötietojen perusteella.[704]

Työntekijän oikeuksien näkökulmasta ongelmallista on se, että työnantaja voi tietyissä tilanteissa sivuuttaa suostumuksen ensisijaisuuden. Mikäli työntekijä ei sanottua suostumusta anna tai sitä on asian laatu huomioon ottaen mahdotonta pyytää häneltä, on työnantajalla oikeus hankkia tietoja ilman suostumustakin kahdella edellytyksellä. Ensinnäkin tietojen on oltava tarpeellisuusvaatimuksen mukaisesti välittömästi työsuhteen kannalta tarpeellisia. Toiseksi niiden hankintaan on oltava selvä peruste.[705] Epäselväksi kuitenkin jää, minkälaisissa tilanteissa nämä poikkeukset tulevat sovellettaviksi.

Biometristen tunnisteiden näkökulmasta asia tulee nähdä siten, että biometrisia tietoja ei ole lupa kerätä muualta kuin työntekijältä itseltään. Tämä on työntekijän itsemääräämisoikeuden näkökulmasta ainoa lähtökohta. Biometristen tunnisteiden kohdalla työntekijällä on korostettu oikeus tietää omien tietojensa käsittelystä, sillä nämä tiedot ovat korostetun henkilökohtaisia.

Tällä hetkellä on kuitenkin vaikea ajatella tilanteita, joissa biometrisia tunnisteita on mahdollista kerätä muualta ilman työntekijän suostumusta. Osa biometrisen tunnistamisen menetelmistä mahdollistaa kuitenkin jo nykyään tunnisteiden keräämisen ja käytön ilman vuorovaikutusta. Biometrisen tunnistamisen menetelmien käytön yleistyessä ja kehittyessä kielto näiden tietojen keräämisestä ilman suostumusta saa korostuneen merkityksen.

---

704 HE 75/2000 vp, s. 4-5 ja *Raatikainen,* Yksityisyyden suoja työelämässä, s. 211.

705 Laissa määritellään näin henkilötietolakia tarkemmin työnantajan oikeus kerätä työntekijän suostumuksetta ulkopuolisilta henkilötietoja ottaen erityisesti huomioon työelämän lähtökohdat ja työntekijöiden suojelun tarve. HE 75/2000 vp, s. 17.

Yhteistoimintamenettely. Tietojärjestelmien kehittymisen ansiosta työnantajilla on käytössään erilaisia valvontajärjestelmiä työprosessien organisointia taikka asiakaspalvelua ja omaisuuden suojelemista varten. Mahdollisuus työntekijöiden ja työprosessien valvontaan erilaisten teknisten laitteiden avulla lisää riskiä käyttää saatua tietoa epäasianmukaisella tavalla.

Tärkeää on säätää menettelytavoista valvonnan järjestämisessä. Työelämässä tarkoituksenmukaisin ratkaisu on yhteistoiminnan vaatimus. Yhteistoimintaa koskevan lainsäädännön tarkoituksena on lisätä työntekijöiden mahdollisuuksia vaikuttaa työtään koskevien asioiden käsittelyyn. Yhteistoiminnan keskeisenä tavoitteena on, että yritysten toiminta ja toimintaympäristö sekä tuottavuus paranevat, kun työympäristössä vallitseva luottamus ja avoin vuorovaikutus lisääntyvät. Tämä toteutuu, kun yhteistoiminta perustuu oikea-aikaisesti henkilöstölle annettuihin riittäviin tietoihin työnantajan suunnitelmista.[706]

Yhteistoiminnalla toteutetaan omalta osaltaan henkilötietolain ja yksityisyyden suojasta työelämässä annetun lain tavoitteita avoimuuden lisäämisestä henkilötietojen käsittelyssä. Keskeinen ajatus yhteistoimintalainsäädännössä onkin, että ennen kuin työnantaja tekee päätöksen tietyissä työntekijöitä koskevissa asioissa, on yrityksessä käytävä yhteistoimintamenettely.[707] Menettelyn piiriin kuuluvat asiat on määritelty joko yhteistoimintalaissa tai yksityisyyden suojaa koskevassa erityislainsäädännössä.

Näiden tavoitteiden toteuttamiseksi työnantajalle on asetettu velvollisuus neuvotella työntekijöiden tai heidän edustajan kanssa muun muassa henkilötietojen käsittelystä ja teknisin menetelmin toteutetus-

706 Näin myös *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2009), s. 171. Yhteistoimintamenettelyistä ja neuvotteluista tarkemmin katso *Hietala – Kaivanto,* Uusi yhteistoimintalaki käytännössä.

707 *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2009), s. 170.

ta valvonnasta. Työnantajan on yksimielisyyden saavuttamiseksi ennen päätöksentekoa neuvoteltava henkilötietojen käsittelyn ja teknisin menetelmin toteutetun valvonnan perusteista, vaikutuksista ja vaihtoehdoista niiden työntekijöiden tai heidän edustajiensa kanssa, joita asia koskee. Lopullinen päätösvalta säilyy kuitenkin työnantajalla eli työnantaja voi tehdä asiassa päätöksen myös ilman yksimielisyyttä.[708] Yt- menettelyssäkään ei kuitenkaan voida sopia sellaisten tietojen keräämisestä tai teknisten valvontamenetelmien käytöstä, jotka eivät täytä lain tarpeellisuusvaatimusta.[709] Myös valvonnan kautta saatujen tietojen tulee täyttää tarpeellisuusvaatimus.[710]

Yhteistoimintavelvoitteeseen on kuitenkin otettu soveltamisalarajoitus. Yhteistoimintavelvoitetta ei edellä mainittujen asioiden kohdalla ole, jos työsuhteessa säännöllisesti työskenteleviä on alle 30. Teknisin menetelmin toteutetun valvonnan kohdalla työnantajan on kuitenkin vähintään kuultava työntekijöitä tai heidän edustajia. Henkilötietojen käsittelyn kohdalla vastaavaa velvollisuutta ei ole annettu.

Työntekijöiden henkilötietojen käsittelyä koskevia asioita on käsiteltävä yhteistoimintamenettelyssä (YksTL 4 § 3 mom. ja YTL 15 §:n 3 k). Henkilötietoja kerättäessä työnatajan on yhteistoimintalainsäädännön mukaisesti toimittava yhdessä työntekijöiden tai henkilöstön edustajien kanssa henkilötietojen suojaamisen ja työntekijöiden yksityisyyden varmistamiseksi. Ennen kuin työnantaja ratkaisee yhteistoimintamenettelyn piiriin kuuluvan asian, tulee tämän neuvotella toimenpiteen perusteista, vaikutuksista ja vaihtoehdoista niiden työntekijöiden kanssa, joita asia koskee.[711]

---

708 *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2009), s. 170.

709 HE 162/2003 vp, s. 8.

710 Työ- ja elinkeinoministeriö, Työelämän tietosuoja –opas, s. 18.

711 *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2009), s. 171.

Yhteistoimintamenettelyn tarkoituksena on työnantajan ja työntekijöiden välinen yhteistyö, jota tulee noudattaa myös henkilötietojen suojaa koskevissa asioissa. Henkilötietojen käsittelyä koskevien asioiden kuuluminen yhteistoimintamenettelyjen piiriin lisää myös avoimuutta, sillä menettelyn kautta työntekijä saa selville, millä tavoin hänen henkilötietojaan käsitellään. Menettely turvaa omalta osaltaan työntekijöiden oikeuksia työnantajan käsitellessä heidän henkilötietoja.

Henkilötietojen kerääminen käsitellään yhteistoimintamenettelyssä sen mukaisesti, miten ja millaisia tietoja on tarkoitus kerätä. Menettelyssä on ainakin käytävä läpi se, mitä tietoja työntekijästä kerätään sekä millä tavoin ja mistä lähteestä tietoja on tarkoitus kerätä.[712] Työntekijän kannalta oleellista on sen läpikäyminen, miksi henkilötietoja kerätään. Yhteistoimintamenettelylläkään ei voi poiketa henkilötietojen käsittelyä koskevista pakottavista lain säännöksistä. Tämä tarkoittaa muun muassa sitä, että kaiken työntekijöistä kerättävien tietojen on oltava välittömästi työsuhteen kannalta tarpeellista.[713]

Yhteistoiminnan piiriin kuuluu myös teknisin menetelmin toteutettu valvonta. YksTL:n voimaan tulon myötä yhteistoimintamenettelyn piiriin kuuluviksi asioiksi lisättiin henkilöstöön kohdistuvan teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät (YTL 19 §:n 3 k ja YksTL 21 §). Työnantajalla on lisäksi velvollisuus määritellä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus ja siinä käytettävät menetelmät yhteistoimintamenettelyn jälkeen. Lisäksi työnantajalla on velvollisuus tiedottaa työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä (YksTL 21 §). Henkilöstöön kohdistuvan teknisin menetelmin toteutetun val-

712 *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2004), s. 157.

713 *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2009), s. 172.

vonnan tarkoitus on lähinnä työturvallisuuden varmistaminen, työajan ja työsuorituksen valvonta tai rikollisuuden torjunta. Valvontamenetelmänä voi olla esimerkiksi biometrinen tunnistaminen osana työpaikan kulunvalvontaa.

Yhteistoimintalain valvontaa koskeva säännös ei kuitenkaan itsessään luo työnantajalle oikeutta työntekijöiden valvontaan, vaan on puhtaasti menettelytapasäännös. Sillä toisin sanoen ohjataan työnantaja noudattamaan tiettyä menettelyä valvonnan toteuttamisessa.[714] Valvonnan oikeutus itsessään ratkeaa erikseen muun muassa rikoslain nojalla.

Erityisesti teknisin menetelmin toteutetussa valvonnassa tiedottaminen on keskeinen vaatimus. Työntekijöillä on oikeus tietää, miksi, milloin ja miten heitä valvotaan. Työnantajan työnjohto- ja valvontaoikeus ei oikeuta käyttämään salaista valvontaa työpaikalla. Yksilön oikeus tietää valvonnasta osana yksityisyyden suojaa on tässä suhteessa vahvempi kuin työnantajan oikeus valvoa työn tekoa ja laatua.

Biometristen tunnisteiden käyttäminen työelämässä tulee siis käsitellä yhteistoimintamenettelyssä ennen niiden käyttöönottoa. Työnantajan tulee neuvotella henkilöstön edustajien kanssa yhteistoimintamenettelyssä esimerkiksi päättäessään biometriseen tunnistamiseen perustuvien kulunvalvontajärjestelmien käyttöönotosta.[715] Tällä tavoin taataan henkilötietojen käsittelyn avoimuus työelämässä ja turvataan työntekijän oikeutta yksityisyyteen ja henkilötietojen suojaan.

Ongelmallista yhteistoimintavelvoitteessa biometristen tunnisteiden kohdalla on kuitenkin se, että työnantajalla on viime kätinen oikeus päättää järjestelmän käyttöönotosta. Tämä ei saa johtaa siihen,

---

714 Tähän on myös perustuslakivaliokunta kiinnittänyt huomiota lausunnossaan PeVL 27/2000. Katso myös *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2009), s. 172 sekä Työ- ja elinkeinoministeriö, Työelämän tietosuoja –opas, s. 18.

715 Näin myös *Saarinen,* Työsuhdeasioiden käsikirja I, s. 995

että työnantaja jättää huomiotta työntekijöiden mielipiteet asiassa. Tällöin vaarana on, että yhteistoimintavelvoite muuttuu vain moraaliseksi velvollisuudeksi.[716] Varsinkin biometrisen tunnistamisen kohdalla työnantajan viimekätisen päätösvallan tulee olla mahdollisimman rajoitettua. Syynä tähän on se, että yhteistoimintamenettelyllä ei ole mahdollista korvata työntekijän henkilökohtaista suostumusta, jos sellainen tarvitaan.

Biometrisen tunnistamisen kohdalla erittäin suuri painoarvo tuleekin antaa työntekijän oikeuksille biometristen tunnisteiden erityispiirteiden vuoksi. Tulkintaa tukee vähimmän puuttumisen periaate osana suhteellisuusperiaatetta. Työnantajan tulee valita käytettävissä olevista vaihtoehdoista se, jolla on vähiten vaikutuksia työntekijän yksityisyydelle. Tällainen velvollisuus on asetettu työnantajalle esimerkiksi kameravalvonnan kohdalla.

Biometristen tunnisteiden käyttäminen ei voi olla ensisijainen vaihtoehto ja sen käyttö tulee rajata vain välttämättömään. Työntekijällä tulee myös olla oikeus jättäytyä biometrisen tunnistamisen ulkopuolelle ilman negatiivisia seurauksia. Työntekijä on kuitenkin yleensä sellaisessa asemassa, että jättämällä antamatta työnantajan vaatimia henkilötietoja, kuten biometrisia tunnisteita, hän voi vaarantaa työpaikkansa. Tarpeellisuusvaatimus yhdessä vähimmän puuttumisen periaatteen kanssa mahdollistavat joka tapauksessa sen, että työntekijä voi jättää antamatta sellaisia henkilötietoja, jotka eivät liity välittömästi työsuhteeseen tai joita ei ole tarkoituksenmukaista käsitellä aiottuun tarkoitukseen.

716 Nyyssölän mukaan yhteistoimintavelvoite ei ole vain muodollisuus, koska työnantaja voidaan tuomita rangaistukseen tämän velvollisuuden laiminlyömisestä. *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2009), s. 171.

Ruotsin tietosuojaviranomainen (Datainspektionen) on esimerkiksi vuonna 2010 antamassaan ratkaisussa todennut työntekijöiden sormenjälkeen perustuvan sisäänkirjautumis- ja työajanseurantajärjestelmän olevan sallittu. Tämä kuitenkin edellyttää, että työntekijät antavat suostumuksensa ja että järjestelmä ei ole pakollinen eli järjestelmälle on oltava vaihtoehto. Vaihtoehtoisen tavan valinneille ei myöskään saa tulla minkäänlaisia negatiivisia seurauksia. [717] Käytännössä tämä tarkoittaa sitä, että käytettäessä biometrisia tunnisteita työelämässä tulee käytössä olla myös vaihtoehtoinen, vähemmän työntekijän yksityisyyteen puuttuva keino tarkoituksen tavoitteiden saavuttamiseksi. Järjestelmän käytön tulee myös perustua vapaaehtoisuuteen.

On aiheellista pohtia, tuleeko työnantajan ylipäätään voida päättää biometrisen tunnistamisen käytöstä pelkästään osana työnjohto- ja valvontaoikeutta. Kameravalvonnan kohdalla on esimerkiksi katsottu, ettei sen käyttö voi perustua työnantajan työnjohto- ja valvontaoikeuteen, koska siitä on säädetty laissa.[718] Biometrinen tunnistaminen kuitenkin eroaa kameravalvonnasta siinä, ettei biometrisen tunnistamisen käytöstä ole laissa tarkentavia säännöksiä.

Ongelmallista on se, että biometristen tunnisteiden käyttämisen perustuessa työnantajan työnjohto- ja valvontaoikeuteen työnantajan on mahdollista kohdistaa negatiivisia seurauksia työntekijään tämän kieltäytyessä käyttämästä biometrisen tunnistamisen järjestelmää. Tällainen muodostaa työntekijälle eräänlaisen välillisen pakon biometristen tunnisteiden antamiselle.

Biometrisella tunnistamisella puututaan työntekijän henkilöön eli kysymys on fyysisen koskemattomuuden piiriin kuuluvasta asiasta. Fyysisen koskemattomuuden suojan tarkoitus on suojata henkilöön

717 Datainspektionen, Tillsyn enligt personuppgiftslagen (1998:204, Dnr 1765-2009) – användning av biometri inom arbetslivet.

718 PeVL 10/2004, s. 6.

kohdistuvilta tarkastuksilta ja pakolla toteutettavilta lääketieteellisiltä ja muilta toimenpiteiltä. Henkilön fyysiseen koskemattomuuteen puuttuminen edellyttää aina suostumusta tai menettelyn oikeuttavaa sääntelyä.

Esimerkiksi henkilö- ja soveltuvuusarviointitestien tekemisen edellytykseksi on YksTL 13 §:ssä asetettu työntekijän suostumus. Työntekijän testauksessa lähtökohtana on suostumus testiin. Tätä vaatimusta tulee soveltaa myös biometriseen tunnistamiseen. Kysymys on työntekijän fyysiseen ja henkiseen koskemattomuuteen puuttuvasta menetelmästä.[719] On siis yksilön oikeuksien näkökulmasta ongelmallista, että kulunvalvonnasta päättäminen on katsottu kuuluvaksi työnantajan työnjohto- ja valvontaoikeuteen.[720] Tämän ei ainakaan toistaiseksi ole

719 Myös puhallustestit osana alkoholitestejä ovat aiheuttaneet tulkinnallisuutta. YksTL ei puhalluskokeisiin ota kantaa. Työnantajalla ei kuitenkaan ole oikeutta puhallustestin tekemiseen. Syynä on se, että asia on jätetty terveydenhuollon palvelujen käyttämiseen velvoittavan säännöksen ulkopuolelle, jolloin puhalluttamisoikeudelta puuttuu perusoikeuden rajoittamiseksi vaadittava lainsäädäntötasoinen peruste. *Korhonen – Koskinen – Ojanen – Pesonen,* Työelämän uusi tietosuoja (2004), s. 54. Vertaa *Nyyssölä,* Yksityisyyden suoja työsuhteessa (2004), s. 100 ja Raatikainen Yksityisyyden suoja työelämässä (2002), s. 169.

720 Tämän on todennut työtuomioistuin antamissaan ratkaisuissa TT 2001-60 ja T:1999-31. Vertaa kuitenkin tietosuojavaltuutetun ratkaisu Internetin käytön ja työntekijöiden verkkoselailun eli ns. verkkosurffailun valvonta työpaikalla. Ratkaisussa tietosuojavaltuutettu on kannanottonaan ja yleisenä ohjauksena todennut, että työntekijöiden verkkoselailusta eli ns. verkkosurffailusta muodostuvia tunnistamistietoja ei saa käyttää työnantajan työn johto- ja valvontaoikeuden eli direktio-oikeuden nojalla siten, että työntekijöitä valvotaan, seurataan ja tarkkaillaan keräämällä ja/tai katsomalla näitä tunnistamistietoja.

katsottu olevan riippuvainen siitä, mitä menetelmää kulunvalvonnassa käytetään.

Tosiasia on, että biometrista tunnistamista käytetään työelämässä.[721] Testejä, analyysejä ja muita henkilön persoonallisuuden arviointiin tarkoitettuja menetelmiä ei kuitenkaan voi ilman erityislainsäädännön tukea käyttää muuten kuin työntekijän antamalla suostumuksella. Asia on yksityisyyden suojan näkökulmasta yksiselitteinen. HetiL 5 §:n perusteella työnantajan velvollisuutena on toimia rajoittamatta työntekijöiden yksityiselämän ja muita yksityisyyden suojaa turvaavia perusoikeuksia ilman laissa säädettyä perustetta. Nämä velvollisuudet viittaavat suoraan eräisiin perustuslaissa säädettyihin perusoikeuksiin. Työnantaja saa rajoittaa työntekijöiden perusoikeuksia ainoastaan, jos siitä on laissa säädetty.[722] Jos laillista perustetta ei ole löydettävissä, ei biometrisia tunnisteita tule käsitellä, vaikka se sinänsä olisi tarpeellinen.[723]

YksTL:n tarjoama mahdollisuus biometristen tunnisteiden käyttöön ei täytä täsmällisyydeltään niitä vaatimuksia, joita henkilötietojen suojaa koskevalta sääntelyltä on vakiintuneesti edellytetty. Biometristen tietojen käsittelyä koskevalle sääntelylle on esimerkiksi eduskunnan perustuslakivaliokunnan aikaisemmassa tulkintakäytännössä

721 *Saarinen,* Työsuhdeasioiden käsikirja I, s. 995.

722 Suomen perustuslain 1 §:n mukaan perustuslaissa vahvistettu, valtiosääntö, turvaa ihmisarvon loukkaamattomuuden ja yksilön vapaudet ja oikeudet ja edistää oikeudenmukaisuutta yhteiskunnassa. Nämä perustavanlaatuiset arvot ilmenevät positiivisissa perusoikeuksissakin, jotka tulee ottaa huomioon huolellisuusvelvolisuuden perusteella henkilötietoja käsiteltäessä. *Raatikainen,* Yksityisyyden suoja työelämässä, s. 83.

723 Raatikainen on todennut saman asian arkaluonteisten henkilötietojen osalta. *Raatikainen,* Yksityisyyden suoja työelämässä, s. 126.

asetettu selvästi tiukempia vaatimuksia kuin muiden henkilötietojen käsittelylle.[724]

Lainsäädännön puutteellisuus johtaa pohtimaan, onko biometrisen tunnistamisen käyttö työelämässä tällä hetkellä oikeutettua työnantajan työnjohto- ja valvontaoikeuden perusteella. Työntekijän oikeuksien näkökulmasta vastaus on kielteinen. Tätä tulkintaa puoltaa myös se, ettei työnantaja direktio-oikeutta käyttäessään saa loukata työntekijän perusoikeuksia, kuten henkilökohtaista koskemattomuutta ja henkilötietojen suojaa.[725] Direktion nojalla annetun käskyn (olennaisesti) loukatessa tällaisia oikeushyviä ei työnjohtokäsky ole oikeusjärjestyksen mukainen.[726] Mikäli työnantaja ylittää direktio-oikeutensa, työntekijä voi kieltäytyä noudattamasta työnantajan määräystä. Jos työnantaja tällaisessa tilanteessa irtisanoo tai purkaa työntekijän työsopimuksen, on kysymyksessä perusteeton irtisanominen tai purkaminen.[727]

724 Katso esimerkiksi PeVL 27/2005 vp., s. 3, PeVL 14/2009 vp., s. 3 ja PeVL 55/2010 vp., s. 2

725 *Saarinen,* Työsuhdeasioiden käsikirja I, s. 978. Tällaisessa tilanteessa on kysymys ns. direktiovallan objektiivisten rajojen ylittämisestä. Työntekijä ei voi direktion vuoksi luopua olennaisesti tai kokonaan henkilökohtaisista perusoikeuksistaan, kuten henkilökohtaisesta vapaudesta tai koskemattomuudesta. *Kairinen,* Työoikeus perusteineen (2001), s. 206.

726 *Kairinen,* Työoikeus perusteineen (2001), s. 206.

727 *Saarinen,* Työsuhdeasioiden käsikirja I, s. 993. Katso myös *Kairinen,* Työoikeus perusteineen (2001), s. 207.

5.5.2. Laki henkilötietojen käsittelystä poliisitoimessa

5.5.2.1. Yleistä

Biometrisia tunnisteita on hyödynetty rikostutkinnassa jo yli sadan vuoden ajan. Tämän seurauksena poliisin ylläpitämät tietojärjestelmät sisältävät laajan kokoelman biometrisia tunnisteita sormenjäljistä DNA- ja ääninäytteisiin. Rikostutkintatarkoituksessa kerättyjen biometristen tunnisteiden lisäksi poliisilla on oikeus käsitellä biometrisia tunnisteita niin sanottuihin hallinnollisiin tarkoituksiin, kuten passin myöntämistä varten. Näiden syiden vuoksi on tärkeää käydä läpi niitä edellytyksiä, joilla poliisi on oikeutettu käsittelemään biometrisia tunnisteita. Osa näistä oikeuksista myös poikkeaa henkilötietolaissa säädetyistä rekisterinpitäjän velvollisuuksista ja rekisteröidyn oikeuksista.

Laki henkilötietojen käsittelystä poliisitoimessa (PolHetiL) tuli voimaan 22.8.2003 ja se korvasi vuonna 1995 annetun lain poliisin henkilörekistereistä.[728] Poliisin henkilötietolakia on viimeisen kahdenkymmenen vuoden aikana uudistettu kokonaisuudessaan kolme kertaa. Viimeisin lain kokonaisuudistus tuli voimaan lokakuun alussa vuonna 2003. Lakia on tarkistettu ja muutettu lukuisia kertoja sen voimaantulon jälkeen. Esimerkkinä voidaan mainita passilain uudistuk-

728 Poliisin henkilörekisteritoimintaa aiemmin säännellyt poliisin henkilörekistereistä annettu laki tuli voimaan 1. päivänä lokakuuta 1995. Eduskunnan hallintovaliokunta edellytti, että yleisen henkilörekisterilain uudistamisen jälkeen eduskunnalle annetaan mahdollisimman pian lakiehdotus koskien poliisin henkilörekistereistä annetun lain uudistamista muun ohella siten, että lain tasolla säädetään riittävän yksityiskohtaisesti poliisin henkilörekistereistä, niihin talletetuista tiedoista, tietojen käyttötarkoituksesta ja tietojen säilytysajoista. HaVM 30/1997 vp.

sen – erityisesti siinä säädetty oikeus tallettaa biometrisia tunnisteita hallintoasiain tietojärjestelmään – aiheuttama lainsäädäntömuutos.

Lain yhtenä tavoitteena on parantaa yksilön oikeusturvaa poliisin toimesta tapahtuvassa henkilötietojen käsittelyssä. Perussäännös yksityiselämän ja henkilötietojen suojasta on perustuslain 10 §:ssä. Pykälän 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Säännökseen ei ole liitetty erityistä rajoituslauseketta. Yksityisyyden suojaamisen henkilötietojen käsittelyssä on näin katsottu edellyttävän aina laintasoista sääntelyä.[729] Tämä koskee myös tilanteita, joissa poliisi käsittelee henkilötietoja.

Laki sisältää yksityiskohtaiset ja tarkkarajaiset säännökset muun muassa rekisterien tietosisällöstä, rekisteriin merkittyjen tietojen säilytysajoista, kerättävien henkilötietojen käyttötarkoituksesta ja käyttötarkoituksesta poikkeamisesta, arkaluonteisten tietojen käsittelystä, rekisteröidyn informoinnista tietojen käsittelystä sekä rekisteröidyn tarkastusoikeuden käyttämisestä. Säännökset on pyritty kirjoittamaan niin selkeästi, että yksilö voi niiden perusteella ennakoida, miten poliisi tulee käyttämään toimivaltuuksiaan henkilötietojen käsittelyssä.[730]

Tässä tarkoituksessa laki sisältää muun muassa tarkkarajaisen luettelon niistä henkilön henkilöllisyyttä koskevista tiedoista, joita saadaan kerätä ja tallettaa poliisin valtakunnallisiin henkilörekistereihin. Ehdottomien rekisteröidyn tarkastusoikeuden rajoitusten osalta rekisteröidyn tarkastusoikeus on toteutettu välillisesti tietosuojavaltuutetun tarkastusoikeuden kautta. Rekisteröity voi näissä tapauksissa pyytää tietosuojavaltuutettua tarkastamaan rekisteröityä koskevien mahdollisten merkintöjen lainmukaisuuden.

729 HE 93/2002 vp. s. 19.

730 HE 93/2002 vp. s. 19

5.5.2.2. Lain soveltamisala

Henkilötietodirektiivi ei soveltamisalaltaan koske yleistä turvallisuutta eikä rikosoikeuden alalla tapahtuvaa valtion toimintaa (artikla 3). Suomessa on kuitenkin vakiintuneesti tulkittu, että henkilötietolakia voidaan tiedon käsittelyn periaatteiden osalta soveltaa yleislakina poliisin toimintaan. Erityislailla, kuten lailla henkilötietojen käsittelystä poliisitoimessa, voidaan antaa menettelysäännöksiä erityistilanteisiin.[731] PolHetiL:ssä tarkennetaan henkilötietojen käsittelyn periaatteita, kun kysymys on poliisin poliisilaissa säädettyjen tehtävien suorittamiseksi tarpeellisten henkilötietojen automaattisesta käsittelystä. Oleellista poliisin henkilötietojen käsittelyn oikeutuksessa on poliisin asema turvallisuutta valvovana ja lailla ohjattuna julkisena viranomaisena. Tiivistetysti voi sanoa, että poliisin henkilötietojen käsittelyn tulee noudattaa erityislakeja, henkilötietolain periaatteita ja hallinnon yleisiä periaatteita.[732]

5.5.2.3. Biometriset tiedot poliisin tietojärjestelmissä

Poliisin käytössä olevat tietojärjestelmät ovat poliisin valtakunnalliseen käyttöön tarkoitettuja, pysyviä ja automaattisen tietojenkäsittelyn avulla ylläpidettäviä henkilörekistereitä. Ne jakautuvat operatiivisiin tietojärjestelmiin ja hallinnollisiin tietojärjestelmiin. Operatiivisilla tietojärjestelmillä tuetaan suoraan poliisitoiminnan valtakunnallisia avainprosesseja, kun taas hallinnollisilla tietojärjestelmillä hoidetaan muun muassa talous- ja henkilöstöhallintoon liittyviä tehtäviä.[733] Näistä tärkeimpiä ovat operatiivisena tietojärjestelmänä poliisiasiain

731 HE 93/2002 vp., s. 1.

732 *Sorvari, S. – Lehtonen,* L., Geneettisen tiedon käsittelyn oikeussääntely, s. 145. Teoksessa Bio-oikeus lääketieteessä. Toimittanut Lasse Lehtonen. Edita Prima. Helsinki 2006. s. 125-150.

733 HE 66/2012 vp, s. 5.

tietojärjestelmä ja hallinnollisena tietojärjestelmänä hallintoasiain tietojärjestelmä. Näiden tietojärjestelmien rekisterinpitäjänä toimii Poliisihallitus.

Poliisiasiain tietojärjestelmään saadaan tallettaa seuraavat henkilön biometriset tiedot:

1. henkilökuulutustietoina valokuva, sormenjäljet sekä muuttumattomat fyysiset erityistuntomerkit.
2. tunnistettavien, kuten kadonneiksi ilmoitettujen ja tunnistamattomien vainajien valokuvat, sormenjäljet, hammaskaaviot ja DNA-tunnisteet.[734]
3. rikoksesta epäillyn tuntomerkkitiedot, kuten valokuva, sormen-, käden- ja jalanjäljet sekä käsiala-, ääni- ja hajunäyte. Myös rikoksesta epäillyn DNA-tunnisteet talletetaan poliisiasiain tietojärjestelmään.

Toinen poliisin lainmukaisten tehtävien suorittamisen kannalta keskeinen rekisteri on hallintoasiain tietojärjestelmä. Kysymyksessä on siis poliisin hallinnolliseen tarkoitukseen perustettu rekisteri. Siihen saadaan tallettaa samoja henkilön henkilöllisyyttä koskevia tietoja kuin poliisiasiain tietojärjestelmään, joiden lisäksi rekisteriin saadaan tallettaa seuraavat biometriset tiedot:

734 PolHetiL 2 §:n 3 momentin 3 kohdan mukaan kadonneiksi ilmoitettujen henkilöiden löytämiseksi ja tunnistamattomina löytyneiden vainajien tunnistamiseksi tarpeellisia lähisukulaisten tietoja voidaan tallettaa vain asianomaisen henkilön suostumuksella. Lainkohtaa täsmennettiin vuonna 2014 voimaantulleella lainmuutoksella. Muutos otettiin lakiin, koska kadonnut henkilö voidaan tunnistaa usein vuosikymmentenkin päästä lähisukulaisten DNA-tunnisteista laskennallisen sukulaisuusindeksin avulla, jos sukulaisen DNA-tunnisteet on talletettu tietokantaan. HE 66/2012 vp, s. 16

1. kuvatiedot eli valokuva ja nimikirjoitusnäyte
2. passin sormenjälkitiedot
3. ulkomaalaisen tunnistamistiedot (muun muassa sormenjäljet).

Nämä tiedot on katsottu tarpeelliseksi tietojärjestelmän tarkoituksen kannalta.[735]

Kuten edellä mainituista rekistereistä käy ilmi, poliisilla on melko laajat oikeudet yksilön biometristen tunnisteiden käsittelyyn. Näistä henkilötietojen kannalta olennaisimpia ovat järjestelmiin tallennettavat sormenjälkitiedot ja DNA-tunnisteet. Yksilön oikeuksien suojan näkökulmasta on siksi perusteltua käydä tarkemmin läpi juuri tässä yhteydessä rekisteröitävien tietojen käyttämistä ja luovuttamista.

5.5.2.4. Rekisteröitävien tietojen käyttäminen

Henkilötietojen käsittelystä poliisitoimessa annetun lain (PolHetiL) 3 luvussa on henkilötietojen käsittelyä koskevia erityisiä säännöksiä, jotka poikkeavat henkilötietolaista. Näiden säännösten ohella sovellettavaksi tulevat kuitenkin myös henkilötietolain säännökset niiltä osin kuin PolHetiL:ssa ei ole toisin säädetty.

Osa poliisin tietojärjestelmiin merkittävistä tiedoista ovat luonteeltaan arkaluontoisia, jolloin niiden käsittely on lähtökohtaisesti kielletty. Käsittelykielto ei kuitenkaan estä muun muassa tietojen käsittelyä, josta on säädetty laissa tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä.

Poliisin yhtenä lakisääteisenä tehtävänä on rikosten ennalta estäminen, paljastaminen ja selvittäminen. Poliisin laissa säädettyjen tehtävien vuoksi on ymmärrettävää, että arkaluonteisten tietojen käsittelykiellosta on poikettu. Näiden tietojen käsittelyn kieltäminen estää poliisilta lakisääteisten tehtäviensä tehokkaan suorittamisen. Arka-

735 HE 66/2012 vp., s.20.

luonteisten tietojen erityisasema on siis voimassa myös poliisin henkilötietojen käsittelyssä, mutta siihen on tehty poliisin lakisääteisten tehtävien hoitamiseksi välttämättömät tarkennukset. Tämän vuoksi arkaluonteisten tietojen käsittelystä säädetään PolHetiL 10 §:ssä erikseen. Näitä tietoja on lupa käsitellä, kun ne ovat rekisterin käyttötarkoituksen kannalta tarpeen (esim. rikollista tekoa koskevat tiedot) tai välttämättömiä poliisin yksittäisen tehtävän suorittamiseksi.

Biometristen tietojen näkökulmasta erityisen mielenkiintoinen on säännöksen 2 momentti, johon DNA-tunnisteesta on otettu erillinen maininta. DNA-tunniste on laissa katsottu arkaluonteiseksi henkilötiedoksi. Vaikka säännöksessä vain todetaankin DNA-tunnisteen tallettamista koskevista rajoituksista säädettävän pakkokeinolain 9 luvun 4 §:ssä, tulee säännöstä pitää osoituksena biometristen tunnisteiden, kuten DNAn, asemasta erityistä suojaa vaativana tietojen ryhmänä.[736] Tämän puolesta puhuu myös PolHetiL 10 a §, jossa säädetään henkilön fyysisiin ominaisuuksiin perustuvien tunnistetietojen eli biometristen tunnisteiden tietoturvan erityisistä vaatimuksista. Muiden arkaluonteisten tietojen kohdalla vastaavaa velvollisuutta ei ole säädetty.

Säännös asettaa poliisille varsin tiukan tietoturvavelvoitteen biometristen tietojen kohdalla. Henkilötietolaista poiketen PolHetiL

736 EIT:n ratkaisussa Peruzzo ja Martens v. Saksa oli kysymys vakavista rikoksista tuomittujen DNA-tunnisteiden säilyttämisestä mahdollisten tulevien rikosten tutkinnan turvaamiseksi. Koska kansallisessa laissa oli asianmukainen sääntely DNA-tunnisteiden ottamista ja säilyttämistä silmällä pitäen ja koska kansallinen sääntely myös sisälsi takeet väärinkäytöksiä vastaan sekä velvoitti viranomaiset säännöllisin väliajoin tarkistamaan tunnisteiden säilyttämisen, EIT katsoi yksityiselämään puuttumisen olleen suhteellista ja välttämätöntä demokraattisessa yhteiskunnassa eikä rikkomusta näin ollen todettu. Vertaa esimerkiksi EIT:n ratkaisu M. M v. Yhdistynyt Kuningaskunta, jossa riittäviä takeita ja kansallista sääntelyä ei ollut.

antaa suhteellisen tarkan kuvauksen biometristen tietojen tietoturvallisuusvaatimuksista, joilla omalta osaltaan turvataan yksilön yksityisyyttä poliisin toimesta tapahtuvassa henkilötietojen käsittelyssä (PolHetiL 10 a §). Ratkaisu on sinänsä ymmärrettävä, sillä julkisen vallan taholta tapahtuvassa henkilötietojen käsittelyssä julkisella vallalla on korostunut huolellisuusvelvoite ja suurempi vastuu henkilötietojen turvallisessa käsittelyssä.

Henkilön fyysisiin ominaisuuksiin perustuvia tunnistetietoja talletettaessa ja muutoin käsitellessä on huolehdittava siitä, että tunnistamisessa ja tunnistetietojen käsittelyssä käytettävät tietojärjestelmät, laitteet ja ohjelmistot ovat turvallisia ja että tunnistetiedot on suojattu asiattomalta pääsyltä sekä tunnistetietojen luottamuksellisuuteen ja eheyteen kohdistuvilta loukkauksilta, muutoksilta ja väärentämiseltä sekä muulta vahingossa tai laittomasti tapahtuvalta käsittelyltä. Tunnistamisessa ja tunnistetietojen käsittelyssä on muutoinkin toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet sen varmistamiseksi, että tunnistaminen ja tunnistetietojen käsittely voidaan toteuttaa tietoturvallisella ja yksityisyyden suojan turvaavalla tavalla.

Tietoturvatoimenpiteet ovat niiden luonteen perusteella jaettavissa neljään kategoriaan. Nämä ovat laitteisto- ja ohjelmistoturvallisuus, toiminnan turvallisuus, tietoliikenneturvallisuus ja tietoaineistoturvallisuus.[737] *Laitteisto- ja ohelmistoturvallisuus* sisältää tietojenkäsittely- ja tietoliikennelaitteiden sekä käyttöjärjestelmien, tietoliikenneohjelmistojen ja sovellusohjelmistojen turvallisuusominaisuudet.

Toiminnan turvallisuus eli *hallinnollinen tietoturvallisuus* pitää sisällään johdon hyväksymät periaatteet, käytettävissä olevat resurssit, vastuunjaon ja riskien arvioinnin. Toiminnan turvallisuus tarkoittaa muun muassa sitä, että ylläpidetään kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan sekä suojataan laitteet ja tiedostot luvatonta

737 HE 234/2008 vp., s. 65.

pääsyä ja käyttöä vastaan. Oleellisena osana toiminnan turvallisuutta on myös se, että pidetään rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia ja mitä oikeuksia milläkin käyttäjätunnuksella on ja valvotaan tietojen, laitteistojen ja tiedostojen tietoturvaan vaikuttavia tapahtumia.

Tietoliikenneturvallisuus kattaa tietoverkoissa siirrettävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseen liittyvät toimenpiteet. Tämä tarkoittaa muun muassa sitä, että laitteistojen ja tiedostojen sisältö ei saa paljastua asiaankuulumattomille ja ettei asiaankuulumattomat saa päästä muuttamaan tai tuhoamaan laitteistojen tai tiedostojen sisältöä.

Tietoaineistoturvallisuudella tarkoitetaan tietojen ja tietojärjestelmien tunnistamista ja luokittelua sekä tietovälineiden hallintaa ja säilytystä koko niiden elinkaaren ajan. Tietoaineistoturvallisuudella tarkoitetaan muun muassa sitä, että järjestetään tietoaineistojen turvallinen käsittely hyvän tietojenkäsittelytavan mukaisesti sekä suojataan tärkeät tietovarastot, asiakirjat ja yksittäiset tiedot.

Rekisterinpitäjän vastuu on ulotettu myös tietojen ulkoistamistapauksiin Rekisterinpitäjä vastaa tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka rekisterinpitäjän toimeksiannosta joko kokonaan tai osittain toteuttaa henkilön fyysisiin ominaisuuksiin perustuvien tunnistetietojen tallettamisen. Rekisterinpitäjä vastaa myös siitä, että toimeksisaajalla on sama velvollisuus suojata tiedot kuin rekisterinpitäjällä sekä siitä, ettei toimeksisaajalla ole muuta oikeutta käsitellä tietoja.

Omalta osaltaan tietoturvavelvoitetta tukee lakiin otettu yleisluonteisempi tietoturvasäännös (PolHetiL 19 b §), jonka mukaan poliisin henkilörekisterien ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan rajaamalla pääsy tietoihin vain niille, jotka tarvitsevat tietoja työtehtäviensä hoitamiseen. Kaikki henkilötietojen siirrot on myös kirjattava tai dokumentoitava.

Tunnistamiseen soveltuva biometrinen ominaisuus on pysyvä, muuttumaton ja peruuttamaton osa yksilöä. Tällaisina tietoina ne asettavat erityisiä vaatimuksia tietoturvalle yksityisyyden suojan toteutumisen varmistamiseksi.

Biometrisen tunnistamisen uhkakuvat liittyvät erityisesti tunnisteen pysyvyyteen. Biometrinen tunniste ei ole vaihdettavissa, vaan se sitoo käyttäjänsä tunnistettuun identiteettiin mahdollisesti koko elinajaksi. Biometrisen ominaisuuden digitaalinen tallenne on myös helposti ja nopeasti kopioitavissa ja samalla levitettävissä tietoverkkojen varaan rakentuvassa verkkoyhteiskunnassa. Jos biometristen tunnisteiden tietoturvasta ei huolehdita riittävästi, vaarana on rekisteriin kuuluvien tietojen joutuminen vääriin käsiin.

Biometristen tunnisteiden herkkyys henkilötunnisteina ja kansallisesti laaja tietokanta sormenjäljistä edellyttävät käytössä olevien rekisterien tietoturvaa koskevien toimintamallien ja käytettävissä olevan teknologian tarkastelua. Tietoturvauhkiin, tietomurtohyökkäyksiin ja tietokannan väärinkäytön mahdollisuuksiin on varauduttava myös lainsäädäntötasolla. Näiltä uhkilta on mahdollista välttyä ja niitä voidaan pienentää ennen kaikkea huolehtimalla asianmukaisesta tietoturvasta.

Yksilön näkökulmasta on erittäin tärkeää suojata tiedot siten, että niiden oikeudeton käyttö estetään mahdollisimman tehokkaasti. Tämä on erityisen tärkeää senkin vuoksi, kun yleisiä säännöksiä biometristen tunnisteiden käytöstä ei ole olemassa.[738]

Poliisin tietojärjestelmiin sisältyvien henkilötietojen käytössä pääsääntönä on tietojen tarpeellisuus. Henkilötietolain mukaiseen tarpeellisuusvaatimukseen nähden PolHetiL:ssa asetettu tarpeellisuusvaatimus on tarkkarajaisempi. Tietojärjestelmiin talletettuja tietoja on lupa käyttää vain, kun ne ovat tarpeen poliisin lakisääteisten tehtävien

738 HE 234/2008 vp, s. 63.

suorittamiseksi. Tiettyjen tehtävien kohdalla edellytetään kuitenkin tiukempaa tarpeellisuutta. Lupahallintoon liittyvien tehtävien kohdalla edellytetään esimerkiksi tietojen tarpeellisuutta sitä tehtävää varten, johon tiedot on kerätty ja talletettu. Passirekisterin tietojen käsittelyssä edellytetään siis tiukempaa tarpeellisuutta.

Merkittävää poliisin tietojärjestelmien kohdalla on niiden käsittelyyn oikeutetun henkilöpiirin laajuus. Poliisin valtakunnalliset rekisterit, kuten hallinto- ja poliisiasiaintietojärjestelmät ovat poliisin valtakunnallisessa käytössä. Käyttöoikeutta näihin järjestelmiin ei käytännössä ole lailla rajoitettu muiden kuin Poliisiammattikorkeakoulun osalta. Ratkaisu on sinänsä ymmärrettävä, sillä lakisääteisten tehtäviensä suorittamiseksi kaikilla poliisin yksiköillä tulee olla pääsy näihin tietojärjestelmiin. Erityistä huomiota tulee kuitenkin kiinnittää käyttöoikeuksien asianmukaiseen rajaamiseen yksiköiden sisällä.

Passin sormenjälkitiedot kuitenkin muodostavat tässä suhteessa poikkeuksen. Näiden tietojen käyttöön oikeutettujen henkilöpiiriä on merkittävästi rajattu. Tiedot eivät ole kenenkään muun käytettävissä kuin sen, jonka työtehtävien hoitaminen tiedon käyttöä välttämättä edellyttää. Käytännössä kysymys on siis lähinnä poliisin lupapalveluita hoitavista virkailijoista, jotka tarvitsevat tietoja passin myöntämis- ja peruuttamisprosessissa.

Poliisin tietojärjestelmien kohdalla myös on pääsääntönä käyttötarkoitussidonnaisuus. Käsiteltäviä henkilötietoja ei saa käyttää tavalla, joka on ristiriidassa määriteltyjen keräämis- ja talletustarkoitusten kanssa. Tästä pääsäännöstä on kuitenkin sallittua poiketa, kun poikkeamisesta on laissa säädetty ja se on välttämätöntä demokraattisessa yhteiskunnassa valtion turvallisuuden, yleisen turvallisuuden, rikosten ehkäisemisen taikka rekisteröityjen tai muiden henkilöiden oikeuksien ja vapauksien suojaamiseksi. Poliisin tietojärjestelmien käytön osalta tätä mahdollisuutta on myös hyödynnetty (PolHetiL 16 §).

Passirekisterin sormenjälkitiedot jäävät kuitenkin tämän poikkeuksen ulkopuolelle. Passin sormenjälkitietojen ja ulkomaalaislain perusteella otettujen sormenjälkitietojen käyttäminen muuhun kuin tietojen keräämis- ja tallettamistarkoitukseen on rajattu vain välttämättömään tunnistamattoman uhrin tunnistamiseen (PolHetiL 16 a §).[739] Tietojen käsittelyyn oikeutettujen henkilöpiiriä on laissa myös voimakkaasti rajoitettu. Tietojen käyttämiselle on säädetty välttämättömyysvaatimus tarpeellisuusvaatimuksen sijaan. Tietoja saa käyttää vain se, jonka työtehtävien hoitaminen tiedon käyttöä välttämättä edellyttää.

Tällaisessa tilanteessa poliisilla on myös oikeus ottaa sormenjäljet ja verrata niitä rekisteröityihin sormenjälkiin. Vertaamista varten otettuja tietoja voidaan kuitenkin käyttää vain vertaamisen ajan, ja ne on hävitettävä välittömästi sen jälkeen. Kysymyksessä on siis erityinen hävittämisvelvollisuus tietojen käytyä tarpeettomiksi tarkoitukseensa.

Käytännössä kysymys on lain nojalla tapahtuvasta poliisimiehen eikä poliisissa työskentelevän hallinnollisen virkamiehen suorittamasta henkilön tunnistamisesta tilanteessa, jossa henkilöä ei muutoin saada tunnistettua, esimerkiksi tunnistamattoman vainajan tai tunnistamatta jääneen rikoksen uhrin henkilöllisyyden selvittämisessä. Mahdollisuutta rikosten ehkäisyyn tai selvittämiseen rekisteriin talletettujen sormenjälkien avulla ei siis ole.[740]

---

739 Perustuslakivaliokunta edellytti ulkomaalaislain nojalla otettavien sormenjälkitietojen käyttämisen rajoittamista vain niiden keräämis- ja tallettamistarkoitusta vastaavaan tarkoitukseen. Tällainen tarkoitus voi kuitenkin sinänsä liittyä myös tarkasti määriteltyjen rikosten estämiseen ja selvittämiseen, mutta ainoastaan siinä laajuudessa kuin tällä toiminnalla on yhteys alkuperäiseen keräämis- ja tallettamistarkoitukseen. PeVL 47/2010 vp.

740 Alkuperäisessä hallituksen esityksessä ehdotettua sääntelyä ei katsottu asianmukaiseksi etenkään käyttötarkoituksen määrittelyltä edellytettävän täsmällisyys- ja tarkkarajaisuusvaatimuksen kannalta.

Vaikka poliisin tietojärjestelmien käyttö on käytännössä järjestetty siten, että käyttöoikeudet myönnetään vain niille, jotka työtehtävissään tietoja nimenomaisesti tarvitsevat, on passin sormenjälkitietojen kohdalla ollut tarkoituksenmukaista säätää nimenomainen käyttöoikeuden rajoitus lain tasolle niiden herkkyyden vuoksi. Nimenomaista säännöstä puoltaa myös se, että passinhakijoiden sormenjälkien rekisteröinnissä on kysymys merkittävästä rekisteröitävien yksityisyyden suojaan liittyvästä kysymyksestä.

Tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin on siis syytä suhtautua hyvin varauksellisesti. Käyttötarkoitussidonnaisuudesta voidaan nimittäin tehdä vain täsmällisiä ja vähäisiksi luonnehdittavia poikkeuksia. Sääntely ei saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötavaksi.

5.5.2.5. Tiedon poistaminen ja korjaaminen

Henkilötietojen käsittelyssä noudatettavia yksilön oikeuksia ja rekisterinpitäjää koskevia erityisiä periaatteita sovelletaan myös poliisin ylläpitämiin henkilörekistereihin. Henkilötietojen käsittelystä poliisitoimessa annettu laki sisältää kuitenkin erityissääntelyä tiedon korjaamisen, poistamisen ja tarkastamisen kohdalla.

Tiedon korjaaminen. Rekisteröidyn oikeus saada tietonsa korjatuksi sekä rekisteripitäjälle asetettu erityinen virheettomyysvaatimus tulevat noudatettavaksi myös poliisin henkilötietojen käsittelyssä. Poliisin on

---

Tämän vuoksi hallintovaliokunta ehdotti 16 a §:n 1 momentin täsmentämistä olennaisesti. Hallintovaliokunnan näkemyksen mukaan passirekisterin sormenjälkitietoja tulee voida käyttää poikkeuksellisissa tilanteissa, joissa vaihtoehtoja ei ole juurikaan käytettävissä. HaVM 9/2009 vp.

siis oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Poliisin on myös estettävä tällaisen tiedon leviäminen, jos tieto voi vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan.[741]

Virheettömyysvaatimus ei poliisin henkilötietojen käsittelyssä ole kuitenkaan täysin ehdoton. Poliisille on säädetty oikeus säilyttää rekisterissään oleva virheellinen tieto korjatun tiedon yhteydessä. Yksilön oikeuksien näkökulmasta tällaisen poikkeuksen tekeminen virheettömyysvaatimukseen edellyttää kuitenkin painavia perusteita ja käytön tarkkaa rajaamista. Vain tällöin poliisille säädetty virheettömyysvaatimuksesta poikkeaminen vaikuttaa oikeutetulta. Tämän vuoksi poikkeuksen on oltava tarpeen rekisteröidyn tai toisen yksilön oikeuksien

741 KHO:n ratkaisussa KHO 2012:51 oli kysymys virheellisen merkinnän poistamisesta. A oli pyytänyt tietosuojavaltuutettua tarkastamaan keskusrikospoliisin SIRENE-toimiston pitämässä Schengen-rekisterissä hänestä olevien tietojen lainmukaisuuden ja pyytämään keskusrikospoliisia poistamaan häntä koskevat virheelliset tiedot. Tiedot siitä, että A olisi ollut etsintäkuulutettu Ranskassa, olivat A:n mukaan virheelliset. Tietosuojavaltuutettu oli hylännyt vaatimuksen. SIRENE-asiankäsittelyjärjestelmän arkistotietokannassa olevat A:han liittyvät merkinnät koostuivat Suomen ja Ranskan SIRENE-toimistojen välisestä tietojenvaihdosta, Suomen SIRENE-toimiston toimenpiteistä sekä Suomen poliisin eri yksiköiden välisestä tietojenvaihdosta. Tietojenvaihtoa koskevina tietoina niitä ei voitu pitää virheellisinä sillä perusteella, että asiassa ei tietojen poistamisen vuoksi enää voitu selvittää alkuperäisen kuulutustiedon oikeellisuutta. Asiassa ei siten ollut ilmennyt, että tietojenvaihtoa ja toimenpiteitä koskevat tiedot olisivat PolHetiL 27 §:ssä tarkoitetulla tavalla virheelliset. Tähän nähden ei ollut perusteita suostua A:n vaatimukseen tietojen poistamisesta virheellisinä.

turvaamiseksi eikä tietoa saa käyttää muuhun tarkoitukseen. Tarkkarajaisuusvaatimuksen vuoksi tietojen säilyttämisaika on sidottu ensisijaisesti oikeuksien turvaamiseen. Myös ehdoton määräaika on kuitenkin säädetty: tiedot tulee poistaa viimeistään viiden vuoden kuluttua tiedon poistamiselle säädetyn määräajan päättymisestä.

Tietojen poistaminen. Tietojen poistaminen on osa henkilötietojen tarpeellisuusvaatimusta. Poliisin kohdalla tästä ei tehdä poikkeusta. Poliisin tulee poistaa tarpeettomiksi käyneet henkilötiedot rekistereistään. Tämän tutkimuksen aihepiirin kannalta keskeisessä asemassa ovat poliisiasiain tietojärjestelmään ja hallintoasiain tietojärjestelmään talletetut tiedot.

Koska tietojen poistaminen on osa henkilötietojen käsittelyssä noudatettavaa tarpeellisuuden vaatimusta, tulee tietojen säilytysajoista säätää riittävän yksityiskohtaisesti. Tarpeettomien tai virheellisten tietojen rekisterissä pitäminen on lisäksi haitallista paitsi yksilön yksityisyyden myös poliisitoiminnan tehokkuudenkin kannalta. Tietojen poistamista koskeva sääntely lähtee siitä ajatuksesta, että virheelliseksi todettu tieto on poistettava viipymättä ja viimeistään sen enimmäissäilytysajan umpeen kuluttua. Enimmäissäilytysajat on laissa määritelty siten, että suurimmassa osassa tapauksia poliisitoimenpiteet on mahdollista saada suoritettua säilytysaikojen puitteissa eri osapuolten oikeudet turvaavalla tavalla. Säilytysaika voi olla sidottu esimerkiksi rikoksen syyteoikeuden vanhentumisaikaan.[742]

Tiettyä tapahtumakokonaisuutta koskevan ilmoituksen eheyden turvaamiseksi siihen liittyviä eri rikoksia ja rikoksesta epäiltyjä koskevia tietoja on kuitenkin tarkoituksenmukaista käsitellä yhden säilytysajan puitteissa. Oikeaan säilytysaikaan voi olla vaikutusta myös säilytettävien tietojen luonteella. Myös tapahtumaan eri rooleissa liittyvien henkilöiden intressit säilytysaikojen suhteen saattavat olla erilaiset.

742 HE 93/2002 vp, s. 37.

Rikoksesta epäilty esimerkiksi haluaa todennäköisesti omat tietonsa poistetuksi rekisteristä nopeammin kuin rikoksen uhri, jolla on intressi tietojen pidempiaikaiselle säilyttämiselle.[743] Näiden syiden vuoksi PolHetiL säätää tietojen poistamiselle eripituisia enimmäissäilytysaikoja. Enimmäissäilytysajat poliisin keräämien biometristen tunnisteiden kohdalla ovat seuraavat:

- Tuntomerkkitiedot on poistettava viimeistään 10 vuoden kuluttua rekisteröidyn kuolemasta, tai yhden vuoden kuluttua esitutkinnan päättymisestä, asian käsittelyn lopettamisesta tai syytteen hylkäämisestä.
- Henkilökuulutustiedot poistetaan pääsääntöisesti 3 vuoden kuluttua kuulutuksen peruuttamisesta tai päättymisestä.
- Tunnistettavien tiedot poistetaan viiden vuoden kuluttua kadonneen henkilön löytymisestä tai vainajan tunnistamisesta.
- Kuvatiedot poistetaan kolmen vuoden kuluttua sen poliisin, ulkoasiainministeriön tai Suomen edustuston myöntämän luvan tai antaman päätöksen voimassaoloajan päättymisestä, jonka valmistamiseen henkilön valokuvaa tai nimikirjoitusnäytettä on viimeksi käytetty.
- Passitiedot ja passin sormenjälkitiedot poistetaan kymmenen vuoden kuluttua passin myöntämistä koskevasta päätöksestä tai sen raukeamisesta taikka päätöksessä mainitun voimassaoloajan päättymisestä.
- Ulkomaalaisen tunnistamistiedot poistetaan kymmenen vuoden kuluttua rekisteröinnistä. Jos rekisteröity on saanut Suomen kansalaisuuden, tiedot poistetaan kuitenkin yhden vuoden kuluttua siitä, kun rekisterinpitäjä on saanut tiedon kyseisestä kansalaisuuden saamisesta.

