SÄHKÖINEN TUNNISTAMINEN TIETOSUOJA– JA TIETOTURVALLISUUSSÄÄNTELYN TOTEUTTAJANA INFORMAATIOHALLINNOSSA

Janne Rintamäki
Lapin yliopisto
Oikeustieteiden tiedekunta
Oikeusinformatiikka
Maisteritutkielma
2018

Lapin yliopisto, oikeustieteiden tiedekunta
Työn nimi: Sähköinen tunnistaminen tietosuoja- ja tietoturvallisuussääntelyn toteuttajana informaatiohallinnossa
Tekijä: Janne Rintamäki
Opetuskokonaisuus ja oppiaine: Oikeusinformatiikka
Työn laji: Tutkielma X Laudaturtyö__ Lisensiaatintyö__ Kirjallinen työ__
Sivumäärä: XIV + 81
Vuosi: 2018

Tiivistelmä:

Tutkielmassa tarkastellaan sähköistä tunnistamista tietosuoja- ja tietoturvallisuussääntelyn toteuttajana osana nykyaikaisen informaatiohallinnon monitasoista sääntelyä. Tutkimuksessa käsiteltävä sähköinen tunnistaminen on keskeinen osa tietoturvallisuuden toteuttamista. Sähköisessä tunnistamisessa on kyse sähköisen identiteettimme käyttämisestä ja siten henkilötietojen käsittelystä, jonka vuoksi huomioon on otettava myös tietosuojakysymykset. Tutkimusmetodina on oikeusdogmatiikka, jonka tarkoituksena on voimassa olevan oikeuden sisällön tutkiminen ja selvittäminen.

Vahva sähköinen tunnistaminen on Suomessa toteutettu pitkälti markkinaehtoisesti ja yleisimmät tunnistusvälineet ovat niin sanotut pankkitunnisteet. Pankkitunnisteiden asemaan markkinoilla voi kuitenkin liittyä esimerkiksi niiden saatavuuteen, käytön hinnoitteluun tai turvallisuuteen liittyviä ongelmia. Sähköisen tunnistamisen kenttä on ollut muutosten kohteena viime vuosina ja Euroopan unionin muuttunut sääntely on esitellyt uuden, rajat ylittävän sähköisen tunnistamisen käsitteen. Rajat ylittävässä sähköisessä tunnistamisessa tarkoituksena on tunnustaa vastavuoroisesti toisessa jäsenvaltiossa myönnetyn vahvan sähköisen tunnistamisen välineellä tehty tunnistautuminen toisen jäsenvaltion julkishallinnon sähköisessä asiointipalvelussa.

Tutkimuksen johtopäätöksinä todetaan, että informaatiohallinnon ja tietoturvallisuuden sääntelykokonaisuudet ovat varsin laajoja. Tietoturvallisuus on osa hyvää informaatiohallintoa ja sillä on keskeinen rooli perusoikeuksiemme turvaajana. Voimassa oleva sääntely koskee vain vahvaa sähköistä tunnistamista. Vaikka yleisesti käytetty heikko sähköinen tunnistaminen jää tunnistamissääntelyn ulkopuolelle, eivät sitä hyödyntävät palvelut toimi sääntelytyhjiössä, vaan niitä säännellään esimerkiksi henkilötietojen suojaa ja viranomaisen asiakirjojen julkisuutta sekä tietoturvallisuutta koskevin säädöksin.

Avainsanat: oikeusinformatiikka, informaatiohallinto, tietosuoja, tietoturvallisuus, sähköinen identiteetti, sähköinen tunnistaminen, sähköinen asiointi

Muita tietoja:

Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön X
Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi X
Suostun tutkielman luovuttamiseen Lapin maakuntakirjastossa käytettäväksi__
(vain Lappia koskevat)

SISÄLLYS

LÄHTEET

Kirjallisuus:

Aarnio, Aulis: Tulkinnan taito – ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. WSOY. Vantaa 2006.

Andersson, Jenna: Organisaation tietoturva- ja tietosuojariskienhallinta sekä lainsäädännön vaatimukset. Edilex 2018/4. Saatavissa: https://www.edilex.fi/artikkelit/18528 [käyty 28.2.2018].

Bygrave, Lee A.: Data Protection Law, Approaching Its Rationale, Logic and Limits. Information Law Series 10. Kluwer Law International. Great Britain 2002.