743 HE 93/2002 vp, s. 37

- Kaikki henkilöä koskevat tiedot poistetaan tietojärjestelmästä kuitenkin viimeistään yhden vuoden kuluttua rekisteröidyn kuolemasta, jollei ole erityistä syytä tietojen edelleen säilyttämiseen.

Kuten edellä mainitusta säilytysaikoja koskevasta listauksesta käy ilmi, poliisillakaan ei ole oikeutta säilyttää tietojärjestelmiinsä sisältyviä tietoja rajoittamatonta aikaa. Abstraktien tietojen tarpeellisuuteen sidottujen säilytysaikojen sijaan poliisin oikeus tietojen säilyttämiseen on myös tarkkaan ajallisesti rajattu. Ratkaisu on ymmärrettävä, sillä viranomaisten henkilötietojen käsittelyssä lainsäädännön tarkkarajaisuusvaatimus saa korostuneen merkityksen.

5.5.2.6. Ilmoittamisvelvollisuus ja tietojen tarkastaminen

Ilmoittamiselvollisuus. Rekisterinpitäjää koskeva erityinen ilmoittamisvelvollisuus tulee noudatettavaksi myös poliisin henkilötietojen käsittelyssä. Vaikka poliisin henkilötietojen käsittelystä säädetäänkin omassa laissa, ei poliisillakaan pääsääntöisesti ole oikeutta salaiseen henkilötietojen käsittelyyn.

Henkilötietojen keräämisestä, tallettamisesta ja luovuttamisesta poliisitoimessa on kuitenkin nimenomaisesti säädetty. Tämän seurauksena jokaisella on mahdollisuus saada yleisellä tasolla tieto siitä, minkälaista poliisin tietojen käsittely on ja minkälaisia häntä koskevia tietoja poliisi saattaa siis mahdollisesti käsitellä. Tarkempia tietoja näistä asioista on saatavissa myös rekistereiden rekisteriselosteista.

Valtion turvallisuuden ja yleisen järjestyksen ja turvallisuuden vuoksi sekä rikosten ehkäisemiseksi tai selvittämiseksi on usein välttämätöntä, että poliisi ei informoi kohdehenkilöitä harjoittamastaan tietojen käsittelystä. Tämä koskee varsinaisten poliisitehtävien lisäksi esimerkiksi lupien peruuttamisasioita. Näiden syiden vuoksi tietojen antaminen rekisteröidylle on usein mahdotonta tai ainakin vaatii koh-

tuutonta vaivaa. Lisäksi tietojen antaminen rekisteröidylle voi aiheuttaa tietojenkäsittelyn tarkoitukselle olennaista vahinkoa tai haittaa. Tämän vuoksi poliisin henkilötietojen käsittelyssä ilmoittamisvelvollisuus on rajoitettu (PolHetiL 43 §).

Yksilön oikeus tarkastaa omat tietonsa on voimassa myös poliisin henkilötietojen käsittelyssä. Tarkastusoikeuden käyttämistä koskeva pyyntö on siis esitettävä rekisterinpitäjälle. Poliisin valtakunnalliseen käyttöön tarkoitettujen henkilörekisterien osalta pyyntö voidaan kuitenkin osoittaa palveluperiaatteen mukaisesti myös muulle rekisterinpitäjän määräämälle poliisiyksikölle, esimerkiksi paikallispoliisille. Pyyntö tarkastusoikeuden käyttämiselle on esitettävä henkilökohtaisesti ja rekisteröidyn on todistettava henkilöllisyytensä.

Tarkastusoikeuden ulkopuolelle on kuitenkin rajattu tietyt poliisin rekisterit. Näihin rekistereihin rekisteröidyn tarkastusoikeus ei ulotu. Näiden tietojen ja tietojärjestelmien osalta yksilön tarkastusoikeus on toteutettu välillisesti. Henkilö voi kääntyä tietosuojavaltuutetun puoleen tarkastusoikeuden toteuttamiseksi. Tietosuojavaltuutettu on rekisteröidyn pyynnöstä oikeutettu tarkastamaan rajoitusten alaisten tietojen rekisteröinnin lainmukaisuuden. Tietojen lainmukaisuuden tarkastamisella ei tarkoiteta niiden alkuperäisen hankkimisen lainmukaisuuden tai tarkoituksenmukaisuuden, vaan niiden käsittelyn lainmukaisuuden tarkastamista.[744]

Havainnollisen esimerkin yksilön oikeuksien turvaamisesta poliisin henkilötietojen käsittelyssä antaa EIT:n ratkaisu M.K. v. Ranska. Tapauksessa oli kysymys kirjanäpistyksestä epäiltynä olleelta otetuista sormenjäljistä. Valittaja oli vaatinut rekisteröinnin poistamista, sillä hänen ei ollut todettu syyllistyneen rikokseen, vaan kysymys oli epäilystä.

744 HE 93/2002 vp, s. 43.

EIT:n mukaan erityisen huolestuttavaa oli se, että valittajan kaltaisia henkilöitä kohdeltiin henkilötietojen rekisteröinnin kohdalla samalla tavoin kuin rikoksista tuomittuja. Vaikka yksityisluonteisten tietojen säilyttämistä ei voitu rinnastaa rikoksesta epäilyyn, säilyttämisellä ei kuitenkaan saanut antaa vaikutelmaa, ettei henkilöä voitu pitää syyttömänä.

EIT kiinnitti tapauksen kohdalla huomiota myös siihen, että sormenjälkirekisterin käyttöä ei ollut kansallisella lailla selkeästi rajattu rikostutkintaan. Lisäksi rekisterin alaan saattoivat lain mukaan kuulua kaikki rikokset. Rekisteröinnin poistamista sai kuitenkin vaatia milloin tahansa, mutta pyyntö voitiin evätä tutkinnallisista syistä. Tämän vuoksi lain ei katsottu perustavan yksilölle mitään oikeutta tietojen hävittämiseen eikä näin ollen tarjonnut yksilölle konkreettista ja tehokasta suojaa. Näiden syiden vuoksi Ranskan katsottiin ylittäneen harkintamarginaalinsa. Kilpailevien julkisten ja yksityisten intressien välillä ei ollut löydetty oikeudenmukaista tasapainoa, jonka vuoksi EIS 8 artiklaa oli rikottu.

Yksilön oikeuksien ja henkilötietojen suojan tarkoituksen näkökulmasta EIT:n tuomiota voidaan pitää oikeana. Henkilötietojen käyttötarkoitus tulee olla tarkkaan määritelty, jotta käsittely olisi oikeutettua. Yksilöllä tulee myös olla asianmukaiset oikeusturvakeinot käytettävissä etenkin julkisen vallan toimesta tapahtuvassa henkilötietojen käsittelyssä. Tässä tapauksessa näin ei ollut.

Tuomiolla on (toivottavasti) oma ohjausvaikutuksensa siihen, millä tavoin henkilötietoja tulee käsitellä poliisitoimessa. Tuomio ohjaa julkista valtaa kiinnittämään erityistä huomiota rekisteröitävien henkilötietojen tarpeellisuuteen. Vaikutuksensa tuomiolla on myös käyttötarkoituksen määrittämiseen ja noudattamiseen yksilön oikeudet turvaavalla tavalla.

5.5.3. Passilaki

5.5.3.1. Yleistä

Biometristen tunnisteiden käyttö lisääntyi voimakkaasti syyskuun 2001 terrori-iskujen jälkeen, kun turvallisuustoimenpiteitä tiukennettiin maailmanlaajuisesti. Näiden iskujen vaikutukset näkyvät Euroopan unionissa muun muassa Euroopan neuvoston 13.12.2004 antamassa passiasetuksessa (EY) N:o 2252/2004, jolla yhtenäistettiin unionin jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä koskevat vaatimukset. Syy biometristen tunnisteiden ottamiselle passiin oli lähes yksinomaan poliittinen. Yhdysvallat painosti EU:ta osallistumaan omalta osaltaan terrorismin vastaiseen sotaan ottamalla käyttöön biometrisen passin[745]

Mielenkiintoista passiasetuksen säätämisessä oli julkisen keskustelun puute biometrisen tunnistamisen käyttämisestä passeissa.[746] Voisi

745 *Ashbourn,* The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies, s. 20 sekä *Goncalves – Gameiro,* Security, Privacy and Freedom and the EU Legal and Policy Framework for Biometrics, s. 322. Heidän mukaansa osoituksena tästä on myös viisumeja ja oleskelulupia koskeva asetus. Katso myös *Tranberg,* Biometric Data in Scandinavia, s. 387.

746 *Goncalves – Gameiro,* Security, Privacy and Freedom and the EU Legal and Policy Framework for Biometrics, s. 324. Katso myös *Joint Research Center,* Biometrics at the Frontiers (2005), s.131-133. Vasta vuonna 2012 Euroopan parlamentti alkoi esittämään kysymyksiä ja käymään keskustelua biometrisen passin käytöstä. Katso esimerkiksi Parlamentin jäsenten esittämät kysymykset 6.3.2012, Aihe: Biometriset passit, 0-000052/2012. Saatavilla osoitteessa: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+OQ+O-2012-000052+0+DOC+XML+V0//FI.

oikeastaan sanoa, että biometrinen tunnistaminen otettiin käyttöön passeissa ilman, että sen toimivuudesta ja vaikutuksista oli tarkkaa tietoa.[747] Myös passiasetuksen lainmukaisuus on epäselvä, sillä Nizzan sopimuksen 18 artiklan mukaan passit, henkilötodistukset, oleskeluluvat ja muut näihin verrattavat asiakirjat jäävät liikkumisvapauden piiriin kuuluvina asioina EU:n lainsäädäntövallan ulkopuolelle.[748] Näiden syiden vuoksi biometrisen tunnistamisen käyttäminen passeissa on kritiikille altis. Oikeudellisesta näkökulmasta kritiikkiä aiheuttaa myös se, että biometrisen tunnistamisen käyttö yliarvioi turvallisuuden ja sisämarkkinoiden arvot ilman huomion kiinnittämistä yksityisyyteen ja muihin ihmisoikeuksiin. Asetusta on myös kuvattu enemmänkin tekniseksi kuin oikeudelliseksi asiakirjaksi sen keskittyessä pääasiassa passin turvatekijöiden määrittelyyn ja standardisointiin.[749]

Biometrinen passi otettiin kuitenkin käyttöön passiasetuksella, jonka mukaisesti jäsenvaltiot ovat ottaneet käyttöön biometrisen passin. Sen käyttöönotto toteutettiin kahdessa vaiheessa. Ensimmäisessä vaiheessa passiin otettiin biometrisena tunnisteena haltijan kasvokuva, joka talletetaan passissa olevaan siruun. Suomessa passin ensimmäinen biometrinen tunniste otettiin käyttöön passilain kokonaisuudis-

747 *Joint Research Center,* Largescale Biometrics Deployment (2008), s. 64. Komissio myönsi tämän puutteen passiasetuksen täydentämistä koskevassa ehdotuksessaan. Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004, COM (2007) 619 final, COM(2007) 619 final,18.10.2007, s.2.

748 *De Hert – Schreurs – Kosta – Kindt - Huysmans,* Legal Grounds for ID Documents in Europe, s. 60-62.

749 *Goncalves – Gameiro,* Security, Privacy and Freedom and the EU Legal and Policy Framework for Biometrics, s. 324 ja 326.

tuksella vuoden 2006 elokuussa.[750] Toisessa vaiheessa passiin lisättiin toiseksi biometriseksi tunnisteeksi passinhaltijan kaksi sormenjälkeä, jotka myös talletetaan passissa olevaan siruun. Suomessa passiuudistuksen toinen vaihe toteutettiin passilain muutoksella, joka tuli voimaan 29.6.2009.[751]

Huomionarvoista passeja koskevassa uudistuksessa on se, että jäsenvaltioille itselleen jätettiin päättäminen mahdollisesta sormenjälkien tallettamisesta ja rekisterin perustamisesta, kuten myös passin sormenjälkitietojen käyttämisestä muuhun kuin niiden tallettamistarkoitukseen. Suomessa päädyttiin ratkaisuun, jossa sormenjälkitiedot talletetaan kansalliseen rekisteriin, mutta niiden käyttö muuhun kuin tallettamistarkoitukseensa sallitaan vain poikkeuksellisesti.

Biometristen tunnisteiden ottamisella passiin on tarkoitus suojata henkilön henkilöllisyyttä, henkilökohtaista turvallisuutta ja estää yksityiselämän suojaa loukkaavaa henkilöllisyyden väärinkäyttöä. Passien turvamekanismien lisääminen koettiin tärkeäksi, sillä passi on kansainvälisesti tärkein matkustusasiakirja. Biometrisilla tunnisteilla haluttiin parantaa passien turvallisuutta ja torjua väärennöksiä, terrorismia, laitonta maahanmuuttoa ja lapsikauppaa. Matkustaminen toisen henkilön passilla, varastetulla tai lainatulla passilla tulee vaikeammaksi ja matkustamisesta tulee näin turvallisempaa.[752] Lisäksi uudistuksen taustalla ovat vaikuttaneet käytännölliset näkökohdat. Perusteena on

750 Samassa yhteydessä biometrinen tunniste otettiin käyttöön myös Suomessa ulkomaalaisille myönnettävissä pakolaisen matkustusasiakirjassa ja muukalaispassissa.

751 Euroopan Unionin asettama takaraja sormenjälkien käyttöönotolle oli 28.6.2009.

752 Goncalves ja Gameiro kuitenkin kritisoivat näitä perusteluja. Heidän mukaansa tällaiset perustelut asaettavat yhteiskunnan edut yksilön edelle. Tällöin on vaarana, että ihmisoikeuksien puolustamisella voi-

käytetty myös matkustamisen helpottumista, kun passien käsittely nopeutuu.[753]

Uudet biometriset passit tehostavat myös merkittävästi passinhaltijan tunnistettavuutta.[754] Ongelmaksi voi tällöin muodostua, että yksilöä on mahdollista seurata hänen passin käyttämisestä jäävien tietojen perusteella. Yksilön oikeuksien ja erityisesti henkilötietojen suojan näkökulmasta asia on ongelmallinen. Vähimmän puuttumisen periaate ihmisoikeusperusteisena periaatteena ohjaa tunnistamisratkaisujen valintaa. Vaihtoehtoisista menetelmistä tulee valita se, jolla vähiten puututaan yksilön oikeuksiin.[755] Ongelmana on myös se, että tunnistamista koskevan lainsäädännön tulee lähtökohtaisesti olla teknologianeutraalia. Sitä ei tulisi sitoa tiettyyn tekniseen ratkaisuun.

5.5.3.2. Biometriset tunnisteet passilaissa

Passin sisältö ja tietojen tarkastaminen. Passin hakijan on passin saamiseksi luovutettava tietyt identiteettitiedot. Näitä ovat muun muassa hakijan sukunimi ja etunimet, sukupuoli, henkilötunnus, kasvokuva sekä sormenjäljet.[756] Passin aitouden ja eheyden varmistamiseksi pas-

---

daan oikeuttaa voimakkaastikin yksilöön puuttuvien keinojen käyttäminen. *Goncalves – Gameiro,* Security, Privacy and Freedom and the EU Legal and Policy Framework for Biometrics, s. 323.

753 Näin myös *Kindt,* Privacy and Data Protection Issues in Biometric Application, s. 731.

754 *Hornung,* Biometric Passports and Identity Cards: Technical, Legal and Policy Issues, s. 502.

755 Perustuslakivaliokunta on arvioinut sormenjälkien rekisteröintiä nimenomaan vähimmän puuttumisen periaatteen näkökulmasta. Katso PeVL 14/2009 vp.

756 Alun perin sormenjälkien ottaminen passiin oli tarkoitus olla vapaaehtoista. Niiden ottaminen muutettiin myöhemmässä asetuksen käsittelyssä pakolliseksi. Tätä edellytti ennen kaikkea oikeus ja sisä-

sin hakijan on myös annettava sähköinen allekirjoitus ja sitä vastaava allekirjoitusvarmenne (5 ja 5 a §:t).

> Sormenjälkien ottaminen passeihin on ollut esillä Euroopan Unionin tuomioistuimen syksyllä 2013 antamassa ratkaisussa C-291/12 Michael Schwartz v. Bochum (17.10.2013). Tapauksessa Schwartz haki Bochumin kaupungilta passia, mutta kieltäytyi antamasta sormenjälkiään, koska katsoi passiasetuksen olevan EU-sääntelyn vastainen ja loukkaa hänen oikeuttaan yksityisyyteen.
>
> Saksan hallintotuomioistuin katsoi asetuksen pätemättömäksi. Tuomioistuimen mukaan sormenjälkien ottaminen on vakava yksityisyyden loukkaus, jonka tulee täyttää suhteellisuusvaatimus. Hallintotuomioistuimen mukaan näin ei ollut, sillä passin väärinkäyttöä on mahdollista estää myös vähemmän yksityisyyteen puuttuvin keinoin. Lisäksi hallintotuomioistuin kiinnitti perusteluissaan huomiota biometrisen tunnistamisen mukanaan tuomiin riskeihin sekä siihen liittyviin teknisiin ongelmiin.
>
> EUT kuitenkin linjasi, että sormenjälkien ottaminen passia varten on EU-sääntelyn mukaista, jos sormenjälkiä käytetään vain ja ainoastaan passinhaltijan tunnistamiseen eikä sormen-

---

asioiden neuvosto. Euroopan parlamentti esitti huolensa sormenjälkien pakollisuudesta sekä keskitetyn EU:n laajuisen passirekisterin luomisen vaikutuksista perus- ja ihmisoikeuksiin. 29 artiklan mukainen tietosuojatyöryhmä, Opinion on Implementing the Council Regulation (EC) No 2252/2004, s. 4–5 sekä Euroopan parlamentin lainsäädäntöpäätöslauselma komission ehdotuksesta neuvoston asetukseksi EU:n kansalaisten passien turvatekijöitä ja biometriikkaa koskevista vaatimuksista (KOM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)).

jälkiä tallenneta muualle kuin passiin. Lisäksi tuomioistuin kiinnitti huomiota siihen, että toista vähemmän yksityisyyteen puuttuvaa keinoa, jolla voitaisiin riittävästi ehkäistä passien väärinkäyttöä, ei ole olemassa.

Mielenkiintoista ratkaisussa on se, että tuomioistuin sovelsi vähimmän puuttumisen periaatetta arvioidessaan sormenjälkien ottamisen aiheuttamaa yksityisyyden loukkausta. Soveltaessaan periaatetta tuomioistuin kuitenkin teki ratkaisunsa teknologisen imperatiivin ajatuksen mukaisesti verratessaan sormenjälkien keräämistä vain toisiin biometrisiin tunnisteisiin (iiristunnistukseen). Toisin kuin hallintotuomioistuimen ratkaisussa, EUT ei ottanut lainkaan huomioon mahdollisia muita käytettävissä olevia keinoja passien väärinkäytön ehkäisemiseksi.

Henkilötietojen suojan periaatteiden mukaisesti yksilön keskeinen oikeus on omien tietojen tarkastusoikeus. Yksilöllä tulee olla oikeus tarkastaa itseään koskevat tiedot, vaikka henkilötietojen käsittely perustuisikin erityislainsäädäntöön. Periaate tulee siis sovellettavaksi myös passin tietojen kohdalla.

Yleistä oikeutta passirekisteriin talletettujen tietojen tarkastamiseen ei kuitenkaan sisälly passilakiin, vaan tästä säädetään henkilötietojen käsittelystä poliisitoimessa annetussa laissa. Passirekisteri on osa poliisin hallintoasiaintietojärjestelmää, jolloin siihen talletettuihin tietoihin sovelletaan edellä mainittua lakia. Tämän lain mukaisia oikeuksia on käsitelty jo aiemmin tässä tutkimuksessa kohdassa 5.4.2.

Passinhaltijan oikeusaseman turvaamisen kannalta on oleellista, että haltijalla on oikeus tarkastaa myös tekniseen osaan talletetut tiedot. Passilakiin onkin otettu eräänlainen tarkastusoikeuden laajennus. Passinhaltijalle on yleisen henkilötietojen tarkastusoikeuden lisäksi säädetty oikeus passin tekniseen osaan hänestä talletettujen tietojen

tarkastamiseen. Ratkaisu on perusteltu, sillä passin teknisen osan tiedot muodostavat käyttötarkoituksensa vuoksi yhtenäisen tietojoukon, jota käsitellään automaattisen tietojenkäsittelyn avulla. Ne tällöin muodostavat henkilörekisterin.[757] Passilaki ei varsinaisesti kuitenkaan ole henkilötietojen käsittelyä koskeva laki, jolloin lakiin on perusteltua ottaa erillinen maininta tarkastusoikeudesta myös teknisen osan tietojen osalta.

Tarkastusoikeutta koskeva säännös on kuitenkin vain informatiivisluonteinen, jossa viitataan EU:n passiasetukseen. Vaikka EU:n passiasetus on suoraan sovellettavaa oikeutta, on lakiin lainsäädännön selkeyden ja sen soveltamisen kannalta katsottu tarpeelliseksi ottaa erityinen viittaussäännös EU:n passiasetukseen passin teknisen osan tietojen tarkastusoikeuden osalta. Tarkastusoikeuden lisäksi passinhaltijalla on luonnollisesti myös oikeus tarvittaessa pyytää tietojen korjaamista tai poistamista.

Passilakia koskevan hallituksen esityksen mukaan tarkastusoikeus käsittää varsinaisen tietojen tarkastamisen ohella myös sirun teknisen toimivuuden ja sormenjälkitunnistuksen toimivuuden tarkastamisen, vaikka näistä ei nimenomaisia erityisiä säännöksiä laissa olekaan. Tarkastusoikeutta voi käyttää ensisijaisesti passinhakupisteessä. Tietojen vastaavuus voidaan luonnollisesti tarkastaa myös rajalla luettaessa passi ja sen sisältämä siru.[758] Tarkastusoikeuden laajennusta ei kuitenkaan ole hallituksen esityksessä mitenkään perusteltu. Passinhaltijan ja –hakijan oikeusturvan vuoksi tarkastusoikeuden laanennus on kuitenkin ymmärrettävä. Viallinen siru ja / tai sormenjälkitunnistin voivat aiheuttaa vakaviakin oikeusturvariskejä passinhaltijalle.

---

757 Vertaa HE 234/2008 vp, s. 42, jossa näiden tietojen ei katsota muodostavan henkilörekisteriä, koska passin tekninen osa sisältää vain yhden henkilön tiedot.

758 HE 234/2009 vp, s. 43.

Sormenjälkitietojen käsittely. Sormenjälkitietojen ottaminen, laajamittainen tallentaminen passirekisteriin ja näiden tietojen käyttäminen merkitsee puuttumista yksityiselämän ja henkilötietojen suojaan. Tämä asettaa velvollisuuden säätää näistä tarkkarajaisesti lain tasolla.

Passilaissa on erikseen säädetty sormenjälkien ottamisesta (6 a §). Passinhakijan sormenjäljet ottaa passin myöntävä viranomainen eli käytännössä poliisi. Sormenjälki otetaan hakijan kahdesta sormesta. Ensisijaiset sormenjäljet ovat vasemman ja oikean etusormen sormenjäljet. Jos sormenjälkien laatu ei ole tyydyttävä, on talletettava keskisormien, nimettömien tai peukaloiden jäljet.

Joidenkin yksilöiden kohdalla sormenjälkien ottaminen on kuitenkin fyysisesti mahdotonta. Lainsäädännöllä ei tällaisessa tapauksessa voida asettaa yksilöitä eriarvoiseen asemaan matkustusoikeuden käyttämisessä heidän fyysisten ominaisuuksiensa vuoksi. Henkilön fyysiset rajoitteet eivät saa muodostaa estettä perustuslaissa turvatun liikkumisvapauden toteuttamiselle.[759]

Henkilöt, joilta sormenjälkiä ei voida ottaa iän taikka vamman, sairauden, fyysisen esteen tai muun vastaavan syyn vuoksi, on vapautettu sormenjälkien antamisesta. Tällöin edellytetään, ettei henkilöltä saada otettua sormenjälkiä mistään sormista siten, että päädyttäisiin kahden tunnistettavissa olevan sormenjäljen tallettamiseen.[760]

Sormenjäljet talletetaan passin tekniseen osaan sekä passirekisteriin sirullisten passien osalta. Siruttomien passien ja matkustusasiakirjojen hakijoiden kohdalla tiedot talletetaan vain passirekisteriin.[761]

---

759 Myös eduskunnan hallintovaliokunta on pitänyt tärkeänä sen varmistamista, ettei passin saaminen esty tai hankaloidu kohtuuttomasti fyysisen rajoitteen seurauksena ja ettei matkustusoikeus siten vaarannu. HaVL 30/2007 vp. Saman asian on esittänyt myös Euroopan tietosuojavaltuutettu lausunnossaan 2008/C 200/01.

760 HE 234/2008 vp, s. 50.

761 HE 234/2008 vp, s. 51.

Passinhaltijalta passin sirua varten otettavat sormenjäljet talletetaan passirekisteriin (29 §), johon sovelletaan henkilötietojen käsittelystä poliisitoimessa annettua lakia, jota on käsitelty jo edellä kappaleessa 5.4.2.

Yksilön näkökulmasta passirekisterin perustamisen tekee hankalaksi se, että EU:n passiasetus ei edellytä passin sormenjälkitietojen rekisteröintiä. Suomessa päädyttiin kuitenkin keskitetyn ratkaisun kannalle. Vastaavaan ratkaisuun on päädytty muissakin Eu:n jäsenvaltioissa, kuten Hollannissa, Virossa, Bulgariassa ja Kroatiassa.[762] Suomen ratkaisu passirekisteristä ei siis ole poikkeuksellinen. Sormenjälkitietojen tallettamista keskitettyyn rekisteriin on perusteltu kansalaisten oikeusturvalla, koska henkilön tunnistaminen voidaan tehdä luotettavasti ja nopeasti sekä passia haettaessa että muissa tunnistamistilanteissa.[763]

Rekisteröinnillä on tarkoitus myös suojata henkilön identiteettiä. Vertaamalla passinhakijan sormenjälkiä tietokannassa oleviin sormenjälkiin on mahdollista varmistua siitä, ettei henkilö hae passia useammalla henkilöllisyydellä tai että passi myönnetään hakijan tiedoilla vain yhdelle henkilölle. Tietokantaan talletetuilla sormenjäljillä voidaan varmistua myös henkilön henkilöllisyydestä tilanteessa, jossa hänen esittämänsä passin siru on rikki tai on rikottu. Lisäksi henkilöllisyys kyetään varmistamaan siinäkin tapauksessa, että henkilöllä ei ole asiakirjan katoamisen tai muun syyn vuoksi esittää asiakirjaa todistukseksi henkilöllisyydestään.[764]

---

762 *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 32

763 HE 234/2008 vp, s. 34. Katso myös HaVM 9/2009 vp sekä *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 7

764 HE 234/2008 vp, s. 34–35. Katso myös *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 7

Todettakoon, että pelkällä passin siruun talletetulla sormenjäljellä ei kyetä varmistamaan passinhakijan henkilöllisyyden luotettavaa todentamista. Se mahdollistaa ainoastaan vertailun, jossa henkilön sormenjälkeä verrataan siruun talletettuun sormenjälkeen. Vertailu ei myöskään mahdollista kaksois- ja monihenkilöllisyyksien estämistä.[765]

Tilanne perustelujen kohdalla on hyvin samanlainen kuin aiemmin kappaleessa 5.3.2.2. mainitussa säteilylain muuttamista koskeneessa hallituksen esityksessä. Tuossa tapauksessahan haluttiin valvoa itsepalvelusolariumien ikärajaa sormenjälkitunnistuksella. Sormenjälki itsessään ei tosiasiassa kuitenkaan ilman jo olemassaolevia vertailutietoja millään tavalla kerro yksilön henkilöllisyydestä. Sormenjälkeä voidaan käyttää vain välineenä henkilöllisyyden todentamisessa.

Passirekisteriin on arvioitu muodostuvan noin kymmenessä vuodessa sen perustamisesta tietokanta, johon sisältyy lähes kaikkien Suomen aikuisväestöön kuuluvien kaksi sormenjälkeä. Kysymyksessä on näin ollen myös suuri periaatteellinen muutos aikaisempaan oikeustilaan verrattuna, sillä perinteisesti sormenjälkien ottaminen ja erityisesti niiden rekisteröinti on liittynyt rikoksesta epäiltyihin henkilöihin.[766] Biometrisia tunnisteita sisältävään poikkeuksellisen laajaan tietokantaan liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille. Jo sormenjälkitietojen tallentaminen tällaiseen rekisteriin voi antaa aihetta huoleen yksityiselämän suojan kannalta.[767]

Edellä tämän tutkimuksen kappaleessa 4.3.2. on tuotu esiin niitä uhkia, joita biometristen tunnisteiden käyttäminen saattaa yleisellä ta-

765 HaVM 9/2009 vp, s. 3.

766 Tämä on todettu myös perustuslakivaliokunnan lausunnossa PeVL 14/2009 vp.

767 Katso PeVL 14/2009 vp sekä EIT:n ratkaisu S ja Marper v. Yhdistynyt kuningaskunta.

solla aiheuttaa. Passilakia koskevassa hallituksen esityksessä on otettu kantaa niihin uhkiin, joita nimenomaan sormenjälkien tallentaminen passirekisterin kaltaiseen keskusrekisteriin saattaa muodostaa.[768] Tällaisia ovat erityisesti tietojen luonteeseen (pysyvyys, muuttumattomuus ja peruuttamattomuus), sähköisen tunnisteen kopioitavuuteen ja levittämiseen liittyvät seikat. Sormenjälkitietojen joutuminen vääriin käsiin aiheuttaa erittäin merkittävää haittaa sekä yksittäisille henkilöille että rekisterin luotettavuudelle. Riskin suuruutta korostaa se, että rekisterissä tulee aikanaan olemaan lähes koko aikuisväestön sormenjälkitiedot.[769]

Passirekisterin perustamista puoltavien perusteiden kannalta asia vaikuttaa ongelmalliselta. Vaikka passirekisterin perustamisen tavoitteiden toteuttamisella pyritään osaltaan suojaamaan henkilökohtaista turvallisuutta ja estämään yksityiselämän suojaa loukkaavaa henkilöllisyyden väärinkäyttöä, ei passirekisterin perustamista tule näiden perusteiden kannalta nähdä täysin välttämättömänä ja oikeasuhtaisena.[770]

Oikeasuhtaisuuden kannalta oleellista olisikin ollut sen arvioiminen, onko sormenjälkien rekisteröinti sillä tavoin välttämätöntä, että passimenettelyyn liittyvä tavoite ei ole saavutettavissa yksityiselämän ja henkilötietojen suojaan vähemmän puuttuvin keinoin. Lisäksi huomiota olisi tullut kiinnittää siihen, merkitseekö rekisteröinti pidemmälle menevää rajoitusta kuin on perusteltua ottaen huomioon rekisteröinnin taustalla olevien passimenettelyyn liittyvien intressien painavuus suhteessa yksityiselämän ja henkilötietojen suojaan. Kysymys on siitä, että lainsäätäjän tulee turvata oikeus yksityiselämän ja

768 Katso HE 234/2008 vp, s. 63

769 PeVL 14/2009 vp, s. 3

770 Perustuslakivaliokunta kiinnitti erityistä huomiota tietoturvallisuuden riittämättömään tasoon, ja edellytti passirekisterin perustamista koskevan sääntelyn poistamista tai ainakin tietoturvallisuuden huomattavaa parantamista. PeVL 14/2009 vp, s. 4.

henkilötietojen suojaan perusoikeusjärjestelmän kokonaisuuden kannalta hyväksyttävällä tavalla. Kaikesta huolimatta estettä keskitetyn passirekisterin perustamiselle ei katsottu olevan.[771]

> Eräissä tämän asian kannalta relevanteissa perustuslakivaliokunnan lausunnoissa, viitataan useita kertoja Euroopan ihmisoikeustuomioistuimen käsittelemään tapaukseen S. ja Marper v. Yhdistynyt Kuningaskunta. EIT:n tuomio sisältää useita huomionarvoisia sormenjälkitunnistusta –ja rekisteröintiä koskevia linjauksia.
>
> Tapauksessa kaksi henkilöä, joista toinen alaikäinen, kantelivat siitä, ettei heidän rikosperusteisesti rekisteröityjä sormenjälkiään ja DNA-tunnisteitaan poistettu poliisin rekistereistä, vaikka S.:ä koskeva tutkinta keskeytettiin ja Marperia vastaan ei nostettu syytettä.
>
> Tapausta arvioidessaan EIT tarkastelee laajamittaista sormenjälkien ja DNA-tunnisteiden keräämistä keskitettyyn poliisin rekisteriin Euroopan ihmisoikeussopimuksen 8 artiklan vaatimuksia vasten. Ratkaisussaan tuomioistuin toteaa muun muassa seuraavaa: yksityiselämän suojaan puuttumista voidaan pitää "välttämättömänä demokraattisessa yhteiskunnassa" oikeutetun tavoitteen saavuttamiseksi, jos sillä vastataan "pakottavaan yhteiskunnalliseen tarpeeseen" ja varsinkin jos se on järkevässä suhteessa tähän oikeutettuun tavoitteeseen, sekä jos kansallisten viranomaisten esiintuomat perusteet ovat "relevantit ja riittävät".
>
> Edelleen tuomioistuin toteaa, että rikostorjunnan oikeutettu intressi saattaa olla suurempi kuin henkilötietojen kohtei-

771 Katso HaVM 9/2009 vp.

den edut ja yhteiskunnan kokonaisetu henkilötietojen, mukaan lukien sormenjälkien ja DNA-tunnisteiden, suojaamisessa

Erityisen mielenkiintoisena on pidettävä ihmisoikeustuomioistuimen tuomion kohdassa 105 kirjaamaa: "Tuomioistuin katsoo olevan kaiken väittelyn yläpuolella, että rikosten, varsinkin organisoidun rikollisuuden ja terrorismin, vastainen taistelu, joka on yksi tämän päivän eurooppalaisten yhteiskuntien haasteista, riippuu suuressa määrin modernien tieteellisten tutkinta- ja tunnistusmenetelmien käytöstä."

Lopputuloksenaan EIT totesi kuitenkin, että keskitetyn rekisterin eduista huolimatta lähtökohdaksi tulee ottaa tasapainon löytäminen yleisen turvallisuuden ja yksityiselämän suojan välille. Tuomioistuimen mukaan yksityiselämän suoja kohtuuttomasti heikkenee, jos modernien tieteellisten rikostutkintakeinojen käytön hyväksytään hinnalla millä hyvänsä menevän yksityiselämän suojan edelle. Tuomioistuimen mielestä tämä rajaa yksityiselämään puuttumisen hyväksyttävyyttä. Tuomioistuin huomautti lopuksi siitä, että jokainen uusien teknologioiden kehittämisessä edelläkävijän roolin ottava valtio kantaa erityisen vastuun oikean tasapainon saavuttamisesta.

Yksilön oikeuksien ja sormenjälkitietojen luonne huomioon ottaen on erittäin tärkeää, että tiedot suojataan siten, että niiden oikeudeton luku estetään mahdollisimman tehokkaasti. Passilakiin onkin otettu säännökset niistä tilanteista, joissa passin tekniiseen osaan sisältyviä sormenjälkitietoja voidaan lukea sekä passin sormenjälkitietojen lukemiseen oikeutetuista tahoista (5 b §). Passin tekniseen osaan talletettuja sormenjälkiä saa lukea sen mukaan kuin siitä säädetään EU:n passiasetuksessa. Lähtökohdan sormenjälkitietojen lukemiseen asettaa siis EU:n passiasetus. Sen 4 artiklan mukaan passien ja matkustusasiakirjojen sisältämiä biometrisia tunnisteita saa käyttää ainoastaan

asiakirjan aitouden toteamiseksi sekä haltijan henkilöllisyyden varmistamiseksi vertaamalla biometrisia tunnisteita suoraan saatavilla oleviin tunnisteisiin tilanteessa, jossa passi tai muu matkustusasiakirja on lain mukaan esitettävä.

Oikeutettuja sormenjälkitietojen lukemiseen ovat passiviranomainen sekä poliisi- tai rajatarkastusviranomainen. Sormenjälkitietoja voidaan näin ollen lukea henkilön henkilöllisyyden varmistamiseksi silloin, kun käyttötarve liittyy passinhakijan tunnistamiseen henkilön hakiessa passia tai passinhaltijan tunnistamiseen tilanteessa, jossa viranomaisella on henkilön matkustusoikeuteen, maastalähtöön ja maahantuloon liittyvä oikeus tarkastaa henkilöllisyys ja esitetyn asiakirjan aitous.

Sormenjälkiä luettaessa passinhaltijalta voidaan ottaa sormenjäljet ja otettuja sormenjälkiä voidaan verrata passin tekniseen osaan talletettuihin sormenjälkiin passin aitouden toteamiseksi ja passinhaltijan henkilöllisyyden varmistamiseksi. Jos passinhaltijan sormenjälkeä ei esimerkiksi sormiin kohdistuneen vamman tai sormenjälkien turmeltumisen vuoksi voitaisi ottaa, passinhaltijan henkilöllisyyden varmistaminen suoritettaisiin muulla luotettavalla tavalla.

On myös mahdollista, että passin sirua ei aina pystytä lukemaan. Jos teknisen osan tietoja ei syystä tai toisesta pystytä lukemaan, on tärkeää varmistaa passinhaltijan henkilöllisyys muulla luotettavalla tavalla. Passinhaltijan henkilöllisyys on tällaisessa tapauksessa mahdollista varmistaa myös vertaamalla passinhaltijalta vertailuun otettavaa jälkeä poliisin hallintoasiain tietojärjestelmään kuuluvaan passirekisteriin talletettuihin sormenjälkiin.[772] Vertaamista varten otetuilla tiedoilla tarkoitetaan sekä vertaamista varten otettavaa passinhaltijan sormenjälkeä (tunnistustapahtumatieto) että tietoa, joka luetaan sirusta tar-

772 HE 234/2008 vp, s. 46.

kastusta varten.[773] Näitä vertaamista varten otettuja sormenjälkitietoja on kuitenkin lupa käyttää vain vertaamisen ajan, ja ne on hävitettävä välittömästi sen jälkeen. Tiedon hävittäminen ei kuitenkaan saa johtaa sirun tiedon häviämiseen.[774]

Erityisesti biometristen tietojen käyttäminen ja luovuttaminen ovat yksityisyyden ja henkilötietojen suojan näkökulmasta erityisen merkityksellinen kysymys. Passirekisterin sormenjälkitietojen kohdalla tämä korostuu entisestään, sillä passirekisteri tulee aikanaan sisältämään lähes kaikkien suomalaisten sormenjäljet. Tämän vuoksi passin sormenjälkitietojen käyttö on tarkkarajaisesti säännelty PolHetiL:ssa (15, 16 ja 16 a §:t) sekä EU:n passiasetuksessa (4 artikla). Passirekisterin tietoja saa käyttää vain ja ainoastaan asiakirjan aitouden toteamiseksi sekä haltijan henkilöllisyyden varmistamiseksi. Passirekisteriin talletettujen sormenjälkien käyttö on näin ollen rajattu käytännössä vain passin käyttämiseen liittyviin tilanteisiin. Vain poikkeuksellisesti tietoja saa käyttää muuhun tarkoitukseen.

Rekisteriin talletettuja passinhakijan sormenjälkitietoja on näin ollen mahdollista käyttää henkilön henkilöllisyyden varmistamiseksi silloin, kun käyttötarve liittyy passinhakijan tunnistamiseen henkilön hakiessa passia tai passinhaltijan tunnistamiseen tilanteessa, jossa viranomaisella on henkilön matkustusoikeuteen, maastalähtöön ja maahantuloon liittyvä oikeus tarkastaa henkilöllisyys ja esitetyn asiakirjan aitous. Hakijalta otettua ja rekisteriin talletettua sormenjälkeä voidaan käyttää myös haetun asiakirjan valmistamiseksi.[775] Varsinaisen tunnistuksen lisäksi vertaamalla passinhakijan sormenjälkiä jo rekisterissä oleviin sormenjälkiin selvitetään, onko samalla henkilöllä rekisterissä useita eri henkilöllisyyksiä (kaksois- tai monihenkilöllisyys). Tällaisissa

773 HE 234/2008 vp, s. 45.
774 HE 234/2008 vp, s. 45.
775 HaVM 9/2009 vp, s. 2.

tapauksissa voi olla kyse tahallisesta usealla eri henkilöllisyydellä esiintymisestä tai rekisterin ylläpitäjän virheestä.[776]

Huomionarvoista on, että henkilön tunnistaminen rekisteriin talletetuista sormenjäljistä ei ole ensisijainen eikä välttämätön tunnistuskeino, sillä usein henkilö on tunnistettavissa myös muulla tavoin. Yleensä tämä tapahtuu esitetyn poliisin myöntämän henkilöllisyyttä osoittavan asiakirjan avulla.[777]

Passin sormenjälkitietojen käyttäminen muuhun kuin tietojen varsinaiseen keräämis- ja tallettamistarkoitukseen on ollut suuren keskustelun aiheena passilain muuttamisesta lähtien. Syynä on se, että poliisi on passilain muutoksesta lähtien halunnut oikeuden käyttää passirekisterin sormenjälkitietoja rikostutkinnassa. Passilain valmistelun yhteydessä vuonna 2009 oli esityksen lausuntokierrokseen saakka esillä mahdollisuus käyttää passin sormenjälkitietoja myös vakavimpien rikosten selvittämiseksi. Mainittu ehdotus kuitenkin poistettiin hallituksen esityksestä ennen sen antamista. Hallituksen esitys passilain uudistamiseksi ei siis sisältänyt ehdotusta passien sormenjälkien käyttämisestä vakavimpien rikosten torjunnassa. Vuonna 2013 julkaistussa sisäministeriön selvityksessä passirekisterin sormenjälkitietojen käyttämisestä vakavien rikosten torjunnassa poliisille esitettiin jälleen oikeutta käyttää passirekisterin sormenjälkitietoja rikostutkinnassa.[778]

---

776 *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 7.

777 *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 6.

778 Katso tarkemmin *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 48. Johtopäätöksestä syntyi eri mielisyyttä työryhmän sisällä. Osa jäsenistä katsoi, ettei poliisille myönnettävä oikeus passirekisterin sormenjälkitietojen käyttämiseen rikostutkinnassa olisi nykyisessä lainsäädäntötodel-

Tällä hetkellä alkuperäisestä keräämis- ja tallettamistarkoituksesta on kuitenkin mahdollista poiketa vain, jos se on välttämätöntä luonnononnettomuuden, suuronnettomuuden tai muun katastrofin taikka rikoksen kohteeksi joutuneen tai muuten tunnistamattomaksi jääneen uhrin tunnistamiseksi. Käytännössä kysymys on lain nojalla tapahtuvasta henkilön tunnistamisesta tilanteessa, jossa henkilöä ei muutoin saada tunnistettua, kuten tunnistamatta jääneen luonnononnettomuuden uhrin henkilöllisyyden selvittäminen. Esimerkiksi tsunami-katastrofin uhrien henkilöllisyyksien selvittämisessä sormenjäljillä oli merkittävä rooli. Vertailujälkiä oli kuitenkin tuolloin hankala saada, koska niitä jouduttiin etsimään erilaisista tunnistettavien henkilöiden käsittelemistä esineistä käyttäen rikostutkinnassa sovellettavia esillehakumenetelmiä.[779] Säännös ei siis mahdollista rikosten ehkäisyä tai selvittämistä rekisteriin talletettujen sormenjälkien avulla.[780]

---

lisuudessa ja perustuslakivaliokunnan tiukkojen kannanottojen tarkoituksenmukaista eikä lainsäädäntöhankkeella olisi menestymisen mahdollisuuksia.

779 *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 8.

780 HaVM 9/2009 vp, s. 5. Katso myös *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 6. Sisäministeriön selvityksessä arvioitiin, että passirekisteriin talletettujen sormenjälkitietojen käyttö rikostorjuntaan edellyttäisi kiinteää/selkeää yhteyttä alkuperäiseen keräämis- ja tallettamistarkoitukseen. Työryhmän näkemyksen mukaan passirekisteriin talletettujen sormenjälkitietojen käyttötarkoitusta olisi voitu laajentaa lailla säätäen kattamaan myös vakavimpien rikosten torjumisen aikaisemmin vakiintuneiden perusoikeuksien rajoitusperiaatteiden mukaisesti, mutta perustuslakivaliokunnan uuden tulkinnan mukaista selkeää/kiinteää yhteyttä sormenjälkien alkuperäisen keräämis- ja tallettamistarkoituksen ja vakavimpien rikosten selvittämisen välillä

Tietojen käyttämiseen varsinaisen keräämis- ja talletamistarkoituksen ulkopuolelle jääviin tarkoituksiin on varsinkin laajojen biometrisia tunnisteita sisältävien rekisterien yhteydessä suhtauduttava kielteisesti. Käyttötarkoitussidonnaisuudesta on mahdollista tehdä vain täsmällisiä ja vähäisiä poikkeuksia. Tämä on tärkeää etenkin käyttötarkoituksen määrittelyltä edellytettävän täsmällisyys- ja tarkkarajaisuusvaatimuksen kannalta. Sääntely ei saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötarkoitukseksi.[781]

> Passirekisterin tietojen käyttäminen muuhun kuin EU:n passiasetuksessa määriteltyihin passin tietojen käyttötarkoituksiin on ollut esillä EU:n tuomioistuimessa. Ratkaisussa C-446/12–C-449/12 Willems tuomioistuin otti kantaa siihen, tuleeko passiasetuksen 4 artiklan 3-kohtaa lukea rinnakkain henkilötietodirektiivin ja EU:n perusoikeuskirjan kanssa. Kysymys oli siis siitä, loukkaako passirekisterin tietojen käyttäminen muuhun kuin keräämistarkoitukseen oikeutta yksityisyyden ja henkilötietojen suojaan.
>
> Ratkaisussa tuomioistuin päätyi siihen, että passirekisterin perustaminen ei perustu passiasetukseen, jolloin siihen ei sovelleta EU:n oikeutta eikä näin ollen myöskään perusoikeuskirjan säännöksiä. Direktiivin soveltamisen osalta tuomioistuin päätyi vain toteamaan, että ennakkoratkaisupyyntö koski vain passiasetusta, ja koska passiasetuksen ei katsottu soveltuvan passirekisterin käyttöön, ei ollut tarvetta tarkastella asiaa myöskään direktiivin näkökulmasta.

---

ei työryhmän selvityksen perusteella löytynyt. *Sisäministeriö,* Selvitys passisorrmenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa, s. 41.

781 Katso PeVL 14/2009 vp.

Tuomioistuimen tulkintaa voidaan pitää arvelluttavana. Esimerkiksi aiemmassa ratkaisukäytännössä (C-617/10 Åkerberg Fransson) on katsottu, että (osittain) EU:n oikeudesta johtuviin kansallisiin toimiin sovelletaan EU-oikeutta eli myös henkilötietodirektiiviä ja perusoikeuskirjaa. Tätä tulkintaa on mahdollista käyttää myös käsillä olevassa tapauksessa. Kansalliset toimet (sormenjälkien tallentaminen passirekisteriin) perustuvat osittain EU:n passiasetukseen. Passiasetus velvoittaa jäsenvaltiot keräämään sormenjäljet passiin. Ilman asetuksen asettamaa velvoitetta sormenjälkiä ei edes kerättäisi eikä tallettaisi passirekisteriin. Asiaa olisi tämän vuoksi tullut arvioida EU-oikeuden, erityisesti perusoikeuskirjan ja henkilötietodirektiivin kannalta.

Tietoturva. Biometriset tunnisteet asettavat luonteensa puolesta erityisiä vaatimuksia tietoturvalle. Tunnistamiseen soveltuva biometrinen ominaisuus on pysyvä, muuttumaton ja peruuttamaton osa yksilöä. Tämän vuoksi biometriset tunnisteet asettavat erityisiä vaatimuksia tietoturvalle. Tällä tavoin voidaan varmistaa rekisteröidyn yksityisyyden suojan toteutuminen. Uhkia voidaan pyrkiä vähentämään muun muassa riittävän tehokkailla tietoturvaratkaisuilla.[782]

EU:n passiasetuksen 1 artiklan 2 kohdan mukaan passien ja matkustusasiakirjojen teknisen osan tiedot on suojattava. Tallennusvälineen on myös oltava kapasiteetiltaan riittävä ja sen on kyettävä takaamaan tietojen eheys, aitous ja luottamuksellisuus. Lisäksi passiasetuksessa säädetään, että passeja ja matkustusasiakirjoja varten on annettava tekniset eritelmät, jotka koskevat lisäturvaominaisuuksia ja -vaatimuksia, muun muassa tehostetut vaatimukset väärentämisen estämiseksi. Lisäksi eritelmät on annettava biometristen tunnisteiden

782 HE 234/2008 vp, s. 5.

tallennusvälineestä ja sen suojaamisesta sekä muun muassa sormenjälkiä koskevista laatuvaatimuksista ja yhteisistä säännöistä.

Komissio on antanut sekä kasvokuvaa että sormenjälkiä koskevat tekniset eritelmät.[783] Nämä sisältävät määräykset biometriikassa noudatettavista standardeista, tyypistä sekä formaatista ja laadusta. Lisäksi niissä on määräyksiä muun muassa sirun asemoinnista, aineistoturvallisuudesta ja tietojen eheydestä sekä vaatimustenmukaisuuden arvioinnista. Käytännössä kysymys on passin ja sirun fyysistä rakennetta ja siruun talletettujen tietojen oikeellisuuteen, aitouteen, eheyteen, luottamukseen ja pääsynhallintaan liittyvistä teknisistä menettelytavoista.

Tietoturvaan liittyvä passin sirun tietoihin kohdistuva pääsynvalvonta on määritelty komission antamissa teknisissä eritelmissä. Pääsynvalvonta on jaettu peruspääsynvalvontaan (Basic Access Control, BAC) ja laajennettuun pääsynvalvontaan (Extended Access Control, EAC). Peruspääsynvalvonta kattaa kaikki sirun sisältämät tiedot. Se toimii siten, että passin optisesta konelukukentästä muodostetaan avain, jota ilman sirun tietoja ei kyetä lukemaan ja jonka avulla sirun ja lukulaitteen välinen tietoliikenne salataan. Passin siruun talletettavat sormenjäljet suojataan lisäksi laajennetulla pääsynvalvonnalla. Laajennettu pääsynvalvonta suojaa sirua siten, että sormenjälkien lukeminen sirusta vaatii passin myöntäjämaan valtuuttamat lukulaitteet.[784]

Passilaissa poliisihallitukselle on asetettu velvollisuus huolehtia passin tekniseen osaan talletettujen tietojen suojaamisesta EU:n pas-

---

783 Kasvokuvaa koskevat tekniset eritelmät annettiin 28 päivänä helmikuuta 2005 (K(2005) 409 lopull.) ja sormenjälkiä koskevat tekniset eritelmät 28 päivänä kesäkuuta 2006 (K(2006) 2909 lopull.).

784 Pääsynvalvonta on saanut osakseen kritiikkiä erityisesti sormenjälkien kohdalla. Esimerkiksi salauksessa käytetyn avaimen hallinnointi on koettu ongelmalliseksi. Ongelmallisena on nähty myös se, että laajennettua pääsynvalvontaa ei tarvitse käyttää kuin sormenjälkien kohdalla. *Joint Research Center,* Large-scale Biometrics Deployment

siasetuksen ja sen soveltamiseksi annettujen säännösten mukaisesti tehokkaasti tunkeutumista, luvatonta lukemista, muuttamista, käyttöä ja muuta luvatonta käsittelyä vastaan. Passin sirun sormenjälkitiedot on suojattu oikeudettomalta lukemiselta EU:n passiasetuksen ja teknisten eritelmien mukaisesti siten, että siruun talletettuja sormenjälkiä on mahdollista lukea vain Suomen valtion valtuuttamilla lukulaitteilla. Tässä tarkoituksessa siruun talletetaan varmennetiedot, joilla varmistetaan, että vain ne tahot, joille Suomi myöntää lukuoikeuden, voivat lukea sormenjäljet passin sirusta. Sormenjälkien lukuoikeudet myönnetään vain niille, joilla on laissa säädetty oikeus sirun sormenjälkitietojen lukemiseen.[785] Varmenteet puolestaan ovat Väestörekisterikeskuksen vastuulla.

Sirun tiedot suojataan oikeudettomalta lukemiselta lisäksi siten, että siruun talletettuja tietoja on mahdollista lukea vain optisen konelukukentän lukemisen jälkeen. Näin estetään se, että tietoja luetaan passinhaltijan tietämättä ja ilman, että hän on antanut passin luettavaksi.[786] Järjestely toisin sanoen turvaa henkilökohtaisen myötävaikutuksen, mikä on tiedollisen itsemääräämisoikeuden kannalta keskeistä.[787]

(2008), s. 81–82, Fumy, Machine Readable Travel Documents, s. 102-106 sekä *Kindt,* Privacy and Data Protection Issues in Biometric Application, s. 733.

785 HE 234/2008 vp, s. 47.

786 HaVM 9/2009 vp, s. 4. Katso myös HE 25/2005 vp, s. 21.

787 Sirun tietoturva sai osakseen paljon kritiikkiä erityisesti biometrisen passin käyttöönoton alkuvaiheessa. Useat tutkijaryhmät ilmoittivat, että sirun tietoja oli mahdollista lukea ja kopioida etäältä ilman passinhaltijan tietoisuutta, koska sirussa käytettävä salausmenetelmä ei ollut riittävän tehokas suojaamaan sirun tietoja. *Avoine – Kalach – Quisquater,* Belgian Biometric Passport does not get a pass…Your

Siruun talletettavien biometristen tunnisteiden luonne huomioiden on erityisen tärkeää, että tiedot suojataan niiden oikeudettomalta käsittelyltä mahdollisimman tehokkaasti.[788] Erityisen merkityksellistä näiden tietojen suojaaminen on sen vuoksi, kun ei ole yleisiä säännöksiä biometristen tunnisteiden käytöstä.[789]

Oleellisen osan sormenjälkitietojen tietoturvassa muodostaa myös passirekisterin tietoturvasta huolehtiminen. Tästä säädetään PolHetiL 10 a §:ssä. Erityisen tärkeää on, ettei tietokannan sisältöä päästä käsittelemään ilman valtuuksia ja että sormenjälkirekisteri on vain sitä tehtävissään välttämättä tarvitsevien ja tämän vuoksi käyttöoikeuksia omaavien virkamiesten käytettävissä. Sormenjäljet talletetaan tietokantaan lukukelvottomassa muodossa, käyttäen digitaalista salausmenetelmää. Salausmenetelmän käytöllä estetään tietojen oikeudeton lukeminen ja käyttö tietokannasta. PolHetiL 10 a §:n säännös yhdessä passilain 5 c §:n kanssa muodostavat passin sormenjälkitietojen tietoturvavelvoiteen.

---

personal data are in danger sekä *Joint Research Center,* Large-scale Biometrics Deployment (2008), s. 83. Katso myös *Kindt,* Belgisch biometrisch paspoort onveilig, s. 221–223.

788 Perustuslakivaliokunta on edellyttänyt tietoturvan parempaa huomioon ottamista jo passiuudistuksen ensimmäistä vaihetta toimeenpantaessa vuonna 2005. Katso PeVL 27/2005 vp. Tuolloin hallintovaliokunta kuitenkin katsoi, että tietoturvan yksityiskohtaisempi sääntely olisi tarpeen vasta passilain uudistuksen toisessa vaiheessa, jolloin siruun talletetaan myös sormenjäljet. HaVM 13/2006 vp.

789 Perustulakivaliokunnan mielestä lähes koko Suomen aikuisväestön kattavaa sormenjälkirekisteriä ja siihen liittyviä korostettuja tietoturvavaatimuksia voidaan jatkossa paremmin arvioida laajempana kysymyksenä esimerkiksi biometrisia tunnisteita ja niiden käyttöä koskevan yleisen henkilötietojen suojaa koskevan lainsäädännön valmistelun yhteydessä. PeVL 14/2009 vp, s. 4.

5.6. Biometrinen tunnistaminen Yhdysvalloissa

5.6.1. Yleistä

Yhdysvalloissa biometristen tunnisteiden hyödyntäminen eri yhteyksissä on huomattavasti laajempaa kuin Suomessa ja Euroopan Unionissa. Yhdysvaltain hallinto on yhä enenevässä määrin kehittämässä ja tutkimassa mahdollisuuksia kehittää luotettavia ja tehokkaita keinoja maan turvallisuuden takaamiseksi. Esimerkkinä toimii ensinnäkin Status Indicator Technology – ohjelma, joka hyödyntää biometrisen tunnistamisen teknologioita Yhdysvaltain lentokentillä. Toisena esimerkkinä on pian vuoden 2001 terrori-iskujen jälkeen voimaantullut US Patriot Act[790], joka on omalta osaltaan ollut rohkaisemassa biometriaan perustuvien tunnistusratkaisujen käyttöönottoa. Biometrisen tunnistamisen laajan hyödyntämisen vuoksi on tärkeää käydä läpi Yhdysvaltain yksityisyyden suojaa ja henkilötietojen suojaa koskevaa lainsäädäntöä.

Yhdysvaltain yksityisyyden ja henkilötietojen suojan sääntely eroaa merkittävästi eurooppalaisesta ja suomalaisesta vastineestaan. Liittovaltiotason yleisestä yksityisyyssääntelystä huolimatta Yhdysvalloissa ei ole samanlaista yleistä henkilötietojen suojan sääntelyä kuin Euroopan Unionissa ja Suomessa. Yhdysvalloissa henkilötietojen ja yksityisyyden suojan taso on tämän vuoksi melko heikko eurooppalaiseen ja suomalaiseen lainsäädäntöön nähden.[791]

---

790 Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act of 2001, 107 P.L. 56, 115 Stat. 272. Laki tuli voimaan lokakuussa 2001, pian syyskuun 11. päivän terrori-iskujen jälkeen.

791 Erityisesti biometriseen tunnistamiseen liittyvä oikeuskäytäntö osoittaa, että biometristen tunnisteiden käyttöä sinänsä ei ole millään tavoin haluttu rajoittaa. Tämä tarkoittaa sitä, että niin julkinen

Yhdysvaltojen lainsäädännön laajuuden vuoksi, tässä jaksossa ei käydä läpi kaikkia Yhdysvalloissa annettuja yksityisyyttä koskevia lakeja. Tarkoituksena on keskittyä yksityisyyden suojan ja biometrisen tunnistamisen kannalta oleellisimpaan lainsäädäntöön pääpiirteittäin.

5.6.2. Yksityisyyden lainsäädännöllinen perusta

Yhdysvalloissa yksityisyyttä suojataan kolmen eri kokonaisuuden kautta. Ensimmäisenä on Yhdysvaltain liittovaltion perustuslaki ja tähän liitetty kansalaisoikeuksien julistus (Bill of Rights). Perustuslaki ei kuitenkaan nimenomaisesti mainitse yksityisyyttä perusoikeutena, mutta Korkeimman oikeuden mukaan yksityisyyttä suojataan perustuslain 1, 3, 4, 5, 9 ja 14 lisäyksien (amendments) kautta.

Toisen kokonaisuuden muodostavat liittovaltiotasolta tulevat yksityisyyden suojaa toteuttavat säädökset. Näistä tämän tutkimuksen kannalta keskeisimpiä ovat vuoden 1974 Privacy Act sekä vuoden 1999 Financial Modernization Act, jota on kuvattu laajamittaisimmaksi yksityisyyden suojaa koskevaksi laiksi.

Kolmas kokonaisuus muodostuu vahingonkorvausoikeusnormiston ja sitä koskevan oikeuskäytännön kautta (privacy in torts). Tämä yksityisyyden suojan muoto sai alkunsa Warren & Brandeis´n artikke-

---

hallinto kuin yksityissektori voivat jopa velvoittaa biometristen tunnisteiden antamiseen. Tosin biometristen tietojen alkuperäistä käyttötarkoitusta vastoin tapahtuvan biometristen tietojen käsittelyn on katsottu loukkaavan yksilön oikeutta yksityisyyteen, ainakin joissain osavaltioissa. Katso tästä esimerkiksi Perkey v. Department of Motor Vehicles (197 Cal. Rptr. 516), jota käsitellään tarkemmin jaksossa 5.5.3.1.

lista ”The Right to Privacy”, jossa ensimmäistä kertaa käytettiin käsitettä yksityisyys (the right to be let alone).[792]

Yksityisyyden lainsäädännöllisen suojan kokonaisuus perustuu hyvin pitkälti William Prosserin 1960-luvulla tekemään jakoon neljään eri suojattavaan oikeushyvään: 1) yksilöivän tiedon luvaton käyttö (misappropriation), 2) yksityiselämää koskevan tiedon levittäminen julkisuudessa (public disclosure of private facts); 3) vääränlaisen kuvan antaminen yksilöstä julkisuuteen (false light in the public eye) ja 4) eristäytyneisyyden loukkaus (unreasonable intrusion upon seclusion).[793]

Myös osavaltiot suojaavat yksityisyyttä perusoikeutena joko nimenomaisesti tai tulkinnan kautta.[794] Yhdysvaltojen osavaltiot ovat antaneet yksityisyyden suojaa koskevaa erityislainsäädäntöä, joista osa koskee myös biometrisia tunnisteita. Näistä voidaan esimerkkeinä mainita Illinois´n osavaltion Biometric Information Privacy Act sekä Texasin osavaltion Business and Commerce Code, johon on otettu biometrisia tunnisteita koskevat säännökset.

---

792 *Warren – Brandeis,* The Right to Privacy. Harvard Law Review. Vol 4, No. 5.

793 *Prosser,* Privacy, s. 383–407.

794 Esimerkkinä yksityisyyden suorasta suojaamisesta perustuslaissa voidaan mainita Kalifornian osavaltion perustuslaki. Texasin osavaltion perustuslaki puolestaan toimii esimerkkinä, jossa yksityisyyttä suojataan välillisesti useiden perustuslain pykälien kautta.

5.6.3. Biometristen tunnisteiden asema yksityisyyttä koskevassa lainsäädännössä

5.6.3.1. Yhdysvaltain perustuslaki

Toisin kuin Suomessa, Yhdysvaltain perustuslaki ei yksiselitteisesti takaa oikeutta yksityisyyteen.[795] Tästä huolimatta oikeus yksityisyyteen on Yhdysvaltain Korkeimman Oikeuden ratkaisukäytännössä katsottu yhdeksi tärkeimmistä perusoikeuksista, joka johdetaan Kansalaisoikeuksia koskevan julistuksen (Bill of Rights) lisäyksistä 1 (uskonnon-, sanan, lehdistön- ja kokoontumisvapaus on turvattu), 3 (turvaa oikeuden olla majoittamatta sotilaita), 4 (kotirauha ja fyysinen koskemattomuus on turvattu), 5 (omaisuus, elämä ja vapaus on turvattu), 9 (myös muut kuin perustuslaissa nimenomaisesti mainitut oikeudet turvataan) ja 14 (yhdenvertaisuus).[796] Biometrisen tunnistamisen kannalta merkityksellisiä ovat lisäykset 1, 4 ja 5, joita tässä jaksossa käydään tarkemmin läpi.[797]

---

795 Jotkut osavaltiot ovat ottaneet yksityisyyden osaksi perustuslakiaan. Näistä voidaan mainita esimerkiksi seuraavat osavaltiot: Alaska, Arizona, California, Florida, Havaji, Illinois ja Washington.

796 *Solove – Schwartz,* Privacy Law Fundamentals, s. 3. Yksityisyyden perustuslaillisesta kehityksestä ja siihen liittyvästä Yhdysvaltain Korkeimman oikeuden ratkaisukäytännöstä katso McWhirter – Bible, Privacy as Constitutional Right. Quorum Books, New York. 1992 sekä erityisesti oikeuskäytännöstä Bartee, Privacy Rights. Cases Lost and Causes Won Before the Supreme Court. Bowman & Littlefield Publishers, Inc. United States of America 2006.

797 Toisaalta tulee kuitenkin huomauttaa siitä, että valvontaa ja biometrista tunnistamista sen osana voidaan käyttää myös syrjiviin tarkoituksiin, jolloin keskeinen on myös kansalaisoikeuksien julistuksen lisäys 14. Valvonnasta sosiaalisena lajitteluna katso Lyon (ed.) Sur-

Huomionarvoinen ero Suomen perustuslakiin nähden on se, että Yhdysvaltain perustuslailla on vain vertikaalivaikutus. Perustuslaki turvaa oikeuden yksityisyyteen vain suhteessa julkishallintoon jättäen yksityiset ja erityisesti kaupalliset toimijat ulkopuolelle. Henkilötietojen suojaa ei mainita perustuslaissa eikä kansalaisoikeuksien julistuksessa.[798] Yksilön tiedollisen yksityisyyden suojaamiseen voidaan käyttää lisäyksien 4. ja 5. säännöksiä.[799]

Yhdysvaltain perustuslain ensimmäinen lisäys takaa jokaiselle uskonnon-, ilmaisun-, ja kokoontumisvapauden.[800] Pykälä on merkityksellinen siksi, että anonymiteetti on osa yksilön oikeutta sananvapauteen, ja sen katsotaan suojaavan yksilöä julkisen vallan perusteettomalta valvonnalta.[801]

---

veillance as Social Sorting.

798 Lähimmäksi henkilötietojen suojan tunnustamisessa perusoikeudeksi on päästy Korkeimman Oikeuden ratkaisussa Whalen v. Roe (429 U.S. 589 (1977)), jossa yksityisyyteen katsottiin sisältyvän kaksi eri intressiä: yksityisten asioiden suojaaminen julkisuudelta ja mahdollisuus tehdä omia asioitaan koskevia päätöksiä.

799 Näin myös *Solove – Schwartz,* Information Privacy Law (2011), s.248.

800 Pykälä on seuraavan sisältöinen: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

801 Ratkaisu McIntyre v. Ohio Elections Commission (514 U.S. 334 (1995), erityisesti tuomari Stevensin mielipide sekä Froomkin, Anonymity and the Law in the United States, s. 437-440. Katso myös Slobogin, Public Privacy. Camera Surveillance of Public Places and the Right to Anonymity. Mississippi Law Journal No. 72 (2002), s. 213–316

Julkisen vallan taholta tapahtuva biometristen tunnisteiden kerääminen sananvapautta harjoittavalta henkilöltä on mahdollista nähdä yksilön anonymiteetin loukkauksena. Tällaisessa tapauksessa julkisen vallan on pystyttävä oikeuttamaan biometrisen tunnistamisen käyttö järkevällä lainvalvonnallisella tarkoituksella. Lisäyksen 1 loukkaus edellyttää kuitenkin, että biometrinen tunnistaminen rajoittaa yksilön oikeutta sananvapauteen.

Anonymiteetti[802] on myös hyvin läheisessä yhteydessä liikkumisvapauteen.[803] Tunnistamismenetelmien käyttö julkisella alueella saattaa aiheuttaa ihmisissä tarpeen julkisten alueiden välttelemiseen, mikä puolestaan rajoittaa yksilön vapautta liikkua vapaasti tunnistamattomana.[804] Toistaiseksi perustuslain, kansalaisoikeuksien julistuksen ja näitä koskevan oikeuskäytännön näkökulmasta yksilöllä ei kuitenkaan ole oikeutta yksityisyyteen ollessaan julkisella paikalla.

---

802 Anonymiteetti johdetaan omalta osaltaan myös 14 lisäykseen sisältyvästä oikeudenmukaisen oikeudenkäynnin lausekkeesta (due process –clause). Froomkin, Anonymity and the Law in the United States, s. 447-455 ja Griswold v. Connecticut (381 U.S. 479 (1965)).

803 Yhdysvaltain perustuslaki ei suoraan takaa oikeutta liikkumisvapauteen, vaan se johdetaan perustuslain 4 artiklan 2 kohtaan sisältyvästä Privileges and Immunities –klausuulista. Wilhelm, Freedom of Movement at a Standstill? Toward the Establishment of a Fundamental Right to Intrastate Travel, s. 2465-2466. Oikeus liikkumisvapauteen on ollut esillä muun muassa Wisconsinin osavaltion valitusoikeuden ratkaisussa State v. Bauman (275 Wis. 2d 278(2004)).

804 Ratkaisussa Kolender v. Lawson (461 U.S. 352 (1983)) katsottiin, että lakisääteinen velvollisuus todistaa henkilöllisyytensä oleskeltaessa julkisella paikalla ilman näkyvää syytä aiheutti huolen yksilön liikkumisvapauden näkökulmasta. Katso myös ratkaisu Carey v. Nevada Gaming Control Board (279 F.3d 873 (9th Cir. 2002)).

Yhdysvaltain perustuslaki takaa sen 4 lisäyksessä jokaiselle oikeuden henkilökohtaiseen koskemattomuuteen sekä kotirauhaan. Suojan piiriin kuuluu myös omaisuus. Oikeudet eivät kuitenkaan ole ehdottomia, sillä näitä oikeuksia suojataan vain valtion taholta tulevilta kohtuuttomilta puuttumisilta.[805]

Perusajatuksena lisäyksessä on yksilöiden suojaaminen mielivaltaiselta puuttumiselta yksilön henkilöön ja omaisuuteen, johon kuuluu myös suojaaminen eri valvonnan muodoilta.[806] Pääasiallisena kohteena lisäyksessä on yksilön fyysisen yksityisyyden suojaaminen.[807]

Yhdysvaltain korkeimman oikeuden oikeuskäytännössä biometrisen tunnisteen (tässä tapauksessa sormenjäljen) ottamista ei ole toistaiseksi pidetty lisäyksen 4 vastaisena kohtuuttomana yksilön henkilöön

805 Pykälä on seuraavan sisältöinen: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

806 Näin myös *Solove – Schwartz,* Information Privacy Law (2011), s. 247, joiden mukaan tarkkailu ja informaation kerääminen ovat suuri uhka yksityisyydelle. He kuitenkin muistuttavat siitä, että tarkkailu ja informaation kerääminen samalla edistävä turvallisuutta.

807 Korkeimman oikeuden ratkaisu Olmstead v. United States (277 U.S. 438 (1928)), jossa Korkein oikeus totesi 4. lisäyksen suojaavan vain fyysisen koskemattomuuden loukkauksilta. Korkein oikeus sovelsi ratkaisun oikeusohjetta lähes 40 vuotta, kunnes kehittyvä teknologia pakotti muuttamaan tulkintaa. Myös ratkaisussa Schmerber v. California (384 U.S. 757 (1966)) Korkein oikeus totesi nimenomaisesti, että 4 lisäyksen kohteena on yksilön henkilöllisen yksityisyyden (personal privacy) ja omanarvontunnon suojaaminen valtion taholta tapahtuvalta oikeudettomalta puuttumiselta.

kohdistuvana etsintänä. Tämä käy ilmi vuonna 1969 Korkeimman oikeuden antamasta ratkaisusta *Davis v. Mississippi*, jossa sormenjäljen ottamista ei pidetty henkilöön kohdistuvana etsintänä, sillä tällaisella toimella ei puututa yksilön elämään ja ajatuksiin.[808]

Asiaa on mahdollista lähestyä myös toisesta näkökulmasta. Davis v. Mississippi -ratkaisun jälkeisen oikeuskäytännön valossa biometrisen tunnisteen keräämistä ja käyttämistä on mahdollista pitää yksilön henkilöön kohdistuvana etsintänä. Tällaisella toimella ensinnäkin puututaan yksilön fyysiseen koskemattomuuteen ja / tai sen kautta saadut tiedot voivat paljastaa yksilön terveyttä koskevia tietoja. Vaikka etsintää sinänsä ei pidettäisikään kohtuuttomana, on se silti mahdollista nähdä lisäyksessä tarkoitettuna etsintänä, jos sen kautta saadut tiedot paljastavat arkaluonteisia yksityisiä asioita.[809]

---

808 Davis v. Mississippi, (394 U.S. 721 (1969)). Sama on todettu ratkaisussa Dunaway v. New York (442 U.S. 200 (1979)). VertaaEIT:n ratkaisu M.K. v. Ranska, jossa sormenjäljet katsottiin kuuluvan yksityisyyden suojan piiriin.

809 Tämä ajatus voidaan johtaa Yhdysvaltain korkeimman oikeuden ratkaisuista Vernonia School District 477 v. Acton (515 U.S. 646 (1995) ja Skinner v. Railway Labour Executives Association (489 U.S. 602 (1989), joissa kysymys oli virtsanäytteen antamisesta. Skinner -tapauksessa Korkein oikeus nimenomaisesti lausui virtsanäytteen ottamisessa olevan kysymys puuttumisesta yksilön henkilöön, vaikka siinä ei fyysisesti puututakaan yksilön fyysiseen koskemattomuuteen. Samanlaista ajattelutapaa kuvaa myös ratkaisu Kyllo v. United States (533 U.S. 27, (2001), jossa lämpötunnistukseen perustuvan laitteen suuntaamista asuntoon pidettiin etsintänä, vaikka laite ei fyysisesti päässytkään taloon sisälle. Ratkaisussa omaksuttua ajattelutapaa voidaan analogisesti soveltaa biometriseen tunnistamiseen, sillä tämän toimen tarkoitus on määrätietoinen tietojen kerääminen yksilön

Biometriseen tunnistamiseen liittyy myös valvonnan näkökulma. Valvontaa on mahdollista tietyissä tilanteissa pitää lisäyksen 4 mukaisena etsintänä[810], mikäli valvonta loukkaa yksilön perusteltua oletusta nauttia yksityisyyteensä kohdistuvaa kunnioitusta.

Käytettäessä biometristä tunnistamista voi kysymyksessä olla perustuslain 4. lisäyksessä tarkoitettu etsintä tai tarkastus, joka ei saa olla kohtuuton.[811] Etsintä tai tarkastus on lähtökohtaisesti mahdollista nähdä kohtuullisena sen perustuessa oikeuden myöntämään etsintälupaan. Tällöin riippumaton taho on arvioinut etsinnän perustuvan perusteltuun epäilyyn rikoksen tapahtumisesta tai todisteiden löytymisestä.[812] Yksityisyyden näkökulmasta kohtuuttomuutta arvioidaan

---

henkilöstä. Katso esimerkiksi Slobogin, jonka mukaan tarkastuksessa on kysymys johonkin katsomisesta tai jonkin etsimisestä. Slobogin, Is the Fourth Amendment Relevant in a Technological Age?, s. 13.

810 Tämä ajattelutapa on kuitenkin vielä ristiriitainen Korkeimman oikeuden ratkaisukäytännössä. Esimerkiksi vuoden 1983 tapauksessa United States v. Knotts (460 U.S. 276 (1983)) valtion kemikaalisäiliöön kiinnittämää seurantalaitetta ei pidetty pykälässä 4 tarkoitettuna etsintänä, koska tällainen seuranta ei Korkeimman oikeuden mukaan aiheuttanut mitään uutta perustuslaillista ongelmaa. Tosin vuonna 2005 antamassaan ratkaisussa U.S. v. Jones (615 F. 3d 544 (2012) Korkein oikeus katsoi, että ajoneuvon ympärivuorokautinen seuranta GPS-järjestelmän avulla yksilön liikkeiden tarkkailemiseksi nähtiin yksilöön kohdistuvana etsintänä, ja perustuslain 4 pykälän vastaisena. Oikeus totesi seuraavaa: ”a Fourth Amendment search occurs whenever the government violates a subjective expectation of privacy that society recognizes as reasonable, which is particularly important in an era where physical intrusion is unnecessary to many forms of surveillance.”

811 Katso *U.S. v. Jones* (615 F. 3d 544 (2012) sekä alaviite 625.

812 Brinegar v. United States (338 U.S. 160 (1949)) ja *Solove – Schwartz,* Information Privacy Law (2011), s. 251.

lisäksi kahden periaatteen kautta: 1) yksilöllä on tilanteessa ollut perusteltu oletus nauttia yksityisyyden suojan kunnioitusta ja 2) oletus on ollut yhteiskunnan kannalta hyväksyttävä.[813]

Yhdysvaltain Korkeimman oikeuden ratkaisukäytännössä on katsottu, että yksilöllä ei lähtökohtaisesti ole perusteltua oletusta yksityisyyteen julkisella paikalla. Tätä on oikeuskäytännössä perusteltu sillä, että tällaisessa tilanteessa yksilö tietoisesti paljastaa nämä asiat toisille, jolloin kysymyksessä ei ole lisäyksen 4 loukkaus.[814] Biometristen tunnisteiden kerääminen julkisella paikalla ei näin ollen loukkaa perustuslain 4 lisäystä, koska yksilö itse tuo julki fyysiset ominaispiirteensä.[815]

On perusteltua kysyä, miten pitkälle tämä periaate on mahdollista viedä. On olemassa tilanteita, joissa yksilöllä on perusteltu oletus yksityisyyteen myös ollessaan julkisella paikalla.[816] Vahingonkorvausnor-

---

813 Katso Katz v. U.S. (389 U.S. 347 (1967)), Chandler v. Miller (520 U.S. 305 (1997)) sekä Berger v. New York (388 U.S. 41 (1967)). Vertaa kuitenkin Rakas et al. v. Illinois (439U.S. 128), jossa henkilöllä ei katsottu olevan perusteltua oletusta yksityisyyden suojaan, koska hän oli matkustajana toisen henkilön omistamassa ajoneuvossa eikä näin katsottu olevan kotirauhan suojaamassa paikassa. Katso myös *Solove – Schwartz,* Information Privacy Law (2011), s. 269.

814 Näin muun muassa Yhdysvaltain Korkeimman oikeuden ratkaisuissa Katz v. U.S. (389 U.S. 347 (1967) sekä U.S. v. Dionisio (410 U.S. 1 (1973). Katso myös *McCoy,* O´ Big Brother Where Art Thou? The Constitutional Use of Facial-recognition Technology. John Marshall Journal of Computer and Information Law, XX (3), s. 471–485.

815 Biometrisen tunnistamisen kohdalla tällainen perustelu on kuitenkin ongelmallinen, sillä kaikki biometriset tunnisteet (esimerkiksi silmän verkkokalvo) eivät ole vaikeudetta julkisesti saatavilla.

816 Esimerkkinä voidaan mainita kasvontunnistusohjelman käyttäminen julkisella paikalla. Tampassa, Floridassa, poliisi käytti kasvotunnistusta Superbowl-tapahtumassa vuonna 2001. Poliisi perusteli kas-

miston perusteella syntyneessä oikeuskäytännössä on katsottu yksilöllä joissain tilanteissa voivan olla perusteltu oletus yksityisyydestä julkisella paikalla (katso jakso 5.5.3.3).

Perustuslain 4. lisäyksen loukkaamisesta ei ole kysymys myöskään, mikäli yksilöön kohdistuva toimi perustuu vapaaehtoisuuteen. Mikäli yksilöllä on mahdollisuus kieltäytyä toimesta, ei kysymys ole oikeudettomasta puuttumisesta yksilöön.[817] Biometrisen tunnistamisen kohdalla tämä tarkoittaa sitä, että yksilön suostumukseen perustuva biometrisen tunnistamisen käyttäminen ei loukkaa yksilön oikeutta yksityisyyteen perustuslain näkökulmasta.[818] Ongelmana on, että yksilölle harvoin annetaan todellista mahdollisuutta jättäytyä biometrisen järjestelmän ulkopuolelle, mikä tekee suostumusinstituution melko turhaksi.

Oman kokonaisuutensa 4. lisäyksen kohdalla muodostavat niin sanottu Special needs –doktriini sekä hallinnolliset tarkastukset (admi-

---

vontunnistuksen käyttöä analogisella tulkinnalla fyysisesti paikalla olevaan poliisiin kuva kädessä. Kasvontunnistusohjelman käyttö on kuitenkin täysin erilainen, sillä poliisimiehen piilottaminen on huomattavasti hankalampaa kuin kameran. Myöskin poliisin mahdollisuudet havainnointiin ovat erilaiset. Moni myös varmasti ymmärtää eron satunnaisen havainnoinnin ja jatkuvan seurannan välillä. Kasvontunnistusohjelma on myös alttiimpi väärinkäytöksille esimerkiksi sosiaalisen kontrollin harjoittamiseen. Näin myös *Agre,* Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places (Sept. 10, 2003). Saatavissa osoitteessa: http://polaris.gseis.ucla.edu/pagre/bar-code.html

817 Katso esimerkiksi *U.S. v. Mendenhall* (446 U.S. 544 (1980)) sekä Florida v. Bostick (501 U.S. 429 (1991)).

818 Tämä ajatus vastaa hyvin pitkälti Euroopan tietosuojadirektiiviä. Erona tosin on se, että yhdysvaltalaisessa järjestelmässä yksilöä ei tarvitse informoida kieltäytymisen mahdollisuudesta.

nistrative searches).[819] Special needs –doktriini oikeuttaa tekemään etsinnän tai tarkastuksen ilman oikeuden myöntämää lupaa tilanteissa, joissa tarkastuksen tekemiseen on erityinen tarve ja luvan hankkiminen on epätarkoituksenmukaista.[820] Doktriinin nojalla tehtyyn etsintään kuitenkin sovelletaan kohtuullisuusarviointia kaikissa tilanteissa.[821] Doktriinia sovelletaan kouluissa, valtionalan työpaikoilla ja tietyillä säännellyillä liiketoiminnan alueilla, eikä tällaista etsintää tehdä lainvalvontatarkoituksessa.[822]

Hallinnollisia tarkastuksia ei myöskään tehdä lainvalvontatarkoituksessa[823], vaan niiden tarkoitus on edesauttaa jotakin hallinnollista tavoitetta kuten turvallisuutta. Näitä tarkastuksia varten ei tarvita oikeuden myöntämää lupaa eikä epäilystä rikoksesta. Niitä kuitenkin koskee sama kohtuullisuuden vaatimus kuin muitakin etsintöjä.[824] Li-

---

819 Hallinnollisista tarkastuksista (administrative search) katso tarkemmin *Eve Brensiker Primus,* Disentangling Administrative Searches, Columbia Law Review, Issue 8,Vol 111 (2011), s. 254-312.

820 Griffin v. Wisconsin (483 U.S. 868 (1987))

821 O´Connor v. Ortega (480 U.S. 709 (1987))

822 Esimerkkinä voidaan mainita lukiossa suoritettava satunnainen huumetesti kouluajan ulkopuoliseen kilpailutoimintaan osallistuville opiskelijoille. Board of Education v. Earls (536 U.S. 822 (2002)) ja *Solove – Schwartz,* Information Privacy Law (2011), s. 252.

823 Huomautettava on siitä, että hallinnollista tarkastusta ei edes saa suorittaa rikostutkintatarkoituksessa. Michigan v. Clifford (464 U.S. 287 (1984).

824 Tämä tarkoittaa sitä, että tarkastuksia ei saa tehdä täysin mielivaltaisesti. Katso *United States v. Davis* (482 F. 2d 893, Court of Appeals, 9th Cir. 1973), jossa hallinnollisten tarkastusten oikeutus ja kohtuullisuusvaatimus vahvistettiin sekä viimeaikaisesta oikeuskäytännöstä U.S. v. McCarty (648 F. 3d 820, 9th Circuit 2011), jossa oikeus totesi kohtuullisuudesta seuraavaa: "a search is constitutionally reasonable

säksi edellytetään, että tarkastukselle on perusteltu pakottava tarve ja että tarkastuksesta päättäminen ei ole yksin kenttävirkailijan tehtävissä.

Oikeuskäytännössä omaksutun ajatuksen mukaan hallinnollisen tarkastuksen kohtuuttomuutta arvioidaan punnitsemalla keskenään yksilön tarvetta yksityisyyteen ja julkisen vallan intressiä yleisen turvallisuuden takaamiseen. Kohtuullisuus on kuitenkin arvioinnin kannalta kaikkein tärkein vaatimus.[825] Julkisen intressin, kuten yleisen turvallisuuden, turvaaminen on yleensä myös oikeutus käyttää biometristä tunnistamista hallinnollisten tarkastusten yhteydessä alueilla, joissa yleisen turvallisuuden takaaminen on erityisen tärkeää.

Tarkastuksissa kysymys ei siis ole yksilön yksityisyyteen puuttumisesta 4. lisäyksen vastaisesti. Edellytyksenä kuitenkin on, että tällainen tarkastus on rajoitettu ja oikeassa suhteessa tavoitteeseen nähden, toisin sanoen toimenpide ei saa olla kohtuuton. Biometristen tietojen kohdalla arvioitavaksi tulee myös tapa, jolla biometrisia tietoja kerätään ja käsitellään sekä keinot, joilla estetään biometristen tietojen luvaton kerääminen ja käyttö.[826]

---

only where it is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives and where it is confinedin good faith to that purpose."

825 Tämä käy hyvin ilmi tapauksesta United States v. Edwards (415 U.S. 800 (1974)) Katso myös *Electronic Privacy Information Center v. United States Department of Homeland Security* (653 F.3d 1(2011), jossa kysymys oli kokovartaloskannereiden käytöstä lentokentillä.

826 Esimerkiksi maahantulotarkastusten yhteydessä kerättyjen biometristen tunnisteiden käyttäminen rikostutkinnassa katso Michigan v. Clifford (464 U.S. 287 (1984), jossa hallinnollisen tarkastuksen kautta saatujen tietojen käyttäminen rikostutkinnassa kiellettiin perustuslain 4 lisäyksen vastaisena. Katso myös tapaus *Kyllo v. United States*, jossa Korkein oikeus totesi valvontamahdollisuuksien kasvus-

Mielenkiintoinen poikkeus on myös poliisin tekemät pysäytykset (ns. Terry Stops). Ratkaisussa *Terry v. Ohio*[827] katsottiin, että poliisi voi pysäyttää yksilön, mikäli poliisilla on perusteltu syy epäillä rikoksen olevan tekeillä. Pysäytyksen tulee kuitenkin olla lyhyt ja tilapäinen. Sen aikana poliisi voi suorittaa ruumiintarkastuksen aseiden etsimiseksi, jos on syytä epäillä henkilön olevan aseistettu. Tällainen pysäytys ei siis ole etsintä, sillä poliisilla ei ole lupa muiden esineiden etsimiseen eikä muiden toimenpiteiden suorittamiseen.[828]

Yhdysvaltain perustuslain 5. lisäys käsittelee itsekriminointisuojaa eli yksilön oikeutta olla todistamatta itseään vastaan. Biometriseen tunnistamiseen liittyy perustuslain näkökulmasta huoli myös 5. lisäyksen näkökulmasta, sillä yksilöllisen fyysisen ominaispiirteen käyttämistä yksilön tunnistamiseen on mahdollista pitää myös itsekriminointisuojan rikkomisena.

Suojan tarkoituksena on yksilön suojaaminen omien tietojensa tai lausuntojensa kautta tapahtuvalta syytteeseenpanolta. Lisäyksessä 5 säädetty itsekriminointisuoja estää säännöksen vastaisesti tapahtuvan todisteiden keräämisen ja näiden käytön oikeudessa.[829] Tällaisena todisteiden keräämisenä on oikeuskäytännössä pidetty muun muassa yk-

---

ta seuraavaa:"it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology…The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."

827 Terry v. Ohio (392 U.S. 1 (1968)).

828 Näin muun muassa ratkaisussa Minnesota v. Dickerson (508 U.S. 366 (1993)) ja *Solove – Schwartz,* Information Privacy Law, s. 254.

829 Tämä on todettu myös ratkaisussa Napolitano v. Ward (457 F.2d 279 (1972)).

silön velvoittamista todistamaan henkilöllisyytensä ollessaan epäiltynä rikoksesta.[830]

Lisäyksen soveltaminen biometriseen tunnistamiseen on kuitenkin varsin ongelmallista. Yhdysvaltain Korkeimman oikeuden ratkaisukäytännössä on nimitäin katsottu, ettei lisäys 5 sovellu muun muassa velvoitettuun sormenjälkien antamiseen, DNA-näytteen antamiseen, valokuvaamiseen eikä kävelemiseen tunnistamistarkoituksessa.[831] Tämä on sinänsä mielenkiintoista, koska oikeuskäytännöstä saa ristiriitaisen kuvan. Oikeuskäytännössä on eräissä tilanteissa katsottu, että rikoksesta epäillyn velvoittaminen todistamaan henkilöllisyytensä loukkaa yksilön perustuslaillisia oikeuksia.[832] Toisaalta kyseistä loukkausta ei

830 Hiibel v. Sixth Judicial District Court (542 U.S. 177 (2004)).

831 Maryland v. King (133 S.Ct. 1), New York v. Quarles (467 U.S. 649 (1984), Gibert v. California (388 U.S. 263 (1976), United States v. Chibarro (361 F. 2d 365 (3rd Cir. 1966) sekä Davis v. Mississippi (394 U.S. 721 (1969). Katso myös valitustuomioistuimen ratkaisu U.S. v. Garcia-Beltran (443 F. 3d 1126(2006)). Vertaa kuitenkin valitustuomioistuimen ratkaisuihin U.S. v. Olivares-Rangel (458 F. 3d 1104) sekä U.S. v. Meza (No. 12–cr–00386–MSK) (annettu tammikuussa 2014), joissa laittoman etsinnän tuloksena saadut sormenjäljet katsottiin pykälän 5 vastaisiksi. Katso myös ratkaisu People v. Buza (129 Cal.Rptr.3d 753 (Court of Appeal, First District, Division 2, California 2013)), jossa rikoksesta epäiltyjen ja pidätettyjen henkilöiden lakiin perustuva velvoite DNA-näytteen antamiseen nähtiin Yhdysvaltain perustuslain pykälien 4 ja 5 vastaisina. Tämä osoittaa sen, että ratkaisukäytäntö on ristiriitaista. Osavaltiotasolla näyttää siltä, että tuomioistuimet ovat olleet tiukemmin yksilön oikeuksien puolella.

832 Esimerkiksi ratkaisussa Kolender v. Lawson (461 U.S. 352 (1983)) Korkein oikeus kumosi lain perustuslain vastaisena, sillä laki asetti yksilölle velvollisuuden todistaa henkilöllisyytensä.

ole, kun yksilö velvoitetaan antamaan biometriset tunnisteensa tämän tunnistamiseksi.

Ongelmalliseksi tilanteen tekee myös hallinnollisiin tarkoituksiin kerätyt biometriset tiedot, joiden ei voida suoranaisesti katsoa kuuluvan lisäyksen 5 soveltamisalueelle. Yhdysvaltain Korkeimman oikeuden ratkaisukäytännössä suojan alueelle kuuluvat vain viestinnällisen ja lausuvan luonteen (evidence that is testimonial and communicative in nature) omaavat todisteet.[833] Hallinnollisen tarkastuksen nojalla kerättyjen biometristen tunnisteiden käyttäminen on myös oikeuskäytännössä kielletty lisäyksen 4 vastaisena yksityisyyden loukkauksena.[834]

Perustuslain säännösten näkökulmasta eräs tapaus on ainutlaatuinen. Kysymys ei kuitenkaan ole liittovaltiotason oikeuskäytännöstä, joten tapauksen merkitys biometrisen tunnistamisen perustuslainmukaisuuden arvioinnissa jäänee vähäiseksi. Tapaus on kuitenkin tämän tutkimuksen kannalta olennainen, joten sitä on tarpeen käydä alla tarkemmin läpi.

> Perkey v. Department of Motor Vehicles.[835] Tapauksessa valittaja kyseenalaisti Kalifornian osavaltion ajoneuvorekisterikeskuksen (Department of Motor Vehicle) asettaman velvoitteen antaa sormenjälki uutta ajokorttia haettaessa yksityisyyttä

833 Schmerber v. California (384 U.S. 757 (1966). Liun mukaan tämä ajatus tosin perustuu oletukselle, että biometrista tunnistamista ei voida pitää tungettelevana ja että siinä ei tapahdu fyysistä kosketusta. *Liu,* Bio-privacy, s. 177.

834 Tosin ratkaisussa McCarthy v. Arndstein (266 U.S. 34(1924)) Korkein oikeus katsoi, että itsekriminoinitisuojaan kuuluvat myös tiedot, joita ei ole kerätty rikostutkintatarkoituksessa, jos rikostutkinta on mahdollinen seuraus.

835 Perkey v. Department of Motor Vehicles (42 Cal.3d 185 (1986)).

loukkaavana. Tapaus päätyi loppujen lopuksi osavaltion Korkeimpaan oikeuteen, joka otti asiaan kantaa.

Kalifornian osavaltion korkein oikeus arvioi tapausta sen kannalta, onko kysymyksessä kohtuuton ruumiilliseen koskemattomuuteen puuttuminen, jolla loukataan yksilön perustuslain 4, 5 ja 14 lisäyksissä turvattuja oikeuksia. Ratkaisussaan korkein oikeus totesi, ettei sormenjälkien ottaminen itsessään loukkaa yksilön perustuslain mukaista oikeutta yksityisyyteen.

Tähän on korkeimman oikeuden mukaan syynä se, ettei sormenjälkien ottamisessa puututa yksilön yksityisyyteen tavalla, jota voidaan pitää pykälässä 4 tarkoitettuna kuulusteluna tai tarkastuksena. Siinä ei korkeimman oikeuden näkemyksen mukaan myöskään ole kysymys yksilön ruumiin pinnan alle menevästä tarkastuksesta. Kyseinen toimi ei näin ollen loukkaa ihmisarvon ja yksityisyyden kunnioittamisen periaatteita, joita suojataan perustuslain 5. ja 14. lisäyksissä. Tämän lisäksi oikeus perusteli ratkaisuaan aikaisemmalla oikeuskäytännöllä, jossa sormenjälkien käyttäminen on sallittu monissa ei-rikosoikeudellisissa yhteyksissä.[836]

Yhdysvaltain biometriaa koskevassa oikeuskäytännössä tapaus on varsin ainutlaatuinen. Kalifornian osavaltion korkein oikeus joutui nimittäin ottamaan kantaa myös sormenjälkien käsittelemisen ja edelleen siirtämisen perustuslainmukaisuuteen.

Korkein oikeus päätyi ratkaisussaan liittovaltion korkeimman oikeuden oikeuskäytännössä omaksuttuun linjaan näh-

836 Katso esimerkiksi ratkaisu Thom v. New York Stock Exchange (306 F.Supp. 1002 (United States District Court S.D. New York 1969)) ja People v. Stuller (10 Cal.App.3d 582 (Court of Appeal, Fourth District, Division 2, California 1970)).

den varsin erikoiseen lopputulokseen. Korkein oikeus totesi ajoneuvorekisterikeskuksen tietojen jakamisen muussa kuin ajoneuvoturvallisuuteen liittyvissä asioissa olevan vastoin lakia. Tulkinnassaan korkein oikeus käytti keskeisenä perusteena vuoden 1977 Information Practices Actia[837], jonka mukaan oikeus yksityisyyteen vaarantuu harkitsemattomassa henkilötietojen keräämisessä, ylläpidossa ja jakamisessa. Sormenjälkien käsittely alkuperäisen käyttötarkoituksen vastaisesti loukkasi Kalifornian osavaltion perustuslaissa taattua yksilön oikeutta yksityisyyteen.

Tapaus on merkityksellinen siitäkin syystä, että Kalifornian korkein oikeus otti kantaa sormenjälkien erityiseen luonteeseen. Sormenjäljet ovat korkeimman oikeuden mukaan suhteellisen ainutlaatuinen ja arkaluontoinen henkilötieto, jolla on vaikutuksia anonymiteettiin ja jonka väärinkäyttö loukkaa yksilön oikeutta yksityisyyteen.

Ratkaisu vaikuttaa omalta osaltaan siihen, että vaikka yksilöllä ei olisikaan perusteltua oletusta nauttia yksityisyyden suojaa biometristen tietojen kohdalla sinänsä, on yksilöllä kuitenkin perusteltu oletus nauttia yksityisyyden suojaa siinä, miten näitä tietoja keräämisen jälkeen käytetään.

Teknologisen muutoksen mukanaan tuomat uudet mahdollisuudet ovat pakottaneet miettimään uudestaan perustuslain mahdollisuuksia pysyä teknologisen kehityksen mukana. Lähtökohtaisesti perustuslain tulisi olla valtion vakaa perusta, mutta ongelmaksi on muodostunut

837 Information Practices Act of 1977 – California Civil Code section 1798-1798.1 (a). Laki on takaa yksilölle huomattavasti paremman suojan henkilötietojen käsittelyssä kuin esimerkiksi liittovaltiotasolta tuleva vuoden 1974 Privacy Act. Information Practices Act nimittäin käytännössä takaa yksilölle oikeuden tiedolliseen yksityisyyteen.

perustuslain kehityksen sovittaminen teknologiseen kehitykseen. Kysymykseksi muodostuu, kuinka sopeutuva perustuslain tulee olla.[838]

5.6.3.2. Liittovaltiotason säädökset yksityisyyden suojasta

Perustuslain takaaman epäsuoran yksityisyyden suojan lisäksi yksityisyyttä suojataan monissa liittovaltiotason säädöksissä. Useimmat näistä säädöksistä perustuvat kuitenkin sille ajatukselle, että yksityisyys suojataan vain suhteessa julkiseen hallintoon. Tämän tutkimuksen kannalta merkityksellisiä liittovaltiotason säädöksiä ovat vuoden 1974 Privacy Act sekä vuoden 1999 Financial Modernization Act.

The Privacy Act of 1974. Keskeisin liittovaltiotason yksityisyyttä suojaavista säädöksistä on vuoden 1974 Privacy Act, joka edellyttää liittovaltion laitoksia noudattamaan tiettyjä toimintatapoja näiden käsitellessä henkilötietoja. Lakia voidaan pitää eräänlaisena henkilötietojen käsittelyn yleisohjeena, jonka tarkoituksena on säädellä liittovaltion organisaatioiden henkilötietojen käsittelyä.

Lakia sovelletaan rekisterissä oleviin henkilötietoihin, joita kerätään, ylläpidetään, käytetään ja levitetään julkisen hallinnon toimesta. Soveltamisalaan on otettu myös mielenkiintoinen rajoitus, sillä lakia sovelletaan vain Yhdysvaltain kansalaisiin ja maassa laillisesti asuviin ulkomaalaisiin. Soveltamisalueen ulkopuolelle jäävät myös osavaltioiden hallinto ja paikallishallinto sekä yksityishenkilöt ja yksityisoikeudelliset oikeushenkilöt.

Laissa henkilötiedolla tarkoitetaan kaikenlaisia yksilöä koskevia tietoja tai tietojoukkoja, joita ylläpidetään viranomaisen toimesta, kuten merkintöjä, jotka koskevat muun muassa yksilön koulutusta, taloudellisia asioita, terveydentilaa, rikos- tai työhistoriaa ja jotka sisältävät yksilön nimen, tunnistenumeron, symbolin tai muun yksilöivän tunnisteen, kuten sormenjäljen, äänen tai valokuvan.

838 *Solove – Schwartz,* Information Privacy Law (2011), s. 261.

Henkilötiedon määritelmä vastaa perusperiaatteiltaan EU:n henkilötietodirektiivin vaatimuksia, sillä ollakseen henkilötieto edellytetään sen olevan yhdistettävissä johonkin tiettyyn yksilöön. Laki myös soveltuu biometriseen tunnistamiseen, sillä henkilötiedon määritelmässä sormenjälki mainitaan nimenomaisesti osana henkilötietoja.

Lakia kuitenkin sovelletaan vain henkilörekisterissä oleviin tietoihin. Henkilörekisterillä laissa tarkoitetaan viranomaisen ylläpitämää henkilötietoja sisältävää tietojoukkoa, josta tietoja haetaan yksilön nimellä tai jollain yksilöivällä numerolla, symbolilla tai tunnisteella.

Vuoden 1974 Privacy Actin perustuu kahdeksaan periaatteeseen.[839] Nämä periaatteet sisältävät keskeiset rekisterinpitäjän velvollisuudet, rekisteröidyn oikeudet sekä rekisterinpitoa yleensä koskevat periaatteet. Ne voidaan tiivistetysti esittää seuraavasti:

1. Rekisterinpidon tulee perustua avoimuuteen eikä salaisia rekistereitä sallita (The Openness Principle).
2. Rekisteröidyllä on oikeus tarkastaa ja kopioida hänestä rekisteriin talletetut tiedot (The Individual Access Principle).
3. Rekisteröidyllä on oikeus korjata virheellisiä tai puutteellisia häntä koskevia rekisterin tietoja (The Individual Participation Principle).
4. Tietojen määrä ja tietojen keräämistavat on rajoitettu (The Collection Limitation Principle).
5. Tietojen käyttötapa on rajoitettu (The Use Limitation Principle).
6. Tietojen luovuttaminen ulkopuolisille on rajoitettu (The Disclosure Limitation Principle).

839 Privacy Protection Study Commission, Personal Privacy in an Information Society (1977). Periaatteet sisältyvät raportin 13. jaksoon. Raportti on saatavissa osoitteessa: http://epic.org/privacy/ppsc1977report/

7. Rekisterinpitäjällä on velvollisuus luoda kohtuulliset ja järkevät tiedon hallinnan käytännöt, joiden tarkoituksena on tietojen käsittelyn tarpeellisuuden ja lainmukaisuuden sekä rekisterissä olevien tietojen ajantasaisuuden ja oikeellisuuden osoittaminen (The Information Management Principle).
8. Rekisterinpitäjä on vastuussa tiedon hallinnan käytänteistään ja tietojärjestelmistään (The Accountability Principle).

Periaatteiden 1-3 tarkoituksena on rekisterinpidon avoimuuden turvaaminen ensinnäkin kieltämällä salaisten rekisterien pitämisen. Toiseksi avoimuus turvataan säätämällä rekisteröidylle oikeus tarkastaa itseään koskevat rekisterissä olevat tiedot ja oikeus virheellisten tai puutteellisten tietojen korjaamiseen (5 U.S.C. 552a§ (d)).

Neljäs periaate (The Collection Limitation Principle) edellyttää, että vain rekisterin käyttötarkoituksen kannalta asianmukaisia ja tarpeellisia henkilötietoja käsitellään. Tiedot tulee myös kohtuullisten keinojen rajoissa kerätä yksilöltä itseltään, kun kerätyillä tiedoilla voi olla suuri vaikutus yksilön oikeuksiin tai velvollisuuksiin. Tämä myös velvoittaa rekisterinpitäjän ilmoittamaan tietojen keräämisestä rekisteröidylle. Tämän ilmoitusvelvollisuuden ulkopuolelle jää salaisesti tapahtuva tietojen hankinta. Ilmoitusvelvollisuuden nojalla rekisterinpitäjän tulee ilmoittaa rekisterinpitäjä, keräämisen tarkoitus, mihin kerättyjä tietoja käytetään sekä tiedon luovuttamisesta kieltäytymisen vaikutukset (5 U.S.C. 552a§ (e) (2) ja 5 U.S.C. 552a§ (e) (3)).[840]

840 Liun mukaan periaate on biometrisen tunnistamisen kannalta keskeinen, sillä se rajoittaa biometristen tunnisteiden oikeudetonta keräämistä. Hänen mukaansa periaatetta ilmentävät säännökset eivät kuitenkaan riittävällä tavalla turvaa biometrisia tunnisteita. Syynä tähän on hänen mukaansa biometristen tunnisteiden asema oikeuskäytännössä sekä säännösten lavea muotoilu. Tähän kritiikkiin on helppo yhtyä. Kritiikistä tarkemmin katso *Liu,* Bio-privacy, s. 180–182.

The Privacy Act sääntelee myös julkisen hallinnon mahdollisuuksia käyttää ja luovuttaa henkilötietoja (5 U.S.C. 552a§ (b)). Rekisteriin sisältyviä henkilötietoja voidaan luovuttaa vain rekisteröidyn kirjallisesta vaatimuksesta tai kirjallisella suostumuksella. Säännökseen on kuitenkin otettu poikkeus luovutuskieltoon. Poikkeuksina ovat lähinnä ne virastot ja virkamiehet, jotka tarvitsevat rekisterin tietoja tehtävänsä hoitamiseksi (U.S.C. 552a (b) (1)).

Oleellisin asia Privacy Actissa on kuitenkin se, että se rajoittaa tietojen jakamista viranomaisten kesken. Se on toteutettu rajoittamalla niin sanottujen vertailuohjelmien (matching programs) käyttöä. Vertailuohjelmalla tarkoitetaan tietokoneistettua tietojärjestelmien vertailua, jonka tarkoituksena on rekisteröityjen henkilöiden aseman, oikeuksien tai etujen selville saaminen. Sitä saa käyttää vain, mikäli viranomaiset ovat keskenään kirjallisesti sopineet asiasta.[841]

Biometriseen tunnistamiseen liittyvästä oikeuskäytännöstä katso esimerkiksi United States v. Doe (457 F.2d 895 (1972)) sekä Brown v. Brannon (399 F Supp 133 (M.D.N.C. 1975)). Periaatetta yleisesti koskevasta kritiikistä katso esimerkiksi Privacy Protection Study Commission, Personal Privacy in an Information Society (1977) sekä Schwartz – Reidenberg, Data Privacy Law, Lexis Law Pub, 1996.

841 5 U.S.C. 552(a) (Supplement 1995). Liun mukaan tämä on omiaan rajoittamaan biometristen tietojen käyttöä. *Liu,* Bio-privacy, s. 182. Huomautettava on kuitenkin siitä, että tietojen vertaileminen on yleensä katsottu rekisterin tavanomaiseksi käytöksi. Tämä on omiaan heikentämään lain mahdollisuuksia henkilötietojen käsittelyn avoimuuden toteuttamiseen sekä tietojen luovuttamisen rajoittamiseen. US Congress Office of Technology Assessment, Federal Government Information Technology: Management, Security, and Congressional Oversight (Helmikuu 1986). Katso myös Schwartz – Reidenberg, Data Privacy Law, Lexis Law Pub (1996).

Periaatteet tiedon hallinnan järjestämisestä ja rekisterinpitäjän vastuusta ovat erityisesti biometristen tietojen kohdalla merkittäviä periaatteita. The Privacy Act asettaa rekisterinpitäjälle tietoturvavelvoitteen. Lain mukaan rekisterinpitäjän tulee huolehtia riittävistä hallinnollisista, teknisistä ja fyysisistä turvatoimenpiteistä tietojen turvallisuuden ja luottamuksellisuuden takaamiseksi ennakoitavissa olevilta uhkilta ja vaaroilta, jotka ovat omiaan aiheuttamaan rekisteröidylle suurta vahinkoa, häpeää tai haittaa (5 U.S.C. 522a§ (e) (10)).

Biometristen tunnisteiden luonteen vuoksi nämä tiedot vaativat erityistä huomiota. Lain joustava ja laaja muotoilu tietoturvavelvoitteen kohdalla on kuitenkin omiaan aiheuttamaan tulkintavaikeuksia riittävistä tietoturvatoimenpiteistä.

Laki on saanut kritiikkiä siitä, että se on helposti sivuutettavissa kirjaamalla tiedot rekisteriin siten, että rekisteriin talletetut tiedot eivät kuvaa tunnistettavaa henkilöä. Kritiikkiä laki on saanut osakseen myös siihen otetusta tavanomaisen käytön poikkeusasemasta ja siitä, että lakia ei sovelleta lainvalvontaan. Kritiikkiin on suurelta osin syynä se, että nämä puutteet tai heikkoudet mitätöivät suurelta osin lain vaikutukset.[842]

Ongelmallista on myös se, että tiedot tulee kohtuullisten keinojen rajoissa kerätä yksilöltä itseltään, kun tiedoilla voi olla suuri vaikutus yksilön oikeuksiin tai velvollisuuksiin. Tällainen avoin muotoilu mitätöi lain vaikutukset, sillä se mahdollistaa tietojen hankkimisen kolmansilta tahoilta helppouden ja tehokkuuden nimissä.[843]

Suurin puute laissa on kuitenkin suostumusinstituution rajallisuus. Laissa rekisteröidyn suostumusta henkilötietojen käsittelyyn edellyte-

842 *Schwartz,* Privacy and Participation: Personal Information and Public Sector Regulation in the United States, s. 584-587. 80 Iowa Law Review 1994. s. 553-618. Katso myös Overview of the Privacy Act of 1974 (2012 edition).

843 Näin myös *Liu,* Bio-privacy, s. 182.

tään ainoastaan, kun henkilötietoja luovutetaan eteenpäin. Yksilöllä ei ole todellista mahdollisuutta päättää omien tietojensa käsittelystä.[844]

Financial Modernization Act of 1999. Liittovaltiotasolla säädellään myös henkilötietojen käsittelyä tietyillä toimialoilla. Yksityisiä toimijoita koskevasta liittovaltiotason yksityisyyden suojaa koskevasta sääntelystä merkittävin on tällä hetkellä vuoden 1999 Financial Modernization Act.[845] Sitä on kuvattu yhdeksi Yhdysvaltain historian kattavimmaksi yksityisyyttä koskevaksi liittovaltiotason säädökseksi.[846]

Laki koskee yrityksiä, jotka toimivat pankki-, vakuutus- ja sijoitusaloilla. Taloussektori oli yksityisen puolen toimijoista ensimmäisiä, jotka ottivat käyttöön biometrisia tunnisteita hyödyntäviä laitteita. Taloussektori on tulevaisuudessa todennäköisesti yksi suurimpia biometrisen tunnistamisen käyttäjiä. Laki on erityisen merkityksellinen myös biometrisen tunnistamisen näkökulmasta.[847] Se on puitelain tyyppi-

---

844 Näin myös *Liu,* Bio-privacy, s. 180–181. Liu huomauttaa osuvasti siitä, että yksilöllä ei aina myöskään ole todellista mahdollisuutta kieltäytyä antamasta vaadittuja tietoja. Syynä on hänen mukaansa se, että seuraus tietojen antamatta jättämisestä voi todellisuudessa pakottaa yksilön antamaan vaaditut tiedot. Katso esimerkiksi ratkaisu Perkey v. Department of Motor Vehicles. Ratkaisua käydän tarkemmin läpi jaksossa 5.5.3.1.

845 Laki tunnetaan myös nimellä Gramm – Leach – Bliley Act. Gramm-Leach-Bliley Financial Services Modernisation Act, Pub. L. no. 106-102 (1999).