Bragg, Roberta: Data Security Architecture. Teoksessa: Bragg – Rhodes Ousley – Strassberg et al. Network Security: The Complete Reference. McGraw-Hill/Osborne. California 2004.

van Dijk, Jan: The Network Society. 3rd edition. SAGE Publications Ltd 2012.

Eriksen, Amund: Rettsregler og informasjonsikkerhet – noen utviklingsstrekk. Teoksessa: Informasjonssikkerhet, Retsslige krav til sikker bruk av IKT (s. 24 – 60), red. Arild Jansen og Dag Wiese Schartum. Fagbokforlaget 2005.

Hakala, Mika – Vainio, Mika – Vuorinen, Olli: Tietoturvallisuuden käsikirja. Docendo Finland Oy. Sanoma WSOY-konserni. WS Bookwell. Porvoo 2006.

Hanninen, Minna – Laine, Elli – Rantala, Kati – Rusi, Mari – Varhela, Markku: Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Kauppakamari. Vantaa 2017.

Hirvonen, Ari: Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisiä oikeustieteen julkaisuja 17. Helsinki 2011. Saatavissa https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf [käyty 20.3.2018].

Jansen, Arild – Skagestein, Gerhard: Sikkerhet i informasjonssystemer og infrastrukturer. Teoksessa: Informasjonssikkerhet, Retsslige krav til sikker bruk av IKT (s. 61 – 77), red. Arild Jansen og Dag Wiese Schartum. Fagbokforlaget 2005.

Korhonen, Rauno: Perusrekisterit ja tietosuoja. Edita Publishing Oy. Sähköinen versio. Edita Prima Oy. Helsinki 2003. Saatavissa: https://www.edilex.fi/kirjat/1126.pdf [käyty 10.4.2018].

Korhonen, Rauno: Sähköinen asiointi ja viestintä julkisella sektorilla. Teoksessa: Oikeus tänään osa 1 (s. 274 – 379). Neljäs uudistettu painos, toim. Marja-Leena Niemi. Lapin yliopiston oikeustieteellisiä julkaisuja, sarja C 64. Rovaniemi 2016.

Korja, Juhani: Biometrinen tunnistaminen ja henkilötietojen suoja, Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta. Lapin yliopisto. PDF -versio. Acta electronica Universitatis Lapponiensis 193. Rovaniemi 2016. Saatavissa http://lauda.ulapland.fi/bitstream/handle/10024/62397/Korja_Juhani_ActaE_193_pdfA.pdf?sequence=2&isAllowed=y [käyty 26.9.2017].

Laine, Juha: Kirja-arvostelu teoksesta Ponka Ilja: Sähköinen tunnistaminen ja allekirjoitus Suomen velvoiteoikeudessa. Lakimies 2/2014 (s. 612 – 630). Saatavissa: https://www.edilex.fi/lakimies/13618 [käyty 16.1.2018].

Magnusson Sjöberg, Cecilia – Nordbeck, Peter – Nordén, Anna – Westman, Daniel: Rättsinformatik. Inblickar I e-samhället, e-handel och e-förvaltning. Studentlitteratur AB. Estonia 2011.

Mayer-Schönberger, Viktor(toim.) – Lazer, David(toim.): Governance and Information Technology. From Electronic Government to Information Government. The MIT Press. Massachusetts Institute of Technology. USA 2007.

Mäenpää, Olli: Yleinen hallinto-oikeus. Alma Talent. Helsinki 2017.

Murray, Andrew: Information Technology Law. The Law and Society. Second edition. Oxford university press. Oxford, UK 2013.

Neuvonen, Riku: Viestintä- ja informaatio-oikeuden perusteet. Lakimiesliiton kustannus. Meedia Zone OÜ. Viro 2013.

Neuvonen, Riku: Yksityisyyden suoja Suomessa. Lakimiesliiton kustannus. Meedia Zone OÜ. Viro 2014.

Pihlajamäki, Antti: Tietojenkäsittelyrauhan oikeudellinen suoja. Datarikoksia koskeva sääntely Suomessa. Suomalaisen lakimiesyhdistyksen julkaisuja. A-sarja N:o 258. Helsinki 2004.

Pitkänen, Olli – Tiilikka, Päivi – Warma, Eija: Henkilötietojen suoja. Sähköinen versio Alma Talent verkkokirjahylly -palvelussa. Alma Talent Oy 2013.

Ponka, Ilja: Sähköinen tunnistaminen ja allekirjoitus Suomen velvoiteoikeudessa. Helsingin yliopisto, oikeustieteellinen tiedekunta. Unigrafia Oy. Helsinki 2013.