846 Katso tarkemmin *Fischer – Camper,* Reform Law and Privacy: A Road Map. American Banker –lehti (Marraskuu 1999).

847 Katso esimerkiksi Sitalakshmi Venkatraman Indika Delpachitra, Biometrics in banking security: a case study, Information Management & Computer Security, Vol. 16 Issue 4, s. 415–430 sekä Digital Persona, Biometrics in Banking: From Unbanked to Lifelong Cus-

nen, sillä se antaa osavaltioille mahdollisuuden säätää vahvemmasta suojasta.[848]

Yksityisyyden suojan kannalta merkityksellinen on lain osa V, joka säätää yksityisyyden suojasta asiakastietojen käsittelyssä. Laissa säädetään rahoituslaitoksille jatkuva velvollisuus asiakkaidensa ei-julkisten henkilötietojen suojaamiseen. Ei-julkisilla henkilötiedoilla tarkoitetaan ensinnäkin yksilön taloutta kuvaavia henkilökohtaisia, ei julkisesti saatavilla olevia merkintöjä, joista yksilö on tunnistettavissa ja jotka:

1. asiakas on rahoituslaitokselle antanut,
2. on saatu maksutapahtuman tai muun vastaavan toimen kautta tai
3. rahoituslaitos on muulla tavoin saanut.

Toiseksi määritelmä kattaa näiden tietojen avulla koottuja asiakasluetteloja ja muita koonnoksia. (§ 509)

Yksilön taloutta kuvaavia henkilöön yhdistettävissä olevia tietoja ovat puolestaan kaikenlaiset asiakasta koskevat tiedot, joita rahoituslaitos käyttää palvelujen ja tuotteiden myöntämiseksi asiakkaalle (§ 509). Näihin on katsottu kuuluvaksi muun muassa asiakkaan nimi, puhelinnumero, luottohistoria sekä tulot.[849] Tähän perustuen myös biometriset tunnisteet on mahdollista katsoa kuuluvaksi yksilön taloutta kuvaaviksi henkilöön yhdistettävissä oleviksi tiedoiksi, mikäli biometriset tiedot kerätään asiakkaalta tämän tunnistamiseksi.[850] Laki

---

tomer (Tammikuu 2014).

848 Tätä mahdollisuutta ovat käyttäneet Alaskan (Alaska Stat. § 06.05.175), Marylandin (Md. Code Ann. § 1-301), Connecticutin (Conn. Gen. Stat. Ann § 36a-42) ja Illinois´n (205 Ill. Comp. Stat. Ann. 5/48.1) osavaltiot, jotka ovat säätäneet tietojen jakamiseen liittyviä tarkempia ja tiukempia rajoituksia.

849 Federal Deposit Insurance Corporation, Privacy Rule Handbook (2001). Saatavilla osoitteessa: https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/index.html.

850 Näin myös *Liu,* Bio-privacy, s. 186

on myös erityisen merkityksellinen biometristen tietojen käsittelyn sääntelyssä.

Asiakkaan yksityisyyden suojaamiseksi lain osaan V on otettu säännökset tietojen jakamisen rajoittamisesta ja yleisestä ilmoitusvelvollisuudesta. Lain mukaan rahoituslaitoksella ei ole oikeutta luovuttaa eteenpäin tilinumeroa, luottokortin tai talletustilin tunnuslukua ulkopuoliselle kolmannelle osapuolelle markkinointitarkoitusta varten (§ 502 (d) ja (e)). Myös ei-julkisten yksilön taloutta kuvaavien henkilökohtaisten tietojen luovuttaminen on kielletty, ellei kysymys ole laissa mainitusta poikkeuksesta (§ 502 (a)).

Laki asettaa rahoituslaitoksille velvollisuuden tiedottaa yksityisyyden suojaan liittyvistä käytännöistään selkeästi asiakkaalle asiakassuhteen alussa sekä vähintään kerran vuodessa asiakassuhteen aikana (§ 503 (a)). Laissa on myös säädetty rahoituslaitoksille velvollisuus huolehtia asiakastietojensa tietoturvasta (§ 501 (a) ja (b)). Rahoituslaitosten on toteutettava tarpeelliset hallinnolliset, tekniset ja organisatoriset toimet tietojen suojaamiseksi oikeudettomalta pääsyltä ja käytöltä sekä mahdollisilta uhkilta ja vaaroilta.

Lain suurimpana puutteena on se, että taloudellisten tietojen jakamisen kielto rahoituslaitoksen ulkopuolisille kolmansille osapuolille edellyttää asiakkaalta aktiivisia toimia. Lain mukaan asiakastiedöt ovat luovutettavissa edelleen ulkopuolisille kolmansille osapuolille (non-affiliates), ellei asiakas ole ennen edelleen luovutusta nimenomaisesti kieltänyt tietojensa luovuttamista kyseiselle luovutuksensaajalle (§ 502 (b)).

Puutteena on myös se, että laki ei millään tavalla rajoita yksilön taloudellisten tietojen jakamista rahoituslaitoksen yhteistyökumppaneiden (affiliates) kesken. Tietojen jakamisen kielto on rajattu vain ulkopuolisiin kolmansiin tahoihin (non-affiliates).

Lisäksi puutteena voidaan pitää sitä, että yksilön taloudellisia tietoja on sallittua jakaa ulkopuolisille myös, jos tämä on tarpeen asiakkaan

maksu- tai muun vastaavan liiketapahtuman toteuttamiseksi (§ 502 (b) (2)) taikka luovutus perustuu rahoituslaitoksen ja kolmannen osapuolen väliseen markkinointisopimukseen. Vaikuttaa siltä, että laki takaa yksilölle varsin huonot oikeudet tietojensa hallitsemiseen. Tällöin varsinkin biometristen tunnisteiden kohdalla yksilön yksityisyyden suoja kohtuuttomasti vaarantuu.[851]

Omana puutteenaan on myös tietoturvavelvollisuuden väljä muotoilu. Laissa käytetään termiä tarpeelliset toimet sen tarkemmin kuvaamatta, mitä tarpeellisilla toimilla tarkoitetaan. Puutteena on erityisesti se, että laki ei takaa yksilölle minkäänlaista oikeutta vaatia rahoituslaitosta vastuuseen tietoturvan laiminlyönnistä, mikä omalta osaltaan johtaa asiakkaan yksityisyyden vaarantumiseen.

Laki tekee eron asiakkaan ja kuluttajan välille. Se koskee nimenomaisesti vain asiakastietoja, kuluttajat jäävät lain soveltamisalan ulkopuolelle. Lain mukaan kuluttajasta tulee asiakas vasta, kun kuluttajan ja rahoituslaitoksen välille on syntynyt jatkuva suhde, jossa rahoituslaitos toimittaa yhden tai useamman rahoitusvälineen tai –palvelun kuluttajalle, joita kuluttaja käyttää omaan henkilökohtaiseen, perheen tai kotitalouden tarkoituksiin (§ 509 (11)). Määritelmän ulkopuolelle jää yksittäiset toimet, kuten käteisen nostaminen automaatista. Tämä on varsin ongelmallista erityisesti biometristen tunnisteiden kohdalla, sillä satunnaisten yksittäisten asiointien kautta saatuja biometrisia tunnisteita laki ei sääntele. Nämä tiedot ovat vapaasti käytettävissä, ja myös edelleen luovutettavissa.

Tapauksessa Messing v. Bank of America oikeus katsoi sormenjälkien keräämisen kuluttajalta olevan lainmukaista, hyväksyttävää ja tarpeellista. Tapaus on ensimmäinen biometristen tunnisteiden käyt-

851 Lain ongelmista ja ratkaisuista näihin ongelmiin katso esimerkiksi *EPIC,* The Gramm – Leach – Bliley Act. Artikkeli saatavilla osoitteessa: http://epic.org/privacy/glba/

töä yksityisellä sektorilla koskeva tapaus. Tapauksessa kantaja haastoi Bank of American oikeuteen sen vuoksi, että hänen tuli antaa sormenjälkensä lunastaakseen sekin pankista. Kyseinen henkilö ei ollut pankin asiakas. Oikeus kuitenkin katsoi, että sormenjäljen käyttö on perusteltua, hyväksyttävää ja tarpeellista. Perusteena oikeus käytti seuraavia argumentteja: 1) sormenjälki on yksi lainmukaisista allekirjoitus- ja vahvistustavoista (Maryland Uniform Commercial Code §1-201 (39)), 2) muiden biometristen tunnisteiden käyttö on hyväksytty muissa ei-rikostutkinnallisissa yhteyksissä ja 3) niiden käyttö on tarpeellista väärennösrikollisuuden torjunnassa. Sormenjäljen käyttö ei oikeuden näkemyksen mukaan myöskään aiheuta kohtuutonta haittaa, sillä sen käyttö on huomaamatonta. Sormenjäljen käytön ei myöskään katsottu loukkaavan yksilön oikeuksia, sillä se toimii vain apuvälineenä yksilön tunnistamisessa.[852]

5.6.3.3. Vahingonkorvausnormisto (privacy in torts)

Koska Yhdysvaltain perustuslaki ja liittovaltion tasolta tuleva The Privacy Act of 1974 eivät turvaa oikeutta yksityisyyteen suhteessa yksityisiin toimijoihin, on yksityisyyttä perinteisesti turvattu myös vahingonkorvausnormiston kautta (Restatement (Second) of Torts).[853] Vahingonkorvauksen soveltuminen biometriseen tunnistamiseen on todella vaikeasti toteennäytettävissä, joten tämänkaltainen suojakeino on varsin heikko.

852 Messing v. Bank of America N.D. (373 Md. 672, 821 A.2d 22 (2003),

853 Restatementit eivät ole varsinaista lainsäädäntöä, vaanyhdysvaltalaisen oikeusyhteisön keräämä kokoelma oikeuskäytännöstä tunnistettavissa olevista säännöistä.

Tällä hetkellä vahingonkorvausnormisto suojaa yksityisyyttä pääosin neljän oikeushyvän kautta[854]:

1) yksilöivän tiedon luvaton käyttö (appropriation of name or likeness)

Yksilöivän tiedon luvattomassa käytössä on kysymys yksilölle kuuluvan yksilöivän tiedon, kuten nimen tai hahmon, luvattomasta käytöstä yleensä kaupallisia tarkoituksia varten (Restatement (Second) §

854 Jaottelun on oikeuskäytännön pohjalta tehnyt William L. Prosser vuonna 1960 48 California Law Review –lehdessä julkaistussa artikkelissa Privacy. Jaottelu on yhä käytössä, tosin kaikki osavaltiot eivät tunnusta tätä jakoa. Esimerkiksi Minnesotan, Texasin ja Floridan osavaltiot tunnustavat näistä neljästä vain kolme suojattavaa oikeushyvää (false light in the public eye –doktriini on katsottu hyväksymättömäksi). Tähän liittyen katso ratkaisut Lake v. Wal-Mart (582 N. W.2d 231(Minnesota 1998), Jews for Jesus, Inc. v. Rapp (997 So.2d 1098 (Supreme Court of Florida 2008)) sekä Cain v. Hearst Corporation d/b/a the Houston Chronicle Publishing Company (878 S.W.2d 577 (Supreme Court of Texas 1994)). Katso myös *Solove –Schwartz,* Privacy Law Fundamentals, s. 2. Syyksi suojaamattomuuteen on ilmoitettu se, että samaa oikeushyvää suojataan kunnianloukkauksen (defamation) kautta, joka on oikeussuojakeinona vanhempi. *Solove – Schwartz,* Information Privacy Law (2011), s. 79. Huomioitava kuitenkin on, että kunnianloukkaus on eri asia, sillä sen kautta suojataan yksilön intressiä hyvän maineen ylläpitämiseen ja sitä miltä hän näyttää ulospäin. Suojaamalla yksilön oikeutta tulla arvioiduksi oikeassa valossa puolestaan suojataan sitä, mitä hän itsestään ajattelee. Katso tarkemmin *Keaton – Dobbs – Keeton – Owen* (toim.), Prosser and Keaton on the Law of Torts (5. uudistettu painos). St. Paul, MN: West Publishing. Katso myös ratkaisu Godbehere v. Phoenix Newspaper, Inc. (783 P.2d 781, 787 (1989) sekä Hart v. Seven Resorts, Inc. (947 P.2d 846, 854 (1997)).

652C)[855]. Tarkoituksena on suojata yksilön intressiä oman identiteettinsä yksinomaiseen kaupalliseen hyödyntämiseen (Restatement (Second) § 652C comment a).Kysymys on toisin sanoen siitä, että suojaamalla yksilön yksilöiviä tietoja turvataan myös yksilön identiteettiä kaupalliselta väärinkäytöltä.[856]

Laki ei suojaa yksilöiviä tietoja pelkästään kaupalliselta hyödyntämiseltä. Näitä tietoja suojataan myös yksityishenkilön käyttäessä

855 One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy. Myös The Federal Lanham Act suojaa yksilön nimeä ja hahmoa kaupalliselta hyväksikäytöltä.

856 Alun perin doktriinin tarkoitus oli yksityisyyslähtöinen: yksilön omanarvontunnon suojaaminen hänen identiteettinsä väärinkäytöltä. Myöhemmin doktriinin tarkoitus on kuitenkin muuttunut omaisuuslähtöiseksi, sillä oikeuskäytännössä on kehitetty niin sanottu oikeus julkisuuteen (right of publicity), joka antaa julkisuuden henkilöille yksinomaisen oikeuden oman identiteettinsä kaupallisen arvon hyödyntämiseen. Ensimmäisen kerran tähän oikeuteen viitattiin ratkaisussa Haelan Laboratories v. Topps Chewing Gum, Inc. (202 F.2d 866 (2d Cir. (1953)) Katso myös ratkaisut Finger v. Omni Publications International, Ltd. (566 N.E.2d 141 (N.Y. Ct. App. 1990)) ja Carson v. Here´s Johnny Portable Toilets (698 F.2d 831 (6th Circuit 1983). Asiasta tarkemmin katso *Solove – Schwartz,* Privacy Law Fundamentals, s. 21 ja *Solove – Schwartz,* Information Privacy Law (2011), s. 221. Oikeus julkisuuteen on myös saanut oman oikeussuojakeinon. The Restatement (Third) of the Law of Unfair Competition 46 § on seuraavan sisältöinen: " One who appropriates the commercial value of a person´s identity by using without consent the person´s name, likeness, or other indicia of identity for purposes of trade is subject to liability for (monetary and injunctive) relief."Tulee kuitenkin huomata, että henkilön ei tarvitse olla julkisuuden henkilö saadakseen suojaa oman identiteettinsä arvolle. Katso esimerkiksi

tietoja omaan yksityiseen tarkoitukseensa ilman kaupallista tai muuta taloudellista tarkoitusta varten (Restatement (Second) § 652C comment b)).

Suoja ei kuitenkaan koske yksilön nimeä sinänsä, vaan tähän nimeen liittyvää arvoa tai siitä saatavaa hyötyä kaupallisessa toiminnassa. Suojaa saa nimeen tai hahmoon liittyvä maine, arvovalta, sosiaalinen tai kaupallinen asema, julkinen merkitys tai muu arvo (Restatement (Second) § 652C comment c). Suoja ei kuitenkaan rajoitu pelkästään yksilön nimeen tai hahmoon, vaan suojaa saa kaikki yksilön persoonallisuuden osa-alueet.[857]

Suojan alueelle kuuluvat tällöin myös yksilön biometriset tunnisteet, jos niitä käytetään kaupallisiin tarkoituksiin ilman lupaa ja tämä teko on omiaan aiheuttamaan henkistä haittaa tai vahinkoa yksilön identiteetin arvolle.[858] Voidaankin oikeastaan kysyä, omistaako yksilö omat biometriset tunnisteensa, kun ne

---

ratkaisu Fanelle v. Lojack corp. (79 F.Supp.2d 558 (2000)). Ratkaisussa Miller v. Collectors Universe, Inc. (159 Cal. App. 4th 988) tämä periaate myös vahvistettiin.

857 Esimerkiksi ratkaisussa Abdul-Jabbar v. General Motors Corp. (85 F.3d 407 (9th Cir. 1996)) suoja ulotettiin yksilön entiseen nimeen. Myös henkilön tunnettu lempinimi on saanut suojaa ratkaisussa Hirsch v. S.C. Johnson, Inc. (280 N.W.2d 129 (Wis.(1979)) Ratkaisuissa Waits v. Firto-lay, Inc. (978 F.2d 1098 (9th Cir. 1992)) ja Midler v. Ford Motor Co. (849 F.2d 460 (9th Cir. (1988)) suojaa puolestaan sai yksilön ääni. Waits -ratkaisussa oikeus nimenomaisesi totesi suojan piiriin kuuluvan mikä tahansa yksilöä kuvaava tieto, josta henkilö on tunnistettavissa.

858 Biometrisiin tunnisteisiin liittyviä haittoja tai vahinkoja ovat Liun mukaan esimerkiksi tietojen yhdisteleminen, profilointi ja seuranta. Myös identiteettivarkauden pelko voidaan katsoa kuuluvaksi tähän ryhmään. *Liu,* Bio-privacy, s. 192–193.

on otettu. Jos omistaa niin, miten pitkälle omistusoikeus ulottuu. Miten pitkälle näiden tietojen hallinnointi ulottuu? Miksi omistusoikeus loppuisi siihen, kun esimerkiksi DNA on ”irrotettu” yksilön kehosta?[859] Jos esimerkiksi DNA nähdään osana yksilön olemusta, sen tulisi kuulua yksilölle, josta DNA on otettu. Tällöin yksilöllä on yksinoikeus oman DNAnsa hyödyntämiseen. Tämä tarkoittaa sitä, että muut eivät saa hyödyntää näitä tietoja ilman lupaa.

Ongelmana on kuitenkin suojan rajallisuus. Jotta vastuu tämän doktriinin nojalla syntyy, edellytetään *nimeen tai hahmoon liittyvän* taloudellisen arvon hyödyntämistä. Klassinen esimerkki on julkisuuden henkilön kuvan käyttäminen tavaran tai palvelun markkinoinnissa ilman tämän henkilön suostumusta.

Biometristen tunnisteiden kohdalla tilanne on kuitenkin haastavampi. Esimerkiksi biometrisia tietoja myytäessä ei hyödynnetä kenenkään henkilön nimeen tai hahmoon liittyvää arvoa. Tietoja myydään pelkästään sen vuoksi, että ne itsessään ovat arvokkaita. Tietojen myymisessä henkilön nimen tai hahmon arvolla ei toisin sanoen ole merkitystä. Oikeudenloukkausta ei ole tapahtunut, jos myynnissä ei ole kysymys yksilön nimeen tai hahmoon liitettävissä olevan sosiaalisen arvon hyödyntämisestä (Restatement (Second) of Torts § 652C comment a).[860]

2) eristäytyneisyyden loukkaus (intrusion upon seclusion);

---

859 Tätä on pohdittu ratkaisussa Moore v. Regents of the University of California (793 P.2d 479 (Cal. 1990)). Katso myös Allen, A.L., Genetic Privacy: Emerging Concepts and Values. Teoksessa Rothstein (ed.) Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era. 1997.

860 Oikeuskäytännössä tätä on sovellettu muun muassa ratkaisussa Waits v. Firto-lay, Inc. (978 F.2d 1098 (9th Cir. 1992))

Eristäytyneisyyden loukkauksessa on kysymys siitä, että yksilön eritäytyneisyyttä tai yksinäisyyttä taikka yksityisiä asioita häiritään erityisen loukkaavasti (Restatement (Second) § 652B).[861] Loukkauksen kannalta merkityksellistä on vain loukkauksen tapahtuminen. Merkitystä ei ole sillä, onko tietoja julkistettu.[862]

Tämän oikeussuojakeinon soveltuminen biometriseen tunnistamiseen voi tulla ajankohtaiseksi, kun kysymys on biometristen tunnisteiden kerääminen valvonnan kautta olosuhteissa, joissa yksilöllä on kohtuullinen oletus yksityisyydestä.[863] Esimerkiksi ratkaisussa Nader v. General Motors Corp. katsottiin, että yli-innokas valvonta julkisella paikalla on ymmärrettävissä eristäytyneisyyden loukkaukseksi, vaikka yksilöllä ei lähtökohtaisesti ole perusteltua oletusta yksityisyyteen julkisella paikalla. Tämä edellyttää, että valvonnan kautta saadut tiedot ovat arkaluonteisia ja loukkaajan käytös on erityisen tungettelevaa.[864]

---

861 One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

862 *Solove – Schwartz,* Information Privacy Law (2011), s. 80.

863 Ratkaisussa Sanders v. ABC (978 P.2d 67 (Cal. 1999)) yksityisyyden ja eristäytyneisyyden todettiin olevan suhteellisia. Ratkaisussa katsottiin, että yksilön esillä oleminen ei itsestään tarkoita, että yksilöllä ei ole yksityisyyttä julkisella paikalla. Ratkaisussa Cefalu v. Globe Newspaper Co. (391 N.E.2d 935, 939 (Mass. App. 1979)) todettiin, että julkisella paikalla esiintyminen tarkoittaa sitä, että yksilö luopuu yksityisyydestään.

864 Nader v. General Motors Corp. (255 N.E.2d 765 (N.Y. Ct. App. 1970)). Myös ratkaisussa Summers v. Bailey (55 F.3d 1564 (11th Cir.1995)) otettiin kantaa valvontaan julkisella paikalla. Katso myös

Vahingonkorvausnormisto soveltuu vain näiden tietojen keräämiseen. Tässäkin lisäksi edellytetään, että yksilö pystyy osoittamaan tietojen keräämisen tapahtuneen salaa. Muussa tapauksessa yksilö ei voi osoittaa oikeudenloukkausta. Tämä tarkoittaa käytännössä sitä, että yksilöllä on huonot mahdollisuudet vaatia vahingonkorvausta biometristen tietojensa luvattomasta käytöstä, jos alkuperäinen tietojen kerääminen on tapahtunut laillisesti.[865] Kysymys on varsin pinnallisesta oikeussuojakeinosta biometristen tietojen keräämistä ja käsittelyä vastaan. Se suojaa periaatteessa vain salaisesti tapahtuvalta biometristen tietojen keräämiseltä ja käsittelyltä.[866]

---

ratkaisut Schuchart v. La Taberna del Alabardero, Inc. (365 F.3d 33 (D.C. Cir. 2004)), jossa oikeudenloukkaus katsottiin tapahtuneen, koska vastaaja oli loukkaavasti tunkeutunut kantajan yksityisyyden alueelle sekä ratkaisu Doe 2 v. Associate Press (331 F.3d 417 (4th Cir. 2003)), jossa todettiin oikeudenloukkauksen olevan kysymyksessä, kun vakoillaan aluetta, jossa henkilö odottaa olevansa valvonnan ulottumattomissa. Klassisempi esimerkki eristäytyneisyyden loukkauksesta on löydettävissä ratkaisusta Dietermann v. Time, Inc. (449 F.2d 245 (9th Cir. 1971).

865 Katso esimerkiksi ratkaisu Humpher v. First Interstate Bank of Oregon (696 P.2d 527 (Oregon 1985)), missä lääkärin ei katsottu loukanneen potilaan yksityisyyttä paljastaessaan luottamuksellisia adoptiota koskevia tietoja. Perusteena tälle johtopäätökselle oikeus käytti sitä, että lääkäri ei urkkinut tietoja, vaan kysymys oli hänen jo tietämistään seikoista.

866 Katso kuitenkin ratkaisu Messing v. Bank of America N.D. (373 Md. 672, 821 A.2d 22(2003)), jossa pakollinen sormenjälkien kerääminen katsottiin hyväksyttäväksi. Vertaa kuitenkin *Liu,* joka huomauttaa siitä, että oikeudenloukkaus voi olla kysymyksessä, jos laillisesti kerättyjä biometrisia tietoja käytetään yhdessä muiden tietojen kanssa profiilien luomista varten. Tämä tarkoittaa sitä, että tietojen

Keskustelua on käyty siitä, onko doktriinia mahdollista soveltaa tietovalvontaan ja sen kautta tapahtuviin yksityisyyden loukkauksiin. Tietovalvonta mahdollistaa yksittäisten tietojen kokoamisen laajoiksi profiileiksi, joiden sisältämät tiedot on koottu ilman tiedon kohteen suostumusta ja tämän tietämättä. Tietovalvonta loukkaa yksilön oikeutta päättää omien tietojensa käytöstä.

Ratkaisuna tähän uhkaan on esitetty, että eristäytyneisyyden loukkaus –doktriinia tulisi soveltaa tietovalvonnan luomiin yksityisyyden loukkauksiin. Doktriinia sovelletaan fyysisesti tai muilla tavoin toteutettuihin yksityisyyden loukkauksiin, jotka kohdistuvat yksilön henkilökohtaisiin asioihin.[867] Biometristen tunnisteiden kohdalla tämä tarkoittaisi sitä, että tietovalvonnan kautta tapahtuva biometristen tunnisteiden käsittely nähdään yksityisyyden loukkauksena.

Tähän ajattelutapaan on kuitenkin suhtauduttu sekä oikeuskäytännössä että –kirjallisuudessa varsin pessimistisesti pääosin kahdesta syystä. Ensinnäkin doktriini suojaa vain tietoja, jotka on pidetty salassa. Tietovalvonnan kohdalla näin ei ole, vaan sitä toteutetaan jo suostumuksella kerättyjen tai julkisten tietojen kautta. Ongelmia on aiheuttanut myös se, että dokrtiinin

---

louhinnalla ja tietojen yhdistelemisellä saatetaan loukata yksilön oikeutta yksityisyyteen. *Liu,* Bio-privacy, s. 190. Asia on ollut esillä myös oikeuskäytännössä. Katso esimerkiksi Weld v. CVS Pharmacy (11 Mass L Rep 21 (1999)), jossa profilointi katsottiin yksityisyyttä loukkaavaksi. Massachusettsin osavaltion korkein oikeus kuitenkin vahvisti valitustuomioituimen ratkaisun, joka kumosi päätöksen (Weld v. CVS Pharmacy, Inc. 454 Mass. 1107 (2009)).

867 Katso esimerkiksi *Zhu,* A Traditional Tort for a Modern Threat: Applying Intrusion upon Seclusion to Dataveillance Observations, s. 2383–2384.

soveltaminen on rajattu vain tietojen keräämisvaiheeseen eli ns. käsittelemättömään tietoon. Tätä ei ole oikeuskäytännössä pidetty yksityisyyden loukkauksena.[868]

Tiedollisen yksityisyyden kannalta tämä on ongelmallista, sillä tietojen avulla luotu profiili on yksityisyyden suojan näkökulmasta yleensä merkityksellisempi. Profiili on kuitenkin yleensä yksilön näkökulmasta arkaluontoisempi kokonaisuutena kuin sen sisältämä yksittäinen tieto, sillä se saattaa paljastaa yksilöstä henkilökohtaisempia asioita.[869] Näin ollen myös yksityisyyden loukkausta tulee arvioida toisin kuin yksittäisten tietojen kohdalla.[870]

Toiseksi doktriini edellyttää teolta erityistä loukkaavuutta. Erityisen loukkaavuuden vaatimusta onkin pidetty suurena ongelmana doktriinin soveltamisessa tietovalvontaan. Tietovalvonta perustuu vapaehtoisesti luovutettuihin tietoihin, ja tällaisiin tietoihin perustuvaa toimintaa ei ole helppoa todistaa yksityisyyttä loukkaavaksi.[871] Ongelmallista on myös se, että

868 Ratkaisussa Busse v. Motorola, Inc. (813 N.E.2d 1013 (Ill. App. Ct.2004)) kiinnitettiin huomiota vain tietojen keräämisvaiheeseen arvioitaessa teon loukkaavuutta yksityisyyden kannalta. Ratkaisussa todettiin: ”none of the personal information – names, telephone numbers, addresses or social security numbers – have been held to be private facts.” Katso myös Dwyer v. American Express Co. (652 N.E.2d 1351 (Ill. App. Ct. 1995))

869 Esimerkiksi yksilön ostosten kautta rakennettava profiili saattaa paljastaa henkilön olevan raskaana.

870 Näin myös *Zhu,* A Traditional Tort for a Modern Threat: Applying Intrusion Upon Seclusion to Dataveillance Observations, s. 2399.

871 *Solove,* The Digital Person, s. 59.

tietovalvontaa toteutetaan pienten yksittäisten tietojen avulla, mitä ei myöskään ole pidetty erityisen loukkaavana.[872]

Asiaa on mahdollista kuitenkin lähestyä myös toisin. Tietovalvonnan kohdalla tulee erottaa toisistaan tietojen kerääminen ja kerättyjen tietojen jatkokäyttö esimerkiksi profiilien luomiseen.[873] Näitä tulee arvioida erillisinä yksityisyyteen kohdistuvina tekoina. Tämä tarjoaa paremmat mahdollisuudet arvioida teon loukkaavuutta yksilön kannalta.[874] Koska tiedollisen yksityisyyden kautta suojataan myös muita yhteiskunnan tärkeitä arvoja, tulee eri ei-toivotut valvonnan muodot, tietovalvonta mukaan lukien, nähdä yksityisyyden loukkauksena.[875]

---

872 Katso esimerkiksi ratkaisu Dwyer v. Am. Express Co. (652 N.E.2d 1351 (Ill. App. Ct. 1995)) sekä ratkaisu Busse v. Motorola, Inc. (813 N.E.2d 1013 (Ill. App. Ct. 2004) Vertaa *Solove,* The Digital Person, s. 58–59, jossa Solove kritisoi vallitsevaa tulkintaa.

873 Yksittäisenä merkityksettömältä näyttävä tieto saattaa toimia puuttuvana lenkkinä, jonka kautta paljastuu uusia asioita eli eräänlaisena yksilön profiilin avaimena. *Solove,* The Digital Person, s. 44 sekä *Solove,* Taxonomy of Privacy, s. 507

874 *Zhu,* A Traditional Tort for a Modern Threat: Applying Intrusion Upon Seclusion to Dataveillance Observations, s. 2401.

875 *Zhu,* A Traditional Tort for a Modern Threat: Applying Intrusion Upon Seclusion to Dataveillance Observations, s. 2403. Tukea Zhun ajatus saa oikeuskäytännöstä, missä esimerkiksi verinäytteen ottamista ja veren analysoimista on pidetty erillisinä yksityisyyden loukkauksina. Doe v. High-Tech Inst., Inc., (972 P.2d 1060, 1069 (Colo. App. 1998)). Tukea näkemykselle saadaan myös ratkaisusta United States Department of Justice v. Reporters Committee for Freedom of the Press (489 U.S. 749 (1989)), jossa FBIn ei tarvinnut luovuttaa rikosrekisteriotetta julkisuuslain nojalla, vaikka nämä tiedot ovatkin

3) yksityiselämää koskevan tiedon levittäminen julkisuudessa (public disclosure of private facts)

Tietyissä tilanteissa yksilön yksityisyyttä suojataan, kun hänen henkilökohtaisia tietojaan paljastetaan ja paljastus on omiaan aiheuttamaan yksilölle vahinkoa tai haittaa. Tällaisessa tilanteessa oikeussuojakeino on vahingonkorvaus yksityiselämää koskevan tiedon levittämisestä julkisuudessa.

Yksityiselämää koskevan tiedon julkisessa levittämisessä oikeudenloukkaus katsotaan tapahtuneen, kun yksityiselämää koskeva tieto levitetään julkisesti erittäin loukkaavalla tavalla eikä tieto palvele kansan oikeutettua tarvetta tietää (Restatement (Second) of Torts § 652D).[876]

Mikä tahansa julkinen levittäminen ei kuitenkaan oikeuta vahingonkorvaukseen, sillä julkisuus edellyttää laaja-alaista levittämistä. Lisäksi edellytetään, ettei kansalla ole oikeutettua tarvetta tiedon saamiseen (Restatement (Second) of Torts § 652D comment f).[877]

---

yksittäisinä saatavilla julkisesti. Oikeuden näkemyksen mukaan siinä on suuri ero, onko tiedot koottuna yhteen tiedostoon vai ovatko ne saatavilla useista eri lähteistä.

876 One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public.

877 Esimerkiksi ratkaisussa Taylor v. Nationsbank N.A. (78 A.2d 893 (Md. Ct. Spec. App. 1999) oikeus katsoi, että teon tulee olla riittävän loukkaava aiheuttaakseen tietojen kohteelle henkistä kärsimystä kohtuuttomasta julkisuudesta. Tämä ratkaistaan niin sanotun newsworthiness –testin avulla Newsworthiness-testin tarkoituksena on sananvapauden turvaaminen. *Solove – Schwartz,* Privacy Law Fundamentals, s. 18. Katso esimerkiksi tunnetut ratkaisut Sipple v. Chro-

Jotta kysymyksessä on julkisuudessa tapahtuva yksityiselämää koskevien tietojen levittäminen, edellytetään tietojen levittämistä julkiselle yleisölle tai niin monelle yksilölle, että sen voidaan varmuudella katsoa tulleen julkiseksi (Restatement (Second) of Torts § 652D comment a).[878] Yksityiselämää koskevan tiedon levittämisen loukkaavuutta arvioidaan puolestaan sen mukaan, miten järkevä ihminen arvioi tiedon julkistamisen seurauksia (Restatement (Second) of Torts § 652D comment c).[879]

Doktriinin merkitystä on huomattavasti vähentänyt oikeuskäytännössä omaksuttu tiukka linja sanan- ja lehdistönvapauden suojaamisesta, joka on perusoikeutena turvattu. Ongelmia on aiheuttanut myös sen arvioiminen, mikä katsotaan yksityiselämää koskevaksi tiedoksi ja milloin kansalla on oikeutettu

---

nicle Publishing Co. (154 Cal. App. 3d 1040 (1984)) sekä Sidis v. F-R Publishing Corp. (113 F.2d 806 (1940)). Newsworthiness-testeistä katso tarkemmin esimerkiksi *Solove – Schwartz,* Information Privacy Law (2011), s. 123–136.

878 Säännös tekee eron julkisuuden (publicity) ja julkaisemisen (publication) välille. Julkaisemisen kohdalla riittää, että tiedot on annettu vain kolmannelle osapuolelle eli kynnys on huomattavasti alempi julkaisemisen kohdalla. Tämä tosin soveltuu ainoastaan kunnianloukkaus-tapauksiin (defamation). Restatement (Second) of Torts §652D comment a.

879 Solove ja Schwartz ovat todenneet tämän doktriinin olevan hieman ironinen, sillä se on kääntynyt alkuperäistä ajatustaan vastaan. Katso tarkemmin, *Solove – Schwartz,* Information Privacy Law, (2011) s. 110

tarve tietää julkaistu asia.[880] Doktriinia onkin osuvasti kuvattu kuolevaksi kirjaimeksi ja jopa lainsäädännön kummitukseksi.[881]

Biometriseen tunnistamiseen tämän doktriinin soveltaminen on näin ollen erittäin hankalaa, sillä biometristen tietojen oikeudeton käyttö harvoin tapahtuu julkisuudessa. Ainoa ajateltavissa oleva tilanne, missä tämä säännös voisi aktualisoitua, on tietojen vuotaminen julkisuuteen esimerkiksi tietomurron kautta. Tällöin ongelmaksi kuitenkin muodostuu loukkaavuuden tai haitan toteennäyttäminen, sillä biometriset tunnisteet eivät yleensä suoraan paljasta mitään loukkaavaa tietoa.[882]

---

880 Katso esimerkiksi ratkaisu Times-Mirror Co. v. Superior Court (198 Cal. App. 3d 1420 (1988)), jossa oikeus katsoi, ettei sananvapaus taannut lehdistölle oikeutta julkaista murhaoikeudenkäynnin todistajan nimeä. Vertaa New York Times Co. v. Sullivan (376 U.S. 254 (1964)) sekä Cox Broadcasting Co. v. Cohn (420 U.S. 469 (1975)). Jälkimmäisessä ratkaisussa katsottiin, ettei raiskauksen uhrilla ollut oikeutta korvaukseen nimensä julkistamisesta mediassa, sillä nimi oli saatu julkisista rekistereistä. Vertaa kuitenkin Anderson v. Blake (469 F.3d 910 United States Court of Appeals, 10th Circuit (2011)), jossa raiskauksesta tehty video julkistettiin mediassa poliisin toimesta. Oikeus katsoi, että kysymyksessä oli yksityiselämää koskevasta tiedosta, jonka levittäminen oli tiedon kohteen kannalta erityisen loukkaavaa eikä yleisöllä ollut tähän tietoon oikeutettua tarvetta.

881 Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, s.2388 ja DeLaTorre, Resurrecting a Sunken Ship: An Analysis of Current Judicial Attitudes Toward Public Disclosure Claims, s. 1184.

882 Yhdysvalloissa asiaa on arvioitu muun muassa Google Street View –palvelua koskeneessa ratkaisussa Boring v. Google (38 Media L. Rep. 1306(2010)). Oikeus totesi, että julkisella paikalla kuvaaminen ei millään tavoin voi loukata yksilön oikeutta yksityisyyteen. Ratkaisu noudattelee oikeuskäytännössä omaksuttua linjaa, jonka mukaan

4) vääränlaisen kuvan antaminen yksilöstä julkisuuteen (false light in the public eye).

Liittovaltiotasolla vääränlaisen kuvan antaminen yksilöstä julkisuudessa on suojeltavista oikeushyvistä toistaiseksi vielä vakiintumaton. Kaikki osavaltiot Yhdysvalloissa eivät tunnusta kyseistä doktriinia. Se on kuitenkin eurooppalaisessa katsannossa erityisen merkittävä, sillä yksilön oikeus yksityisyyteen ja tiedolliseen itsemääräämiseen osana ihmisarvon kunnioitusta takaavat yksilölle oikeuden tulla arvioiduksi oikeassa valossa. Doktriinin ajatuksena on, että yksilölle taataan oikeus vaatia vahingonkorvausta, kun hänestä levitetään julkisuudessa tietoja, jotka antavat hänestä väärän kuvan, ja teko on erityisen loukkaava (Restatement (Second) § 652E).[883]

---

yksilöllä ei ole perusteltua oikeutta yksityisyyteen julkisella paikalla eikä tällä tavoin julkistetut tiedot myöskään voi aiheuttaa yksilölle haittaa tai vahinkoa.

883 One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if the false light in which the other was placed would be highly offensive to a reasonable person, and the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed. Katso ratkaisu Braun v. Flynt (726 F.2d 245 (5th Cir. 1984)). Epäselvää kuitenkin on vaaditaanko tekijältä tällaisessa tapauksessa täyttä piittaamattomuutta vai riittääkö tuottamus. Toistaiseksi tähän ei ole vielä löytynyt ratkaisua oikeuskäytännössä. Katso kuitenkin Korkeimman oikeuden ratkaisu Time, Inc. v. Hill (U.S. 374 (1967)), jossa todettiin, että Yhdysvaltain perustuslain ensimmäinen lisäys oikeuttaa vahingonkorvaukseen vain, jos loukkaaja on julkisesti levittänyt tiedon täysin totuudesta piittaamatta ja täysin tietoisena levitetyn tiedon paikkansapitämättömyydestä. Yksityis-

Julkisuutta ei tämän oikeussuojakeinon kohdalla ole tulkittu samalla tavoin kuin yksityiselämää koskevan tiedon levittämisen kohdalla. Riittäväksi on katsottu, että tiedot vastaanottavien tahojen ja tiedon kohteen välillä on erityinen suhde (special relationship). Näin ollen tietojen julkisuudeksi riittää, että pienikin joukko vastaanottaa tiedot ja näiden tietojen kautta muodostuu vääränlainen kuva tietojen kohteesta.[884]

Vääränlaisen kuvan antaminen (false light) on hyvin lähellä kunnianloukkausta. Molemmat suojaavat yksilöä virheellisiltä julkilausumilta. Erona on kuitenkin se, että kunnianloukkaus edellyttää tietynasteista vahingon aiheuttamista henkilön maineelle. Vääränlaisen kuvan antaminen puolestaan antaa oikeuden vaatia vahingonkorvausta yksinomaan teosta aiheutuneesta henkisestä kärsimyksestä. Vääränlaisen kuvan antamisen koh-

---

kohtaisempi kuvaus teon edellytyksistä katso Digital Media Law Project, Arizona: False Light. Saatavissa osoitteessa: http://www.dmlp.org/legal-guide/arizona-false-light. Katso myös *McKenna*, False Light: Invasion of Privacy. Tulsa Law Review, Vol. 15, Issue 1 (1979).

884 Tämä on todettu muun muassa ratkaisussa McSurely v. McClellan (753 F.2d 88 (United States Court of Appeals, District of Columbia Circuit 1985). Ratkaisussa painoarvoa annettiin sille, että pienellekin ihmisjoukolle julkaistut tiedot voivat aiheuttaa yksilölle suurta vahinkoa ja kärsimystä. Oikeus päätyi ratkaisuun siitä huolimatta, että yleensä julkisuudella tarkoitetaan suurta yleisöä (Restatement (Second) . Ratkaisu on kuitenkin hyvin ymmärrettävä, sillä väärien tietojen levittäminen esimerkiksi työpaikalla (esimerkiksi huhu intiimistä suhteesta esimiehen kanssa) voi pahimmassa tapauksessa pakottaa työntekijän vaihtamaan työpaikkaa. Vertaa kuitenkin esimerkiksi Bodah v. Lakeville Motor Express, Inc. (663 N.W. 2d 550(Supreme Court of Minnesota 2003)).

dalla riittää, että henkilöön kohdistuu kohtuutonta huomiota, joka antaa hänestä vääränlaisen kuvan julkisuuteen (Restatement (Second) of Torts § 652E comment b). Tämä tarkoittaa sitä, että henkilö voi periaatteessa vaatia korvausta jopa maineen paranemisesta.[885]

Biometrisen tunnistamisen kohdalla tämä oikeussuojakeino voi näin ollen tulla merkitykselliseksi, jos yksilön virheellisiä biometrisia tietoja jaetaan eteenpäin ja näiden virheellisten tietojen avulla luodaan profiili, joka antaa yksilöstä väärän kuvan. Tiedot voivat esimerkiksi virheellisesti kuvata yksilön terveydellistä tilaa, joka pahimmassa tapauksessa vaikuttaa yksilön oikeusasemaan.[886]

Suurimmaksi ongelmaksi oikeussuojakeinon soveltamisessa biometriseen tunnistamiseen on kuitenkin se, ylittääkö tällainen tietojen oikeudeton käyttö asetetun julkisuusvaatimuksen. Lisäksi, kun huomioidaan se, että profiilien luomisessa tulee olla kysymys puhtaasti tietojen värinkäytöstä, oikeussuojakeinon merkitys jää oikeastaan varsin pieneksi biometristen tietojen kohdalla.

885 *Ray,* Let There Be False Light: Resisting the Growing Trend Against an Important Tort, s, 735.

886 Yksilö saattaa virheellisten tietojen avulla luodun profiilin takia jäädä tiettyjen palvelujen tai paikkojen ulkopuolelle. Näin myös *Liu,* Bio-privacy, s. 192. Vääränlaisen kuvan antamisesta on ollut kysymys mm. kun henkilön kuvaa on käytetty väärässä yhteydessä. Katso esimerkiksi ratkaisut Thompson v. Coles-up, Inc. (98 N.Y.S.2d 300 (1950)) ja Morrell v. Forbes, Inc. (603 F. Supp. 1305 (D. Mass. (1985))

5.6.4. Biometrista tunnistamista koskeva erityislainsäädäntö Yhdysvalloissa

Yhdysvalloissa biometrisia tunnisteita koskeva erityislainsäädäntö on melko vähäistä. Muutamat osavaltiot ovat kuitenkin säätäneet biometrisia tunnisteita koskevaa erityislainsäädäntöä.[887] Osa näistä laeista, kuten Illinois´n osavaltiossa vuonna 2008 voimaan tullut Bio-

887 Yhdysvalloissa useat osavaltiot ovat säätäneet julkisen vallan toimesta tapahtuvaa biometristen tunnisteiden käyttöä koskevaa lainsäädäntöä. Lait ovat kuitenkin hyvinkin vaihtelevat. Esimerkiksi Washingtonin ja Oregonin osavaltioissa kasvontunnistuksen käyttö ajoneuvorekisterikeskuksissa on sallittu huijaus- ja väärinkäytöstapausten estämiseksi. Washingtonin laki tosin rajoittaa näiden tietojen luovuttamista. Mainen, Missourin ja New Hampshiren osavaltioissa on nimenomaisesti kiellettyä käyttää biometrisia tunnisteita ajokorteissa. Arizona ja Louisiana puolestaan kieltävät biometristen tunnisteiden keräämisen oppilailta ilman huoltajien suostumusta, ja säätävät rajoituksia biometristen tunnisteiden käytölle, säilytykselle ja hävittämiselle. Kaiken kaikkiaan biometrista tunnistamista koskevaa lainsäädäntöä on löydettävissä 18 osavaltiosta. Joissain osavaltioissa, kuten Kaliforniassa ja New Jerseyssä (Biometric Identifier Privacy Act, ehdotus saatavilla osoitteessa http://www.njleg.state.nj.us/2002/Bills/A2500/2448_I1.HTM), on ehdotettu biometrista tunnistamista koskevaa lainsäädäntöä, mutta nämä esitykset eivät ole toistaiseksi menestyneet. Myöskään liittovaltiotasolla ei toistaiseksi ole säädetty biometrisia tunnisteita koskevaa erityislainsäädäntöä. Huomautettava on kuitenkin siitä, että huhtikuussa 2014 on annettu esitys senaatille liittovaltiotason säädökseksi biometrisista tunnisteista (Biometric Information Privacy Act, ehdotus saatavilla osoitteessa: https://www.govtrack.us/congress/bills/113/hr4381/text). Ehdotuksella on kuitenkin arvioitu olevan hyvin pienet mahdollisuudet menestyä.

metric Information Privacy Act[888] sekä Texasin osavaltion Business and Commerce Code[889], pyrkivät kokonaisvaltaisesti säätelemään yksityisten toimijoiden taholta tapahtuvaa biometristen tunnisteiden käyttöä.[890]

Illinois: Biometric Information Privacy Act. Laissa tunnustetaan biometriseen tunnistamiseen liittyviä erityisiä näkökohtia, joiden vuoksi niistä tulee säätää laissa. Lain puutteena on, että se koskee vain yksityisiä toimijoita, joilla laissa tarkoitetaan yksilöitä ja kaikenlaisia muita yhteenliittymiä kuin osavaltion tai paikallishallinnon viranomaisia ja virastoja.[891] Tätä voidaan sinänsä pitää myös lain vahvuutena, sillä liittovaltiotasolla ei toistaiseksi ole säädetty biometrisia tunnisteita koskevaa erityislainsäädäntöä.[892] Lain ansiosta Illinois´n osavaltio takaa liittovaltiota paremman suojan yksilön biometrisille tunnisteille.

Laissa biometrisella tunnisteella tarkoitetaan silmän verkko- ja värikalvoa, sormenjälkeä, ääntä, kämmenenjälkeä sekä kasvojen rakennetta. Määritelmän ulkopuolelle on rajattu hyvin suuri joukko erilaisia ihmisistä saatuja biologisia näytteitä sekä tietyt ihmisen käyttäytymistä kuvaavat tiedot, kuten kirjoitusnäytteet, allekirjoitukset, valokuvat,

888 Biometric Information Privacy Act, 2007 ILL. SB 2400.

889 Business and Commerce Code, Title 11, Subtitle A, Chapter 503 Biometric Identifiers

890 Näiden lakien lisäksi usean osavaltion (muun muassa Nebraska, Iowa, North Carolina ja Wisconsin) lainsäädännössä biometriset tunnisteet on mainittu henkilötiedon määritelmässä. New Yorkin osavaltiossa puolestaan on lailla kielletty yksityisiä työnantajia ottamasta sormenjälkiä osana työsuhteen varmistamiseksi tai jatkamiseksi. Laki tosin säätää poikkeuksia tähän kieltoon.

891 Biometric Information Privacy Act Section 5 ja Section 10.

892 Kuten edellä on ollut puhetta, biometristen tunnisteiden voidaan kuitenkin katsoa kuuluvaksi vuoden 1974 Privacy Actin soveltamisalueelle.

tieteellisiin tarkoituksiin kerätyt ihmisen biologiset näytteet, tatuoinnit sekä sellaiset fyysistä olemusta kuvaavat tiedot kuten pituus, paino, hiusten ja silmien väri sekä veri.[893] Näiden tietojen katsotaan olevan biometrisia tietoja (”biometric information”), jos niitä käytetään yksilön tunnistamisessa. Keräämis- ja muille tietojen käsittelytavoille laki ei anna merkitystä. Lain arkaluonteisia tietoja koskevan määritelmän perusteella biometriset tiedot ovat arkaluonteisia. Laissa arkaluonteisena ja luottamuksellisena pidetään henkilötietoja, joiden perusteella yksilö on nimenomaisesti yksilöitävissä (”information that can be used to uniquely identify an individual”).[894]

Biometrisen tunnisteen käsittely on laissa lähtökohtaisesti kielletty. Laki kuitenkin sallii tietojen käsittelyn tietyin edellytyksin. Nämä ovat:

1) yksilön kirjallinen informointi tietojen käsittelystä;

2) yksilön kirjallinen informointi tietojen käsittelyn tarkoituksesta ja tietojen säilytysajasta sekä

3) yksilön kirjallinen suostumus tietojen käsittelyyn.[895]

Mainittujen edellytysten lisäksi rekisterinpitäjän on tehtävä kirjalliset käytännesäännöt, jossa annetaan tieto biometristen tietojen säilytysajasta ja ohjeet tietojen tuhoamisesta tietojen käydessä tarpeettomiksi alkuperäisen käyttötarkoituksen kannalta kuitenkin viimeistään 3 vuoden kuluttua yksilön viimeisestä asioinnista rekisterinpitäjän

893 Biometric Information Privacy Act Section 10. Voidaan näin ollen oikeastaan sanoa lain ulkopuolelle jäävän käyttäytymispiirteeseen perustuvat biometrisen tunnistamisen menetelmät.

894 Biometric Information Privacy Act Section 10.

895 Biometric Information Privacy Act Section 15 (b) (1), (2) ja (3) Edellytykset tietojen käsittelylle ovat näin ollen tiukemmat kuin esimerkiksi henkilötietolaissa asetetut henkilötietojen käsittelyn edellytykset.

kanssa. Säilytysajasta on kuitenkin mahdollista poiketa oikeuden määräyksellä.[896]

Laki takaa yksilölle vahvan oikeuden omiin biometrisiin tietoihinsa, sillä laki säätää absoluuttisen kiellon biometristen tunnisteiden ja biometristen tietojen kaupalliselle hyödyntämiselle. Myös näiden tietojen luovuttaminen, edelleen levittäminen ja muunlainen jakaminen on lähtökohtaisesti kielletty.

Tietoja voidaan luovuttaa vain, jos:

1) yksilö antaa luovutukseen luvan;

2) tietoja luovutetaan rekisteröidyn vaatiman tai hyväksymän taloudellisen toimenpiteen, kuten sopimuksen toimeenpanemiseksi;

3) tietojen luovuttaminen tapahtuu osavaltion tai liittovaltion lainsäädännön tai kunnallisen määräyksen nojalla taikka

4) luovutus tapahtuu oikeuden määräyksestä.[897]

Laissa vahvuutena on myös se, että siinä säädetään rekisterinpitäjälle tietoturvavelvoite. Lain nojalla rekisterinpitäjän tulee suojata tiedot toimialalla yleisesti käytössä olevin kohtuullisin toimenpitein. Suojan on oltava vähintään samaa tasoa kuin mitä käytetään arkaluonteisten tietojen suojaamiseksi.[898]

Tietoturvavelvoitteen heikkous on kohtuullisten toimenpiteiden määritteleminen. Vahvuutena on tosin se, että suojamekanismeilta edellytetään vähintään samaa tasoa kuin millä arkaluonteisia tietoja suojataan. Lisäys on omiaan tuomaan lisää turvaa yksilön oikeuksille.

Huomionarvoisena seikkana ja myös lain vahvuutena on se, että yksilö voi vaatia vahingonkorvausta lain säännösten rikkomisen vuok-

---

896 Biometric Information Privacy Act Section 15 (a).

897 Biometric Information Privacy Act Section 15 (c) ja (d). Laki turvaa näin ollen hyvin voimakkaasti yksilön tiedollista itsemääräämisoikeutta, sillä sekä tietojen keräämiseen että luovuttamiseen tulee lähtökohtaisesti olla yksilön suostumus.

898 Biometric Information Privacy Act Section 15 (e).

si.[899] Tähän kuuluu myös vahingonkorvaus tietoturvavelvoitteen laiminlyönnistä. Vahingonkorvausvelvollisuus omalta osaltaan vahvistaa yksilön oikeuksia biometristen tunnisteiden käsittelyssä.

Texas: Business and Commerce Code. Texasin osavaltiossa biometristen tunnisteiden käsittelyä ei säädellä varsinaisessa omassa laissaan. Se on osa isompaa sääntelykokonaisuutta, Business and Commerce Codea. Kysymyksessä on kaupallisia toimia koskeva kodifikaatio, johon on otettu erityinen biometrisia tunnisteita koskeva osa (Business and Commerce Code, Title 11, Subtitle A, Chapter 503 Biometric Identifiers).

Lain tarkoitus on hyvin yksinkertainen: kaupallisten toimenpiteiden yksinkertaistaminen, selkeyttäminen ja modernisoiminen sekä kaupallista alaa koskevan lainsäädännön yhtenäistäminen osavaltiossa.[900] Biometristen tunnisteiden yleistymisen vuoksi lakiin on katsottu tarpeelliseksi ottaa myös biometrisia tunnisteita koskevat säännökset.

Soveltamisalan vuoksi laki rajoittaa vain kaupallisiin toimiin tapahtuvaa biometristen tunnisteiden käsittelyä. Tosin laista ei suoraan käy ilmi, onko kysymys vain yksityisten harjoittamasta kaupallisesta toiminnasta, vai kattaako laki myös julkisen vallan harjoittamat kaupalliset toimet. Voidaan kuitenkin katsoa lain soveltuvan myös julkisen vallan organisaatioihin, sillä laissa henkilö (”person”) on määritelty käsittämään kaikki kaupallisen alan toimijat yksilöistä oikeushenki-

899 Korvausta voi vaatia niin tuottamuksellisen kuin tahallisen lain säännösten rikkomisen vuoksi. Korvaus on vähintään 1000 $ tuottamuksellisen rikkomisen tapauksessa ja vähintään 5000 $ tahallisen rikkomisen tapauksessa. Korvausta voi vaatia myös kohtuullisista oikeudenkäyntikuluista. Biometric Information Privacy Act Section 20.

900 Business and Commerce Code, Title 1, Chapter 1, Subchapter A, Section 1.103 (a).

löihin. Määritelmä nimenomaisesti mainitsee myös julkisen hallinnon toimijat henkilöiksi, joita laki koskee.[901]

Biometrisiksi tunnisteiksi laissa katsotaan lähinnä yksilön fyysiset ominaispiirteet, sillä lain mukaan biometrisilla tunnisteilla tarkoitetaan silmän verkko- ja värikalvoa, sormenjälkeä, ääntä ja käden tai kasvojen rakennetta (Section 503.001 (a)). Lain soveltamisalan ulkopuolelle näin ollen jäävät käyttäytymiseen perustuvat biometrisen tunnistamisen menetelmät.

Laki asettaa biometristen tunnisteiden keräämiselle tiukat edellytykset. Yksilön biometrista tunnistetta ei ensinnäkään ole lupa kerätä kaupalliseen tarkoitukseen ilman yksilön suostumusta. Lisäksi edellytetään, että biometristen tunnisteiden keruusta ilmoitetaan yksilölle ennen tunnisteen keräämistä.[902] Se myös suojaa suhteellisen tehokkaasti yksilön oikeuksia biometristen tunnisteiden käsittelyssä, sillä biometrisia tunnisteita ei ole lähtökohtaisesti lupa myydä, vuokrata tai muutenkaan luovuttaa.

Tietyissä laissa erikseen mainituilla poikkeuksilla tietoja on kuitenkin lupa luovuttaa. Nämä ovat: 1) tietojen luovuttaminen rekisteröidyn suostumuksella tunnistamistarkoitukseen rekisteröidyn kuoleman- tai katoamistapauksessa; 2) luovutus tapahtuu yksilön vaatiman tai valtuuttaman liiketoimen viimeistelemiseksi; 3) luovutus tapahtuu osavaltion tai liittovaltion lainsäädännön nojalla[903]; taikka 4) luovutus

901 Business and Commerce Code, Title 1, Chapter 1, Subchapter B, Section 1.201 (a)(27)

902 Business and Commerce Code, Title 11, Subtitle A, Chapter 503, Section 503.001. (b)

903 Poikkeus ei kuitenkaan koske Texasin osavaltion lakia Government Code, Section 552.

tapahtuu lainvalvontaviranomaiselle tai lainvalvontaviranomaisen toimesta lainvalvontatarkoitukseen oikeuden määräyksestä.[904]

Laki suojaa yksilön biometrisia tunnisteita asettamalla rekisterinpitäjälle tietoturvavelvoitteen ja velvollisuuden hävittää tarpeettomat biometriset tunnisteet. Lain mukaan biometrisia tunnisteita käsiteltäessä tulee noudattaa kohtuullista, mutta vähintään samanlaista varovaisuutta kuin muiden luottamuksellisten tietojen käsittelyssä. Tietojen hävittämiselle on asetettu joustava kohtuullisen ajan vaatimus, mutta lain mukaan tietoja ei kuitenkaan saa säilyttää vuotta pidempään käyttötarkoituksen päättymisestä.[905]

Poikkeuksena aikarajoista ovat tilanteet, joissa biometrista tunnistetta käytetään jonkin toisen välineen tai asiakirjan yhteydessä. Asiakirjan säilyttämiselle on jossain toisessa laissa säädetty pidempi säilytysaika. Tällöin tietoja voidaan säilyttää kohtuullinen aika tai vuosi sen jälkeen, kun välinettä tai asiakirjaa ei enää lain mukaan vaadita säilytettäväksi. Toisena poikkeuksena ovat työnantajan turvallisuustarkoituksiin (esim. kulunvalvonta) keräämät biometriset tunnisteet. Näiden katsotaan lain mukaan tulevan tarpeettomiksi työsuhteen päättyessä eikä niitä tällöin ole enää missään tilanteessa lupa käsitellä.[906]

Omalta osaltaan yksilön tiedollisia oikeuksia suojataan myös säätämällä lainvastaisesta menettelystä siviilioikeudellinen rangaistus, joka yksittäisestä loukkauksesta on enintään 25 000 $. Rangaistussäännöstä vahvistaa se, että rangaistusvaatimusta voi ajaa myös yleinen syyttäjä.

Yhteenveto. Molemmat lait säätelevät biometristen tunnisteiden kaupallista käyttöä, luovuttamista ja tuhoamista. Lähtökohdaksi kum-

---

904 Business and Commerce Code, Title 11, Subtitle A, Chapter 503, Section 503.001. (c)

905 Business and Commerce Code, Title 11, Subtitle A, Chapter 503, Section 503.001. (c) (1) ja (2).

906 Business and Commerce Code, Title 11, Subtitle A, Chapter 503, Section 503.001. (c-1) ja (c-2).

paankin lakiin on otettu käsittelykielto. Kumpikin laki sallii tietojen keräämisen yksilön suostumuksella. Lisäedellytyksenä on yksilön informointi tietojen keräämisestä ennen kuin tiedot tosiasiassa voidaan kerätä. Lait myös kieltävät lähtökohtaisesti tietojen luovuttamisen. Se on sallittu vain laissa mainituissa tilanteissa.

Illinois´n laki tosin suojaa tältä osin yksilöä vahvemmin, sillä informoinnilta ja suostumukselta edellytetään kirjallista muotoa. Illinois´n laki määrää myös rekisterinpitäjälle tiukemmat velvollisuudet ennen käsittelyn aloittamista. Laki velvoittaa luomaan kirjalliset käytännesäännöt, joissa kuvataan biometristen tunnisteiden keräämistavat ja säilytysaika.

Texasin laki kuitenkin turvaa paremmin yksilön oikeuksia biometristen tunnisteiden käsittelyssä, sillä laissa ei tehdä eroa julkisen vallan ja yksityisten toimesta tapahtuvalle biometristen tunnisteiden kaupalliselle käytölle. Illinois´n laki rajoittuu vain yksityisiin toimijoihin.

Heikkoutena kummassakin laissa on tietoturvavelvollisuuden välj ä muotoilu. Rekisteripitäjältä edellytetään vain kohtuullisia toimia tai kohtuullista varovaisuutta biometristen tietojen käsittelyssä. Mitä kohtuullisuus tässä yhteydessä tarkoittaa, jää kuitenkin tarkemmin määrittämättä. Ainoastaan vaaditaan vähintään samanlaista varovaisuutta kuin mitä muiden arkaluonteisten ja luottamuksellisten tietojen käsittely vaatii. Toisaalta tämä on myös kummankin lain vahvuus, sillä tällä tavoin lait rinnastavat biometriset tunnisteet arkaluonteisiin ja luottamuksellisiin tietoihin, jotka vaativat normaaleja tietoja vahvempaa suojaa.

Texasin osavaltion laki on Illinois´n lakia vahvempi myös sen vuoksi, että biometristen tietojen säilytysajat ovat lyhyemmät. Texasin laki myös ottaa huomioon työelämässä tapahtuvan biometristen tunnisteiden hyödyntämisen säätämällä tiukat aikarajat tietojen säilytykselle työpaikalla (tietojen katsotaan tulleen tarpeettomiksi työsuhteen päättyessä).

Vahvuutena kummassakin laissa on kuitenkin se, että yksilölle taataan oikeus vahingonkorvaukseen säännösten vastaisesta menettelystä. Illinois´n laki erottaa toisistaan tarkoituksellisesti tapahtuvan lain säännösten vastaisen menettelyn (korvaus vähintään 5000 $ tai todellisen vahingon määrä) sekä tuottamuksellisesti tapahtuvan lain säännösten vastaisen menettelyn (korvaus vähintään 1000 $ tai todellisen vahingon määrä). Texasin laissa tällaista eroa ei tehdä (korvaus enintään 25 000 $).

JAKSO III TUTKIMUKSEN YHTEEN-VETO JA JOHTOPÄÄTÖKSIÄ

6. Biometrisen tunnistamisen yhteiskunnalliset ja eettiset kysymykset

6.1. Kuuluuko valvonta demokraattiseen oikeusvaltioon?

Kansalaisen näkökulmasta oikeusvaltiolle on tunnusomaista, että ihmisillä on demokraattisessa järjestyksessä ennalta asetetuin normein määritellyt oikeudet, velvollisuudet ja vastuut, joita toteutetaan tehokkaasti ja yhtäläisesti. Oikeusvaltion ytimenä on näin ollen mielivallan ehkäiseminen. Oikeusvaltio rakentuu demokratian pohjalle.

Demokraattinen oikeusvaltio käsitteenä ei ole vain oikeudellinen, vaikka se viittaa eräisiin keskeisiin valtiosääntöperiaatteisiin, kuten demokratiaan ja perusoikeuksiin. Normatiivisena mittapuuna demokraattisen oikeusvaltion käsite asettaa vaatimuksia myös valtiota ja oikeutta eräällä tavalla välittävälle kansalaisyhteiskunnalle sekä sen kantamalle poliittiselle ja oikeudelliselle kulttuurille.[907]

Käsite demokraattinen oikeusvaltio on perusteltavissa siitä legitimiteettiperiaatteesta, jota moderni oikeus edellyttää. Moderni oikeus puolestaan on modernin valtion oikeutta. Moderni valtio nähdään keskitettynä valtiokoneistona, jota voi kuvata hierarkkisena ja oikeudellisille säännöille alistettuna byrokratiana.[908] Historiallisessa katsannossa modernin valtion institutionaalisen hahmon muotoutumista seurasi valtion erkaantuminen yhteiskunnasta. Julkisen vallan ja yksityinen alue erkaantuivat toisistaan.[909]

907 *Tuori,* Oikeus, valta ja demokratia, s. 269 sekä *Tuori,* Demokraattinen oikeusvaltio Suomessa, s.205.

908 *Tuori,* Oikeus, valta ja demokratia, s. 269.

909 *Tuori,* Oikeus, valta ja demokratia, s. 269.

Demokraattisen oikeusvaltion käsite nojaa valistusajan valtiosääntöperintöön. Tämän perinnön ajankohtaistaminen edellyttää kahden keskeisen periaatteen, kansansuvereniteetin sekä ihmis- ja perusoikeuksien uudelleenarviointia. Demokraattisessa oikeusvaltiossa kansansuvereniteetin periaatetta toteuttaa itsenäinen ja pluralistinen kansalaisyhteiskunta sekä sen kantama autonomisten osajulkisuuksien verkosto.

Demokraattisessa oikeusvaltiossa poliittinen päätöksenteko on avoinna kansalaisyhteiskunnan vaikutukselle ja kontrollille. Perusoikeudet takaavat kansalaisyhteiskunnan, sen järjestäytymisen ja sisäisten kommunikaatioprosessien autonomisuuden sekä pitävät avoinna kansalaisyhteiskunnan ja valtioinstituution kommunikaatiokanavat.[910]

Demokraattinen oikeusvaltio ei ole vain juridinen käsite, jonka tunnusmerkkien täyttämiseen riittäisivät vain perustuslakiin kirjatut säännökset. Säännökset itsessään eivät synnytä aktiivista ja pluralistista kansalaisyhteiskuntaa ja julkisuutta.[911] Demokraattisessa oikeusvaltiossa yhteiskunnan jäsenten välillä tulee vallita oikeudellinen yhdenvertaisuus, valtiosäännön tulee sisältää säännökset poliittisista perusoikeuksista ja kansanedustuslaitoksen tulee olla demokraattisesti valittu.[912]

Demokraattisen oikeusvaltion käsite on saanut osakseen myös kritiikkiä. Poliittisen vallankäytön katsotaan sekoittuvan oikeudelliseen vallankäyttöön. Ongelma on siinä, että jokaisen oikeusvaltion ei ole välttämätöntä olla demokratia, vaikka jokainen länsimainen demokratia on ainakin jonkinasteinen oikeusvaltio.[913]

---

910 *Tuori,* Demokraattinen oikeusvaltio Suomessa, s. 209.

911 *Tuori,* Demokraattinen oikeusvaltio Suomessa, s. 209.

912 *Tuori,* Oikeus, valta ja demokratia, s. 273–274.

913 *Aarnio,* Oikeusvaltio – tuomarivaltio?, s. 4

Asiaa on mahdollista tarkastella myös tuomalla esiin käsitteiden *demokratia* ja *oikeusvaltio* erilaiset tarkoitukset ja vaikutussuunnat. Demokratia periaatteena on vastaus kysymykseen julkisen vallan haltijasta ja käyttäjistä eli sen viimekätisenä tarkoituksena on julkisen vallan käytön legitimointi. Oikeusvaltio puolestaan vastaa periaatetasolla kysymykseen, mitä ovat julkisessa toiminnassa noudatettavat menettelytavat sekä toiminnan sisältö ja laajuus. Oikeusvaltioperiaatteessa on kysymys yksilön suojaamisesta sekä julkista valtaa että toisia yksilöitä vastaan, mutta myös demokraattisen legitimaatiorakenteen suojaamisesta.[914]

Merkityksellistä ei kuitenkaan ole demokraattisen oikeusvaltion tarkastelu pelkästään valtiomuotoajattelun tai poliittisten päämäärien kautta. Näkökulman tulee olla laajempi yksilön oikeuksien suuntaan.[915] Ihmisoikeuksien tunnistaminen kansallisella tasolla määrittää valtion luonteen. Tällöin korostetaan demokratian olevan valtio, joka on rakennettu poliittisten oikeuksien varaan. Oikeusvaltio puolestaan on rakennettu yksilön oikeuksien varaan. Näin ollen oikeusvaltio tarvitsee aktiivista ihmisoikeuksien soveltamista. Tämä voidaan nähdä yhdeksi oikeusvaltion ydinelementeistä.[916]

Demokraattisessa oikeusvaltiossa erilaiset poliittiset oikeudet yhdistyvät yksilön muihin oikeuksiin.[917] Yksilöllä on mahdollisuus aktiivisesti osallistua oikeuksiensa toteuttamiseen ja toisaalta myös vaatia

914 *Jyränki,* Oikeusvaltio ja demokratia, s. 13–14.

915 *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 32.

916 *Smith,* Human Rights as a Foundation of Society, s. 16.

917 *Tornberg,* Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, s. 32.

niiden toteuttamista.[918] Demokraattisen oikeusvaltion käsite ei kuitenkaan esiinny vain oikeuskirjallisuudessa. Euroopan unionin perusoikeuskirjan johdanto-osa sisällyttää demokraattiseen oikeusvaltioon ajatuksen ihmisen asettamisesta oman toimintansa keskipisteeksi.

Demokraattisessa oikeusvaltiossa ihmis- ja perusoikeudet saavat korostuneen merkityksen. Oikeusvaltion perustana on sellainen yksilön vapauksien, oikeuksien sekä yksityisyyden piirin määrittely, johon valtion voimankäytön ei ole lupa kajota. Tilanne on oikeastaan päinvastainen, sillä valtion tulee oikeudellisesti turvata tämä vapaan toiminnan alue. Oikeusvaltiossa perustuslain säännökset välittävät oikeuden yhteyttä arvoihin ja moraaliin. Näin ollen valtion ja oikeuden legitiimiys perustuu perustuslain säännösten arvopohjaan ja moraaliseen luonteeseen.

Demokraattisessa oikeusvaltiossa erilaiset arvonäkökohdat on turvattu ja demokraattinen prosessi antaa mahdollisuuden rationaaliselle päätösten teolle ilman turhaa vallankäyttöä. Tämä on myös osoituksena itsemääräämisoikeuden merkityksen korostumisesta demokraattisessa oikeusvaltiossa. Voidaan oikeastaan puhua ihmis- ja perusoikeusvelvoitteisesta demokraattisesta oikeusvaltiosta.

Demokraattisen oikeusvaltion näkyvän julkisivun pimeänä puolena on kurinpitoyhteiskunta tai oikeastaan valvontayhteiskunta. Perusteena on, että oikeudenkäyttö eri muodoissaan on aina luonteeltaan yhteiskunnallisen vallan käyttämistä. Oikeus myös heijastaa aina yhteiskunnallisia ja kulttuurisia olosuhteita. Oikeus ei myöskään synny luonnonvoimaisesti, vaan on luonteeltaan positiivista ja päätöksiin perustuvaa.

---

918 Oikeusasiamies on katsonut, että ihmisoikeustilanteen kehittyminen oikeaan suuntaan vaatii tätä aktiivisuutta demokraattisessa oikeusvaltiossa. Eduskunnan oikeusasiamiehen kertomus toiminnastaan vuonna 1998, s.40.

Foucault´lle kurinpito on tietty mikrovallan teknologia, jolle ominaisia menetelmiä ovat muun muassa jatkuva tarkkailu ja valvonta. Vallan teknologiana kurinpito ei ole sidottu vain tietyntyyppisiin yhteiskunnallisiin laitoksiin tai instituutioihin. Se voi levittäytyä koko yhteiskuntaan kurinpitosuhteiden verkostona.[919] Tarkkailu, valvonta, rekisteröiminen, arkistoiminen, luokittelu ja tietojen hankinta luonnehtivat tätä vallan muotoa.

Organisaatiot pyrkivät hallitsemaan ja valvomaan ihmisiä kansalaisina, asiakkaina tai työntekijöinä keräämällä heistä tietoja. Näiden organisaatioiden intressinä on tehokas sosiaalinen kontrolli. Ajatusta kuvaa se, että valvonta on osa vallankäyttöä ja että modernissa valtiossa pääsy tietoon liittyy kiinteästi valtaan.

Vapauden ja tasa-arvon ideat ja niille perustuva laki ja oikeudellinen diskurssi voivat kuitenkin kääntyä kurinpitovaltaa vastaan. Valtaan kytkeytyy aina vastarintaa. Kurinpidollinen valta synnyttää uusia vastarinnan muotoja, jotka ovat tunnusomaisia moderneille yhteiskunnille. Vastarinta ei kuitenkaan kohdistu vallan käyttäjiin, vaan ensisijaisesti valtaan itsessään ja sen seurauksiin. Moderni vastarinta kohdistuu niihin vallan seurauksiin, jotka ovat sidoksissa tietoon, kompetenssiin ja pätevyyteen, mutta myös salailuun ja manipulointiin. Se kohdistuu tekniikoihin, kuten tarkkailuun. Yhteiskunta on jatkuvassa liikkeessä, jolloin yhteiskuntaa tulee lähestyä jatkuvasti muuntuvana strategisena kenttänä.[920]

---

919 *Foucault,* Power/Knowledge, s.93 ja The History of Sexuality, s. 92. Katso myös Foucault Discipline and Punish(1979). Foucault´n tarkastelemat prosessit ja suhteet paikantuvat ikään kuin oikeudellisen tason alapuolelle, oikeuden infastruktuuriin.

920 *Foucault,* The History of Sexuality, s. 92–93. Foucault on sanonut, että myös demokraattisessa oikeusvaltiossa lain tehtävänä on legitimoida ja peittää kurinpidollinen vallankäyttö.

Edellä mainitun perusteella on esitettävä kysymys: Kuuluuko valvonta demokraattiseen oikeusvaltioon? Vastaus kysymykseen on kielteinen. Valvonta osana vallankäyttöä ei itsessään kuulu demokraattiseen oikeusvaltioon, vaikka yksilöiden erilainen valvonta osana kontrollia on välttämätön työväline. Yleisen järjestyksen ja turvallisuuden ylläpito on yhteiskunnan keskeisiä tehtäviä yksilöiden oikeuksien turvaamiseksi. Demokraattisessa oikeusvaltiossa pelkästään yksilöiden oikeuksien toteutumisen takaaminen ei kuitenkaan ole riittävä peruste oikeuttamaan liiallista valvontaa.

Laajamittainen valvonta vaarantaa yksilön oikeudet. Valvonnan oikeutusperusteena on kuitenkin se, että julkisella vallalla on oikeus suojella itseään valtionvastaiselta toiminnalta ja hyökkäyksiltä. Tämän tulee tapahtua yksilön oikeudet huomioon ottavalla tavalla, sillä valtiollakin on velvollisuus kunnioittaa näitä oikeuksia.

Poliisin tarkkailuvaltuuksien käyttö esimerkiksi ilman rajoja tai ilman riittävää valvontaa ovat tunnusomaista autoritaariselle vallankäytölle. Ilman riittäviä rajoja poliisista itsestään tulee uhka yksilölle ja yhteiskunnalle, vaikka sen tarkoitus on nimenomaan suojata yhteiskuntaa ja sen jäseniä. Tällöin vaarana on, että demokraattinen oikeusvaltio omalla toiminnallaan murentaa perusedellytyksiään eli yksilöiden vapauksia ja oikeuksia, ja näin omaa olemassaoloaan. [921]

Perus- ja ihmisoikeudet asettavat laillisen ja legitiimin valvonnan rajat. Vähimmän puuttumisen periaatteen mukaan demokraattisessa oikeusvaltiossa oikeuksiin ja vapauksiin on lupa puuttua vain siinä määrin, kuin se on välttämätöntä. Periaate on tärkeä sen vuoksi, että käytännössä tehokkuuteen pyrkiminen eri toiminnoissa muodostaa riskin yksilön oikeuksien toteutumiselle.

---

921 *Hadjimatheou,* Ethics and surveillance in authoritarian and liberal states, s. 3 ja Metsäranta, Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja, s. 5

Demokraattinen oikeusvaltio korostaa kansansuvereniteettia ja perusoikeuksia keskeisinä valtiosääntöperiaatteinaan. Ajattelutavan teoreettiset juuret ovat yhteiskuntasopimusteoriassa, jossa moderni yhteiskunta nähdään vapaiden, tasa-arvoisten ja rationaalisesti toimivien yksilöiden yhteiskuntana. Yksilösubjektien keskinäiset suhteet perustuvat olennaisesti heidän vapaina ja tasa-arvoisina solmimiinsa sopimuksiin. Yhteiskunnan poliittista organisoitumista myös kuvataan ja selitetään sopimusmallilla: vapaat ja tasa-arvoiset subjektit luovuttavat osan suvereniteettiaan keskitetylle poliittiselle vallalle. Lakien säätämiseen päättyvä poliittinen päätöksenteko noudattaa niin ikään sopimusmallia: lait ovat eräänlaisia yksilösubjektien edustajiensa välityksellä solmimia sopimuksia, jotka tiivistävät yleistahdon ja ilmentävät kaikkien yksilösubjektien yhteisiä intressejä.[922]

Tehokkaalle ja salaiselle valvonnalle perustuva yhteiskunta on vastoin oikeusvaltiolle keskeisiä ihmisen vapausoikeuksia. Siksi yksilöön kohdistuvan valvonnan tulee perustua yksityisen ja yhteisen edun keskinäiseen punnintaan ja lainsäädäntöön. Lisäksi valvonnan tulee olla laillisuusvalvonnan alaista. Salainen valvonta ei kuulu demokraattiseen oikeusvaltioon.

Lähtökohtaisesti demokraattiset olot yhteiskunnassa ovat ne tekijät, jotka tarjoavat kasvualustan oikeusvaltiollisille käytännöille. Kansalaiset ovat paitsi laillisen, myös legitiimin oikeudellisen vallankäytön kohteina.[923] Demokratian ongelmat avaavat oven tilanteille, joissa kansalaiset kokevat joutuvansa oikeudettoman ja illegitiimin oikeudel-

---

922 *Tuori,* Oikeus, valta ja demokratia, s. 134. Katso myös Habermas, Theorie des kommunikativens Handeln.

923 Vallankäytön legitimiteetillä voidaan tarkoittaa eri asioita. Empiirisen legitimiteettikäsityksen mukaan legitiiminä pidetään jokaista sellaista järjestelmää, jonka sen piiriin kuuluvat henkilöt ainakin passiivisesti hyväksyvät. Normatiivisen legitimiteettikäsityksen mukaan poliittisen ja oikeudellisen vallankäytön legitiimisyyttä arvioitaessa

lisen vallankäytön kohteeksi. Tällöin siirrytään lain ylivallasta vallankäyttöön, jossa oikeudelliset näkökohdat sivuuttavan poliittisen harkinnan osuus korostuu liikaa. Vaikka oikeudellinen toiminta on aina vallankäyttöä, tulee sen silti pysyä niissä rajoissa, joita oikeusvaltiolliset periaatteet sille asettavat.

Syyskuun 11. päivän terrori-iskut ovat tuoneet oman lisänsä ihmisten valvonnan tiukentumiseen monin tavoin. Esimerkkinä voidaan mainita biometrisen tunnistamisen yleistyminen ja kehittäminen turvallisuutta lisäävänä tekijänä. Tämä on sinänsä luonnollista, sillä poikkeustilanteiden uhka on oikeusvaltiossa aina olemassa ja se saattaa johtaa väliaikaisesti perusoikeuksia supistaviin toimiin. Ongelmallisempaa tähän liittyen on henkilötietojen käsittelyn lisääntyvä sääntely, johon terrorismin uhkan luomia mielialoja ja pelkoja on toisinaan käytetty perusteluina. Biometrinen tunnistaminen on esimerkki tällaisesta sääntelystä.

Ennen kaikkea kysymys on kuitenkin julkisten ja yksityisten organisaatioiden toiminnan tehostamisesta yksityisyyttä välittömästi tai välillisesti rajoittaen. Tällaista sääntelyä haitallisempaa on välillinen sääntely, jossa esimerkiksi viranomaisille annetaan tietyn erityislain ja sen tavoitteiden puitteissa oikeus henkilötietojen käyttöön tai kansalainen ohjataan käyttämään palveluita, jotka edellyttävät digitaalista identifiointia.

Biometriseen tunnistamiseen liittyy tiedollisen puolen lisäksi henkilökohtaisen koskemattomuuden näkökulma. Tämä itsemääräämisoikeuteen, yksityisyyteen ja turvallisuuteen läheisesti liittyvä näkökulma jää monesti huomiotta. Biometrisella tunnistamisella on vaikutuksensa myös henkilökohtaiseen koskemattomuuteen, sillä biometrisen tun-

---

on otettava huomioon se, täyttääkö järjestelmän puitteissa harjoitettu vallankäyttö tietyt eettiset ja moraaliset vähimmäisvaatimukset. Erikkson, Valta, s. 1242–1243.

nisteen keräämisellä aina rajoitetaan yksilön itsemääräämisoikeutta ja puututaan yksilön fyysiseen koskemattomuuteen. Perusteena tälle rajoitukselle ja puuttumiselle on käytetty turvallisuuden takaamista, joka on yhteiskunnan toimivuuden edellytys ja näin yksilön ja yhteiskunnan edun mukaista.

Oikeusjärjestykseemme ei sisälly mitään sellaista yleistä oikeutusta henkilön itsemääräämisoikeuden sivuuttamiseen sillä perusteella, että puuttumista ihmisen ruumiilliseen koskemattomuuteen voitaisiin objektiivisesti arvioiden pitää hänen etujensa mukaisena. *Saarenpää* huomauttaakin osuvasti siitä, että vaikka näitä rajoituksia tehtäessä toteutetaan muodollisesti oikeusvaltioon liittyvää lailla säätämisen vaatimusta, lisääntyvä sääntely on aina riski identiteetin suojan kannalta. Lopputuloksena on helposti yksityisyyden ja siihen liittyen identiteetin suojan pirstoutuminen. Tällöin vaarana on, että yhteys yksityisyyden perusperiaatteisiin katkeaa, minkä seurauksena sosiaalinen kontrolli ja hyötyorganisaation tehokkuus asettuvat perusoikeuksien edelle arkipäivän oikeudellisessa elämässä. Valitettavan usein tämän tehokkuuden lisäämisen taustalla on ajatus ihmisestä väärinkäytösten tekijänä. [924] Tällaista ajattelua kuvaa poliisin toive saada pääsy passirekisterin sormenjälkitietoihin.

6.2. Biometrisen tunnistamisen eettiset kysymykset

Etiikalla tarkoitetaan moraalin tutkimusta tai oppia moraalista eli moraalifilosofiaa. Eettiseen keskusteluun kuuluu pohdinta myös siitä, tulisiko biometrisen tunnistamisen hyödyntämisen perustua yksilön valinnanvapauteen vai ei. Kysymys ei kuitenkaan ole sen enempää kansalaisten uskomusten, mielipiteiden tai moraalikäsitysten empiirisestä

924 *Saarenpää,* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 58.

kartoittamisesta kuin biometrisen tunnistamisen teknologiaa ohjaavan lainsäädännön yhtenäistämisestäkään. Pikemminkin kysymys on oikean ja perustellun vastauksen löytymisestä arvokysymyksiin.

Eettinen ongelma syntyy tavallisesti siksi, että tarjolla on useampia eettisiä periaatteita, jotka antavat toisistaan poikkeavia suosituksia ja ohjeita. Koska periaatteet ovat luonteeltaan yleisiä ja abstrakteja, ei niistä välttämättä saa vastausta mihinkään konkreettiseen tilanteeseen. Eettisistä periaatteista joudutaankin usein tulkinnalla johtamaan yksityiskohtaisempia ja konkreettisempia moraalisääntöjä ja -normeja. Tämän vuoksi aidot eettiset ongelmat kärjistyvät usein eettisten periaatteiden erilaisiin tulkintoihin tai periaatteista johdettavissa oleviin ristiriitaisiin toimintasuosituksiin.

Biometriseen tunnistamiseen liittyvät eettiset kysymykset tulee erottaa tähän teknologiaan liittyvistä oikeudellisista kysymyksistä. Oikeudellisten kysymysten kohdalla on kysymys siitä, miten biometristä tunnistamista on mahdollista käyttää lainmukaisesti. Eettisissä kysymyksissä puolestaan on kysymys siitä, tuleeko biometristä tunnistamista ylipäätään käyttää yhteiskunnassa yksilöiden tunnistamisessa.

Biometriseen tunnistamiseen liittyvät eettiset periaatteet ovat johdettavissa biotekniikkaan sovellettavista eettisistä periaatteista, joita ovat ihmisarvon kunnioittaminen, vahingon välttäminen, hyödyn maksimoiminen, itsemääräämineninen ja oikeudenmukaisuus.[925]

925 *Launis,* Geeniteknologia, arvot ja vastuu, s. 33 sekä *Beauchamp – Childress,* Principles of Biomedical Ethics, s. Periaatteista osa on vakiinnuttanut paikkansa kansainvälisessä bioeettisessä keskustelussa. Kuten Wolf asian ilmaisee: ”The four principles…have become the most familiar litany recited in bioethics…” Wolf, Shifting Paradigms in Bioethics and Health Law: The Rise of a New Pragmatism, s.400

Humanistisen etiikan perustan muodostaa *ihmisen kunnioittamisen periaate:* jokaista ihmisyksilöä tulee kunnioittaa päämääränä sinänsä eikä välineenä jonkin päämäärän saavuttamiseksi.[926]

Ihmisarvon kunnioittaminen on perustana kaikessa toisiin ihmisiin kohdistuvassa toiminnassa. Ihmisarvon kunnioittamisen periaate rajaa piiristään valtaosan muuhun kuin ihmiseen kohdistuvasta bioteknologiasta. Ihmisarvon kunnioittamisen periaatteen mukaan jokaisella ihmisellä on yhtäläinen moraalinen arvo. Monissa keskusteluissa ihmisarvon kunnioittamisen vaatimus liitetään ihmisoikeuksiin, joiden kantajia kaikki ihmisyksilöt ovat yhtäläisesti.[927]

Ihmisarvon kunnioittamisen periaate liittyy biometrisen tunnistamisen kohdalla siihen, että biometrisessa tunnistamisessa ihminen muutetaan koneella luettavaksi välineeksi, johon ihmisellä ei välttämättä ole hallintaa. Ihmisarvon periaatteen mukaan ihmistä tai ihmisen osaa ei kuitenkaan saa välineistää.[928] Ihmisen välineellistämistä ei ole ihmisarvoisen kohtelun mukaista, sillä se loukkaa oikeutta tulla tunnustetuksi yksilönä yhteiskunnassa.[929] Välineellistäminen vaikuttaa myös yksilön yksityisyyteen, sillä fyysisen yksityisyyden kunnioittamisessa tärkeä ulottuvuus on yksilön suojaaminen välineellistämiseltä. Biometrisen tunnistamisen seurauksena ihmisruumiista tulee vain väline yksilön automaattisessa tunnistamisessa.[930] Ennen biometrisen

---

926 *Pietarinen,* Geenitutkimus ja etiikka, s. 46

927 *Launis,* Geeniteknologia, arvot ja vastuu, s. 38.

928 Näin myös *Lötjönen,* Lääketieteellinen tutkimus ihmisillä, s. 85.

929 Viime kädessä ihmisarvo on siis palautettavissa Immanuel Kantin käsitykseen, jonka mukaan ihmistä ei koskaan tulisi kohdella välineenä, vaan päämääränä. Katso Kantin käsityksestä ihmisarvosta tarkemmin Knox, Dignity and the Essence of Man.

930 Näin myös *Kindt,* Privacy and Data Protection Issues of Biometric Technologies, s. 389 sekä Hendrickx, Privacy en Arbeidsrecht, s. 12.

tunnistamisen laillisuutta tulee arvioida sitä, missä ja milloin biometrisen tunnistamisen käyttäminen on sallittua ja lainmukaista.

Vahingon välttämisen periaate on yksi tärkeimmistä yksittäisistä ohjenuorista bioteknologian ja sen sovellusten eettisessä ennakkoarvioinnissa. Periaate on kiteytettävissä seuraavasti: on vältettävä sellaista toimintaa, joka aiheuttaa tarpeetonta tai kohtuutonta vahinkoa muille tai loukkaa muiden oikeuksia.[931] Kysymys on toisin sanoen siitä, miten ja missä rajoissa biometrisen tunnistamisen käyttäminen yhteiskunnassa on suotavaa.

Biometrisen tunnistamisen sovellusten vaikutuksia arvioitaessa vahinkoperiaate tulkitaan usein vaatimukseksi arvioida ja hyväksyttää toimintaan liittyvät riskit. Biometriseen tunnistamiseen liittyvien riskien arviointi on erityisen ongelmallista, sillä nykytiedon valossa nämä riskit ovat yleensä mahdollisia riskejä.[932]

Launiksen mukaan vahingon välttämisen periaatteen tärkein sovellus on ns. ennalta varautumisen periaate (precautionary principle), jonka mukaan tekniikan käytöstä on pidättäydyttävä, jos käyttö voi johtaa kohtuuttomiin tai peruuttamattomiin vaaroihin.[933] Kuten edellä jaksossa 4.3.2. on esitetty, biometrisen tunnistamisen käyttöön liittyy monia riskejä, jotka vaarantavat yksilön perus- ja ihmisoikeudet. Biometrisen tunnistamisen käyttö voi johtaa yksilön oikeuksien kannalta kohtuuttomiin tai peruuttamattomiin vaaroihin, minkä vuoksi biometrisen tunnistamisen laajamittaisesta käytöstä tulee pidättyä.

---

931 *Launis,* Geeniteknologia, arvot ja vastuu, s. 40.

932 Sarvaksen mukaan tämä tarkoittaa sitä, että mahdollisia riskejä arvioitaessa ei voida turvautua kokemusperäiseen tietoon. Arvio perustuu hänen mukaansa yleensä teoreettiseen tarkasteluun ja rinnastuksiin joihinkin tunnettuihin ilmiöihin. Sarvas, Biotekniikka, riskit ja etiikka, s. 349

933 *Launis,* Geeniteknologia, arvot ja vastuu, s. 43.

Hyödyn maksimoimisen periaate edustaa puhtaasti utilitaristista seurausetiikkaa.[934] Siinä toiminnan moraalisuuden mittarina pidetään toiminnan välittömiä ja välillisiä seurauksia. Pietarinen kiteyttää periaatteen seuraavasti: *"On toimittava niin, että odotettavissa oleva hyöty suhteessa haittoihin on niin suuri kuin mahdollista."*[935]

Periaatteessa hyödyn käsite viittaa tehokkuuteen. Tehokkuus puolestaan tarkoittaa sitä, että saavutettujen hyötyjen suhde kustannuksiin on mahdollisimman suuri.[936] Kysymys on toisin sanoen eräänlaisesta kustannustehokkuudesta biometrista tunnistamista käytettäessä.

Yksilön autonomian eli *itsemääräämisen kunnioittaminen* on kaiken ihmiseen kohdistuvan toiminnan eettinen kulmakivi. Pietarinen on kiteyttänyt asian seuraavasti: *"Autonominen yksilö on oikeutettu päättämään itseään koskevista asioista, toimimaan vapaasti harkitsemallaan tavalla ja saamaan muilta päätöksen toteuttamisen edellyttämää apua, esimerkiksi tietoa."*[937]

Biometrisen tunnistamisen kohdalla itsemääräämisen periaate tarkoittaa sitä, että yksilöiden vapautta ja itsemääräämisoikeutta ei tule rajoittaa esimerkiksi pakottamisella tai tietoisella harhaanjohtamisella. Käytännössä tämä tarkoittaa sitä, että velvollisuuden sijasta noudatetaan niin sanottua vapaaehtoisen suostumuksen sääntöä (informed consent). Näin siksi, että toiminnan autonomisuuden kannalta ratkaisevassa asemassa on päätöksenteon edellyttämä riittävä informaatio,

---

934 *Launis,* Geeniteknologia, arvot ja vastuu, s. 43

935 *Pietarinen,* Lääkintä- ja hoitoetiikan keskeiset periaatteet, s. 51

936 Saavutettuja tehokkuusarvoja voivat olla mitä erilaisimmat asiat. Hyödyn mittapuuna voidaan tämän vuoksi käyttää myös muita kuin vain taloudellisia arvoja. *Launis,* Geeniteknologia, arvot ja vastuu, s. 44.

937 *Pietarinen,* Lääkintä- ja hoitoetiikan keskeiset periaatteet, s. 42.

jonka perusteella yksilö on kykenevä tekemään vapaaseen tahdonmuodostukseen perustuvan päätöksen.[938]

Oikeudenmukaisuuden periaate soveltuu niin yksilöihin kuin yhteiskuntiin. Se ei tarkoita samaa kuin moraalisesti oikea. Jokin asia voi nimittäin olla oikea olematta silti oikeudenmukainen. Moraalisesti oikeat ratkaisut ovat sellaisia, joihin on yleisesti pyrittävä. Oikeudenmukaiset ratkaisut eivät aina ole tällaisia. Oikeudenmukaisuudessa on kysymys vain yhdestä hyveestä muiden joukossa. Yhteiskunnan toiminnan kannalta oikeudenmukaisuus on kuitenkin hyveistä tärkeimpiä.[939]

Yksi tavallisimmista modernia biometrista tunnistamista ja sen sovelluksia koskevista oikeudenmukaisuusongelmista liittyy sen tarjoamiin mahdollisuuksiin valvoa ja tarkkailla yksilöitä yhteiskunnassa. Ongelmana on myös se, että biometrisiin tunnisteisiin sisältyvä informaatio antaa aivan uudenlaisen mahdollisuuden ihmisten syrjinnälle näiden tietojen avulla. Ulkopuolisten tahojen pääseminen käsiksi tähän informaatioon voisi lisätä huomattavasti tiettyjen yksilöiden

938 Saarenpään mukaan yksilöiden identiteetti ja yksityisyys jää muiden käsiin, mikäli he eivät voi itse hallita henkilötietojaan. Samalla heistä tulee tietoalamaisia sen sijaan, että he itse hallitsisivat henkilötietojaan. *Saarenpää,* Suostumus ja hyvä tietojenkäsittelytapa, s. 4.

939 Launis erottaa oikeudenmukaisuudessa muodollisen ja sisällöllisen puolen. Muodollinen oikeudenmukaisuus vaatii meitä kohtelemaan kaikkia merkityksellisiltä osiltaan samanlaisia tapauksia samalla tavalla ja kaikkia merkityksellisiltä osiltaan erilaisia tapauksia eri tavalla. Sisällöllinen oikeudenmukaisuus puolestaan osoittaa sellaisen perusteen, jonka nojalla luokittelu yhtäläisiin ja epäyhtäläisiin tapauksiin voidaan tehdä. Moraalisesti merkitykselliset eroavuudet tapausten välillä oikeuttavat niiden erilaisen kohtelun ja moraalisesti merkitykselliset yhtäläisyydet niiden samanlaisen kohtelun. *Launis,* Geeniteknologia, arvot ja vastuu, s. 50.

ja ryhmien syrjintää.[940] Tämän kaltaisiin epätoivottaviin seurauksiin viitattaessa on oikeastaan mahdollista puhua biologisesta syrjinnästä.

6.3. Biometrisen tunnistamisen soveltamiseen liittyvät periaatteet

Eettisten periaatteiden lisäksi biometrisen tunnistamisen soveltamiseen liittyy tiettyjä yleisiä periaatteita.[941] Näiden periaatteiden avulla biometrisen tunnistamisen soveltamisessa tämän teknologian käyttöön liittyvät erityiskysymykset tulevat huomioiduksi. Koska biometrisella tunnistamisella on voimakkaita vaikutuksia yksilön oikeuksiin, tulevat nämä oikeudet paremmin huomioiduksi näiden yleisten periaatteiden avulla.

Vaikka biometriasta ei ole Suomessa eikä Euroopan Unionin tasolla säädetty erityissäädöstä, ei tämä tarkoita biometrisen tunnistamisen olevan lainsäädännöstä vapaa. Biometrista tunnistamista koskee *lainalaisuuden periaate*. Biometrisen tunnistamisen soveltamisessa lainsäädännön – erityisesti henkilötietolain – asettamat vaatimukset tulee ottaa huomioon.

Lähtökohtana biometrisen tunnistamisen soveltamisessa tulee olla *yksityisyyden suojan kunnioittaminen*. Biometrinen tunnistaminen vaikuttaa ennen kaikkea yksilön yksityisyyteen ja henkilötietojen suojaan. Sen käyttämisessä tulee ottaa lähtökohdaksi vähimmän puuttumisen

940 Katso esimerkiksi *David Lyon* (ed.), Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination.

941 Monet tässä mainituista periaatteista on mainittu myös kansainvälisen toimijan, Biometrics Instituten, laatimissa biometrisen tunnistamisen yksityisyysohjeissa. Ohjeet on saatavissa osoitteessa: http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute_BIOMETRICS_GUIDELINES_V1.pdf

periaate ihmis- ja perusoikeusluonteensa vuoksi. Biometrisen tunnistamisen sovelluksista tulee valita käytettäväksi sellainen, joka mahdollisimman vähän loukkaa yksilön yksityisyyden suojaa. Tässä tarkoituksessa tulee toteuttaa arvio teknologian vaikutuksesta yksityisyyteen. Tällainen arvio pakottaa järjestelmän käyttäjiä ottamaan yksityisyyden suojan toteutumisen huomioon koko järjestelmässä.

Yksityisyyden suojan kunnioittamiseen liittyy läheisesti *suhteellisuusperiaate.*[942] Biometristen tunnisteiden kohdalla kerättävien tietojen suhteellisuus nousee usein esille. Koska biometrisia tunnisteita on mahdollista käsitellä vain, jos nämä tiedot ovat asianmukaisia, oleellisia ja oikeassa suhteessa käyttötarkoituksen kanssa, tulee näiden käyttöä harkita suhteellisuuden ja tarkoituksenmukaisuuden näkökulmista.

Lähtökohtana tulee olla sen selvittäminen, onko biometrinen tunnistaminen todella tarpeellista kyseiseen käyttötarkoitukseen. Toiseksi tulee selvittää, onko biometrinen tunnistaminen tehokas keino valittuun tarkoitukseen. Lisäksi tulee miettiä, ovatko biometrisen tunnistamisen riskit yksityisyydelle hyväksyttäviä saavutettuun etuun nähden.

Suhteellisuusperiaatteessa on toisin sanoen kysymys siitä, että punnitaan biometrisen tunnistamisen sovelluksen mukanaan tuomia etuja ja haittoja keskenään.[943] Biometrista tunnistamista ei tule ottaa käyt-

---

942 Suhteellisuusperiaate on merkityksellinen hyvin monella eri oikeuden alalla. Ensisijassa sitä on tutkittu muun muassa hallinto-, rikos- ja kansainvälisen oikeuden aloilla. Suurin merkitys suhteellisuusperiaatteella on kuitenkin perus- ja ihmisoikeuksien alalla, jossa sitä käytetään perus- ja ihmisoikeuksien rajoittamisen päälähtökohtana. Periaatteesta on kuitenkin tullut keskeinen tavoite-keinot -suhteen arviointisääntö. *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 405 ja 415. Suhteellisuusperiaatteesta tarkemmin katso *Van Drooghenbroeck,* La proportionnalité. Prendre l'idée simple au sérieux.

943 Näin myös *Liu,* Bio-Privacy, s. 259

töön vain helppouden ja tehokkuuden nimissä, vaan tämän teknologian käyttämiselle tulee olla aito ja perusteltu tarve. Tämän tarpeen arvioinnissa suhteellisuusperiaate toimii työkaluna. Suhteellisuusperiaatteen mukaan arvioitavaksi tulevat ainakin seuraavat asiat:

1) Onko biometrisen tunnistamisen käyttäminen välttämätöntä vaadittuun tarkoitukseen eli onko välttämätöntä tarvetta käyttää biometrisen tunnistamisen kaltaista pysyvää ja ainutlaatuista tunnistamista?

2) Onko biometrisen tunnistamisen käytöstä saatavat hyödyt suuremmat kuin käytön mukanaan tuomat riskit?

3) Onko käytettävissä muita yhtä tehokkaita tapoja tavoitteeseen pääsemiseksi?

Esimerkkinä toimii kuntosalin sisäänkirjautumisessa käytettävä biometrinen tunnistaminen. Kuntosalin intressissä on valvoa, että vain salin käyttöön oikeutetut käyttävät salia. Tällainen biometrisen tunnistamisen käyttö ei kuitenkaan täytä suhteellisuusperiaatetta. Samaan päämäärään päästään käyttämällä muita kulunvalvontaan tarkoitettuja laitteita, jotka vähemmän puuttuvat yksilön oikeuksiin.

Biometrisen tunnistamisen luonteen vuoksi tärkeä periaate on *avoimuuden periaate*. Biometrisen tunnistamisen käytön tulee lähtökohtaisesti aina perustua nimenomaiseen, vapaasti annettuun ja yksiselitteiseen suostumukseen. Vain tietyissä lain edellyttämissä tapauksissa suostumuksen vaatimuksesta voidaan poiketa.[944]

Itsemääräämisen kunnioittamisen periaatteen mukaisesti suostumuksen tulee perustua mahdollisimman yksityiskohtaiseen informaatioon biometrisen tunnistamisen käytöstä. Informaatiota on annettava ainakin kerättävistä tiedoista ja siitä, mitä biometrisen käyttö tarkoittaa ja mitä vaikutuksia siitä on yksilölle. Suostumuksen vapaaehtoisuuden vuoksi on tärkeää, että annettu suostumus tulee olla peruutettavissa.

944 Näin myös *Liu,* Bio-Privacy, s. 259–260

Yksilön tulee voida milloin tahansa ja ilman perusteluja peruuttaa antamansa suostumus biometrisen tunnisteen käyttöön. Suostumuksen peruuttamisella ei myöskään saa olla mitään haitallisia seuraamuksia yksilölle.

Avoimuuden periaate edellyttää myös, että rekisteröityjen tulee olla tietoisia biometristen tietojensa käsittelystä. Tämä tarkoittaa sitä, että salaiset biometrisen tunnistamisen järjestelmät eivät ole henkilötietolain mukaisia, ja ovat näin ollen lainvastaisia.[945] Avoimuuteen kuuluu myös se, että keneltäkään ei oteta biometrista tunnistetta henkilön tietämättä. Rekisterinpitäjän tulee myös varmistaa, että rekisteröidyillä on tieto henkilötietojen käsittelyn keskeisistä asioista.

Yksilön oikeuksien näkökulmasta merkityksellinen periaate on *yksityisyyden suojan kannalta herkkien menetelmien kielto*. Kuten tämän tutkimuksen jaksossa 4.2. mainittiin, biometrisen tunnistamisen menetelmät ovat jaettavissa koviin ja pehmeisiin menetelmiin. Periaate koskee ennen kaikkea kovia biometrisen tunnistamisen menetelmiä. Kovilla biometrisen tunnistamisen menetelmillä on suurimmat vaikutukset yksilön yksityisyyden suojaan. Yksityisyyden suojan kannalta herkkien menetelmien käyttöä tulee välttää aina, kun se on mahdollista.

Biometristen tunnisteiden hyvin yksilöivän ja peruuttamattoman luonteen vuoksi biometristen tietojen tietoturvasta huolehtiminen on erittäin tärkeää. *Tietoturvaperiaatteen* mukaan biometrisen tunnistamisen avulla kerätyt tiedot tulee suojata asianmukaisella tavalla väärinkäytösten estämiseksi. Tällä tarkoitetaan tiedon käsittelyn huolellista suunnittelua, käsittelyn pitämistä mahdollisimman vähäisenä ja salaa-

945 Näin myös 29 artiklan mukainen tietosuojatyöryhmä, Opinion 3/2012 on developments in biometric technologies, s. 14 Vertaa 29 artiklan mukaisen tietosuojatyöryhmän lausunto WP193 Valmisteluasiakirja biotunnisteista, jossa työryhmä toteaa, että salaisia biometrisen tunnistamisen järjestelmiä tulee välttää.

mista tiedonsiirron sekä tallennuksen yhteydessä. Lisäksi on huolehdittava tiedon oikeellisuuden turvaamisesta.

Biometristen tietojen kohdalla tietoturva saa korostuneen merkityksen. Biometriset tunnisteet ovat peruuttamattomia eli niitä ei voida vaihtaa. Niitä on kuitenkin mahdollista kerätä ja käyttää ilman yksilön tietämystä ja suostumusta. Toisen biometriset tiedot haltuunsa saanut voi käyttää keräämiään tietoja esiintyäkseen tänä henkilönä. Tietoturva on myös yksi tapa suojata yksilön oikeutta tiedolliseen yksityisyyteen.

Biometrisen tunnistamisen luonteen ja sen mukanaan tuomien riskien vuoksi ensiarvoisen tärkeä on oikeusturvaperiaate. Rekisteröidyllä tulee olla käytössään riittävät oikeusturvatakeet biometristen tunnisteiden käsittelyssä. Rekisteröidyllä on oikeus tarkastaa omat rekisteriin talletetut tiedot, mukaan lukien biometriset tiedot. Rekisteröidyllä on tarkastusoikeutensa puitteissa oikeus tarkastaa myös biometristen tietojen pohjalta muodostetut mahdolliset profiilit.

Rekisteröidyn on myös tarvittaessa saatava sellaiset tiedot oikaistuiksi tai pyyhityiksi, joita on käsitelty lainvastaisesti. Lisäksi on tärkeää turvata niiden henkilöiden oikeudet, jotka biometrisen tunnistamisen järjestelmä hylkää. Tällaisessa tilanteessa on oleellista, että rekisteröidyllä on mahdollisuus ilmaista oma näkemyksensä asiassa.[946]

946 Näin myös 29 artiklan mukainen tietosuojatyöryhmä, Opinion 3/2012 on developments in biometric technologies, s. 14

Keskeiseen asemaan oikeusturvaperiaatteen kohdalla nousee myös toimivan viranomaiskoneiston olemassaolo. Yksilöllä tulee viimekädessä olla mahdollisuus saattaa asiansa puolueettoman viranomaisen ratkaistavaksi. Henkilötietojen käsittelyn kohdalla kysymykseen tulevat ennen kaikkea tietosuojavaltuutettu ja tietosuojalautakunta, joiden käsiteltäväksi laiton tai epäasiallinen henkilötietojen käsittely voidaan saattaa. Oleellinen osa oikeusturvaa on myös toimivan sanktiojärjestelmän olemassaolo. Oikeusvaltioperiaatteen mukaisesti kiistatilanteet on voitava saattaa tuomioistuimen ratkaistavaksi. Oikeusturvakysymykset ovat biometristen tunnisteiden erityisluonteen vuoksi hyvin tärkeitä sekä toimenpiteen kohteeksi joutuvien että koko oikeusjärjestelmän uskottavuuden kannalta.

7. Sääntelytarve

7.1. Yleistä

Modernissa yhteiskunnassa laki ja riski ovat kiinteässä yhteydessä toisiinsa. Lainsäädännöllä pyritään usein hallitsemaan riskejä. Sosiaalisina konstruktioina riskit suojaavat yhteiskunnan normeja ja heijastavat sen sosiaalista tilaa.[947]

Yhteiskunnan katsoessa jonkin tietyn teknologian edellyttävän oikeudellista sääntelyä, ei ole selvää, millä tavalla kysymystä tulee lähestyä. Tietty teknologia saattaa tarvita sääntelyä merkittävien oikeusvaikutustensa vuoksi. Toisaalta teknologia voi myös synnyttämiensä haittojen ja riskien vuoksi joutua rajoitusten kohteeksi. Se, miten rajoituksia tai ohjausta käytetään, on paljolti poliittinen kysymys.

Biometristen tunnisteiden käyttäminen yksilöiden tunnistamisessa on lisääntynyt voimakkaasti viimeisen vuosikymmenen kuluessa. Kehitys kuvaa myös sitä, että tämän teknologian hyödyntämistä tullaan edelleen lisäämään tulevaisuudessa. Kehitys tuo mukanaan myös tarpeen yksilön oikeuksien uudelleenarviointiin.

Lisääntyneestä käytöstä huolimatta biometrisen tunnistamisen mukanaan tuomiin yksityisyyden ja henkilötietojen suojaan kohdistuviin riskeihin ei ole riittävästi reagoitu. Henkilötietojen suojan sääntelyyn tulee tulevaisuudessa kohdistumaan suuria paineita yksityisyyden ja henkilötietojen suojan takaamiseksi biometrisessa tunnistamisessa.[948]

---

947 *Pohjola,* Moderni yhteiskunta, riski ja vaaralliset rikoksentekijät, s. 156–157.

948 Näin myös *Liu,* Bio-Privacy, s. 243. Katso myös *Blume,* joka toteaa eurooppalaisen henkilötietojen suojaa koskevan sääntelyn jääneen kehityksessä jälkeen. *Blume,* The Importance of Information Privacy

Tämän jakson tarkoituksena on tuoda esiin, tarvitseeko lainsäädäntöä kehittää biometrisen tunnistamisen vuoksi. Biometrista tunnistamista on henkilötietojen suojan sääntelyn näkökulmasta pidettävä alueena, joka vaatii uudenlaista oikeudellista lähestymistapaa.[949] Siinä yksilön oikeuksille ja velvollisuuksille tulee antaa suuri painoarvo. Kysymys on kuitenkin tunnistamisteknologiasta, jolla puututaan fyysisen koskemattomuuden lisäksi identiteettitietoihin. Lisäksi jaksossa otetaan kantaa siihen, minkälainen sääntelyn muoto ottaa parhaiten huomioon biometrisen tunnistamisen erityispiirteistä aiheutuvat tarpeet, ts. millä tavoin biometrisia tunnisteita tulisi säännellä.

Biometrisen tunnistamisen sääntelytarvetta on mahdollista lähestyä kahdesta näkökulmasta. Ensimmäinen näistä näkökulmista on lainsäädäntö, johon pelkistetysti ilmaistuna kuuluvat yleislait ja erityislait. Toinen näkökulma on itsesääntelyn eli käytännesääntöjen näkökulma.

Oman mielenkiintoisen näkökohdan biometrisen tunnistamisen sääntelylle tuo Euroopan Unionin tuleva henkilötietojen suojaa koskeva asetus, jota koskevassa ehdotuksessa biometriset tunnisteet on otettu huomioon. Asetus ei kuitenkaan välttämättä ratkaise kaikkia biometriseen tunnistamiseen liittyviä lainsäädännöllisiä erityistarpeita. Esimerkkinä voidaan mainita, että biometrisia tunnisteita ei asetuksessakaan ole nimenomaisesti mainittu erityistä suojaa vaativana henkilötietojen ryhmänä tai arkaluonteisina henkilötietoina. Osin syynä on todennäköisesti se, että Euroopan Unionissa on historialliselta, uskonnolliselta ja kulttuuriselta taustaltaan hyvin erilaisia maita, joiden suhtautuminen uusiin biotekniikan menetelmiin, kuten biometriseen tunnistamiseen vaihtelee suurestikin. Euroopan Unionin laajuista yksimielisyyttä biometrisen tunnistamisen sääntelystä voi näin ollen olla

---

and its Future, s. 168.

949 Näin myös *Liu,* Bio-Privacy, s. 243

vaikea saavuttaa. Tämän vuoksi biometrisen tunnistamisen sääntelyssä jää ainakin toistaiseksi varsin paljon päätäntävaltaa kansalliselle lainsäätäjälle.

7.2. Lainsäädännön näkökulma

Lainsäädännön tarkoituksena on yhteiskunnassa syntyvien ristiriitojen estäminen ja sovittelu. Yhteiskunnan kehitys ja erityisesti muutosprosessien nopeus vievät pohjaa hitaasti reformoituvalta lainsäädännöltä. Teknologisen kehityksen ja lainsäädännön kehityksen välillä näyttääkin olevan pysyvä jännite: teknologia uudistuu nopeammin kuin yhteiskuntakehitystä ohjaamaan tarkoitetut lait.[950] Viimeaikainen nopea teknologinen kehitys on synnyttänyt sellaisia uusia moraalisia ja oikeudellisia ongelmia, joiden ratkaisemiseen perinteiset eettiset ja oikeudelliset normistot taikka ohjaus- ja valvontajärjestelmät eivät tarjoa riittävästi keinoja. Erityisesti teknologisen kehityksen aiheuttama yhteiskunnallinen muutos on antanut aiheen puhua oikeuden jälkeenjääneisyydestä. Oikeuden ei nähdä kehittyvän yhteiskunnan kanssa samassa tahdissa.

Huolimatta siitä, että henkilötietolaki on säädetty yli 15 vuotta sitten, on laki edelleen pääperiaatteiltaan sovellettavissa biometristen tunnisteiden mukanaan tuomiin oikeudellisiin ongelmiin. Biometriset tunnisteet ovat kuitenkin erityinen henkilötietojen ryhmä, joka eroaa niin sanotuista tavallisista henkilötiedoista. Tämä vaatii eräiden eri-

950 Tietotekniikan kehitystä sääntelevät kolmenlaiset tekijät: 1) hallinnolliset kontrollit (esim. lait ja asetukset), 2) taloudelliset kontrollit (esim. verot) ja 3) informatiiviset kontrollit (esim. koulutus). Freese – Persson, Etik och ny teknik, s. 11 sekä *Kuopus,* Hallinnon lainalaisuus ja automatisoitu verohallinto, s. 16.

tyispiirteiden huomioon ottamisen myös biometristen järjestelmien ja alan lainsäädännön suunnittelussa.

Biometriset tunnisteet ovat peruuttamattomia ja yksilöiviä. Ne asettavat erityisiä vaatimuksia tietosuojalle sekä tietoturvalle, jotta yksityisyyden suojan toteutuminen voidaan varmistaa. Biometristen tunnisteiden tietosuojaan liittyy lisäksi joitakin erityisiä piirteitä, jotka on huomioitava.

Piirteistä esimerkkeinä ovat seuraavat:

- Monia biometrisia tunnisteita on vaikeaa pitää salassa. Esimerkiksi lähes kenestä tahansa on mahdollista hankkia kasvokuva ja sormenjäljet.
- Biometrisia tunnisteita ei voi vaihtaa, kuten vääriin käsiin joutuneita salasanoja tai puhelinnumeroa.
- Biometrian avulla on mahdollista valvoa ihmisen liikkumista hänen tietämättään.

Onko biometrinen tunniste oikeudellisesti erityistä? Lainsäädännössä ja oikeuskäytännössä tarkennetaan yleensä muualla syntyneitä määritelmiä oikeudellisiin tarkoituksiin, annetaan ohjeita siitä, mikä on luvallista ja mitä menettelyitä yhteiskunnassa tulee noudattaa. Lakiin otettuja määritelmiä ja niiden suhteita on toisinaan pakko tulkita soveltamisympäristön muuttuessa. Tätä tulkintaa ei kuitenkaan voi korvata eettisillä periaatteilla. Toisaalta niin kauan kuin tulkinnat täyttävät tehtävänsä antaen toimijoille oikeussuojaa ja ollen ennustettavissa, ei ole välttämätöntä tarvetta uudelle sääntelylle. Biometristen tunnisteiden kohdalla tämä ajatus ei enää täysin toteudu. Tulkintaongelmia on aiheutunut ennen kaikkea siitä, mikä on biometristen tunnisteiden asema henkilötietojen joukossa. Perustuslakivaliokunta on esimerkiksi passilain osalta todennut (PeVL 14/2009 vp) sormenjäljen olevan biometrisena tunnisteena pysyvä, muuttumaton ja peruuttamaton osa yksilöä. Sormenjäljet myös sisältävät yksilöstä sellaista informaatiota,

joka mahdollistaa hänen tarkan tunnistamisensa hyvin erilaisissa yhteyksissä. Tällöin ne ovat monin tavoin rinnastettavissa henkilötietolaissa määriteltyihin arkaluonteisiin tietoihin.

Tällä hetkellä biometrisia tunnisteita ei kuitenkaan pidetä kaikissa tilanteissa arkaluonteisina henkilötietoina. On vaikea ajatella esimerkiksi ihmisen puhetyylin olevan arkaluonteinen henkilötieto. Tietyissä tilanteissa, kuten kasvontunnistuksessa, biometriset tunnisteet ovat kuitenkin luokiteltavissa arkaluonteisiksi henkilötiedoiksi näiden paljastaessa esimerkiksi rodulliset erityispiirteet.[951]

Henkilötietodirektiivissä säädetty yksilöllisen tunnisteen käsite tukee kuitenkin näkemystä, että biometrinen tunniste on luonteeltaan arkaluonteinen henkilötieto. Ne ovat ainutlaatuisia ja useimmilla niistä voidaan luoda yksilöllinen kuva henkilöstä. Laajasti käytettynä – erityisesti, jos tiedot kattavat merkittävän osan väestöstä – biometrisia tunnisteita on mahdollista pitää henkilötietodirektiivin 8 artiklan 7 kohdassa tarkoitettuina yksilöllisinä tunnisteina, jotka tarvitsevat erityistä lainsäädännöllistä suojaa.[952] Biometristen tunnisteiden käytölle tulee tällöin määritellä olosuhteet, joiden vallitessa tietoja on lupa käsitellä. Esimerkiksi Norjan tietosuojaviranomaisen ratkaisukäytännössä biometriset tunnisteet on rinnastettu yksilöllisiin tunnisteisiin, joista

951 Esimerkiksi pelkkä yksilön sormenjälki itsessään ei paljasta yksilöstä mitään noloja yksityiskohtia, joiden julkistaminen aiheuttaisi haittaa yksilölle. Tällaisesta voidaan mainita esimerkkinä Saksassa sattunut tapaus, jossa saksalainen hakkeriryhmä Chaos Computer Club julkaisi vuonna 2008 silloisen Saksan valtionvarainministerin sormenjäljen internetissä. Hakkeriryhmä halusi teollaan osoittaa, miksi sormenjälkien käyttäminen passeissa ei ole hyvä ajatus.

952 Näin myös 29 artiklan mukainen tietosuojatyöryhmä, Opinion 3/2012 on developments in biometric technologies, s. 9.

Norjan henkilötietolaissa on oma säännös (personopplysningsloven § 12).[953]

Rekisteritietojen helppo yhdistäminen on yksi keskeinen henkilötietoihin kohdistuvista uhkista. Hyödyntää voi jotain samaa yksikäsitteistä hakuavaimeksi kelpaavaa tietoa, kuten biometristä tunnistetta. Tällä tavoin on mahdollista pystyä päättelemään henkilöstä asioita, joita minkään yksittäisen rekisterin avulla ei ole mahdollista tietää. Vaarana on myös, että yhdistettyjen tietojen avulla tehdään vääriä päätelmiä henkilöstä. Tämän vuoksi tietojen yhdistelemistä on haluttu rajoittaa lainsäädännöllä. Kuten jaksossa 4.3.2. on kuvattu, tällainen uhka on erityisen merkityksellinen biometristen tietojen kohdalla.

Biometrisen tunnistamisen sääntelytarve on ilmeinen.[954] Henkilötietolainsäädäntö ei tällä hetkellä riittävästi ota huomioon biometristen tunnisteiden luonteesta aiheutuvaa lainsäädännöllistä erityisasemaa. Kysymys ei ole vain lievästä lainsäädännöllisestä tarpeesta. Perusteltua on sanoa, että biometristen tietojen käsittelyssä tietosuojalainsäädäntö ei riittävällä tavalla turvaa yksilön oikeutta yksityisyyteen ja henkilötietojen suojaan.

Lainsäädäntö ei ohjaa palvelujen kehittäjiä riittävästi turvaamaan tunnistettavien yksityisyyden suojaa. Palvelujen kehittäjien ja käyttäjien on käytännössä vaikeaa arvioida voimassa olevasta sääntelystä, millä edellytyksin ja mihin tarkoitukseen biometrista tunnistamista voi

953 Katso esimerkiksi PVN-2011-12, PVN-2006-09 ja PVN-2006-08. Katso myös *Schartum – Bygrave,* Personvern i informasjonssamfunnet, s. 131–132.

954 Myös eduskunnan hallintovaliokunta on passilakia koskeneessa mietinnössään vuonna 2006 todennut saman asian ja edellyttänyt, että hallitus käynnistää biometrisiä tunnisteita ja niiden käyttöä koskevan yleisen henkilötietojen suojaa koskevan lainsäädännön valmistelutyön. HaVM 13/2006, s. 4.

käyttää sekä miten palvelut tulee toteuttaa tunnistettavien yksityisyyden suoja huomioon ottavalla tavalla.

Lainsäädännöllinen epäselvyys on uhka yksilön oikeuksille. Tavoitteena tulee kuitenkin olla sellainen lainsäädännöllinen tila, joka turvaa yksilön ja tämän oikeudet henkilötietojen käsittelyssä. Eri asia on, päästäänkö tavoitteeseen substanssilakeja muuttamalla vai tarvitaanko asiasta erityislainsäädäntöä, jossa biometristen tunnisteiden luonteesta aiheutuvat erityispiirteet otetaan huomioon yksilön oikeudet turvaavalla tavalla.

Tietosuojavaltuutettu on esimerkiksi ottanut kantaa biometristen tunnisteiden sääntelytarpeeseen jo vuoden 2002 tietosuojavaltuutetun katsauksessa. Katsauksessa tietosuojavaltuutettu totesi, että *"…biometristen tunnisteiden käytön yleistymisen myötä biometriset tunnistamisjärjestelmät kaipaavat nimenomaan tietosuojalainsäädännön uudelleen arviointia. Riittävänä ei ole pidettävä vain substanssilakien muuttamista."*

Lainsäädännöllinen tarve on perusteltavissa myös sillä, että Euroopan Neuvoston tietosuojasopimuksen 6 artiklaa päivitettiin vuonna 2012 lisäämällä arkaluonteisten tietojen joukkoon biometriset tiedot. Sopimuksen 4 artikla velvoittaa sopimukseen liittynyttä valtiota takaamaan sopimuksen oikeudet kansallisessa lainsäädännössään. Arkaluonteisten tietojen kohdalla kansallinen lainsäädäntömme ei tätä velvoitetta täytä.

Oikeudellisten näkökohtien huomioiminen biometrisen tunnistamisen ongelmia pohdittaessa voi tapahtua monin tavoin. Harkittavat oikeudellisen sääntelyn muodot ja valvontakeinot sekä niiden mahdollisen käyttöönoton vaikutukset tulee tarkoin eritellä.

Oikeuspoliittisella argumentoinnilla on paljon yhtymäkohtia moraalikeskusteluun. Sillä on kuitenkin omat erityispiirteensä. Lain säätäminen on institutionaalista ja kollektiivista toimintaa. Rationaaliseen päätöksentekoon tähtäävän lainsäätäjän tulee tiedostaa laille tai muulle oikeudelliselle sääntelylle asetettavat tavoitteet ja arvot. Sääntelyn

soveltuvuutta on myös punnittava noiden tavoitteiden ja arvojen toteuttamiseen. Kun moraalikeskustelun perusteella päädytään tiettyyn kannanottoon jostakin asiaintilasta tai ongelmasta, ei ole selvää, että asiassa tarvitaan lainsäädäntöä tai muutakaan sääntelyä.[955]

7.3. Käytännesäännöt

Maamme sääntelykulttuurissa on merkittävä asema legalitisella sääntelyllä, yhdistettynä perustuslain tiukkaan lakisääteisyyden vaatimukseen, kun säädetään perusoikeuksista ja niiden horisontaalivaikutusten laajentamisesta. Selkeillä, yksityiskohtaisilla ja täsmällisillä eduskuntalakien käytöllä on merkittävä asema. Tämä kehitys on osaltaan haitannut vaihtoehtoisten sääntelykeinojen, kuten käytännesääntöjen käyttöönottoa.

Käytännesäännöt ovat ikään kuin kertomuksia lain sisällöstä. Niiden avulla välitetään lakitekstiä yksityiskohtaisemmalla tavalla ohjeita ja tietoa hyvästä, yksilön oikeudet huomioon ottavasta henkilötietojen käsittelystä. Ne ovat tärkeä väline lain tuntemisessa sekä hyvän tietojenkäsittelytavan ymmärtämisessä ja kehittämisessä. Ne ovat ratkaisumalli oikeudesta viestinnän ongelmaan.[956]

Henkilötietolain 42 §:n mukaan rekisterinpitäjät tai näitä edustavat yhteisöt voivat laatia toimialakohtaisia käytännesääntöjä tämän lain soveltamiseksi ja hyvän tietojenkäsittelytavan edistämiseksi. Käytännesääntöjen laatimiseen otetaan kantaa myös henkilötietodirektiivissä. Sen (95/46/EY) 27 artiklan 1 kohdan mukaan jäsenvaltioiden on edistettävä sellaisten käytännesääntöjen laatimista, joiden tarkoi-

955 *Lahti,* Johdanto, s. 8–9.

956 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 353. Käytännesäännöt tulee kuitenkin erottaa tavanomaisista hyvän tavan ohjeistoista.

tuksena on jäsenvaltioiden direktiivin mukaisesti säätämien kansallisten säännösten moitteeton soveltaminen ottaen huomioon eri alojen erityiset piirteet.

Henkilötietolaissa ja –direktiivissä korostetaan rekisterinpitäjien itseohjauksen tarpeellisuutta. Tässä tarkoituksessa käytännesääntöjen laatimisella on keskeinen merkitys. Itseohjauksen kautta on lakia paremmin mahdollista huomioida kuhunkin erityisalaan liittyvät erityispiirteet ja –tarpeet.

Tarkoituksena on kannustaa laatimaan alakohtaiset ohjeet, jotka mahdollistavat kansallisen lainsäädännön moitteettoman soveltamisen ja joissa otetaan huomioon biometristen tunnisteiden käsittelyn erityispiirteet. Eräänä välineenä voidaan mainita biometrisen tunnistamisen eurooppalaisten tai kansainvälisten standardien laatiminen sellaisten biometrisen tunnistamisen järjestelmien edistämiseksi, jotka on suunniteltu tietosuojaa parantaviksi, minimoivat sosiaaliset riskit ja ehkäisevät biometristen tunnisteiden väärinkäytön.

Lainsäädäntöön nähden käytännesäännöillä on omat etunsa. Lainsäädäntö on ensinnäkin sidottu tiukan muodolliseen prosessiin. Tällainen menettely on yleensä käytännesääntöjen luomista hitaampaa. Se voi johtaa lainsäädännön myöhästymiseen sääntelyä vaativalla alalla. Voidaan yleisellä tasolla puhua lainsäädännön tulevan yleensä askeleen yhteiskunnallista kehitystä perässä. Syitä tähän on monia, mutta lainsäädäntöprosessin hitaus edesauttaa asiaa.

Lainsäädännöllinen menettely ei myöskään aina ota huomioon tietyn alan erityispiirteitä. Kaikkiin biometrisen tunnistamisen menetelmiin liittyy omat ongelmat ja mahdollisuudet, joiden huomioiminen lainsäädännössä on haastavaa.

Hyvät käytännesäännöt luovat tosiasiallisen olettaman menettelyn oikeellisuudesta niitä noudatettaessa. Käytännesääntöjen kautta laki saadaan tuotua käyttäjien omin sanoin kuvattuna lähemmäksi käytän-

töä, jolloin laki on helpompi ymmärtää ja hyväksyä.[957] Itsesääntelyn muotona käytännesäännöt ovat tärkeitä myös biometrisessa tunnistamisessa. Käytännesäännöillä alan toimijat saadaan paremmin mukaan sääntelyyn, mikä mahdollistaa myös biometrisen tunnistamisen eri sovelluksiin liittyvien erityistarpeiden huomioimisen.

Käytännesääntöihin liittyy kuitenkin ongelmia, jotka vaikuttavat niiden käyttökelpoisuuteen. Niihin ei liity laintasoista velvoittavuutta, eikä niiden noudattamatta jättämisestä aiheudu sanktioita. Keskeinen ongelma käytännesääntöihin liittyen onkin niiden noudattamisen valvonta. Ongelmana on myös se, että alan toimijat ovat yleensä kaupallisia toimijoita, joita kiinnostaa voiton tekeminen perus- ja ihmisoikeuksia enemmän. On vaikeaa saada alan kaupalliset toimijat noudattamaan yksityisyyttä turvaavia käytännesääntöjä, jotka rajoittavat kaupallisia mahdollisuuksia.[958] Tähän liittyen Clarke onkin todennut seuraavaa: "*wolves self-regulate for the good of themselves and the pack, not the deer.*"[959] Lisäksi käytännesääntöihin liittyy ongelmia niiden tehokkaan soveltamisen näkökulmasta. Jotta käytännesäännöt yltäisivät tehokkuudeltaan lain tasolle, tulee niiden olla sovellettavissa kaikkiin alan toimijoihin. Ongelmana käytännesäännöissä on myös se, että niihin voi sisältyä virheellisiä käsityksiä. Esimerkkinä ovat sukututkimuksen käytännesäännöt, joissa annetaan ymmärtää henkilötietolain soveltuvan vain eläviin henkilöihin.

Käytännesääntöjen noudattamiseen ja soveltuvuuteen liittyvien ongelmien vuoksi biometristen tunnisteiden säänteleminen pelkästään

---

957 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2015), s. 354.

958 Artiklan 29 mukainen tietosuojatyöryhmä korostaa sellaisten käytännesääntöjen tärkeyttä, joiden tarkoituksena on edistää tietosuojaan liittyvien periaatteiden asianmukaista noudattamista ottaen huomioon eri alojen erityispiirteet.

959 *Clarke,* Dataveillance. Saatavilla osoitteesta: http://www.rogerclarke.com/VD/PPSwamp.ppt

alaa koskevilla käytännesäännöillä ei riittävästi ota huomioon tämän teknologian käyttämiseen liittyviä perus- ja ihmisoikeuskysymyksiä. Jos alan eurooppalaisia tai kansainvälisiä käytännesääntöjä on tarpeen laatia, ne tulee valmistella yhteistyössä tietosuojaviranomaisten kanssa sellaisten biometristen järjestelmien edistämiseksi, jotka on suunniteltu tietosuojaa parantaviksi, minimoivat sosiaaliset riskit ja ehkäisevät biometristen tietojen väärinkäytön.

7.4. Tarvitaanko biometriaa koskeva erityislaki?

Biometrian säädöstarve on ilmeinen.[960] Tunnistamisvälineiden käyttöön liittyy yksityisyyden suojan, henkilöiden oikeusturvan sekä myös muiden perusoikeuksia turvaavien oikeuksien kannalta sellaisia ominaisuuksia, että jo perustuslaki edellyttää niiden käytön ja käsittelyn edellytykset säädettäväksi lailla.

Millainen lainsäädäntöratkaisu on omiaan turvaamaan yksilön oikeudet biometrisessa tunnistamisessa? Pelkistetysti vaihtoehtoja on kaksi: 1) sopeuttaa jo olemassa oleva lainsäädäntö muuttuneisiin olosuhteisiin tai 2) kehittää uusia, spesifejä normeja ilmeneviin oikeudellisiin ongelmiin.

Biometrisen tunnistamisen sääntelyvaihtoehdot noudattavat tavanomaisia sääntelyteknisiä valintoja. Ensisijaisesti lainsäätäjän säädöstyypin ja sääntelystrategian valinnassa ovat käytettävissä lähinnä seuraavat vaihtoehdot: toissijainen, lailla syrjäytettävä yleislaki, eri puolille lainsäädäntöä sijoitettavat yksittäiset biometrista tunnistamista koskevat säännökset, erityislainsäädäntöön luettavat biometrisen tunnistamisen säädökset ja erityislainsäädäntöön sijoitettavat yksittäiset biometrista tunnistamista koskevat säännökset.

960 Katso esimerkiksi *Sisäasiainministeriö,* Henkilöllisyyden luomista koskevan hankkeen loppuraportti, s. 4.

Biometristen tunnisteiden erityispiirteiden vuoksi on tarkoituksenmukaista säätää erikseen kansalaisten yksityiselämän ja henkilötietojen suojan turvaamisesta biometrisia tunnisteita käytettäessä. Tätä puoltaa myös se, että biometrisella tunnistamisella puututaan tunnistettavan henkilöön, jolloin sen käyttö edellyttää suostumusta tai käytön oikeuttavaa sääntelyä.

Henkilötietojen suojan kohdalla huolena on kuitenkin kansalaisten velvollisuus tuntea laki. Liiallisen sääntelyn riskinä on, ettei kansalainen tunne lain sisältöä, eikä lain tavoitteita näin tulla saavuttamaan.[961] Aidossa demokratiassa oikeuden tulee olla yksinkertainen, mahdollisimman monen ymmärrettävissä ja hyvin hallittavissa oleva asia.[962] Henkilötietojen suojan kohdalla näin ei enää välttämättä ole, sillä henkilötietojen suojan oikeudellinen viitekehys on vaikeasti hallittavissa ja ymmärrettävissä. Kysymys ei ole vain kansalaisten ymmärryksestä, vaan myös lakimiehillä on enenevässä määrin vaikeuksia henkilötietojen suojaa koskevan lainsäädännön hallitsemisessa. Sääntelyn sirpaloitumisen vuoksi jo soveltuvan lainsäädännön tunnistaminen ja omaan toimintaan kohdistuvien oikeudellisten velvoitteiden löytäminen vaatii ammattitaitoa. Perusoikeudet vaarantuvat sirpaloituneen ja tulkinnaltaan hajanaisen lainsäädännön vuoksi.[963]

Suomen lainsäädännössä on käytetty useissa yhteyksissä oikeusinstituutiokohtaista sääntelytapaa. Tällöin tietty instituutio tai sen merkittävä osa pyritään sääntelemään yleislain avulla. Henkilötietojen suoja on esimerkki tällaisesta sääntelystä. Biometrisen tunnistamisen kohdalla sääntelyperinne puoltaa biometrisen tunnistamisen sääntele-

961 *Råman,* Yleislaki, yleiset opit ja vaikutusten arviointi, s. 335.
962 *Saarenpää,* Henkilö- ja persoonallisuusoikeus (2011), s. 232.
963 *Råman,* Yleislaki, yleiset opit ja vaikutusten arviointi, s. 335.

mistä henkilötietojen käsittelyn yleislain eli henkilötietolain tasolla.[964] Henkilötietojen käsittelystä tarvitaan erityissäännöksiä, vain seuraavista syistä:

• on tarkoitus poiketa henkilötietolaissa säädetystä

• rekisterinpidon laillisuus jäisi henkilötietolain mukaan arvioituna tulkinnanvaraiseksi ja kysymys on valtakunnallisesta tietojärjestelmästä, johon kerätään ja talletetaan arkaluonteisia henkilötietoja

• on tarkoitus sallia salassa pidettävien henkilötietojen luovuttaminen,

• henkilörekisteriin talletettuja tietoja on tarkoitus luovuttaa teknisen käyttöyhteyden avulla tai pitää saatavilla yleisessä tietoverkossa taikka

• henkilörekistereitä on tarkoitus yhdistää (erityisesti valvontatarkoituksessa).[965]

Ilmeisestä sääntelytarpeesta huolimatta biometrisia tunnisteita koskevalle erityislaille ei välttämättä ole tarvetta. Vaarana on, että erityislaki hukkuu henkilötietojen suojan normitulvaan[966] niin, ettei lainsäädäntö saavuta tavoitteitaan perusoikeuksien turvaamisessa. Biometristen tunnisteiden sääntäleminen olemassa olevan yksityisyyden

964 Lainkirjoittajan oppaassa painotetaan yleislaista poikkeamatta jättämisen tärkeyttä. *Oikeusministeriö,* Lainkirjoittajan opas (2013), s. 234.

965 *Oikeusministeriö,* Lainkirjoittajan opas (2013), s. 234.

966 Normitulva on termi, jota käytetään kuvaamaan yhteiskunnan eri toimintojen ja instituutioiden jatkuvasti lisääntyvää sääntelyä. Oikeudellistumisen myötä säädösten määrä kasvaa ja niitä muutetaan yhä lyhyemmin aikavälein. Taustalla vaikuttavat osaltaan Euroopan unionin tuottamat direktiivit sekä teknologian nopean kehityksen tuomat vaatimukset lainsäätäjälle. *Korhonen,* Sähköisen asioinnin ja viestinnän normitulvaa, s. 1

ja henkilötietojen suojaa koskevan sääntelyn pohjalta turvaa biometristen tunnisteiden sääntelyn kattavuuden.[967]

Oikeusjärjestyksen sisäisen rationaalisuuden kannalta lain säätäminen on usein pikemminkin epäjärjestystä kuin järjestystä tuottava tekijä: oikeuden koherenssia ylläpitävät muut oikeudelliset käytännöt.[968] Yleislait ovat tästä harvinainen poikkeus, sillä niiden avulla oikeudellisen sääntelyn selkeyttä, ymmärrettävyyttä ja käyttökelpoisuutta on mahdollista parantaa lainsäätäjän toimesta.[969]

Mahdollisessa sääntelyssä tulisi tämän vuoksi lähteä liikkeelle jo olemassa olevan henkilötietojen käsittelyä koskevan lainsäädännön kehittämisestä. Uuden välinekohtaisen lainsäädännön syntymistä tulee välttää, jotta lainsäädäntö säilyy välineneutraalina. Biometrisista tunnisteista tulee säätää yleislain tasolla eli henkilötietolaissa. Tämä on tällä hetkellä tilanne myös Yhdysvalloissa, jossa ei ole annettu biometrista tunnistamista koskevaa liittovaltiotason erityislakia. Osavaltiotasolla biometristen tunnisteiden käsittelystä on kuitenkin annettu erityislainsäädäntöä esimerkiksi Texasissa ja Illinois'ssa. Texasin biometristen tunnisteiden sääntely eroaa kuitenkin siinä, että käyttöä säännellään osana suurempaa henkilötietojen käsittelyä koskevaa sääntelyä.

Mikäli henkilötietolaki yleislakina pystyy ratkomaan intressiristiriidat Suomen oikeusjärjestyksen kannalta optimaalisesti, ei tarvetta erityislaille ole. Biometristen tunnisteiden huomioiminen henkilötietojen suojan yleislaissa tuo erityislakia paremmin selkeyttä ja yhteneväisyyttä alan sääntelyyn.[970] Samalla se osoittaa biometristen tun-

967 *Liu,* Bio-Privacy, s. 249–250.

968 *Tuori,* Kriittinen oikeuspositivismi, s. 154.

969 *Råman,* Yleislaki, yleiset opit ja vaikutusten arviointi, s. 339

970 Tämä on todettu myös valtioneuvoston sähköistä tunnistamista koskevassa periaatepäätöksessä. Valtioneuvoston periaatepäätös sähköisestä tunnistamisesta, s. 9.

nisteiden yhteiskunnallisen merkityksen ja vakiinnuttaa biometrisen tunnistamisen järjestämisen perusteet sekä luo yhteisen sääntely- ja tulkintapohjan, josta poikkeaminen erityislaeissa vaatisi perusteluja. Yleislaissa säätämisen puolesta puhuu myös se, että henkilötietolain osalta lainkirjoittajan oppaassa perustellaan erikseen, miksi ei ole tarpeen eikä asianmukaista ottaa erityislakeihin säännöksiä seikoista, joista säädetään henkilötietolaissa. Oppaan mukaan *"erityisen haitallisina voidaan pitää säännöksiä, joissa toistetaan henkilötietolain velvoitteita näitä konkreettisemmassa muodossa. Tällaisen säännöksen ottamisella erityislakiin luodaan helposti se virheellinen käsitys, että kyseinen oikeussääntö ei ole aikaisemmin sisältynyt voimassa olevaan oikeuteen."*[971]

Yleislaissa säätämisen puolesta puhuu myös se, että nimenomaisen lainsäädännön puutteesta huolimatta kysymyksessä ei tavallisesti ole välttämättä aito oikeudellinen tyhjiö. Oikeusjärjestys on kokonaisuus, johon sisältyy lukuisien eri oikeudenalojen normistoja ja nuo normistot sääntelevät myös eri henkilöryhmien asemaa ja henkilöiden vastuuta normien rikkomisesta. Sellaiset enemmän tai vähemmän yleisluonteiset oikeussäännöt ja –periaatteet voivat tulla sovellettaviksi, vaikkei joltakin erityisalalta ole nimenomaista sääntelyä olemassa.

Asettamalla biometristen tunnisteiden käytölle tavallisia henkilötietoja tiukemmat käsittelyn edellytykset henkilötietojen käsittelyn yleislaissa eli henkilötietolaissa erottuu biometrinen tunniste tavallisista henkilötiedoista saamatta varsinaisesti arkaluonteisen henkilötiedon asemaa. Niiden käsittelylle on tällöin kuitenkin tavallisia henkilötietoja tiukemmat edellytykset, kuten on esimerkiksi henkilötunnuksella. Näin on toimittu esimerkiksi Texasin osavaltiossa Yhdysvalloissa ja Pohjoismaista Norjassa. Kummassakin maassa biometristen tunnisteiden käsittelyä koskevat säännökset sisältyvät yleislakiin.

971 *Oikeusministeriö,* Lainkirjoittajan opas 2013, s. 234

Biometristen tunnisteiden huomioiminen yleislain tasolla ei välttämättä kuitenkaan vielä takaa sääntelyn onnistumista. Henkilötietolain abstrakti luonne saattaa aiheuttaa epävarmuutta ja epätietoisuutta säännösten soveltamisessa. Yksi keino ratkaista tällaista epävarmuutta on yleisen ohjeistuksen laatiminen biometrisen tunnistamisen käyttämiselle. Biometrisen tunnistamisen sääntelyssä myös käytännesäännöt voivat olla tehokas väline ylisääntelyn välttämiseksi henkilötietojen suojan alalla. Käytännesääntöihin liittyy kuitenkin ongelmia ja riskejä, jotka vaarantavat yksilön perus- ja ihmisoikeuksien toteutumisen biometristen tunnisteiden käytössä. Käytännesäännöt voivat kuitenkin olla merkityksellisiä sääntelyssä. Kun biometriset tunnisteet huomioidaan yleislaissa ja käytännesääntöjen kautta, tulevat ne kattavammin säännellyiksi. Käytännesääntöjen kautta biometrista tunnistamista koskeva sääntely saadaan tuotua käyttäjien omin sanoin kuvattuna lähemmäksi käytäntöä, mikä helpottaa lain ymmärtämistä.

Sääntelytapa on perusteltavissa sillä, että biometriset tunnisteet eivät sinänsä luo täysin uusia oikeudellisia ongelmia henkilötietojen suojan alalla. Täysin uudelle lainsäädännölle ei tämän vuoksi välttämättä ole tarvetta.

Biometristen tunnisteiden erityispiirteet tulee kuitenkin ottaa huomioon nykyistä paremmin voimassa olevassa sääntelyssä. Tämä voidaan erityislakia paremmin saavuttaa ottamalla biometrisia tunnisteita koskevat säännökset henkilötietojen käsittelyn yleislakiin ja laatimalla lainsäädäntöä täydentävät biometrisia tunnisteita koskevat käytännesäännöt. Niiden tulee kuitenkin perustua henkilötietolakiin ja ne tulee luoda yhteistyössä eri sidosryhmien kanssa, jotta ne saisivat mahdollisimman tehokkaan toimivuuden.[972] Käytännesääntöjen kohdalla

972 On myös mahdollista, että käytännesäännöt tulisivat EU-tasolta, jolloin ne kattaisivat koko unionin alueen. Näin myös *Liu,* Bio-Privacy, s. 249–250.

vaihtoehtona on myös sitoutua biometrisen tunnistamisen kansainvälisen järjestön Biometric Instituten laatimiin biometrista tunnistamista koskeviin ohjeisiin. Ohjeet on laadittu ottaen huomioon kansainväliset ja monet kansalliset periaatteet henkilötietojen suojasta. Pääperiaatteiltaan ohjeet ovat henkilötietolain kanssa yhdenmukaiset.[973]

Suomen tämän hetkistä yhteiskuntaa on oikeudellisesta näkökulmasta kutsuttu keinotekoiseksi, ylisääntelyn yhteiskunnaksi: yhteiskunnallisiin ongelmiin on pyritty ensisijassa löytämään lainsäädännöllinen ratkaisu.[974] Pöysti kuvaa suomalaista yhteiskuntaa vahvasti lainsäädäntöyhteiskunnaksi, jossa lainsäätäjä on oikeusjärjestyksen ja sen kehittämisen keskiössä. Hänen mukaansa lainsäädäntöriski on tällöin merkittävin sääntelyriski.

Lainsäädäntöriskillä tarkoitetaan *Pöystin* mukaan riskiä siitä, että laki epäonnistuu tavoitteissaan ja tehtävissään oikeuden toteuttamisessa ja täsmentämisessä tai siitä, että laki aiheuttaa kohtuuttoman paljon oikeuden, oikeudenmukaisuuden tai yhteiskunnan ja sen jäsenten kannalta kielteisiksi arvioitavia sivuvaikutuksia. Hänen mukaansa yksityisyyden suoja ja henkilötietojen suoja ovat alueita, joiden yhteydessä tulee usein esille lainsäädäntöriski. Syynä tähän on henkilötietojen suojan luonne oikeusjärjestyksen horisontaalisesti leikkaavana perusoikeutena. Henkilötietojen suojaa koskevaa lainsäädäntöä yleisemminkin koettelee suomalaisen oikeusjärjestyksen ongelmana oleva sääntelykierre. Siitä huolimatta, että henkilötietolaki on tietosuojan

973 Katso alaviite 867 sivulla 297.

974 Saarenpää on tähän liittyen todennut: "When society changes, legislation is often the first element of law to react – sometimes even a bit too readily." *Saarenpää,* The Importance of Information Security in Safeguarding Human and Fundamental Rights, s. 45.

yleislaki, on henkilötietojen suojaa koskeva lainsäädäntö kokonaisuutena pirstaleinen. [975]

Lainsäädäntöriskiin liittyy läheisesti kysymys sääntelyriskistä. Tällä tarkoitetaan uhkaa siitä, että sääntely epäonnistuu tai aiheuttaa tarkoittamattomia kustannuksia ja muita epäedullisia vaikutuksia tai sääntelystä aiheutuvia epäoikeudenmukaisia seurauksia. Sääntelyriskien välittöminä syinä saattavat olla sääntelyn epätarkoituksenmukainen sisältö, systematiikka ja tekninen muoto tai myös lainsäätäjän tai muun sääntelijän harkitsematon tai muuten oikeudenmukaisuuden vajeisiin johtava passiivisuus nopeasti kehittyvässä ja muuttuvassa yhteiskunnassa.[976]

Biometrisen tunnistamisen käytön yleistymisen vuoksi on ensiarvoisen tärkeää, että lainsäädäntö pysyy mukana kehityksessä. Biometriseen tunnistamiseen liittyvien riskien vuoksi on perusteltua väittää, että voimassaolevaan henkilötietolainsäädäntöön tulee ottaa biometrisia tunnisteita koskevat yleiset säännökset. Näiden säännösten tehokkaaksi toteuttamiseksi on syytä miettiä käytännesääntöjen luomista lainsäädännön rinnalle. Jotta lainsäädäntö- ja sääntelyriski eivät biometrisen tunnistamisen kohdalla toteudu, täytyy sääntelytapaan kiinnittää erityistä huomiota. Tällaisella biometristen tunnisteiden vähimmäissääntelyllä[977] on mahdollista ottaa huomioon niiden erityis-

975 *Pöysti,* Oikeudellisen tiedon niukkuus ja henkilötietojen suoja, s. 304–306.

976 *Saarenpää,* A. – *Pöysti, T.* – *Sarja, M.* – *Still, V.* – *Balboa, R.*: Tietoturvallisuus ja laki, näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä, s. 45–47 sekä *Pöysti,* Oikeudellisen tiedon niukkuus ja henkilötietojen suoja, s. 303.

977 Vähimmäissääntelyllä tarkoitetaan tässä sitä lainsäädännöllistä vähimmäistasoa tai suojaa, jota biometriset tunnisteet tarvitsevat.

piirteistä aiheutuvat lainsäädännölliset tarpeet ja turvata yksityisyyden suojaa henkilötietojen käsittelyssä.[978]

Oikeudellisella sääntelyllä on monia rajoituksia. Lainsäätäjän tulisikin moniarvoisessa yhteiskunnassa pitäytyä sellaisten, mahdollisimman väljien reunaehtojen asettamisessa, joiden puitteissa yksilöt ja ryhmät voivat harjoittaa moraalista autonomiaansa.[979]

Tässä tutkimuksessa on omaksuttu se ajatus, että biometristen tunnisteiden käsittelyyn ja käyttötarkoituksiin löytyy keskeinen pohja nykyisestä henkilötietojen sääntelystä. Biometristen tunnisteiden erityisyys kuitenkin laajentaa perinteisiä henkilötietojen käsittelyn sääntöjä ja tulkintaperiaatteita. Tulkinnalla ei kuitenkaan voida ohittaa lain sanamuotoa tai tarkoitusta. Esimerkkinä tästä voidaan mainita biometristen tunnisteiden erikoinen asema tavallisten henkilötietojen ja arkaluontoisten tietojen välissä.[980]

Yksi huolenaihe biometrista tunnistamista koskevassa sääntelyssä on se, mikä on tulevan tietosuoja-asetuksen lopullinen sisältö ja sen mahdollinen vaikutus biometrisen tunnistamisen sääntelyyn. EU:n tietosuojalainsäädännön uudistus voi nimittäin tältä osin muuttaa tilannetta, koska uudistuksen yhteydessä on ollut esillä myös kysymys biometrisen tunnisteen määrittelemisestä arkaluonteiseksi tiedoksi. Tällöin myös biometrisia tunnisteita koskevista tiedoista tulisi yksityisyyden suojan ytimeen kuuluvia henkilötietoja. Tämän hetkisen asetusehdotuksen mukaan biometriset tunnisteet on erikseen mainittu,

978 Kindt huomauttaa kuitenkin siitä, että myös biometrisia tunnisteita koskevat vastuukysymykset vaativat tarkempia säännöksiä. *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 748-749.

979 *Lahti,* Johdanto, s. 10.

980 Näin myös *Sisäministeriö,* Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten tutkinnassa, s. 38 ja 41. Katso myös PeVL 14/2009 vp.

mutta niille ei ole myönnetty erityistä asemaa. Tästä huolimatta yhteiskunnallinen keskustelu biometrista tunnistamista koskevan lainsäädännön tarpeesta on aiheellista.[981]

981 Saman huolen on esittänyt Antti Ketola muun kuin lääketieteellistä tutkimusta koskevan erityislain säätämisen kohdalla. *Ketola,* Tiedollinen itsemääräämisoikeus ja laaja suostumus ihmistieteellisessä tutkimuksessa, s. 87.

8. Yksityisyyden, henkilötietojen suojan ja tietojärjestelmien tulevaisuudennäkymiä

8.1. Perus- ja ihmisoikeuksien merkityksen kasvun vaikutus biometriseen tunnistamiseen

Perus- ja ihmisoikeuksista puhuttaessa tulee huomioida oikeudet, jotka eivät välttämättä sellaisenaan ole kirjautuneet esimerkiksi ihmisoikeussopimuksiin tai perustuslakeihin. Tällaiset metaoikeudet ovat yhteiskuntasopimusten tasoisia tavoitteellisia, moraalisia päämääräoikeuksia[982], jotka toimivat perusoikeuksien ja muiden oikeuksien kantavien arvojen ilmentäjinä. Nämä oikeudet ovat myös oikeusjärjestelmän abstraktille tasolle institutionalisoituja arvoja, joita oikeusjärjestys kokonaisuudessaan pitää oikeuden normatiivisesti velvoittavina tavoitteina.[983]

Metaoikeudet ovat oikeusjärjestyksen syvätasolla olevia arvoja ja periaatteita, jotka ovat hahmotettavissa ihmis- ja perusoikeuksien taustalla oleviksi oikeuksien oikeuksiksi. [984] Metaperiaatteet ovat näin

982 *Saarenpää,* Informaatio-oikeus, s. 210.

983 *Pöysti,* Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta, s. 96. Vertaa *Dworkin,* jonka mukaan oikeudet voidaan erotella abstrakteihin ja konkreettisiin. Abstrakteista oikeuksista hän toteaa seuraavaa: ”An abstract right is a general political aim, the statement of which does not indicate how that general aim is to be weighed or compromised in particular circumstances against other political aims.” *Dworkin,* Taking Rights Seriously, s. 93.

984 *Pöysti,* Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet, s. 41.

ollen oikeussääntöjen ja oikeusperiaatteiden taustalla olevia syvärakenteita, jotka toimivat kantavina periaatteina rakennettaessa oikeudellisia systeemejä ja jäsennettäessä oikeusjärjestystä oikeudenalakohtaisiin lokeroihin. Tällaisina oikeuksina ne muodostavat oikeuskulttuurimme selkärangan, koska ne kertovat, mitä yhteiskunnassamme pidetään tärkeänä, arvokkaana ja suojaamisen arvoisena.[985]

Metaoikeuksien kautta perus- ja ihmisoikeudet saavat korostuneen merkityksen ihmis- ja perusoikeusvelvoitteisessa demokraattisessa oikeusvaltiossa. Syynä on se, että metaoikeudet korostavat kehitystä, jossa yksilön oikeudet ovat nousseet keskiöön. Merkitystä on entisestään lisännyt se, että perus- ja ihmisoikeudet kuuluvat niihin tuntomerkkeihin, joilla määritetään hyvää inhimillistä elämää.[986] Tämän vuoksi ne ovat osa niin ihmisten kuin oikeudenkin arkipäivää. Ihmisoikeussopimusten merkityksen kasvu on omalta osaltaan vahvistanut perusoikeuksien merkitystä yhteiskunnassa.

Ihmis- ja perusoikeuksien kohdalla tulee kuitenkin muistaa, että ne ovat olleet taustalla vaikuttavia arvoja ja metaoikeuksia jo kauan ennen kansainvälisiä sopimuksia tai perustuslakeja. Tällaiset perustavanlaatuiset oikeudet ovat aina kiinnittyneet yksilön asemaan henkilönä, kansalaisena tai yksilön kykyyn toimia. Näiden asemien pohjalta oikeudet voidaan edelleen jakaa kaikille ihmisille kuuluviin ihmisoikeuksiin, kansalaisuuteen sidottuihin yleisiin oikeuksiin, toimintakykyisille kuuluviin kansalaisoikeuksiin sekä toimintakykyisten, kansalaisuuden omaavien henkilöiden poliittisiin oikeuksiin.[987]

Tämän tutkimuksen kannalta merkityksellisimpiä metaoikeuksia ovat ennen kaikkea ihmisarvon kunnioittaminen, oikeus itsemäärää-

985 *Tornberg,* Edunvalvonta, itsemääräämisoikeus jaoikeudellinen laatu, s. 35.

986 *Aarnio,* Tulkinnan taito, s. 310.

987 *Ferrajoli,* Fundamental Rights, s. 4–5.

miseen, oikeus tietoon, oikeus yksityisyyteen ja oikeus tietoturvallisuuteen. Biometrisen tunnistamisen käytössä ja biometristen tietojen käsittelyssä ihmisarvon kunnioittaminen ja itsemääräämisoikeus nousevat esille keskeisinä periaatteina. Oikeus tietoon, oikeus yksityisyyteen ja oikeus tietoturvallisuuteen ovat erityisesti biometristen tietojen käsittelyn kannalta tärkeitä ja korostuvat rekisteröidyn ja rekisterinpitäjän välisessä suhteessa.

Ihmis- ja perusoikeuksien merkityksen kasvu vaikuttaa myös voimassaolevaan ihmiskäsitykseen. Yhteiskunnassa oikeudellisen ajattelun lähtökohtana tulee olla ihminen oikeuksien haltijana. Yhteiskunnan velvollisuutena on myös ihmis- ja perusoikeuksien turvaaminen, sillä turvaamalla yksilön oikeudet ja niiden toteutumisen yhteiskunta samalla turvaa omia oikeuksiaan. Tällä tavoin perus- ja ihmisoikeudet tuovat oman lisänsä voimassaolevaan ihmiskäsitykseen.

Perus- ja ihmisoikeuksien korostumisen vuoksi yksilön asema vahvistuu suhteessa julkiseen valtaan kuin myös suhteessa markkinoihin, ja myös suhteessa työnantajaan. Teknologian kehitys ja tietotekniikan yleistynyt käyttö kasvattavat kuitenkin perusoikeuksien vaarantumisen riskiä. Teknologinen imperatiivi luo uusia ja usein yllättäviä riskejä yksilön oikeuksille.

Eräs teknologisen imperatiivin mukana tullut uhka yksilön oikeuksille on biometrinen tunnistaminen. Biometrisessa tunnistamisessa ihmisruumis muutetaan koneellisesti luettavaksi tunnistamisvälineeksi. Tämä aiheuttaa uudenlaisia kysymyksiä ihmisarvon kunnioittamisen, itsemääräämisoikeuden sekä yksityisyyden ja henkilötietojen suojan näkökulmista. Koska biometrinen tunnistaminen vaikuttaa voimakkaasti yksilön ihmisarvoiseen kohteluun, itsemääräämisoikeuteen ja yksityisyyteen, tulee sen käyttöönoton suunnittelussa ja toteuttamisessa lähtökohtana olla ihmisen oikeuksien turvaaminen ennen yhteis-

kunnan oikeuksien turvaamista.[988] erityisesti itsemääräämisoikeuden korostumisen vuoksi biometrisen tunnistamisen tulisi olla yksilön itsemääräämisoikeutta tukevaa eli sitä tulisi käyttää itsemääräämisoikeutta tukevalla ja kunnioittavalla tavalla henkilön omaan myötävaikutukseen perustuen. Vain tällä tavoin biometrinen tunnistaminen voi saavuttaa yhteiskunnallisen hyväksynnän.

8.2. Tietotekninen kehitys ja sen vaikutus henkilötietojen käsittelyyn, yksityisyyden suojaan ja valvonnan mahdollisuuksiin

Rauno Korhonen kirjoitti vuonna 2003 julkaistussa väitöskirjassaan vuoden 2001 WTC: in kohdistuneiden terrori-iskujen vaikutuksista: *”Vielä on ehkä vaikea analysoida tarkkaan sen kaikkia suoria ja välillisiä vaikutuksia. Terrorismi ja muu rikollisuus vaikuttavat kuitenkin aikaisempaa voimakkaammin siihen, että yleisen turvallisuuden nimissä pyritään rajoittamaan henkilötietojen suojan ohella muitakin yksityisyyteen liittyviä oikeuksia. Kansalaisten valvontaa tehostetaan ja poliisin toimintavaltuuksia lisätään asteittain kansallisin ja kansainvälisin perustein…”*[989]

Mainituista terrori-iskuista on kulunut kohta 14 vuotta, ja vasta viime vuosina näiden iskujen vaikutukset yksilön yksityisyydelle ovat alkaneet hahmottua. Vuoden 2001 terrori-iskut antoivat voimakkaan

988 Näin myös *Goncalves – Gameiro,* Security, Privacy and Freedom and the EU Legal and Policy Framework for Biometrics, s. 323.

989 *Korhonen,* Perusrekisterit ja tietosuoja, s. 301. Perusoikeuksien korostumisen myötä nousevat yleisemminkin esille eri perusoikeuksien väliset kollisiotilanteet ja perusoikeuksien yhteensovittaminen näissä ristiriitatilanteissa, joissa eri tahoilla on erilaisia, samanarvoisiksi koettavia intressejä.

sysäyksen uusien valvontateknologioiden kehittämiselle. Näistä tällä hetkellä suurinta huomiota on saanut biometrinen tunnistaminen, jonka käyttöä perustellaan turvallisuuden takaamisella. On jopa sanottu biometrisen tunnistamisen toimivan terrorismin hopealuotina eli lopullisena ja pettämättömänä ratkaisuna terrorismin torjunnassa.

Asia ei kuitenkaan ole näin yksiselitteinen. Kiistatonta toki on, että biometrinen tunnistaminen tarjoaa perinteisiä tunnistamisratkaisuja tehokkaamman keinon yksilön tunnistamiselle, mutta samalla tämän teknologian lisääntyvä käyttö mahdollistaa yksilön tehokkaamman seurannan yhteiskunnassa. Tämän vuoksi on tärkeää luoda tarkat rajat tämän teknologian käyttämiselle yhteiskunnassa, jotta vältytään väärinkäytöksien aiheuttamilta oikeudenloukkauksilta. Biometrinen tunnistaminen ja yksilön digitaalinen identiteetti ovat yksi 2010-luvun suurimpia yksilön valvontaan ja tunnistamiseen liittyviä oikeudellisia kysymyksiä, joihin yhteiskunnan, lainsäätäjän ja oikeustieteen tulee vastata.

Tutkimuksen johdanto-osiossa käsiteltiin yhteiskunnan muutosta. Kehitys on kulkenut informaatioyhteiskunnasta oikeudelliseksi verkkoyhteiskunnaksi ja kohti oikeudellista valvontayhteiskuntaa. Termi on perusteltu siksi, että terrorismin uhan aiheuttama yhteiskunnallinen turvattomuuden tunne on antanut mahdollisuuden kehittää uusia, osin lainsäädännöllisiä muotoja valvoa yksilöä yhteiskunnassa.

Terrorisminvastaisten toimenpiteiden ei kuitenkaa pitäisi laskea demokraattisiin yhteiskuntiin kuuluvien perusoikeuksien suojan tasoa. Terrorismin torjunnan keskeisenä tehtävänä on säilyttää niiden demokraattisten yhteiskuntien perustana olevien arvojen säilyttäminen, joita väkivallan käyttäjät yrittävät tuhota. Yhteiskunnallisen turvattomuuden tunteen ei saisi antaa johtaa yksityisyyden suojan kaventumiseen, vaan pikemminkin sen vahvempaan turvaamiseen.

Oma osansa valvonnan mahdollisuuksien kasvuun on tietoteknisellä kehityksellä, joka on viimeisen kahden vuosikymmenen aikana

edennyt suurin harppauksin. Ihmisten käytössä on nyt teknisiä laitteita, joista aiemmin ei osattu juuri haaveillakaan. Tällaisen uuden teknologian eri sovellukset ovat mahdollistaneet yhä tehokkaamman kansalaisten valvonnan. Kehitykseen on liitetty voimakkaasti uhkakuva yksityisyyden suojan nopeasta heikkenemisestä tai jopa täydestä rapautumisesta.[990]

Uusien valvontamahdollisuuksien lisäksi uusi yhteiskunnallinen haaste yksilön oikeuksille on uuden identiteettikäsityksen esiinnousu. Tietotekniikan laaja hyödyntäminen on nostanut esiin ihmisen fyysisen identiteetin rinnalle niin sanotun digitaalisen identiteetin.[991] Riippuvuus tästä digitaalisesta identiteetistä tulee myös kasvamaan, mitä enemmän kansalaisten oikeudet ja vaikuttamismahdollisuudet kytketään digitaaliseen toimintaympäristöön. Tämä kehitys asettaa yksityisyyden suojalle uusia haasteita, joihin yhteiskunnan tulee vastata. Uudessa verkkoyhteiskunnassa digitaalisen identiteetin varastaminen ja erilaisten digitaalisten profiilien käyttö päätöksenteossa ja valvonnassa tulevat todennäköisesti lisääntymään.

Tietoteknologian aikaansaaman vallankumouksen ohella on mahdollista puhua valvonnan vallankumouksesta. Yhteiskunnallisen kehi-

990 Aihe on ollut keskustelun aiheena niin kotimaisessa kuin ulkomaisessakin oikeustieteessä. Katso aiheesta tarkemmin mm. *Aarnio,* Häviääkö yksityisyyden suoja, s. 51–57; *Heinonen,* Digitaalinen minä, s.151–155 sekä *Garfinkel,* Database Nation. The Death of Privacy in the 21st Century.

991 Digitaalisesta identiteetistä Suomessa katso tarkemmin esimerkiksi *Heinonen,* Digitaalinen minä. Digitaalisesta identiteetistä katso tarkemmin *Sullivan,* Digital Identity. An Emergent Legal Concept. Sullivanin teos kuvaa yksilön lainsäädännöllisen digitaalisen identiteetin muodostumista Iso-Britanniassa, Australiassa ja Uusi-Seelannissa. Sullivanin mukaan osana yksilön digitaalista identiteettiä ovat tämän biometriset tiedot.

tyksen lisäksi on huomioitava myös toimintaympäristössä tapahtunut muutos. Fyysinen toimintaympäristö on saanut rinnalleen uuden digitaalisen toimintaympäristön.

Tässä uudessa toimintaympäristössä perus-ja ihmisoikeuksilla on tärkeä rooli vanhojen oikeusnormien tulkinnassa uudessa ympäristössä. Perus- ja ihmisoikeudet ovat digitaalisessa ja ei-fyysisessä toimintaympäristössä myös helpommin loukattavissa. Digitaalisessa toimintaympäristössä perus- ja ihmisoikeudet saavat korostuneen merkityksen juuri niiden helpon loukkaamisen ja haavoittuvan luonteen vuoksi.

Informaatioyhteiskunnassa oikeuskulttuurin kehityksen kannalta on ongelmallista, että nopeasti kehittyvän teknologian suuntauksia on tietyllä tavalla helpompi ennustaa ja selittää kuin lainsäädännön, etiikan ja moraalin hidasta kehitysvauhtia. Lainsäädännön jälkeen jääminen teknologisesta kehityksestä ei kuitenkaan saa johtaa yksilön oikeuksien vaarantumiseen. Lainsäätäjällä on velvollisuus huolehtia perus- ja ihmisoikeuksien toteutumisesta digitaalisessa toimintaympäristössä. Tämä toimintaympäristön muutos on osaltaan vaikuttanut valvonnan ja sen mahdollisuuksien lisäämiseen yhteiskunnassa.

Valvonnan mahdollisuuksien lisääntyminen yhdessä nopean teknologisen kehityksen kanssa vaikuttavat voimakkaasti yksityisyyteen ja sen tulevaisuuteen. Teknologisen kehityksen aikaansaamien yhteiskunnallisten muutosten on eniten nähty vaikuttavan yksityisyyden suojan tulevaisuuteen. Valvonnan ja läpinäkyvyyden lisääntyessä yksityisyyden on arvioitu vähenevän. Toisaalta yksityisyyden suojaan on sanottu vaikuttavan eniten se, miten yhteiskunnallisten arvojen ristiriidat ratkaistaan yhteiskunnallisella tasolla.[992]

Merkitystä yksityisyyden suojan tulevaisuuden arvioinnissa ei kuitenkaan ole pelkästään teknologisella kehityksellä, sillä tämä on vain yksi yksityisyyden suojaan ja sen tulevaisuuteen vaikuttavista tekijöis-

992 6, *Perri,* The Future of Privacy, s. 12–14.

tä. Teknologisen kehityksen ohella yksityisyyden suojan tulevaisuutta voidaan hahmottaa historiallisen kehityksen kautta. Tällöin selvitetään niitä keskeisiä tekijöitä, jotka aiemmin ovat johtaneet yksityisyyden suojan muuttumiseen. Näiden tekijöiden kautta on mahdollista luoda tapahtumiin perustuvia kuvauksia mahdollisista tapahtumaketjuista, jotka vaikuttavat yksityisyyden suojan kehitykseen.[993]

Valvonnan mahdollisuuksien lisäämisen taustalla olevalla teknologisella kehityksellä pelkästään ei näin ollen vielä ole suurta vaikutusta yksityisyyden ja henkilötietojen suojan tulevaan kehitykseen. Suurempi merkitys on muilla yhteiskunnallisilla ja sosio-poliittisilla tekijöillä, kuten sillä ketkä päättävät kulloinkin voimassa olevista yksityisyyttä suojaavista normeista. Yksityisyyden suojan tulevaa kehitystä on tämän vuoksi vaikea ennustaa. Nämä tekijät ovat yksityisyyden tavoin muuttuvia.

Tämän hetkinen valvonnan kulttuuri kuitenkin antaa perustellun aiheen puhua yksityisyyden tulevaisuudesta. Yhteiskuntamme on muuttumassa valvonnan yhteiskunnaksi, jossa yksityisyydellä on vain vähän tilaa. Valvonnan lisääntyminen saattaa aiheuttaa toivottuja tai ei-toivottuja seurauksia riippuen siitä, mitkä tekijät tai toimijat saavat yliotteen. Suurin yksittäinen yksityisyyden suojaan vaikuttava tekijä tällä hetkellä on yleinen turvallisuuden tunteen puuttuminen, joka on saanut yliotteen yhteiskunnassa. Tämä puolestaan vaikuttaa yhteiskunnan kehityksessä merkityksellisiin sosiopoliittisiin tekijöihin, jotka hyvin voimakkaasti vaikuttavat yksityisyyden suojaan sitä kaventavasti ja valvontaa lisäävästi.

993 *Minkkinen,* Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change, s. 53–57.

9. Lopuksi

Yhteiskuntamme on muuttunut lyhyessä ajassa informaation ja verkkojen varaan rakentuvaksi verkkoyhteiskunnaksi. Tämän hetkinen muutos perustuu suurelta osin teknologiseen kehitykseen, joka nostaa esille uusia oikeudellisia ongelmia. Kehityksessä ei kuitenkaan aina pystytä vastaamaan riittävän nopeasti uusien teknologisten innovaatioiden mukanaan tuomiin lainsäädännöllisiin muutostarpeisiin.

Teknisellä kehityksellä on kuitenkin varjopuolensa, sillä teknologia on saanut yliotteen arkipäivän toiminnoissa. On mahdollista jopa puhua teknologisesta intoilusta. Yksilölle kuuluvat perus- ja ihmisoikeudet eivät kuitenkaan saisi jäädä teknologisen intoilun varjoon. Tällä hetkellä teknologiaan liittyvä ihailu vie pois huomion biometriseen tunnistamiseen liittyvistä perus- ja ihmisoikeuskysymyksistä, kuten yksilön oikeudesta yksityisyyteen ja henkilötietojen suojaan.

Uuden teknologisen innovaation kohdalla keskiöön nousee helposti teknologian tehokkuuden ja nopeuden käytännölliset vaikutukset. Esimerkiksi biometrista tunnistamista on markkinoitu teknologiana, joka tekee arkipäivän asioiden hoitamisesta nopeampaa ja tehokkaampaa. Kansalaisen näkökulmasta biometrinen tunnistaminen vaikuttaakin monesti helposti käytettävältä teknologialta. Biometrista tunnistamista käytetään nykyään monissa erilaisissa toiminnoissa, kuten maahantulotarkastuksissa ja kaupan kassan maksujärjestelmissä. Teknologian katsotaan tulleen helpottamaan arkeamme.

Teknologinen kehitys on osa suurempaa yhteiskunnallista muutosta. Tarve vahvempaan tunnistamiseen yhdessä uusien rikollisuuden muotojen kanssa ovat johtaneet ihmisten valvonnan tiukentumiseen. Tämä on sinänsä luonnollista, sillä poikkeustilanteiden uhka on aina olemassa oikeusvaltiossa, ja se saattaa johtaa väliaikaisesti perusoikeuksia supistaviin toimiin. Esimerkiksi terrorismin uhkan luomia

mielialoja ja pelkoja käytetään toisinaan perusteluina henkilötietojen käsittelyn lisääntyvään sääntelyyn.

Kysymys on erityisesti siitä, että julkisten ja yksityisten hyötyorganisaatioiden toimintaa tehostetaan yksityisyyttä välittömästi tai välillisesti rajoittaen. Tämänlaisessa sääntelyssä haitallisempaa on välillinen sääntely, jossa esimerkiksi viranomaisille annetaan tietyn erityislain ja sen tavoitteiden perusteella oikeus henkilötietojen käyttöön. Kansalainen voidaan myös esimerkiksi ohjata käyttämään palveluita, jotka edellyttävät digitaalista identifiointia. Vaikka näitä rajoituksia tehtäessä toteutetaan muodollisesti oikeusvaltioon liittyvää lailla säätämisen vaatimusta, lisääntyvä sääntely on aina riski identiteetin suojan kannalta. Lopputuloksena on helposti yksityisyyden ja siihen liittyen identiteetin suojan pirstoutuminen.

Yksilön tunnistamiseen osana valvontaa liittyy sekä vallankäytön että demokratian näkökulma. Yhteiskunta tarvitsee valvontaa välttämättömänä työvälineenä ja mahdollisuutena toimintansa tehostamiseen. Valitettavan usein tämän tehokkuuden lisäämisen taustalla on ajatus ihmisestä väärinkäytösten tekijänä.[994] Valvonnan tehostuessa vallankäyttö on kuitenkin helpompaa. Demokratian toteutumisen kannalta merkityksellistä on se, kuka hallitsee yksilöä koskevia tietoja.

---

994 *Saarenpää,* Tietoturva ja tietosuoja, identiteetin näkökulma, s. 58. Tähän liittyen on alettu puhua perinteisen rangaistusopin rinnalla uudesta rangaistusopista. Vanhan rangaistusopin painottaessa rangaistuksen määräämistä syyllisyyden perusteella uusi rangaistusoppi perustuu ennakolliseen rikostorjuntaan kategorisoimalla ja tunnistamalla yksilöt. Tämä uusi rangaistusoppi juontaa juurensa siitä, että valtion pitää tehdä kaikki mahdollinen turvallisuuden takaamiseksi. Katso tarkemmin *Feeley, M. - Simon, J., Actuarial Justice*: The Emerging New Criminal Law. Tällaista ajattelua kuvaa poliisin toive saada pääsy passirekisterin sormenjälkitietoihin.

Valvonta on lisääntynyt teknisen, yhteiskunnallisen ja poliittisen kehityksen seurauksena. Uusien teknologioiden olemassaolo tai halu toiminnan tehostamiseen eivät kuitenkaan riitä selittämään nykyistä kehitystä. Sen voidaan katsoa olevan seurausta kaikkien tekijöiden yhteisvaikutuksesta. Samalla ne luovat mahdollisuuksia tulevalle kehitykselle.[995] Biometrinen tunnistaminen on erinomainen esimerkki tästä kehityksestä.

Valvonnan tekninen järjestäminen on tieteen ja tekniikan kehityksen myötä yksinkertaistunut merkittävästi. Yhteiskunnan ja julkisten sekä yksityisten valtarakenteiden tarkkailumahdollisuuksien lisääntyminen on vaikuttanut kansalaisten mahdollisuuteen päättää itseään koskevista tiedoista. Teoriassa olisi mahdollista rakentaa yhteiskunta, joka rakentuu tehokkaalle ja salaiselle valvonnalle. Tekniikan nopean kehityksen vaikutus valvonnan mahdollisuuksiin antaa aiheen vanhan sääntelyn päivittämiseen.[996]

Oikeusvaltiossa vapausoikeudet kuuluvat yksilölle, jolloin yksilöön kohdistuvan valvonnan tulee olla yksityisen ja yhteisen edun punnintaan perustuvaa. Lisäksi siitä on säädettävä lain tasolla. Perus- ja ihmisoikeusnäkökohtien huomioimisessa eräänlaisena lähtökohtana on periaate, jonka mukaan ihmisen etu ja hyvinvointi ovat tärkeämpiä kuin yhteiskunnan hyöty.[997] Vain tällä tavoin valvonta voi olla edes jossain määrin osa demokraattisen oikeusvaltion toimintaa.

Henkilötietojen suoja on tärkeä osa yksilön persoonallisuusoikeuksia. Henkilötietojen suojan kohteena on yksilön itsemääräämisoikeuden tiedollinen puoli henkilötietojen käsittelyssä. Siinä on tällöin kysymys yksilön persoonan suojaamisesta henkilötietojen käsittelyn

995 Näin myös *Lyon,* The New Surveillance: Electronic technologies and the maximum security society, s. 163.

996 *Marx,* Ethics for the New Surveillance, s. 173.

997 Tämän on myös perustuslakivaliokunta todennut biopankkilakia koskeneessa mietinnössään PeVL 10/2012 vp.

yhteydessä. Se on myös oikeus, jolla on korostunut merkitys digitaalisen toimintaympäristön ympärille rakentuvassa verkkoyhteiskunnassa. Tietoisuus tämän oikeuden merkityksestä on erityisen tärkeää, sillä henkilötietojen käsittelystä on tullut arkipäivää. Tietosuojalainsäädäntö henkilötietojen suojaa koskevana lainsäädäntönä muodostaa vastakohdan yksilön valvonnalle, joka tapahtuu henkilötietojen välityksellä. Sen avulla pyritään suojaamaan yksityisyyttä, tekemään henkilötietojen sallittu käyttö avoimeksi ja rajoittamaan henkilötietojen käsittelyä.

Verkkojen varaan rakentuvassa yhteiskunnassa ja digitaalisessa toimintaympäristössä ihmisen tunnistamisesta on tullut entistä tärkeämpää myös oikeudellisesti. Tämä on vaikuttanut uusien tunnistamisteknologioiden kehittämiseen. Verkkoyhteiskunnan uusien tunnistamisratkaisujen joukkoon kuuluu esimerkiksi tässä väitöskirjatutkimuksessa tarkasteltava biometrinen tunnistaminen, jonka teknologinen kehitys on mahdollistanut. Sen avulla pyritään vastaamaan yksilön tunnistamisen haasteisiin verkkoyhteiskunnassa. Siinä hyödynnetään automaatiota, joka tekee tunnistamisesta tarkkaa, tehokasta ja helppoa.[998] Biometrisen tunnistamisen kehittämisen taustalla vaikuttaa myös yhteiskunnan kasvu ja liikkuvuuden lisääntyminen. Perinteiset tunnistamisratkaisut eivät enää välttämättä pysty tarjoamaan tarpeeksi nopeaa, tehokasta sekä luotettavaa ja turvallista tunnistamista nyky-yhteiskunnan tunnistamistarpeisiin.[999]

---

998 Osin tästä syystä biometrista tunnistamista on pidetty niin sanottuna hopea luotina terrorismin vastaisessa sodassa.

999 Yksilön tunnistaminen ei ole uusi ongelma. Yhteiskunnassa on omaksuttu erilaisia tapoja tunnistaa yksilöt. Nämä tavat voidaan jakaa kolmeen kategoriaan: 1) Tunnistamisvälineen (esim. avain, passi tai henkilökortti) hallussapito, 2) Tieto (esim. salasana tai tunnusluku) ja 3) Biometrinen ominaisuus. Näitä tapoja voidaan myös yhdistellä. *Bolle – Connell – Pankanti – Ratha – Senior,* Guide to Biometrics, s. 4. Yhdistämällä näitä tapoja puhutaan vahvasta tunnistamisesta.

Teknologiseen imperatiiviin perustuvat näkemykset eivät yksistään kuitenkaan ole hyväksyttäviä perusteita biometrisen tunnistamisen käyttöönotolle. Biometrisen tunnistamisen toteutustavat kuuluvat usein sekä julkisella että yksityisellä sektorilla välineisiin, joiden avulla tavoitellaan varmuutta, tehokkuutta ja hallintotaakkojen vähentämistä eri toiminnoissa. Yksilön oikeudet jäävät tällöin helposti taka-alalle. Tietoteknisten mahdollisuuksien vastapainona yksilön itsemääräämisoikeuden suojana on ihmisoikeusperusteinen vähimmän puuttumisen periaate. Tämä tulee tunnistaa oikea-aikaisesti ja oikealla tavalla, jotta tietoteknisen kehityksen ja ihmisoikeuksien välillä ei synny merkittäviä jännitteitä.

Biometrisen tunnistamisen sääntelyn yhteydessä tulee muistaa teknologianeutraalisuuden periaate. Sääntelyperiaatteena se merkitsee sitä, ettei lainsäädännössä pääsääntöisesti tule säännellä yksittäisen teknologisen ilmiön hyödyntämistä tai puoltaa taikka kieltää jotain kilpailevaa tekniikkaa.[1000]

Yleisemmällä tasolla teknologianeutraliteetilla viitataan teknologian luonteeseen. Perinteinen näkemys teknologiasta on se, että teknologia itsessään on neutraali, mutta sen käyttötapa määrittää sen luonteen.[1001] Teknologian neutraalisuuteen liittyy myös toinen näkemys, jonka mukaan teknologia voidaan nähdä uudenlaisena kulttuurisena järjestelmänä, joka muokkaa koko sosiaalista maailmaa vallan välikappaleeksi.[1002] Tämän seurauksena teknologia on muuttunut välineestä

1000 *Saarenpää,* Oikeusinformatiikka (2015), s. 161.

1001 Feenberg on sanonut teknologian neutraaliudesta seuraavaa: "Technology is not inherently good or bad, and can be used to whatever political or social ends desired by the person or institution in control." Feenberg, Critical Theory of Technology, s. 6.

1002 Pacey, Technology in World Civilization: A Thousand-Year History, s. 2. Liberatoren mukaan teknologia ei ole neutraali tosiasia, vaan sosiaalista toimintaa, jonka käyttämiseen liittyy normatiivisia valin-

ympäristöksi ja elämäntavaksi.[1003] Tällä hetkellä olemme siirtymässä teknologian varaan rakentuvaan yhteiskuntaan, jossa teknologia on eräänlaisen ihailun kohde.

Bygraven mukaan mitään teknologiaa ei käytetä tai luoda sosiaalisessa tyhjiössä. Tällä hän tarkoittaa sitä, että teknologian käyttöyhteys tekee tyhjäksi teknologian mahdollisesti nauttiman neutraliteetin. Hän katsoo, että teknologioilla on yleensä luontainen logiikkansa ja ennakkoasetelma, joka vaikuttaa teknologioiden käyttöön. Tämä tulee ottaa huomioon teknologisten tekijöiden vaikuttaessa valvonnan mahdollisuuksiin.[1004]

Yhteiskunnalliset ja poliittiset tekijät ovat vaikuttaneet suuresti biometristen tunnisteiden käyttöönottoon. Vielä ennen 2000-lukua biometrista tunnistamista pidettiin epäkypsänä ja paljon kehitystä vaativana teknologiana. Toisen vuosituhannen alussa biometrinen tunnistaminen nähtiin kuitenkin riittävän kehittyneenä ja turvallisena. Tämän taustalla vaikutti osaltaan pelon ja turvattomuuden ilmapiiri, joka sai alkunsa vuoden 2001 syyskuun terrori-iskusta.

Biometrinen tunnistaminen on alkujaan suunniteltu yksilöiden tunnistamiseen, jota voidaan pitää vallankäytön välineenä tässä tutkimuksessa kuvatuin tavoin. Tämän ja biometrisen tunnistamisen käyttöönoton taustalla olevien poliittisten vaikuttimien vuoksi sitä ei voida pitää täysin neutraalina. Sille on asetettu yhteiskunnassa tietty rooli

---

toja. *Liberatore,* Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union, s. 111.

1003 David Lyon on viitannut tähän jo vuonna 1988 julkaistussa teoksessaan Information Society. Lyonin mukaan jo tuolloin oli alettu kiinnittää huomiota yhteiskunnan sopeutumisesta teknologiaan eikä teknologian sopeuttamisesta yhteiskuntaan. *Lyon,* Information Society, s. 8.

1004 *Bygrave,* Data Protection Law. Approaching its Rationale, Logic and Limits, s. 101.

ja tarkoitus. Koska biometrista tunnistamista on mahdollista käyttää sekä hyvään että huonoon tarkoitukseen, sen käyttötarkoitus tule pitää mielessä pohdittaessa biometrisen tunnistamisen (laaja-alaista) käyttöä.[1005]

Biometrisen tunnistamisen käyttämiseen liittyy kuitenkin paljon perus- ja ihmisoikeuskysymyksiä, jotka jäävät usein huomiotta ennen teknologian käyttöönottoa. Biometrisen tunnistamisen käyttö ei ole suositeltavaa silloin, kun tähän teknologiaan liittyvät uhkat, riskit ja oikeudelliset kysymykset ovat epäselviä. Tämä puolestaan asettaa hyvin tarkan rajan sille, milloin biometristen tunnisteiden käyttö on perusteltua.

Biometrisen tunnistamisen ominaispiirteiden vuoksi tätä teknologiaa on mahdollista lähestyä kahdesta näkökulmasta. Se voidaan nähdä joko tehokkaana välineenä turvallisuuden takaamisessa tai suurena uhkana yksilön yksityisyydelle.[1006] Jos tutkimuksen luvussa 4.2.4.

1005 Kuten Ashbourn on asian todennut:"Technology is a tool which may be developed and used intelligently or unintelligently, ethically or unethically, for the common good or against the common good. When we introduce new technologies which will affect the lives of many millions of individuals, we must bear such realities in mind and strive to do so in a responsible manner. Biometrics and related enabling technologies are a case in point." *Ashbourn,* The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies, s. 1.

1006 Biometrisen tunnistamisen käyttöä on perusteltu muun muassa sillä, että sen avulla on paremmat mahdollisuudet rikosten torjuntaan ja selvittämiseen. Tällainen perustelu on kuitenkin vaarallinen, sillä demokraattisessa oikeusvaltiossa rikosten torjunnassa ja selvittämisessä ei saa perusteetta ja ilman oikeutusta rajoittaa tai loukata kansalaisten oikeuksia. Näin myös *Kindt,* Privacy and Data Protection Issues of Biometric Applications, s. 305.

mainittuja riskejä ei oteta riittävällä tavalla huomioon, biometrisen tunnistamisen käyttäminen saattaa muodostua suuremmaksi uhkaksi turvallisuudelle, jota sen on tarkoitus suojata.

Biometrisen tunnistamisen kohdalla ei kuitenkaan tarvitse valita yksityisyyden ja turvallisuuden väliltä. Nämä oikeudet tulisi ennemminkin tasapainottaa keskenään, sillä biometrinen tunnistaminen on alkujaan kehitetty turvaamaan perusoikeuksia, kuten oikeutta turvallisuuteen ja yksityisyyteen. Tämän vuoksi biometrisen tunnistamisen kohdalla tulisi kiinnittää erityistä huomiota sääntelytarpeeseen, koska lainsäädännön avulla on mahdollista kontrolloida biometristen tunnisteiden käyttämistä yksilön oikeudet turvaavalla tavalla. Lainsäädännön ohella tämän teknologian käyttämisen kontrollointi esimerkiksi lupa- tai ilmoitusmenettelyllä voisi toimia tehokkaana välineenä. Tällä tavalla biometrisen tunnistamisen käyttämiseen liittyviin ongelmiin voidaan puuttua ennakolta. Jos lainsäädännöllä ei rajoiteta biometrisen tunnistamisen käyttämistä, siitä aiheutuu uhka tämän teknologian käyttämisestä perusoikeuksia loukkaavalla tavalla. Tämän vuoksi biometrisen tunnistamisen käyttö nähdään uhkana yksityisyydelle.

Yksityisyydellä ja biometrisella tunnistamisella on oma historiansa, ja molemmat ovat edelleen kehittymässä. Yksityisyyttä voidaan käyttää teknologian perusperiaatteiden uudelleenarvioinnin välineenä, jotta on mahdollista yhdistää teknologian mahdollisuudet sen tarkoitukseen. Sekä biometrisen tunnistamisen historian ymmärtäminen että yksityisyyden tarkoituksen ymmärtäminen auttaa yksityisyyden periaatteiden soveltamisessa biometriseen tunnistamiseen. Tämä mahdollistaa myös niiden vaikutusten arvioimisen, mitä biometrisella tunnistamisella on yksityisyyden suojaan. Kysymys on pohjimmiltaan siitä, miten biometrisen tunnistamisen periaatteet sovitetaan yhteen yksityisyyden periaatteiden kanssa. Tällä tavoin toimittaessa on mahdollista luoda turvalliset ja tehokkaat biometrisen tunnistamisen oikeudelliset perusteet,

jotka asettavat oikeuden yksityisyyteen ja biometrisen tunnistamisen keskenään tasapainoon.

Biometrisen tunnistamisen kohdalla perus- ja ihmisoikeuskysymys koskee ennen kaikkea yksityisyyden ja henkilötietojen suojaa. Onkin huolestuttavaa, ettei suuri osa suomalaisista välitä tietosuojasta.[1007] Lisäksi tietosuoja koetaan helposti hallinnollisena rasitteena. Biometriasta ei ole kuitenkaan omaa erityislakia. Henkilötietolaki henkilötietojen käsittelyn yleislakina koskee myös biometrisia tunnisteita. Työelämän yksityisyyttä koskeva lainsäädäntö jättää myös biometriset tunnisteet huomiotta. Oikeustilan epäselvyys on riski yksilön yksityisyyden suojalle.

Perustuslain mukaan oikeus yksityisyyteen on perusoikeus. Henkilötietojen keräämisestä ja muusta käytöstä tulee perustuslain mukaisesti säätää lailla. Biometrisen tunnistamisen käyttöä perustellaan turvallisuuden lisäämisellä, jolloin merkityksellinen on myös perustuslaissa turvattu oikeus turvallisuuteen.

Vähimmän puuttumisen periaate ihmisoikeuslähtöisenä periaatteena jo edellyttää, ettei pelkästään turvallisuuden varjolla voida perustella biometristen tunnisteiden käyttöä. Kysymys on yksilön perusoikeuksien turvaamisesta, sillä periaate asettaa velvollisuuden valita vähiten yksilön oikeuksiin puuttuvan toimintatavan. Perusoikeussäännösten systemaattisesta luonteesta sekä ihmisoikeussopimusten ilmentämästä oikeuksien väärinkäytön kiellosta lisäksi seuraa, ettei mitään perusoikeutta ole lupa käyttää perusteena toisen perusoikeuden mitätöimiseksi tai karkeaksi loukkaamiseksi.

Biometristen tunnisteiden käyttämisen perusteleminen ei voi perustua pelkästään turvallisuuden ja tehokkuuden parantamiseen, jos

1007 Reijo Aarnio on jo vuonna 2004 kirjoittanut Tietosuoja-lehdessä suomalaisten välinpitämättömyydestä tietosuojaan ja tietoturvaan. *Aarnio,* Omat toimet, s. 3.

tällä menettelyllä samalla karkeasti loukataan jotain toista perusoikeutta, tässä tapauksessa oikeutta yksityisyyteen. Biometriseen tunnistamiseen liittyy erityisen keskeisesti yksi kysymys: Mitä ovat ne yhteiskunnalliset muutokset, jotka edellyttäisivät henkilön tunnistamista nimenomaan biometristen ominaisuuksien perusteella? Sähköisen asioinnin ja palvelujen tarjonnan lisääminen vaikuttavat melko kevyiltä perusteilta biometristen tunnisteiden rekisteröimiseen nykyinen toimintakulttuuri ja voimassa oleva lainsäädäntö huomioon ottaen.

Suomen tietoturvastrategian yhtenä keskeisimmistä tavoitteista on rakentaa kansalaisten ja yritysten luottamusta tietoyhteiskuntaan.[1008] Avoin ja selkeä viestintä palvelun turvallisuudesta ja mahdollisista riskeistä luo perustan sille luottamukselle, jota arjen tietoyhteiskunnassa toimimisessa tarvitaan. Luottamus on välttämätön edellytys myös biometrisen tunnistamisen yleistymisen kannalta ja tietoturvasta huolehtiminen on keskeinen tekijä näitä menetelmiä koskevan luottamuksen rakentamisessa. Palveluntarjoajat ja muut toimijat, jotka biometriaa hyödyntävät, tarvitsevat selkeää ja helposti omaksuttavaa tietoa siitä, mitä tietoturvaan liittyviä seikkoja niiden tulee ottaa huomioon biometriaa hyödyntävissä palveluissaan ja järjestelmissään.

Tosiasia kuitenkin on, että biometrinen tunnistaminen on tullut osaksi verkkoyhteiskunnan tunnistamisratkaisuja. Jotta biometrinen tunnistaminen voisi oikeudellisesta näkökulmasta kehittyä turvalliseksi ja yksilön oikeudet riittävällä tavalla huomioivaksi teknologiaksi, tulee tämä tosiasia hyväksyä ja keskittyä biometrisen tunnistamisen oikeudelliseen ja yhteiskunnalliseen puoleen. Tällä hetkellä biometrinen tunnistaminen on vielä yhteiskunnallisen kehityksensä alussa. Siihen liittyy myös paljon riskejä ja uhkia, minkä vuoksi sen käyttöön tulee

1008 Katso tarkemmin Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta ”Turvallinen arki tietoyhteiskunnassa – Ei tuurilla vaan taidolla” (annettu 1.12.2008).

suhtautua pidättyvästi, eikä sitä myöskään tule vielä pitää tehokkaana välineenä terrorismin torjunnassa.

Biometrinen tunnistaminen on perustellusti mahdollista nähdä uhkana yksityisyyden suojalle. Sen käyttöönottoon tulee suhtautua kriittisesti, sillä tällä hetkellä sen käyttäminen herättää enemmän kysymyksiä kuin antaa ratkaisuja. Ensimmäinen askel yksityisyyden suojan turvaamisessa on vallitsevan tilanteen tiedostaminen. Biometrisen tunnistamisen kohdalla tämän ensimmäisen askeleen ottaminen on vaikeaa, koska asiasta ei ole Suomessa vielä riittävästi käyty oikeustieteellistä eikä yhteiskunnallista keskustelua, josta kävisi ilmi tämän teknologian vaikutukset yksilön oikeuksiin. Lähtökohdaksi tässä keskustelussa tulee ottaa yksilö, sekä yksityisyys ja henkilötietojen suoja ihmis- ja perusoikeustasoisina yksilön vapautta turvaavina oikeuksina. Yksilön oikeuksia ei tule sivuuttaa vain yhteiskunnan etuun vetoamalla. Kaikkien osapuolten etujen mukaista on turvata kansalaisille yksityisyyden suojan sellainen perustaso, jonka myötä he välttyvät tekniikan mahdollisesti mukanaan tuomilta haitallisilta lieveilmiöiltä.

Mikäli biometrinen tunnistaminen halutaan saada jokapäiväiseen käyttöön, tulee huomioida se, että biometristen tunnistusmenetelmien tulee olla toiminnallisuudeltaan edistyksellisempiä kuin mikään olemassa oleva vaihtoehtoinen menetelmä. Pelkkä tekninen edistyksellisyys ei kuitenkaan riitä. Biometrisen tunnistamisen kohdalla edistyksellisyyden tulee myös näkyä yksilön oikeuksien kohdalla eli teknologian tulee paremmin huomioida myös yksilön oikeudet tunnistamisprosessissa.

Nykyisissä biometrisen tunnistamisen järjestelmissä on kuitenkin edelleen ongelmia niin oikeudellisesta kuin teknisestä näkökulmasta[1009], jotka tulee ratkaista ennen kuin biometrinen tunnistaminen voi syrjäyttää perinteiset tunnistusmenetelmät.

Mihinkään asiaan ei ole ehdotonta oikeaa ratkaisua. On vain valittava käytettävissä olevista vaihtoehdoista se, joka parhaiten toteuttaa yhteiskunnassa voimassa olevia arvoja. Sir Karl Popper on sanonut: *”Jokainen ratkaisu johonkin ongelmaan nostaa esille uusia ratkaisemattomia ongelmia, sitä enemmän, mitä syvällisempi alkuperäinen ongelma oli ja mitä rohkeampi sen ratkaisu. Mitä enemmän opimme todellisuudesta ja mitä syvällisempää oppimisemme on, sitä tietoisempaa, spesifisempää ja artikuloituneempaa on tietomme siitä, mitä emme tiedä, tietomme tietämättömyydestä.”*[1010]

1009 Teknisen puolen ongelmista katso *Nanavati – Thieme – Nanavati,* Biometric Identification. Identity Verification in a Networked World.

1010 *Popper,* Arvauksia ja kumoamisia, s. 29.

LÄHTEET

Kirjallisuus

6, P.: The Future of Privacy. Volume 1. Private Life Public Policy. Demos. Lontoo 1998.

Aarnio, A.: Oikeussäännösten tulkinnasta: tutkimus lainopillisen perustelun rationaalisuudesta ja hyväksyttävyydestä. Juridica. Vantaa 1982.

Aarnio, A: Laintulkinnan teoria. Yleisen oikeustieteen oppikirja. WSOY. Juva 1989.

Aarnio, A: Oikeussäännön systematisointi ja tulkinta. Teoksessa Minun metodini. Toim. Juha Häyhä. WSOY. Helsinki 1997. s. 35–56.

Aarnio, A: Oikeusvaltio – tuomarivaltio? Teoksessa Oikeusvaltio. Toim. Aulis Aarnio & Timo Uusitupa. Lakimiesliiton kustannus. Helsinki 2002. s. 1-12.

Aarnio, A: Tulkinnan taito – ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. Werner Söderström Osakeyhtiö. Helsinki 2006.

Aarnio, A.: Luentoja lainopillisen tutkimuksen teoriasta. Forum Iuris. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki 2011

Aarnio, A.: Oikeutta etsimässä. Erään matkan kuvaus. Talentum. Viro 2014.

Aarnio, R.: Omat toimet. Tietosuoja 4/2004. s. 3.

Aas, *F.:* From Narrative to Database: Technological Change and Penal Culture. Punishment & Society, vol. 6 no. 4. October 2004. s. 379–393

Agre, P.E.: Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places (Sept. 10, 2003). Saatavissa osoitteessa: http://polaris.gseis.ucla.edu/pagre/bar-code.html (käyty 27.2.2015)

Allardt, E.: Ihminen ja moraali hyvinvointivaltiossa. Teoksessa Juhlajulkaisu Paavo Kastari 1907, 13/11, 1977 (1978)

Appelbaum, P.S. – Lidz, C.W. – Meisel, A.: Informed Consent. Legal Theory and Clinical Practice. Oxford University Press. New York 1987.

Ashbourn, J.: The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies. Background paper for the Institute of Prospective Technological Studies, DG JRC – Seville, European Commission, January 2005. Saatavilla osoitteessa: http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf (käyty 19.5.2015)

Avoine, G. – Kalach, K. – Quisquater, J-J.: Belgian Biometric Passport does not get a pass...Your personal data are in danger! UCL Crypto Group, Louvain-la-Neuve, Belgium. Saatavilla osoitteessa: http://www.uclouvain.be/crypto/passport/index.html. (käyty 18.3.2016).

Backman, E: Oikeustiede yhteiskuntatieteenä. Tutkimus oikeustieteen luont
eesta erityisesti rikosoikeuden kannalta. Lakimiesliiton kustannus. Helsinki 1992.

Barroso, J.M.: Human Rights: A Thread of Light through Europe´s History. Equal Voices. Issue 21. October 2007.

Beauchamp, T. L. – Childress, J. F.: Principles of Biomedical Ethics. Seventh edition. Oxford University Press. 2013.

Beck, U.: Risk Society: Towards a New Modernity. Sage Publishing. Lontoo 1992.

Beck, U.: Riskiyhteiskunnan vastamyrkyt: organisoitu vastuuttomuus. Vastapaino. Tampere 1990

Bell, D.: The Coming of Postindustrial Society: A Venture in Social Forecasting. Basic Books. United States of America. 1973.

Benn, S.L.: Privacy, Freedom, and Respect for Persons. Teoksessa J.R. Pennock ja J.W. Chapman (toim.) Privacy. Atherton Press. New York 1971. s. 1–26.

Bing, J.: Classification of personal information with respect to the sensitivity aspect. Teoksessa The International Oslo Symposium on Data Banks and Society. Oslo, June 13th and 14th 1971. The Proceedings. Toim. K. Lenk – L.J. Blaock. Universitetforlaget. Oslo 1972. s. 98-141.

Bing, J: Information Law. Teoksessa Et tilbakeblikk på fremtiden. Artikler samlet I anledning Jon Bings 60-årsdag. Torvund – Bygrave (red.). Institutt for rettsinformatik. Oslo 2004. s. 26-40.

BiometricsInstitute: Biometrics: The Body and Soul of Security. Saatavilla osoitteessa: http://www.biometricsinstitute.org/data/Press_Releases/2002_Body_and_souls.pdf (käyty 19.5.2015)

BiometricsInstitute: Biometrics Privacy Guidelines 2012–2013. Saatavilla osoitteessa: http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute_BIOMETRICS_GUIDELINES_V1.pdf (käyty 19.5.2015)

Björne, L.: Oikeusjärjestelmän kehityksestä. Suomalainen Lakimiesyhdistys 1979.

Black, J.: The Rise, Fall and Fate of Principles Based Regulation. LSE Legal Studies Working Paper No. 17/2010.

Blume, P: Personregistrering. 3. uudistettu painos. Kööpenhamina 1996.

Bloustein, E.J.: Privacy as an Aspect of Human Dignity. Teoksessa F.D. Schoeman (toim.) Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press. Cambridge 1984. s. 156–201.

Blume, P: The Importance of Information Privacy and its future. Teoksessa Vem Reglerar Informationssamhället. Nordisk Årsbok i Rättsinformatik 2006-2008. Tukholma 2010. s. 161-170.

Bolle, R.M. – Connell, J – Pankanti, S. – Ratha, N.K. – Senior, A.W.: Guide to Biometrics. Springer-Verlag. New York 2004.

Brouwer, E.: Legality and Data Protection Law. The Forgotten Purpose of Purpose Limitation. Teoksessa The Eclipse of the Legality Principle in the European Union. Toimittanut Leonard Besselink – Frans Pennings – Sascha Prechal. Kluwer Law International. Alankomaat 2011. s. 273–294.

Brownlie, I.: Principles of Public International Law. Seventh edition. Oxford University Press. 2008.

Burkert, H.: Information Law: From Discipline to Method. Teoksessa Jon Bing. En Hyllest / A Tribute. Toimittanut Dag Wiese Schartum, Lee A. Bygrave, Anne Gunn Berge Bekken. Gyldendal. Latvia 2014. s. 388–400.

Bygrave, L.A.: The Place of Privacy in Data Protection Law. University of New South Wales Law Journal Vol. 24, No. 1. 2001. Artikkeli saatavilla osoitteessa: http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html (käyty 16.7.2014)

Bygrave, L.A.: Data Protection Law. Approaching its Rationale, Logic and Limits. Kluwer Law International. Great Britain 2002.

Bygrave, L. A.: The body as data? Reflections on the relationship of data privacy law with the human body. Saatavilla osoitteessa: http://www.privacy.vic.gov.au/privacy/web2.nsf/files/body-as-data-conference-2003-lee-bygrave-presentation/$file/conference_03_no2.pdf (käyty 12.11.2014)

Bygrave, L.: International Agreements to Protect Personal Data. Teoksessa Global Privacy Protection: The First Generation. Toim. James B. Rule – Graham Greenleaf. Edward Elgar Publishing Limited. Cheltenham Iso-Britannia. 2008. s. 15-49.

Bygrave, L.A.: Data Privacy Law. An International Perspective. Oxford University Press. Oxford 2014.

Cate, F: Privacy in the Information Age. Washington 1997.

Caeton, D.: The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science, Technology and Society, Vol. 27, no 1. February 2007. s.11–23.

Chawki, M: Anonymity in Cyberspace: finding balance between privacy and security. Teoksessa Legal, Privacy, and Security Issues in Information Technology. Volume 1. Toimittanut Kierkegaard, Sylvia Mercado. Complex 3/06. Institutt for rettsinformatikk. Oslo 2006. s. 137–158.

Clarke, R.: Information Technology and Dataveillance. Information of the ACM, Vol. 31, no. 5. May 1988. s. 498–512.

Clarke, R.: Dataveillance. Artikkeli saatavilla osoitteesta: http://www.rogerclarke.com/VD/PPSwamp.ppt.

de Hert, P. – Gutwirth, S.: Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Teoksessa S. Gutwirth et al. (toim.), Reinventing Data Protection? Springer Science+Business Media B.V. 2009. s. 3–44.

de Hert, P. – Schreurs, W. – Kosta, E. – Kindt, E. – Huysmans, X.,: Legal Grounds for ID Documents in Europe. (Contribution to Deliverable 3.6. Study on ID Documents). Future of Identity in the Information Society. 2006. Saatavilla osoitteessa: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.6.study_on_id_documents.pdf. (Käyty 18.3.2016.)

DeLaTorre, P.E.: Resurrecting a Sunken Ship: An Analysis of Current Judicial Attitudes Toward Public Disclosure Claims. 38 SouthWestern Law Journal. 1985

Denning, D.E: Information Warfare and Security. ACM Press. USA. 2000.

Digital Persona. Biometrics in Banking: From Unbanked to Lifelong Customer (Tammikuu 2014).

Dommering, E.J.: An Introduction to Information Law. Works of Fact at the Crossroads of Freedom and Protection. Teoksessa Dommering Egbert J. & Hugenholtz P. Bernt: Protecting Works of Fact, Copyright, Freedom of Expression and Information Law. Information Law Series 1. Kluwer Law and Taxation Publishers. Deventer 1991.

Doumbia-Henry, C.: How Biometrics Helps Seafarers and World Trade? ISO Focus - the Magazine of the International Organization for Standardization, Vol. 3, No. 2, 2006. s. 35–37.

Dworkin, R.: Life´s Dominion. An Argument about Abortion and Euthanasia. HarperCollins Publishers. Lontoo 1993.

Dworkin, R.: Taking Rights Seriously. Harvard University Press. Fifth printing edition. 1978.

Engblom, M.: Työnjohto-oikeus erityisesti työtuomioistuimen käytännön valossa. Työoikeudellisen yhdistyksen vuosikirja 2006.

EPIC: Comments to the FTC. Face Facts. January 31, 2012. Artikkeli saatavilla osoitteessa: https://epic.org/privacy/facerecognition/EPIC-Face-Facts-Comments.pdf (käyty 7.9.2012)

Erikkson, L.D.: Valta. (s. 1240–1246). Sana-artikkeli teoksessa: Encyclopaedia Iuridica Fennica (EIF) VII (Oikeuden yleistieteet). Gummerus. Jyväskylä 1999.

Etzioni, A.: Modern Organisations. Prentice Hall. 1964.

Etzioni, A.: The Limits of Privacy. Basic Books. United States of America. 1999.

Feenberg, A.: Critical Theory of Technology. Oxford University Press. 1991.

Feinberg, J: Social Philosophy. Prentice-Hall, Englewood Cliffs (NJ) 1973.

Ferrajoli, L.: Fundamental Rights. International Journal for the Semiotics of Law. Vol 14 (2000).

Foucault, M.: Power/Knowledge: Selected Interviews and Other Writings, 1972-1977. Edited by Colin Gordon. Pantheon Books. New York 1980.

Foucault, M.: The History of Sexuality, Vol. 1: An Introduction. Random House. New York 1978.

Fowler, H.W. – Fowler, F.G.: The Concise Oxford Dictionary. 8th revised edition. Clarendon Press. 1990

Freese, J. – Persson, G.: Etik och Ny Teknik. Rapport till SNS-konferensen " Etikfrågor i företag och samhälle". Tukholma 1984.

Froomkin, A.M.: Anonymity and the Law in the United States. Teoksessa Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society. Toimittanut Ian Kerr – Valerie Steeves – Carole Lucock. Oxford University Press. New York 2009. s. 441–464.

Fumy, W.: Machine Readable Travel Documents. Teoksessa Handbook of eID Security. Concepts, Practical Experiences, Technologies. Toimittanut Fumy, Walter & Paeschke, Manfred. Publicis Publishing. Germany 2011. s. 94–106.

Garfinkel, S.: Database Nation: The Death of Privacy in the 21st Century. O´Reilly & Associates. California. 2000

Gercke, M.: Legal Approaches to Criminalize Identity Theft. Teoksessa Handbook on Identity-Related Crime. United Nations Office on Drugs and Crime. Vienna 2011. s. 1–54.

Goncalves, M.E. – Gameiro, M.I.: Security, Privacy and Freedom and the EU Legal and Policy Framework for Biometrics. Computer Law & Security Review. 28 (2012), s. 320–327.

Goold, B: How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy and the Political Value of Privacy. Teoksessa Overvåking i en Rettsstat. Toim. Dag Wiese Schartum. Fagbokforlaget Vigmostad&Bjorke As. 2010. s. 38–48.

Götting, H-P – Schertz, C – Seitz, W: Handbuch des Persönlichkeitsrechts. Verlag C.H. Beck. München 2008.

Hadjimatheou, K.: Ethics and surveillance in authoritarian and liberal states. SURVEILLE Deliverable 4.4. Surveille: Surveillance: Ethical Issues, Legal Limitations, and Efficiency. Collaborative Project. 2013. Saatavil-

la osoitteessa: http://surveille.eui.eu/wp-content/uploads/2015/04/D4.4-Ethics-and-surveillance-in-authoritarian-and-liberal-states.pdf (käyty 13.5.2015)

Hall, S.: Identiteetti. Suomentanut ja toimittanut Mikko Lehtonen ja Juha Herkman. Vastapaino. Tampere 1999

Hallberg, P.: Perusoikeusjärjestelmä. Teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka: Perusoikeudet. WSOYpro Oy. Helsinki 2011. s. 29–60.

Harisalo, R.: Riskit yhteiskunnassa ja markkinoilla: itävaltalaisen teorian näkökulma. Teoksessa Riskit ja riskienhallinta. Toimittanut Kuusela, Hannu & Ollikainen, Reijo. Tampere University Press. Tampere 2005. s. 55–71.

Harris, D – O´Boyle, M – Bates, E – Buckley, C: Law of the European Convention of Human Rights. Oxford University Press. Oxford 2009.

Hart, H.L.A: The Concept of Law. Clarendon Press. Oxford 1961.

Heinonen, R.; - Hannula, I.: Valvonta tietoyhteiskunnassa. Edita. Helsinki 1999.

Heinonen, R.: Digitaalinen minä. Edita. Helsinki 2001.

Heinonen, R: Arjen tietoyhteiskunnassa ei ole yksityisyyttä. Teoksessa Paratiisi vai panoptikon? Toimittanut Päivikki Karhula. Eduskunnan kirjaston julkaisuja. Helsinki 2008. s. 162–192.

Heiskala, R.: Yhteiskuntatutkimuksen vaikuttavuus ja uusi uljas maailma. Tieteessä tapahtuu, Vol. 34 Nro 1, 2016. s. 27–33.

Hendrickx, F.: Privacy en Arbeidsrecht. IDEA / Centrum voor Didactiek / UAMS, Het Brantijser, Antwerpen 2002.

Hildebrand, M.: Profiling and the Identity of the European Citizen. Teoksessa: Profiling the European Citizen: Cross-Disciplinary Perspectives. Toimittanut Hildebrant, M. – Gutwirth, S. Springer Science+Business Media B.V. Alankomaat 2008. s. 303–343.

Hirvelä – Heikkilä: Ihmisoikeudet – käsikirja EIT:n oikeuskäytäntöön. Edita Publishing. Helsinki 2013.

Hornung, G.: Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues. European Public Law Vol. 11, Issue 4. 2005. s. 501–514.

Häyhä, J: Johdanto. Teoksessa Minun metodini. Toim. Juha Häyhä. WSOY Lakitieto Oy. Porvoo 1997. s. 15–34.

Jiang. X: Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces. Privacy in Ubicomp´2002. Göteborg 2002.

Julkunen, R.: Työprosessi ja pitkät aallot. Työn uusien organisaatiomuotojen synty ja yleistyminen. Vastapaino. Tampere 1987.

Juntunen, M: Edmund Husserlin filosofia. Fenomenologia ja apodiktisen tieteen idea. Gaudeamus. Helsinki, Mänttä 1986.

Jyränki, A: Oikeusvaltio ja demokratia. Teoksessa Oikeusvaltio. Toim. Aulis Aarnio & Timo Uusitupa. Lakimiesliiton kustannus. Helsinki 2002. s. 13–26.

Jyränki, A.: Uusi perustuslakimme. IuraNova. Jyväskylä 2000.

Jyränki, A.: Valta ja vapaus. Talentum, Lakimiesliiton Kustannus. Helsinki 2003.

Jyränki, A. – Husa, J.: Valtiosääntöoikeus. Lakimiesliiton kustannus. Hämeenlinna 2012.

Kairinen, M.:Työoikeus perusteineen 2001. Työelämän tietopalvelu Oy. Masku 2001.

Kamppinen, M. – Raivola, P. – Jokinen, P. – Karlsson, H.: Riskit yhteiskunnassa. Maallikot ja asiantuntijat päätösten tekijöinä. Gaudeamus. Tampere 1995.

Kamppinen, M.: Teknologian riskit ja tulevaisuus. Teoksessa Geenit ja tekniikka. Toimittanut Launis & Räikkä. Edita. Helsinki 1997. s. 121–141.

Kangas, U: Lesken oikeudellinen asema. Oikeusdogmaattinen tutkimus lesken sosiaaliturvan laajuudesta. Suomalaisen lakimiesyhdistyksen julkaisuja. A-sarja nro 156. Vammala 1982.

Kangas, U: Minun metodini. Teoksessa Minun metodini. Toim. Juha Häyhä. WSOY Lakitieto. Porvoo 1997. s. 90–109.

Kangas, U.: Digitaalinen jäämistövarallisuus. Talentum Media. Hansaprint. 2012.

Kangasniemi, Identiteettivarkaudet – haasteita rikostutkinnalle ja –oikeudelle, paljon vaivaa ja harmia uhrille. Teoksessa Perus- ja ihmisoikeudet

rikosprosessissa. Helsingin hovioikeuden julkaisuja. Hakapaino. Helsinki 2012. s. 217–238.

Karapuu, H.: Oikeus yksityiselämän suojaan. Valtiosääntökomitea. 21.4.1972

Karhula, P: Sähköpaimen – kansalainen ubiikkiyhteiskunnan varjossa. Teoksessa Paratiisi vai panoptikon? Toim. Päivikki Karhula. Eduskunnan kirjaston julkaisuja. Helsinki 2008. s. 11–82.

Kateb, G: Human Dignity. Harvard University Press. Cambridge, Massachusetts and London, England 2011.

Katsh, M.E.: Law in a Digital World. Oxford University Press. New York 1995

Ketola, A.: Tiedollinen itsemääräämisoikeus ja laaja suostumus ihmistieteellisessä tutkimuksessa. Teoksessa Ihmistieteellisten tutkimusaineistojen jatkokäyttö ja tietosuoja. Toimittaneet Antti Ketola ja Raimo Lahti. Forum Iuris. Helsinki 2014. s. 3-97.

Kindt, E.J.: Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis. Springer Science+Business Media. Dodrecht 2013.

Kivimäki, T.M. – Ylöstalo, M: Suomen siviilioikeuden oppikirja. Yleinen osa. WSOY. Porvoo 1973.

Knee, C.R. – Hadden, B.W. – Porter, B. – Rodriguez, L.M.: Self-Determination Theory and Romantic Relationship Processes. Personality and Social Philosophy Review Vol 17, No. 4. November 2013. s. 307–324.

Koillinen, M.: Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 2/2013. s. 171–193.

Koivumaa, A. – Korhonen, R.: Ahti Saarenpää suomalaisen oikeusinformatiikan tienraivaajana. Teoksessa: Syntymästä kuolemaan, oikeudesta informaatioon. Ahti Saarenpää 60 vuotta. Suomalaisen Lakimiesyhdistyksen julkaisuja. E-sarja N:o 17. Gummerus, Vaajakoski 2006. s. 241–253

Konstari, T: Asiakirjajulkisuudesta hallinnossa – tutkimus yleisten asiakirjain julkisuudesta hallinnon kontrollivälineenä. Suomalaisen lakimiesyhdistyksen julkaisuja. A-sarja N:o 121. Suomalainen lakimiesyhdistys. Helsinki 1977.

Konstari, T.: Henkilörekisterilaki. Lakimiesliiton kustannus. Jyväskylä 1992.

Konstari, T.: Matkalla kohti eurooppalaista tietosuojaa. Tietosuoja 4/1997. s. 18-22.

Koosel, S.: Exploring Digital Identity: Beyond the Private Public Paradox. Teoksessa Runnel, Pille – Pruulmann-Vengerfeldt, Pille – Viires, Piret – Laak, Marin (eds.) The Digital Turn: User's Practices and Cultural Transformations. Peter Lang International Academic Publishers. 2013. s. 154–166.

Korhonen, R: Perusrekisterit ja henkilötietojen suoja. Acta Universitatis Lapponiensis. Lapin yliopistopaino. Rovaniemi 2003.

Korhonen, R: Perusrekisterit ja tietosuoja. Edita. 2003.

Korhonen, R.: Oikeusinformatiikan kansainvälisiä haasteita tietoverkkojen yhdentyvässä maailmassa. Teoksessa Kansainvälistyvä oikeus: juhlakirja professori Kari Hakapää. Toim. Timo Koivurova. Lapin yliopiston oikeustieteiden tiedekunta, Rovaniemi 2005. s. 175–190

Korhonen, R.: Sähköisen asioinnin ja viestinnän normitulvaa. Artikkeli saatavilla osoitteessa: http://www.ulapland.fi/loader.aspx?id=-5de17ea2-ede4-4ac1-9c73-79bb8fa461f8 (käyty 12.11.2014)

Korhonen, V. – Koskinen, S. – Ojanen, M. – Pesonen, P.: Työelämän uusi tietosuoja: huumetestit, kameravalvonta ja sähköpostiviestit. Edita Publishing. 2004.

Korja, J: Kameravalvonnan oikeudellinen sääntely – lainsäädännön ja toimeenpanon tarkastelua. Pro gradu –tutkielma. Lapin yliopisto. 2010.

Korpisaari, P.: Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta. Lakimies 7-8/2015. s. 987–1004.

Koskinen, S: Yksityisyyden suoja työelämässä. Teoksessa Martti Kairinen – Seppo Koskinen – Kimmo Nieminen – Vesa Ullakonoja – Mika Valkonen. Työoikeus. WSOY pro. Talentum. Helsinki 2006. s.

Koskinen, S. – Alapuranen, L. – Heino – Salli: Henkilötietojen käsittely työelämässä. Edita. 2012.

Kulla, H: Biometriset tunnisteet ja tiedollinen itsemääräämisoikeus. Teoksessa Lex Ry 45 vuotta: 1961–2006. Toim. Taija Kautto. Lex ry. Turku 2007. s. 31–43.

Kumpula, A.: Vaarojen varjoista nousevat riskit. Oikeus 4/1994, s. 319–334.

Kuopus, J.: Hallinnon lainalaisuus ja automatisoitu verohallinto. Lakimiesliiton kustannus. Jyväskylä 1988.

Kuokkanen, A. – Alvesalo-Kuusi, A.: Työn elektroninen valvonta osana työntekijän hallinnan jatkumoa ja turvallistamista. Oikeus 1/2014. s. 30–49.

Kuusela, O. – Ollikainen R.: Riskit ja riskinhallinta-ajattelu. Teoksessa Riskit ja riskienhallinta. Toimittanut Kuusela, Olli & Ollikainen Reijo. Tampere University Press. Tampere 2005. s. 15–54.

Lagerspetz, E.: Itsemääräämineninen ja valta. Teoksessa Itsemääräämisoikeus. Toimittanut Launis, Veikko ja Räikkä, Juha. Turun yliopiston offsetpaino. Turku 1993. s. 25–67

Lahti, R.: Johdanto. Teoksessa Biolääketiede ja laki. Toimittanut Raimo Lahti. Sosiaali- ja terveyshallituksen raportteja 54. Valtion painatuskeskus. Helsinki 1992. s. 7–18.

Launis, V.: Geeniteknologia, arvot ja vastuu. Gaudeamus. Helsinki 2003.

Lessig, L.: Code and other laws of cyberspace. Basic Books. New York. 1999.

Liberatore, A.: Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union. Springer Science + Business Media B.V. 2007. s. 109–137.

Liu, N.Y.: Bio-Privacy: Privacy Regulations and the Challenge of Biometrics. Routledge. Oxon 2012.

Lohiniva-Kerkelä, M.: Verosalaisuus: julkisuudesta ja salassapidosta verohallinnossa. Lapin yliopistopaino. Rovaniemi 1989.

Lyon, D.: The Information Society. Issues and Illusions. Polity Press. New York 1988.

Lyon, D.: The New Surveillance: Electronic technologies and the maximum security society. Crime, Law and Social Change n:o 18. Kluwer Academic Publishers. Alankomaat 1992. s. 159–175.

Lyon, D.: Surveillance Society: Monitoring Everyday Life. Issues in Society Open University Press. Buckingham & Philadelphia. 2001.

Lyon, D.: Surveillance after September 11. Polity Press. Cambridge, UK. 2003.

Lyon, D.: The search for surveillance theories. Teoksessa Theorizing Surveillance. The Panopticon and Beyond. Willan Publishing. 2006. s. 3–21.

Lyon, D.: Surveillance, Power, and Everyday Life. Teoksessa The Oxford Handbook of Information and Communication Technologies. Toim. Avgerou, Chrisanthi – Mansell, Robin – Quah, Danny – Silverstone, Roger. Oxford University Press. Oxford 2009. s. 449–471.

Lögdberg, Å: Personlighetsrätt. Med särskilt beaktande av dess funktioner och dess begränsning för vissa personkategorier. P.A. Nordstedt & Söners Förlag. Carl Bloms Boktryckeri AB. Lund 1972

Lötjönen, S.: Lääketieteellinen tutkimus ihmisillä. Oikeudellisia ja eettisiä näkökohtia ruumiilliseen koskemattomuuteen puuttumisesta lääketieteellisessä tutkimuksessa. Forum Iuris. Helsinki 2004.

Macklin, R.: Dignity is a useless concept. British Medical Journal 2003; 327. s. 1419–1420

Magnusson-Sjöberg, C.: Rättsautomation - särskilt om statsförvaltningens datorisering. Norstedts juridik. Tukholma 1992

McMahon, Z.: Biometrics: History. Indiana University, Indiana University Computer Science Department, 24 January 2005.

Mahkonen, S: Oikeus yksityisyyteen. Werner Söderström Lakitieto Oy. Porvoo 1997.

Makkonen, K: Luentoja yleisestä oikeustieteestä. Yleisen oikeustieteen laitoksen julkaisuja 16. Yliopistopaino. Helsinki 1998.

Mamia, T. – Alvesalo-Kuusi, A. – Kuokkanen, A. – Virtanen, S.: Työn elektroninen valvonta Suomessa. "Työn elektroninen valvonta – hyödyt ja haitat" -tutkimushankkeen loppuraportti 6/2011. Työterveyslaitos. Helsinki 2011.

Marshall, J.: Personal Freedom through Human Rights Law? : Autonomy, Identity and Integrity under the European Convention on Human Rights. International Studies in Human Rights, volume 98. Martinus Nijhoff Publishers. Leiden 2009.

Marx, G. T.: Ethics for the New Surveillance. The Information Society, Vol. 14, No. 3. 1998. s. 171-184

Mathiesen, T: I Michel Foucault´s "Panopticon" – en gjenvisitt. Retfaed. 70/18. 1995.

McCombs, T. – Gonzalez, J.S.: Right to Identity. International Human Rights Law Clinic. University of California, Berkley School of Law. November 2007. Artikkeli saatavilla osoitteessa: http://scm.oas.org/pdfs/2007/CP19277.PDF (käyty 5.11.2015).

Merton, R.K.: The Sociology of Science. Theoretical and Empirical Investigations. The University of Chicago Press. 1973.

Metsäranta, T.: Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. Julkisoikeuden sarja. A 38. Turku 2015.

Miller: Vital Signs of Identity. IEEE Spectrum, Volume 31, Issue 2. February 1994. s. 22–30.

Minkkinen, M.: Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change. Futures 73 (2015). s. 48–60.

Monahan, T.: Surveillance as Cultural Practice. The Sociological Quarterly 2011, s. 495–508.

Morawetz, T: Epistemology of Judging. Wittgenstein and Deliberative Practices. Teoksessa Wittgenstein and Legal Theory. Toim. Dennis M. Patterson. Boulder, San Fransisco, Oxford: Westview Press, 1992, s.3–27.

Murphy, R.S.: Property Rights in Personal Information: An Economic Defense of Privacy. Georgetown Law Journal 84. 1996

Muukkonen, M.: Perusoikeuslähtöisen laintulkinnan hahmottelua yhdistysoikeudessa. Edilex 2007/29.

Määttä, T.: Monitieteisyys ympäristöoikeudessa – oikeustieteen sisäiset ja ulkoiset yhteydet oikeustieteellisen tutkimuksen haasteena. Oikeus 2000. s. 333–355.

Nabeth: Identity of Identity. Teoksessa The Future of Identity in the Information Society (2009)

Nagel, T.: Concealment and Exposure. Philosophy and Public Affairs. Volume 27, Issue 1. January 1998. s. 3–30.

Nanavati, S. - Thieme, M. - Nanavati, R.: Biometrics. Identity Verification in a Networked World. A Wiley Tech Brief. John Wiley&Sons, Inc. New York. 2002.

National Science and Technology Council: Privacy & Biometrics: Building a Conceptual Foundation. Teoksessa Biometrics, Privacy, Progress and Government. Toimittanut: Rachel B. Jefferson. Nova Science Publishers, Inc. New York 2010. s. 119–152.

Neethling, J. – Potgeiter, J.M. – Visser, P.J: Neethling's Law of Personality. 2nd Edition. Butterworths. South Africa 2005.

Neethling, J.: Personality rights: A comparative overview. The Comparative and International Law Journal of Southern Africa, Vol. 38, No. 2. JULY 2005. s. 210–245.

Nelson, L.S.:America Identified: Biometric Technology and Society. The MIT Press. Cambridge, Massachusetts 2011.

Neuvonen, R.: Yksityisyyden suoja Suomessa. Lakimiesliiton kustannus. Viro 2014.

Neuvonen, R. – Rautiainen, P.: Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä. Lakimies 1/2015. Vammalan kirjapaino Oy. Sastamala 2015. s. 28–53.

Niiniluoto, I: Johdatus tieteenfilosofiaan. Otava. Keuruu 1980.

Nissenbaum, H.: Protecting Privacy in an Information Age: the Problem of Privacy in Public. 17 Law and Phil. 1998. s. 559–596.

Nyyssölä, M.: Yksityisyyden suoja työsuhteessa. Werner Söderström Osakeyhtiö. Porvoo 2004.

Nyyssölä, M.: Yksityisyyden suoja työsuhteessa. WS Bookwell OY. Juva 2009.

Ojanen, T.: Perus- ja ihmisoikeudet terrorismin vastatoimissa Euroopan unionissa. Lakimies 7-8 / 2007. s. 1053–1074.

Ojanen, T.: Perus- ja ihmisoikeudet – Eurooppalaisen konstitutionalismin Akilleen kantapää?, Lakimies 7-8/2009. s. 1106-1124.

Ojanen, T – Scheinin, M: Suomen valtiosäännön perusperiaatteet. Teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka: Perusoikeudet. WSOYpro Oy. Helsinki 2011. s. 217–226.

Ojanen, T. – Scheinin, M.: Liikkumisvapaus (PL 9 §). Teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori,

Kaarlo – Viljanen, Veli-Pekka: Perusoikeudet. WSOYpro Oy. Helsinki 2011. s.317–387.

Paanetoja, J.: Vallankäytöstä työsuhteessa. Teoksessa Työoikeudellisen Yhdistyksen vuosikirja 2012–2013. Toimittanut Jorma Saloheimo. Unigrafia Kirjamyynti. Helsinki 2013. s. 129–150.

Paasilehto, S: Digitaalinen kulttuuri – tulevaisuuden oikeuskulttuuri? Teoksessa Demokraattisen oikeuden ehdot. Kritiikki, politiikka, kulttuuri. Kaarlo Tuorin 60-vuotisjuhlakirja. Toimittanut Samuli Hurri. Tutkijaliitto. Helsinki 2008. s. 330–336.

Pacey, A.: Technology in World Civilization: A Thousand-Year History. MIT Press. Cambridge, Massachusetts 1990.

Pajulammi, H.: Lapsi, oikeus ja osallisuus. Talentum. Viro 2014.

Palm, E.: Privacy Expectations at Work – What is Reasonable and Why? Ethical Tehory and Moral Practice. Volume 12, Issue 2. s. 201-215.

Peczenik, A.: Juridikens teori och metod. En introduktion till allmän rättslära. Norstedts Juridik. Göteborg 1995.

Peczenik, A.: The Basis of Legal Justification. Lund 1993.

Peczenik, A.: Vad är rätt?: om demokrati, rättssäkerhet, etik och juridisk argumentation. Fritzes. Stockholm 1995.

Pellonpää, M.: Henkilökohtainen koskemattomuus (PL 7 §). Teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka: Perusoikeudet. WSOYpro Oy. Helsinki 2011. s. 281–302.

Pesonen, P: Viestintäoikeuden käsikirja. Edita Prima Oy. Helsinki 2011.

Pietarinen, J: Itsemääräämisoikeus. Teoksessa Itsemääräämisoikeus. Toim. Launis, Veikko – Räikkä. Juha. Turun yliopisto. Turku 1993.

Pietarinen, J: Itsemääräämisen periaate. Teoksessa Itsemääräämisoikeus. Toim. Launis, Veikko – Räikkä. Juha. Turun yliopisto. Turku 1993.

Pietarinen, J.: Lääkintä- ja hoitoetiikan keskeiset periaatteet. Teoksessa Lääkintä- ja hoitoetiikka. Toim. Launis, Veikko. Painatuskeskus Oy. Helsinki 1995. s.33–54.

Pietarinen, J.: Geenitutkimus ja etiikka. Teoksessa Geenit ja etiikka. Toimittanut Launis & Räikkä. Edita. Helsinki 1997. s. 30–47.

Pitkänen, O. – Tiilikka, P. – Warma, E.: Henkilötietojen suoja. Talentum Media. Vantaa 2013.

Pohjola, A.: Moderni yhteiskunta, riski ja vaaralliset rikoksentekijät. Teoksessa Biolääketiede, tutkimus ja oikeus. Toimittanut Raimo Lahti. Forum Iuris. Helsinki 2012. s. 149–182.

Popper, K.R.: Arvauksia ja kumoamisia. Tieteellisen tiedon kasvu. Tammer-Paino Oy. Tampere 1995.

Pratt, J.: Governing the Dangerous: dangerousness, law and social change. The Federation Press. Leichhardt 1997.

Prins, C.: Biometric technology law, making our body identify for us: legal implications of biometric technologies. Computer Law & Security Review. Vol. 14, Issue 3. 1998. s. 159–165.

Prosser, W.L.: Privacy. California Law review. Vol. 48, No. 3. California. 1960. s. 383–423.

Pöyhönen, J: Oikeus (s. 693–694). Sana-artikkeli teoksessa: Encyclopedia Iuridica Fennica (EIF) VII (Oikeuden yleistieteet). Gummerus. Jyväskylä 1999.

Pöysti, T: Sähköinen identiteetti (s. 1112–1116). Sana-artikkeli teoksessa: Encyclopaedia Iuridica Fennica (EIF) VII (Oikeuden yleistieteet). Gummerus. Jyväskylä 1999.

Pöysti, T.: Communicational Quality of Law. Teoksessa Festskrift Peter Seipel. Toimittanut Cecilia Magnusson-Sjöberg – Peter Wahlgren, Nordsteds Juridik 2006, s. 463-493.

Pöysti, T.: Future of Privacy in the Emerging Electronic Marketplace in Europe. Teoksessa Function and Future of European Law. Proceedings of the International Conference on the Present State, Rationality and Direction of European Legal Integration. Toimittanut: Veijo Heiskanen & Kati Kulovesi. Forum Iuris. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki 1999. s. 159–184.

Pöysti, T: Tehokkuus, informaatio ja eurooppalainen oikeusalue. Forum Iuris. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki 1999.

Pöysti, T: Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta. Oikeus 1/2000, s. 91–112.

Pöysti, T: Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet. Teoksessa: Viestintäoikeus. WSOY Lakitieto. Vantaa 2002.

Pöysti, T: Oikeudellisen tiedon niukkuus ja henkilötietojen suoja. Teoksessa Syntymästä kuolemaan, oikeudesta informaatioon. Ahti Saarenpää 60 vuotta. Suomalaisen Lakimiesyhdistyksen julkaisuja, E-sarja N:o 17. Gummerus Kirjapaino. Vaajakoski 2006. s. 303–328.

Raatikainen, A.: Yksityisyyden suoja työelämässä. Edita Prima. Helsinki 2002.

Rannenberg, K. – Royer, D. – Deuker, A.: Introduction. Teoksessa The Future of Identity in the Information Society. Challenges and Opportunities. Toimittanut Rannenberg, K. – Royer, D. – Deuker, A. Springer. Berlin 2009. s. 1–12.

Rawls, J.: A Theory of Justice. Harvard University Press. Cambridge 1978.

Ray, N.E.: Let There Be False Light: Resisting the Growing Trend Against an Important Tort. 84 Minnesota Law Review. 2000.

Reich, C.: The Individual Sector. The Yale Law Journal Vol. 100, No. 5. The Yale Law Journal Company, Inc. Danvers, Massachusetts 1991. s. 1409–1448

Roosendaal, A.: Elimination of Anonymity in regard to Liability for Unlawful Acts on the Internet. Teoksessa Legal, Privacy, and Security Issues in Information Technology. Volume 2. Toim. Kierkegaard, Sylvia Mercado. Institutt for rettsinformatikk. Complex nr. 4/2006. Oslo 2006. s. 213–228.

Råman, J.: Yleislaki, yleiset opit ja vaikutusten arviointi. Teoksessa Syntymästä kuolemaan, oikeudesta informaatioon. Ahti Saarenpää 60 vuotta. Suomalaisen Lakimiesyhdistyksen julkaisuja, E-sarja. N:o 17. Gummerus kirjapaino. Vaajakoski 2006. s. 329–350.

Räikkä, J.: Yksityisyyden filosofia. WSOY. Vantaa 2007.

Saarenpää, A.: ATK ja yksilön suoja. Teoksessa Oikeusinformatiikka. Pohjoismaisen oikeuden instituutin julkaisu. Lakimiesliiton kustannus. Rovaniemi 1987. s. 200–219

Saarenpää, A.: Tieto, suoja ja byrokratia – näkökohtia suomalaisen tietosuojan kehityksestä ja tulkinnoista. Teoksessa Martikainen, Petri (toim.): Oikeuskirja. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja B 25. Rovaniemi 1995. s. 581–621.

Saarenpää, A.: Potilas, oikeus, ihminen. Oikeustiede Jurisprudentia XXX 1997. Suomalaisen lakimiesyhdistyksen vuosikirja. Juhlajulkaisu Aulis Aarnio. Gummerus. Jyväskylä 1997. s. 265–278.

Saarenpää, A. – Pöysti, T. – Sarja, M. – Still, V. – Balboa, R.: Tietoturvallisuus ja laki, näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä.

Saarenpää, A.: Oikeusinformatiikka. Teoksessa Oikeustiede Suomessa 1900–2000. Toimittanut Urpo Kangas. WSOY Lakitieto. Juva 1998. s. 211–220.

Saarenpää, A.: Henkilöoikeus. Teoksessa Timonen Pekka: Johdatus Suomen oikeusjärjestykseen. Kauppakaari Oyj. Helsinki 1999.

Saarenpää, A.: Informaatio-oikeus (s. 206–215); Oikeudellinen informaatioyhteiskunta (s. 554–562); Oikeusinformatiikka (s.713–726). Sana-artikkelit teoksessa: Encyclopedia Iuridica Fennica (EIF) VII (Oikeuden yleistieteet). Gummerus. Jyväskylä 1999.

Saarenpää, A.: Verkkoyhteiskunnan oikeutta - johdatusta aiheeseen. Oikeus 1/
2000, s. 3–14.

Saarenpää, A.: Verkoissa, verkoista, verkkoon - verkkoyhteiskunnan niukkenevaa oikeutta? Oikeustieteen rajoja etsimässä. Juhlajulkaisu Juha Tolonen. Kirjapaino Grafia 2001. s. 203–219.

Saarenpää, A.: Oikeusvaltio ja verkkoyhteiskunta. Teoksessa: Oikeusvaltio. Toim. Aulis Aarnio & Timo Uusitupa. Kauppakaari. Lakimiesliiton Kustannus. Helsinki 2002. s. 106–130

Saarenpää, A.: Yksityisyys, yksityiselämä, yksilön suoja – yksityisyyden käsitteellistä kuvausta. Teoksessa Professori Kyösti Holman juhlakirja. Toim. Risto Haavisto. Lapin yliopiston oikeustieteiden tiedekunta. Lapin yliopistopaino. Rovaniemi 2002. s. 313–337.

Saarenpää, A.: Tietoturva ja tietosuoja, identiteetin näkökulma. Teoksessa Pohjois-Suomen tuomarikoulu. Julkaisuja 2/2002. Rovaniemi 2002. s. 33–76.

Saarenpää, A.: Suostumus ja hyvä tietojenkäsittelytapa. Kide: Lapin yliopiston tiedotuslehti. 3/2003. s. 4–5.

Saarenpää, A.: Ihmiskäsitys ja laki. Teoksessa Kansainvälistyvä oikeus: juhlakirja professori Kari Hakapää. Toim. Timo Koivurova. Lapin yliopiston oikeustieteiden tiedekunta. Rovaniemi 2005. s. 461–478

Saarenpää, A.: Information Government and Legal Information. Teoksessa: Knowledge Rights – Legal, Societal and Related Tecnological Aspects. Österreichische Computer Gesellschaft 2008. s. 181–195.

Saarenpää, A.: Kansalaisen oikeudet tiedon valtatiellä. Teoksessa Paratiisi vai panoptikon. Toim. Päivikki Karhula. Eduskunnan kirjaston julkaisuja. Helsinki 2008. s. 141–161.

Saarenpää, A.: Oikeusinformatiikka. Teoksessa Oikeusjärjestys osa 1. 5. täydennetty painos. Toim. Risto Haavisto. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 47. Rovaniemi. 2008. s. 1–110.

Saarenpää, A.: Perspectives on Privacy. Teoksessa Legal Privacy. Toim. Ahti Saarenpää. Prensas Universitarias de Zaragoza. 2008. s. 19–64.

Saarenpää, A.: Oikeusinformatiikka. Teoksessa Oikeusjärjestys osa I. 6. täydennetty painos. Toim. Maarit Niskanen. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 52. Rovaniemi 2009. s. 1–127.

Saarenpää, A.: Henkilö- ja persoonallisuusoikeus. Teoksessa Oikeusjärjestys osa I. 6. uudistettu painos. Toim. Maarit Niskanen. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 52. Rovaniemi 2009. s. 263–472.

Saarenpää, A.: The Importance of Information Security in Safeguarding Human and Fundamental Rights. Teoksessa Vem Reglerar Informationssamhället. Nordisk Årsbok i Rättsinformatik 2006-2008. Tukholma 2010. s. 45–60.

Saarenpää, A.: Kansalainen, yksilö oikeudellisesti kaiken keskipisteenä. Teoksessa Laitinen, M. & Pohjola, A. (toim.) Asiakkuus sosiaalityössä.: Gaudeamus Helsinki University Press Oy Yliopistokustannus. Helsinki 2010. s. 75–137.

Saarenpää, A.: Oikeusinformatiikka. Teoksessa Oikeusjärjestys osa I. 7. täydennetty painos. Toim. Maarit Niskanen. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 56. Rovaniemi. 2011. s. 411–545.

Saarenpää, A.: Henkilö- ja persoonallisuusoikeus. Teoksessa Oikeusjärjestys osa I. 7. Täydennetty painos. Toim. Maarit Niskanen. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 56. Rovaniemi 2011. s. 231–410.

Saarenpää, A.: Henkilö- ja persoonallisuusoikeus. Teoksessa Oikeusjärjestys osa 1. 8. Täydennetty painos. Toimittanut Timo Tammilehto. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 59. Rovaniemi 2012. s. 218–409.

Saarenpää, A.: Personrätt – integritetsrätt. Teoksessa Finlands civil- och handelsrätt. En introduktion. Toim. Bärlund – Nybergh – Petrell. Talentum Media Oy. Helsinki 2013.

Saarenpää, A.: Henkilö- ja persoonallisuusoikeus. Teoksessa Oikeus tänään osa 2. Kolmas uudistettu painos. Toimittanut Marja-Leena Niemi. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 63. Rovaniemi 2015. s. 203–430.

Saarenpää, A.: Oikeusinformatiikka. Teoksessa Oikeus tänään osa 2. Kolmas uudistettu painos. Toimittanut Marja-Leena Niemi. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 63. Rovaniemi 2015. s. 17–205.

Saarinen, M.: Työsuhdeasioiden käsikirja I. Edita Publishing. Helsinki 2014.

Salonen, T.: Tieteenfilosofia. Lapin yliopistokustannus. Rovaniemi 2007.

Sandgren, C.: Vad är rättsvetenskap? Jure Bokhandel. 2009.

Sandström, M. – Peterson, C.: Lex Lata – Lex Ferenda. Fakta eller Fiktion? Teoksessa Lex Ferenda. Toimittanut Rosén J. Norstedts Juridik. Tukholma 1996. s. 159–177.

Santoro, E.: Autonomy, Freedom and Rights. A Critique of Liberal Subjectivity. Kluwer Academic Publishers. Dordrect 2003.

Saraviita, I.: Suomalainen perusoikeusjärjestelmä. Talentum Media Oy. Jyväskylä 2005.

Saraviita, I.: Perustuslaki. Talentum Media Oy. Hämeenlinna 2011

Sarvas, M.: Biotekniikka, riskit ja etiikka. Teoksessa Tiede ja etiikka. Toim. Löppönen, P. – Mäkelä, P.H. – Paunio, K. WSOY. Helsinki 1991. s. 343–357.

Schartum, D.W. – Bygrave, L.A.: Personvern i informasjonssamfunnet. En innfoering i vern av personopplysninger. 2. utgave. Fagbokforlaget. Bergen 2011.

Scheinin, M.: Punninnasta ja ehdottomista ihmisoikeuksista terrorismia torjuttaessa. Teoksessa Demokraattisen oikeuden ehdot. Kritiikki, politiikka, kulttuuri. Kaarlo Tuorin 60-vuotisjuhlakirja. Toimittanut Samuli Hurri. Tutkijaliitto. Helsinki 2008. s. 196–206.

Schwartz, B.: Self-Determination: The Tyranny of Freedom. American Psychologist. Volume 55 (1). The American Psychological Association. Tammikuu 2000. s. 79–88.

Schwartz, P.M.: Privacy and Participation: Personal Information and Public Sector Regulation in the United States. 80 Iowa Law Review. 1994. s. 553–618.

Seipel, P.: Juristen och Datorn. Introduktion till rättsinformatiken. Femte upplagan. Norstedts Juridik. Kristianstad 1994.

Seipel, P: Juridik och IT. Introduktion till rättsinformatik. Norstedts Juridik AB. Tukholma 2004.

Seipel, P: Legal informatics broad and narrow. Teoksessa: Legal Management of Information Systems – incorporating law in e-solutions (Ed. Cecilia Magnusson-Sjöberg). Studentlitteratur. Lund 2010. s. 17–36.

Siltala, R: Oikeustieteen tieteenteoria. Suomalaisen Lakimiesyhdistyksen julkaisuja. A-sarja N:o 234. Vammala 2003.

Siltala, R: Oikeudellinen tulkintateoria. Suomalaisen Lakimiesyhdityksen julkaisuja. A-sarja N:o 261. Jyväskylä 2004.

Slobogin, C.: Is the Fourth Amendment Relevant in a Technological Age? Governance Studies at Brookings. Washington, DC. 2010. s. 1–23.

Smith, C: Human Rights as a Foundation of Society. Teoksessa Lodrup, Peter – Modvar, Eva: Family Life and Human Rights. Gyldendal. Oslo 2004

Smith, R. E.: Privacy. How to Protect What´s Left of It. Anchor Books. Garden City, New York. 1980.

Solove, D.J.: The Digital Person: Technology and Privacy in the Information Age. New York University Press. New York ja Lontoo 2006.

Solove, D.J.: A Taxonomy of Privacy. University of Pennsylvania Law Review. Vol. 154, N:o 3. Janyary 2006. s. 477

Solove, D.J. – Schwartz, P.M.: Information Privacy Law. Fourth Edition. WolterKluwer Law & Business. USA 2011.

Solove, D.J.: Understanding Privacy. Harvard University Press. Cambridge, Massachusettes, USA. 2009.

Solove, D.J. – Schwartz, P.M.: Privacy Law Fundamentals. International Association of Privacy Professionals. Portsmouth, USA 2011.

Sorvari, S. – Lehtonen, L.: Geneettisen tiedon käsittelyn oikeussääntely. Teoksessa Bio-oikeus lääketieteessä. Toimittanut Lasse Lehtonen. Edita Prima. Helsinki 2006. s. 125-150.

Stahl, B.C.: Privacy and Security as Ideology. Teoksessa Legal, Privacy, and Security Issues in Information Technology. Volume 2. The First International Conference on Legal, Privacy and Security Issues in IT. Toimittanut Sylvia Mercado Kierkegaard Institutt for rettsinformatik. Oslo 2006. s. 283–304.

Stalley, R.F.: Self-determination. Journal of Medical Ethics. Vol. 4(1). Maaliskuu 1978. s. 40–41.

Stets, J.E.: Justice, Emotion, and Identity Theory. Teoksessa: Advances in Identity Theory and Research. Toimittanut Peter J. Burke – Timothy J. Owens – Richard T. Serpe – Peggy A. Thoits. Kluwer Academics / Plenum Publicshers. New York 2003. s. 105–122

Stoll, H: The General Right to Personality in German Law: An Outline of its Development and Present Significance. Teoksessa Protecting Privacy. Toim. Basil Markesinis. The Clifford Chance Lectures. Volume Four. Oxford University Press. 1999.

Sullivan, C.: Digital Identity. An Emergent Legal Concept. The role and legal nature of digital identity in commercial transactions. University of Adelaide Press. Adelaide 2011.

Sullivan, C.: Is Your Digital Identity Property? An examination of digital identity in the era of e-government and digital citizenship. European Property Law Journal. Volume 2, Issue 2. 2013. s. 122–143

Syrjänen, J.: Oikeudellisen ratkaisun perusteista. Suomalaisen Lakimiesyhdistyksen julkaisuja. A-sarja N:o 285. Gummerus Kirjapaino Oy. Jyväskylä 2008

Tammi-Salminen, E.: Vanha ja uusi esineoikeus. Lakimies 3/ 2009 s. 453–458.

Tarasti, L.: Yhteiskunnan oikeudellistuminen. Defensor Legis N:o 4/2002. s. 575–585.

Taylor, F.W.: Principles of Scientific Management. New York 1911/1967.

Tiilikka, P.: Sananvapaus ja yksilönsuoja. Lehtiartikkelin aiheuttaman kärsimyksen korvaaminen. WSOYpro. 2007.

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

Tolonen, H.: Oikeuslähdeoppi. SanomaPro Oy. 2007

Tolonen, H.: Oikeuden kaleidoskooppi. Kirjoituksia oikeudesta ja sen historiasta. Suomalaisen lakimiesyhdistyksen julkaisuja, E-sarja N:o 19. Vaajakoski 2008.

Tolonen, J.: Oikeusvaltio ja oikeustiede. Teoksessa Oikeusvaltio. Toim. Aulis Aarnio & Timo Uusitupa. Lakimiesliiton kustannus. Helsinki 2002. s. 27–38.

Tornberg, J.: Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu. Lapin yliopistopaino. Rovaniemi 2012.

Tuori, K.: Oikeus, valta ja demokratia. Lakimiesliiton kustannus. Mänttä 1990.

Tuori, K.: Oikeusvaltio. (s. 932–936). Sana-artikkeli teoksessa Encyclopaedia Iuridica Fennica (EIF) VII (Oikeuden yleistieteet). Gummerus. Jyväskylä 1999.

Tuori, K.: Oikeustiede. (s.857–860). Sana-artikkeli teoksessa: Encyclopaedia Iuridica Fennica (EIF) VII (Oikeuden yleistieteet). Gummerus. Jyväskylä 1999.

Tuori, K.: Yleinen järjestys ja turvallisuus – perusoikeusko? Lakimies 6-7/1999. s. 920–931

Tuori, K.: Kriittinen oikeuspositivismi. WernerSöderström Lakitieto Oy. Vantaa 2000.

Tuori, K.: Demokraattinen oikeusvaltio Suomessa. Teoksessa Foucault´n oikeus. Kirjoituksia oikeudesta ja sen tutkimisesta. WSOY Lakitieto. Vantaa 2002. s. 205–230.

Tuori, K.: Tuomarivaltio – uhka vai myytti? Lakimies 6/2003. s. 915–943.

Tuori, K.: Oikeudenalajaotus – strategista valtapeliä ja normatiivista argumentaatiota. Lakimies 7-8/2004. s. 1196–1224.

van Aerschot, P.: Oikeudellistuminen julkishallinnossa. LM 7/1996. s. 1036–1043.

van der Ploeg, I.: Biometrics and the body as information. Teoksessa Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. Toim. David Lyon. Routledge. Lontoo 2003. s. 57–74

van der Ploeg, I.: Genetics, biometrics and the informatization of the body. Ann Ist Super Sanità Vol. 43, no. 1. 2007. s. 44-50

van der Ploeg, I.: The Politics of Biometric Identification.Normative aspects of automated social categorization. Biometric Technology & Ethics. BITE Policy Paper no.2. November 2005. s. 1–16.

van Dijk, J.: The Network Society. 3rd Edition. Sage Publications. Lontoo 2012.

Vanto, J.: Henkilötietolaki käytännössä. Sanoma Pro Oy. 2011.

Viljanen, V-P.: Perusoikeusuudistus ja kansainväliset ihmisoikeussopimukset. Lakimies 5-6/1996. s. 788–815

Viljanen, V-P.: Yksityiselämän suoja (PL 10 §). Teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka: Perusoikeudet. WSOYpro Oy. Helsinki 2011. s. 389–412.

Viljanen, V-P.: Perusoikeuksien rajoittaminen. Teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka: Perusoikeudet. WSOYpro Oy. Helsinki 2011. s. 139–170

Viljanen, V-P.: Perusoikeuksien rajoitusedellytykset. Sanoma Pro Oy. Helsinki 2001.

Voutilainen, T.: ICT-oikeus sähköisessä hallinnossa. ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely. Edita Prima. Helsinki 2009.

Voutilainen, T.: Oikeus tietoon. Informaatio-oikeuden perusteet. Edita publishing. Porvoo 2012.

Wallin, A.R. – Nurmi, P.: Tietosuojalainsäädäntö – henkilörekisterilaki ja siihen liittyvät säädökset. Lakimiesliiton kustannus. Jyväskylä 1991.

Wallin, A-R.: Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnustettuina perusoikeuksina. Teoksessa Perusoikeudet EU:ssa. Toimittanut Liisa Nieminen. Lakimiesliiton kustannus. Helsinki 2001. s. 351–388.

Warren, S. – Brandeis, L.: The right to Privacy. Harvard Law Review. Vol. 4, No. 5. Massachusettes 1890. Artikkeli löytyy osoitteesta: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Wayman, J.L.: Biometrics – Now and Then: The development of biometrics over the last 40 years. Teoksessa H. Daum (ed.) Biometrics in the Reflection of Requirements: Second BSI Symposium on Biometrics 2004. SecuMedia, Bonn 2004.

Wayman, J.L.: Fundamentals of Biometric Technologies. Saatavilla osoitteessa: http://www.engr.sjsu.edu/biometrics/publications_tech.html.

Westin, A.: Privacy and Freedom. Atheneum. New York 1967.

Whitaker, R.: The End of Privacy. How Total Surveillance is Becoming a Reality. The New Press. New York 1999

Wickins J.: The Ethics of Biometrics. Science and Engineering Ethics Volume 13 N:o 1. Springer. 2007. s. 45–54.

Wilhelm, K.E.: Freedom of Movement at a Standstill? Toward the Establishment of a Fundamental Right to Intrastate Travel. Boston University Law Review Vol. 90. s. 2461–2497.

Wilhelmsson, T.: Social civilrätt: om behovsorienterade element i kontraktsrättens allmänna läror. Lakimiesliiton kustannus. Vammala 1987.

Wolf, S.: Shifting Paradigms in Bioethics and Health Law: The Rise of a New Pragmatism. American Journal of Law and Medicine 20:4. s. 395–415.

Zhu, B.: A Traditional Tort for a Modern Threat: Applying Intrusion Upon Seclusion to Dataveillance Observations. New York University Law Review. Vol 89. New York 2014. s. 2381–2415.

Virallislähteet

Euroopan Unioni

29 artiklan mukainen tietosuojatyöryhmä: Working Document on Biometrics. 12168/02/FI WP 80. Annettu 1.8.2003.

29 artiklan mukainen tietosuojaryhmä: Geneettisiä tietoja käsittelevä valmisteluasiakirja 12178/03/FI WP 91. Annettu 17.3.2004.

29 artiklan mukainen tietosuojatyöryhmä: Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. 1710/05/EN-rev WP 112 04/09/12. Annettu 29.12.2004.

29 artiklan mukainen tietosuojatyöryhmä: Opinion 3/2012 on developments in biometric technologies. 00720/12/EN WP193. Annettu 27.4.2012

Euroopan tietosuojavaltuutettu: Euroopan tietosuojavaltuutetun lausunto ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista annetun neuvoston asetuksen (EY) N:o 2252/2004 muuttamisesta 2008/C 200/01

Euroopan Komissio: Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla. KOM/2007/228FINAL

Euroopan Komissio: Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004, COM (2007) 619 final, COM(2007) 619 final.

Euroopan komissio: Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus). COM(2012) 11 final

Euroopan Parlamentti: Euroopan parlamentin lainsäädäntöpäätöslauselma komission ehdotuksesta neuvoston asetukseksi EU:n kansalaisten passien turvatekijöitä ja biometriikkaa koskevista vaatimuksista (KOM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)).

Joint Research Centre: Biometrics at the Frontiers: Assessing the Impact on Society. Helmikuu 2005.

Joint Research Centre: Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats. 2008.

Euroopan Neuvosto

Neuvoston puitepäätös 2008/977/YOS rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta

Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data (2013)

The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data – Propositions of Modernisation

Euroopan neuvoston suositus. Protection of personal data used for employment purposes; Rec n:o R (89) 2/18.1.1989

Suomi

Hallituksen esitykset

Hallituksen esitys (HE 84/1974 vp.) Eduskunnalle laeiksi 1) rikoslain 27 luvun, 2) painovapauslain 18 ja 39 §:n sekä 3) oikeudenkäytön julkisuudesta annetun lain 1 ja 2 §:n muuttamisesta

Hallituksen esitys (HE 49/1986 vp.) Eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi.

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

Hallituksen esitys (HE 6/1997 vp.) Eduskunnalle oikeudenkäyttöä, viranomaisia ja yleistä järjestystä vastaan kohdistuvia rikoksia sekä seksuaalirikoksia koskevien säännösten uudistamiseksi

Hallituksen esitys (HE 1/1998 vp.) Eduskunnalle uudeksi Suomen Hallitusmuodoksi

Hallituksen esitys (HE 96/1998 vp.) Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi

Hallituksen esitys (HE 75/2000 vp.) Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi

Hallituksen esitys (HE 93/2002 vp.) Eduskunnalle laiksi henkilötietojen käsittelystä poliisitoimessa ja eräiksi siihen liittyviksi laeiksi

Hallituksen esitys (HE 125/2003 vp.) Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi

Hallituksen esitys (HE 162/2003 vp.) Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta.

Hallituksen esitys (HE 234/2008 vp.) Eduskunnalle laiksi passilain ja eräiden siihen liittyvien lakien muuttamisesta

Hallituksen esitys (HE 36/2009 vp.) Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi

Hallituksen esitys (HE 146/2011 vp.) Eduskunnalle laiksi säteilylain ja terveydensuojelulain 50 §:n muuttamisesta

Hallituksen esitys (HE 32/2012 vp.) Eduskunnalle arvopaperimarkkinoita koskevaksi lainsäädännöksi

Hallituksen esitys (HE 66/2012 vp.) Eduskunnalle laeiksi henkilötietojen käsittelystä poliisitoimessa annetun lain ja henkilötietojen käsittelystä rajavartiolaitoksessa annetun lain sekä eräiden niihin liittyvien lakien muuttamisesta

Perustuslakivaliokunnan lausunnot ja mietinnöt

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 7/1997 Hallituksen esityksestä laiksi pakkokeinolain 5 a ja 6 luvun muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 11/1997 Hallituksen esityksestä laeiksi konkurssisäännön ja konkurssipesien hallinnon valvonnasta annetun lain 7 §:n muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 23/1997 Hallituksen esityksestä oikeudenkäyttöä, viranomaisia ja yleistä järjestystä vastaan kohdistuvia rikoksia sekä seksuaalirikoksia koskevien säännösten uudistamiseksi

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 33/1997 vp Hallituksen esityksestä passilain muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 14/1998 Hallituksen esityksestä laiksi poliisin henkilörekistereistä

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 17/1998 Hallituksen esitys laiksi rajavartiolaitoksesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 25/1998 Hallituksen esityksestä henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 27/1998 vp Hallituksen esityksestä laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 27/2000 vp Hallituksen esitys laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi.

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 39/2001 vp Hallituksen esityksestä työterveyshuoltolaiksi sekä laiksi työsuojelun valvonnasta

ja muutoksenhausta työsuojeluasioissa annetun lain 4 ja 11 §:n muuttamisesta
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 14/2002 vp Hallituksen esityksestä Kansaneläkelaitoksen toimeenpanemiin etuuksiin liittyviin tietojen saamista ja luovuttamista koskevien säännösten muuttamiseksi
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 51/2002 vp Hallituksen esityksestä laiksi henkilötietojen käsittelystä poliisitoimessa ja eräiksi siihen liittyviksi laeiksi
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 59/2002 vp Hallituksen esityksestä laeiksi sukusolujen ja alkioiden käytöstä hedelmöityshoidossa ja isyyslain muuttamisesta
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 10/2004 vp Hallituksen esityksestä laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 26/2004 vp Hallituksen esityksestä laiksi rikoslain 17 luvun, kokoontumislain ja järjestyksenvalvojista annetun lain 8 §:n muuttamisesta
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 35/2004 vp Valtioneuvoston kirjelmä ehdotuksesta neuvoston puitepäätökseksi (yleisesti saatavilla olevien sähköisen viestinnän palvelujen tarjoamiseen liittyvien ja sen yhteydessä käsiteltyjen ja tallennettujen tietojen ja julkisia viestintäverkkoja koskevien tietojen säilyttämisestä rikosten ja rikollisten tekojen, terrorismi mukaan lukien, torjumiseksi, tutkimiseksi ja selvittämiseksi ja niistä syytteeseen asettamiseksi)
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 13/2005 vp Hallituksen esityksestä laiksi Kansaneläkelaitoksen kuntoutusetuuksista ja kuntoutusrahaetuuksista
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 27/2005 vp Hallituksen esityksestä passilaiksi ja eräiksi siihen liittyviksi laeiksi
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 30/2005 vp Hallituksen esityksestä työntekijän eläkelaiksi ja eräiksi siihen liittyviksi laeiksi
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 5/2006 vp Hallituksen esityksestä laiksi lastensuojelulain muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 17/2006 vp Hallituksen esityksestä kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen ihmiskauppaa ja maahanmuuttajien salakuljetusta koskevien lisäpöytäkirjojen hyväksymisestä ja niiden lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain 20 luvun ja järjestyslain 7 ja 16 §:n muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 23/2006 vp Hallituksen esityksestä laeiksi ulkomaalaislain ja ulkomaalaisrekisteristä annetun lain 8 §:n muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 11/2008 vp Valtioneuvoston kirjelmä ehdotuksesta neuvoston puitepäätökseksi matkustajarekisterin käytöstä lainvalvontatarkoituksiin (matkustajarekisterin käyttö lainvalvontatarkoituksiin)

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 18/2008 vp Hallituksen esityksestä laiksi tilatukijärjestelmän täytäntöönpanosta annetun lain muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 19/2008 vp Hallituksen esityksestä laiksi Jokelan koulukeskuksessa sattuneiden kuolemaan johtaneiden tapahtumien tutkinnasta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 29/2008 vp Hallituksen esityksestä sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 32/2008 vp Hallituksen esityksestä laiksi terveydenhuollon ammattihenkilöistä annetun lain muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 14/2009 vp Hallituksen esityksestä laiksi passilain ja eräiden siihen liittyvien lakien muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 47/2010 vp Hallituksen esityksestä laeiksi ulkomaalaislain, ulkomaalaisrekisteristä annetun lain ja löytötavaralain muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 55/2010 vp Hallituksen esityksestä laiksi ulkomaalaislain muuttamisesta

PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 10/2012 vp Hallituksen esityksestä eduskunnalle biopankkilaiksi sekä laeiksi ihmisen elimien, kudoksien ja solujen lääketieteellisestä käytöstä annetun lain ja potilaan asemasta ja oikeuksista annetun lain muuttamiseksi
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 19/2012 vp Hallituksen esityksestä eduskunnalle henkilötietojen käsittelyä Rikosseuraamuslaitoksessa koskevaksi lainsäädännöksi
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 20/2014 vp Hallituksen vuosikertomus 2013
PERUSTUSLAKIVALIOKUNNAN LAUSUNTO 29/2014 vp Hallituksen esityksestä valtion talousarvioksi vuodelle 2015
PERUSTUSLAKIVALIOKUNNAN MIETINTÖ 25/1994 hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta

Hallintovaliokunnan lausunnot ja mietinnöt

HALLINTOVALIOKUNNAN LAUSUNTO 2/2001 vp Hallituksen esityksestä laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi
HALLINTOVALIOKUNNAN LAUSUNTO 30/2007 vp Hallituksen esityksestä Valtioneuvoston kirjelmä ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista (muutos)
HALLINTOVALIOKUNNAN MIETINTÖ 30/1997 vp Hallituksen esityksestä eduskunnalle laiksi poliisin henkilörekistereistä annetun lain muuttamisesta.
HALLINTOVALIOKUNNAN MIETINTÖ 13/2006 vp Hallituksen esityksestä passilaiksi ja eräiksi siihen liittyviksi laeiksi
HALLINTOVALIOKUNNAN MIETINTÖ 9/2009 vp Hallituksen esityksestä laiksi passilain ja eräiden siihen liittyvien lakien muuttamisesta
HALLINTOVALIOKUNNAN MIETINTÖ 36/2010 vp. Hallituksen esityksestä laiksi ulkomaalaislain muuttamisesta

Työelämä- ja tasa-arvovaliokunnan mietinnöt

TYÖELÄMÄ- JA TASA-ARVOVALIOKUNNAN MIETINTÖ (TyVM 8/2004 vp.) Hallituksen esityksestä (162/2003 vp.) laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta.

Komiteamietinnöt

Valtiosääntökomitean välimietintö KM 1974:27
Henkilötietotoimikunnan mietintö KM 1997:9

Eduskunnan oikeusasiamies

Eduskunnan oikeusasiamiehen kertomus toiminnastaan vuonna 1998

Tietosuojavaltuutetun oppaat

Henkilötietolain mukainen ilmoitusvelvollisuus
Tietosuoja suoramarkkinoinnissa
Rekisterinpitäjän yleinen informointivelvollisuus
Henkilörekisteriin talletettujen tietojen tarkastaminen

Tietosuojavaltuutetun toimisto

Katsaus toimintaan vuodelta 2002.

Valtioneuvosto

Valtioneuvoston periaatepäätös sähköisestä tunnistamisesta. 5.3.2009. Löytyy sähköisesti osoitteesta: http://www.valtioneuvosto.fi/tiedostot/julkinen/periaatepaatokset/2009/periaatepaatos-sahkoinen-tunnistaminen/145451.pdf (käyty 18.10.2014)

Työ- ja elinkeinoministeriö

Työelämän tietosuoja –opas.

Sisäministeriö

Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. Sisäasiainministeriön julkaisuja 32/2010. Helsinki 2010.

Selvitys passisormenjälkitietojen käyttämisestä vakavimpien rikosten torjunnassa. Arviomuistio. Sisäministeriön julkaisuja 20/2014. Helsinki 2014.

Oikeusministeriö

Lainkirjoittajan opas. Oikeusministeriön selvityksiä ja julkaisuja 37/2013.

Oikeusministeriön mietintö 27/2014. Tietoverkkorikosdirektiivin täytäntöönpano.

Ruotsi

Statens Offentliga Utredningar (SOU)

SOU 2002:18 Personlig integritet i arbetslivet

SOU 2002:110 Allmän kameraövervakning

SOU 2009:44 Lag om personlig integritet i arbetslivet

Belgia

Commissie voor de Bescherming van de Persoonlikje Levensfeer

Avis n° 17/2008 du 9 avril 2008: Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017)

Yhdysvallat

Federal Deposit Insurance Corporation: Privacy Rule Handbook (2001). Saatavilla osoitteessa: https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/index.html (Käyty 22.9.2014).

The United States Department of Justice: Overview of the Privacy Act of 1974 (2012 edition)

US Congress Office of Technology Assessment: Federal Government Information Technology: Management, Security, and Congressional Oversight (Helmikuu 1986)

Privacy Protection Study Commission: Personal Privacy in an Information Society (1977) Raportti saatavissa osoitteessa: http://epic.org/privacy/ppsc1977report/ (käyty 22.9.2014)

OECD

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

A Borderless World: Realising the Potential of Global Electronic Commerce.

Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)

Online Identity Theft

ILO

Työntekijöiden henkilötietojen suojaaminen.

Inter-American Juridicial Committee

OPINIÓN APROBADA POR EL COMITÉ JURÍDICO INTERAMERICANO SOBRE EL ALCANCE DEL DERECHO A LA IDENTIDAD

Oikeuskäytäntö

Euroopan ihmisoikeustuomioistuin:

Marckx v. Belgia No. 6833/74 (13.6.1979)

Airey v. Irlanti No. 6289/73 (9.10.1979)
X ja Y v. Alankomaat No. 8978/80 (25.3.1985)
Leander v. Ruotsi No. 9248/81 (26.3.1987)
Gaskin v. Yhdistynyt Kuningaskunta No. 10454/83 (7.7.1989).
B. v. Ranska No. 13343/87 (25.3.1992)
Costello-Roberts v. Yhdistynyt kuningaskunta No. 13134/87 (25.3.1993.)
Burghartz v. Sveitsi No. 16231/90 (22.2.1994)
Murray v. Yhdistynyt kuningaskunta No. 14310/88 (28.8.1994)
Kroon ym. v. Alankomaat No. 18535/91 (27.10.1994)
Stjerna v. Suomi No. 18131/91 (25.11.1994)
Friedl v. Itävalta No. 15225/89 (31.1.1995)
Z v. Suomi No. 22009/93 (25.2.1997)
Kopp v. Sveitsi No. 23224/94 (25.3.1998)
Rotaru v. Romania No. 28341/95 (4.5.2000)
P.G. ja J.H. v. Yhdistynyt Kuningaskunta No. 44787/98 (25.12.2001)
Schussel v. Itävalta. No. 42409/98 (21.2.2002) (julkaisematon, hylätty hakemus)
Pretty v. Yhdistynyt kuningaskunta No. 2346/02 (29.7.2002)
Peck v. Yhdistynyt Kuningaskunta No. 44647/98 (28.4.2003)
Perry v. Yhdistynyt Kuningaskunta No. 63737/00 (17.10.2003)
Odievre v. Ranska No. 42326/98 (13.2.2003)
M.C. v. Bulgaria No. 39272/98 (4.3.2004),
von Hannover v. Saksa No. 59320/00 (24.9.2004)
Sciacca v. Italia No. 50774/99 (11.1.2005)
S. ja Marper v. Yhdistynyt Kuningaskunta No. 30562/04 ja 30566/04 (4.12.2008)
Gillan ja Quinton v. Yhdistynyt kuningaskunta No. 4158/05 (28.6.2010).
M.M. v. Yhdistynyt kuningaskunta (13.11.2012)
Peruzzo ja Martens v. Saksa (4.6.2013)
M.K. v. Ranska No. 19522/09 (18.7.2013)

Euroopan unionin tuomioistuin

Bodil Lindqvist (C-101/01, 6.11.2003)

Euroopan komissio v. Saksa (C-581/07, 9.3.2010)
Michael Schwartz (C-291/12, 17.10.2013).
Willems (C-446/12-C-449/12, 16.4.2015)

Suomi

Korkein oikeus

KKO 1993:12
KKO 1994:62
KKO: 1998:85
KKO 1999:110
KKO 2005:82

Korkein hallinto-oikeus

KHO 27.9.2013/3084 (Dnro 1025/2/122) Antopäivä 27.9.2013
KHO 2006:18
KHO 2012: 51
KHO 2015:145

Tietosuojalautakunta

Tietosuojalautakunnan ratkaisu 5/04 (Dnro 9/932/2004)
Tietosuojalautakunnan ratkaisu 2/2009 (Dnro 1/933/2008)
Tietosuojalautakunnan ratkaisu 1/10 (Dnro 2/932/2009)
Tietosuojalautakunnan ratkaisu 4/2010 (Dnro 1/933/2010, 4/932/2010)

Tietosuojavaltuutetun ratkaisut

Henkilötietojen käsittely opiskelijoiden läsnäolon kirjaamisessa (Dnro 236/41/2006)
Henkilötietojen kerääminen internetistä hakukoneen avulla ns. Googlaamalla työnantajan toimesta ja tietojen poistaminen google-hakukoneesta (Dnro 626/452/2006).

Internetin käytön ja työntekijöiden verkkoselailun eli ns. verkkosurffailun valvonta työpaikalla (julkaistu 27.1.2014)

Työtuomioistuin

TT 1999–31
TT 2001–60

Eduskunnan oikeusasiamiehen ratkaisut

EAOA Petri Jääskeläisen 8.6.2009 antama päätös: Lentoaseman turvatarkastuksissa otettava huomioon perustuslain vaatimukset yksityisyyden suojasta. Dnrot 1242/4/07, 1447/2/07, 1223/2/08

EAOA Jussi Pajuojan 26.4.2012 antama päätös: Ihmisarvoinen kohtelu ja vähimmän haitan periaate koskevat myös viranomaisen tiedottamista. Dnro 2893/2/11

EAOA Jussi Pajuojan 20.9.2012 antama päätös: Valokuvaaminen Kelan toimistossa. Dnro 1140/4/11.

EOA Riitta-Leena Paunion 23.1.2006 antama päätös: Asiamiehen käyttäminen potilastietojen tarkastamisessa. Dnro 2022/4/04

Ruotsi

Kammarrätten i Stockholm

Kammarrättens i Stockholm dom 2005-11-01.

Datainspektionen

Samråd enligt personuppgiftslagen (1998:204) Dnro 84-2006

Tillsyn enligt personuppgiftslagen (1998:204) – användning av biometri inom arbetslivet. Dnro 1765-2009.

Norja

Personvernnemnda

PVN-2005-12: Klage på vedtak om begrensninger i adgangen til kameraovervåking av bussenes publikumsområder. Personvernnemndas avgjørelse av 2. august 2006 (Jon Bing, Gro Hillestad Thune, Hanne Bjurstrøm, Tom Bolstad, Jostein Halgunset, Tore Hauglie, Leikny Øgrim)

PVN-2006-11 REMA 1000 - fingeravtrykk ved registrering av timer. Personvernnemndas avgjørelse av 9. mars 2007 (Jon Bing, Gro Hillestad Thune, Leikny Øgrim, Siv Bergit Pedersen, Jostein Halgunset, Hanne I Bjurstrøm, Tom Bolstad)

PVN-2011-12: Adgangskontroll ubetjent treningssenter Klage på Datatilsynets pålegg om at Fitness24Seven må avslutte enhver bruk av fingeravtrykk eller andre biometriske kjennetegn i forbindelse med adgangskontroll. Personvernnemndas avgjørelse av 18. april 2012 (Eva I. E. Jarbekk, Arve Føyen, Tom Bolstad, Leikny Øgrim, Gisle Hannemyr, Jostein Halgunset, Ørnulf Rasmussen).

Yhdysvallat

McCarthy v. Arndstein 266 U.S. 34 (1924)
Olmstead v. United States 277 U.S. 438 (1928)
Sidis v. F-R Publishing Corp. 113 F.2d 806 (1940)
Brinegar v. United States 338 U.S. 160 (1949)
Thompson v. Coles-up, Inc. 98 N.Y.S.2d 300 (1950)
Haelan Laboratories v. Topps Chewing Gum, Inc. 202 F.2d 866 (1953)
New York Times Co. v. Sullivan 376 U.S. 254 (1964)
Griswold v. Connecticut 381 U.S. 479 (1965)
Schmerber v. California 384 U.S. 757 (1966)
United States v. Chibarro 361 F. 2d 365 (1966)
Katz v. U.S. 389 U.S. 347 (1967)
Berger v. New York 388 U.S. 41 (1967)

Time, Inc. v. Hill U.S. 374 (1967)
Terry v. Ohio 392 U.S. 1 (1968)
Davis v. Mississippi 394 U.S. 721 (1969)
Thom v. New York Stock Exchange 306 F.Supp. 1002 (1969)
People v. Stuller 10 Cal.App.3d 582 (1970).
Nader v. General Motors Corp. 255 N.E.2d 765 (1970).
Dietermann v. Time, Inc. 449 F.2d 245 (1971)
United States v. Doe 457 F.2d 895 (1972)
Napolitano v. Ward 457 F.2d 279 (1972).
U.S. v. Dionisio 410 U.S. 1 (1973)
United States v. Davis 482 F. 2d 893 (1973)
United States v. Edwards 415 U.S. 800 (1974)
Brown v. Brannon 399 F Supp 133 (1975)
Cox Broadcasting Co. v. Cohn 420 U.S. 469 (1975)
Gibert v. California 388 U.S. 263 (1976)
Whalen v. Roe 429 U.S. 589 (1977)
Rakas et al. v. Illinois 439 U.S. 128 (1978)
Dunaway v. New York 442 U.S. 200 (1979)
Cefalu v. Globe Newspaper Co. 391 N.E.2d 935, 939 (1979)
Hirsch v. S.C. Johnson, Inc. 280 N.W.2d 129 (1979)
U.S. v. Mendenhall 446 U.S. 544 (1980)
U.S. v. Knotts 460 U.S. 276 (1983)
Carson v. Here´s Johnny Portable Toilets 698 F.2d 831 (1983)
Kolender v. Lawson 461 U.S. 352 (1983)
Michigan v. Clifford 464 U.S. 287 (1984).
Braun v. Flynt 726 F.2d 245 (1984)
Michigan v. Clifford 464 U.S. 287 (1984)
New York v. Quarles 467 U.S. 649 (1984)
Sipple v. Chronicle Publishing Co. 154 Cal. App. 3d 1040 (1984)
McSurely v. McClellan 753 F.2d 88 (1985)
Humpher v. First Interstate Bank of Oregon 696 P.2d 527 (1985)
Morrell v. Forbes, Inc. 603 F. Supp. 1305 (1985)
Perkey v. Department of Motor Vehicles 42 Cal.3d 185 (1986)

Griffin v. Wisconsin 483 U.S. 868 (1987)
O´Connor v. Ortega 480 U.S. 709 (1987)
Times-Mirror Co. v. Superior Court 198 Cal. App. 3d 1420 (1988)
Midler v. Ford Motor Co. 849 F.2d 460 9th Cir. (1988)
Godbehere v. Phoenix Newspaper, Inc. 783 P.2d 781, 787 (1989)
United States Department of Justice v. Reporters Committee for Freedom of the Press 489 U.S. 749 (1989)
Skinner v. Railway Labour Executives Association 489 U.S. 602 (1989)
Finger v. Omni Publications International, Ltd. 566 N.E.2d 141 (1990).
Moore v. Regents of the University of California 793 P.2d 479 1990)
Florida v. Bostick 501 U.S. 429 (1991)
Waits v. Firto-lay, Inc. 978 F.2d 1098 (1992)
Minnesota v. Dickerson 508 U.S. 366 (1993)
Cain v. Hearst Corporation d/b/a the Houston Chronicle Publishing Company 878 S.W.2d 577 (1994)
McIntyre v. Ohio Elections Commission 514 U.S. 334 (1995)
Vernonia Scool District 477 v. Acton 515 U.S. 646 (1995)
Summers v. Bailey 55 F.3d 1564 (1995)
Dwyer v. Am. Express Co. 652 N.E.2d 1351 (1995)
Abdul-Jabbar v. General Motors Corp. 85 F.3d 407 (1996)
Chandler v. Miller 520 U.S. 305 (1997)
Hart v. Seven Resorts, Inc. 947 P.2d 846, 854 (1997)
Lake v. Wal-Mart 582 N. W.2d 231(1998)
Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1069 (1998)
Weld v. CVS Pharmacy, Inc. 11 Mass L Rep 21 (1999)
Weld v. CVS Pharmacy, Inc. 454 Mass. 1107 (2009)).
Taylor v. Nationsbank N.A. 78 A.2d 893 (1999)
Sanders v. ABC 978 P.2d 67 (1999)
Fanelle v. Lojack corp. 79 F.Supp.2d 558 (2000)
Kyllo v. United States 533 U.S. 27 (2001)
Board of Education v. Earls 536 U.S. 822 (2002)
Carey v. Nevada Gaming Control Board 279 F.3d 873 (2002)
Bodah v. Lakeville Motor Express, Inc. 663 N.W. 2d 550 (2003)

Messing v. Bank of America N.D. 373 Md. 672, 821 A.2d 22 (2003)
Doe 2 v. Associate Press 331 F.3d 417 (2003)
Busse v. Motorola, Inc. 813 N.E.2d 1013 (2004)
Hiibel v. Sixth Judicial District Court 542 U.S. 177 (2004)
Schuchart v. La Taberna del Alabardero, Inc. 365 F.3d 33 (2004)
State v. Bauman 275 Wis. 2d 278 (2004)
U.S. v. Garcia-Beltran 443 F. 3d 1126 (2006)
U.S. v. Olivares-Rangel 458 F. 3d 1104 (2006)
Miller v. Collectors Universe, Inc. 159 Cal. App. 4th 988 (2008)
Jews for Jesus, Inc. v. Rapp 997 So.2d 1098 (2008)
Weld v. CVS Pharmacy, Inc. 454 Mass. 1107 (2009)
Flores-Figueroa v. U.S. 556 U.S. 646 (2009)
Boring v. Google 38 Media L.Rep. 1306 (2010)
Anderson v. Blake 469 F.3d 910 (2011)
U.S. v. Ozuna-Cabrera 663 F.3d 496 (2011)
U.S. v. McCarty 648 F. 3d 820, (2011)
Electronic Privacy Information Center v. United States Department of Homeland Security 653 F.3d 1 (2011)
U.S. v. Jones 615 F. 3d 544 (2012)
People v. Buza 129 Cal.Rptr.3d 753 (2013)
Maryland v. King 133 S.Ct. 1 (2013)
U.S. v. Meza No. 12–cr–00386–MSK (2014)

Verkkosivut

Surveillance Studies Network. The International Research and Information Network on Surveillance: An Introduction to the Surveillance Society. Saatavissa osoitteesta: http://www.surveillance-studies.net/?page_id=119.(käyty 15.7.2014)