Pönkä, Ville – Parkkali, Leena: Pikaluottojen oikeudelliset ongelmat. Defensor Legis N:o 5/2010 (s. 585 – 605). Saatavissa: https://www.edilex.fi/defensor_legis/7396.pdf [käyty 28.2.2018].

Pöysti, Tuomas: Tehokkuus, informaatio ja eurooppalainen oikeusalue. Forum Iuris. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki 1999.

Pöysti, Tuomas: Sisäinen tarkastus valtionhallinnossa ja tietoturvallisuuden hallinta. Teoksessa: Tietoturvallisuus ja laki. Pohjois-Suomen tuomarikoulun julkaisuja 2/2002 (s. 233 – 262). Lapin yliopistopaino. Rovaniemi 2002.

Rhodes-Ousley, Mark: Network Security Overview. Teoksessa: Bragg – Rhodes Ousley – Strassberg et al. Network Security: The Complete Reference. McGraw-Hill/Osborne. California 2004.

Råman, Jari: Tietoturvallisuus on myös perusoikeus. Lakimies 5/2006 (s. 818 – 824). Saatavissa: https://www.edilex.fi/lakimies/3759 [käyty 6.2.2018].

Saarenpää, Ahti: Oikeusinformatiikka. Teoksessa: Oikeus tänään osa 1 (s. 67 – 273). Neljäs uudistettu painos, toim. Marja-Leena Niemi. Lapin yliopiston oikeustieteellisiä julkaisuja, sarja C 64. Rovaniemi 2016.

Saarenpää, Ahti: Personrätt – integritetsrätt. Teoksessa: Finlands civil- och handelsrätt. En introduktion, 4 reviderade upplagan, toim. Johan Bärlund, Frey Nybergh och Katarina Petrell. Sähköinen versio Alma Talent verkkokirjahylly -palvelussa. Alma Talent Oy 2013.

Saarenpää, Ahti(toim.) – Pöysti, Tuomas(toim.) – Sarja, Mikko – Still, Viveca – Balboa-Alcoreza, Ruxandra: Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Tutkimusraportti. Valtiovarainministeriö, Hallinnon kehittämisosasto. Lapin yliopiston oikeusinformatiikan instituutti. Edita Oy. Helsinki 1997.

Soininen, Heidi: Identiteettivarkaus kyberrikoksena – termit ja tunnusmerkistö. Defensor Legis N:o 1/2017 (s. 84 – 101). Saatavissa: https://www.edilex.fi/defensor_legis/17540.pdf [käyty 8.5.2018].

Voutilainen, Tomi: Hyvä sähköinen hallinto. Edita Publishing. Helsinki 2006.

Voutilainen, Tomi: ICT-oikeus sähköisessä hallinnossa – ICT oikeudelliset periaatteet ja sähköinen hallintomenettely. Edita Publishing Oy. Helsinki 2009.

Voutilainen, Tomi: Palveluarkkitehtuuria tukeva lainsäädäntö. Tutkimusraportti. Valtiovarainministeriön julkaisuja 22/2014, elokuu 2014. Juvenes Print – Suomen Yliopistopaino Oy 2014. PDF-versio. Saatavissa: http://vm.fi/julkaisut/julkisen-hallinnon-ict [käyty 11.10.2017].

Voutilainen, Tomi: Sähköisen identiteetin käytöstä julkisessa hallinnossa. Referee-artikkeli. Edita Publishing 2008. Saatavissa: https://www.edilex.fi/artikkelit/5227? [käyty 12.1.2018].

Virallislähteet:

HE 9/2018 vp Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

HE 159/2017 vp Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä sekä eräiksi siihen liittyviksi laeiksi.

HE 74/2016 vp Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta sekä eräiksi siihen liittyviksi laeiksi.

HE 59/2016 vp Hallituksen esitys eduskunnalle laeiksi hallinnon yhteisistä sähköisen asioinnin tukipalveluista sekä yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain muuttamisesta.

HE 272/2014 vp Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta.

HE 36/2009 vp Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi.

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

PeVL 16/2009 vp Perustuslakivaliokunnan lausunto. Hallituksen esitys laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi.

LiVM 17/2017 vp Liikenne- ja viestintävaliokunnan mietintö. Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta.

LiVM 18/2016 vp Liikenne- ja viestintävaliokunnan mietintö. Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta sekä eräiksi siihen liittyviksi laeiksi.

Ratkaisujen Suomi. Pääministeri Juha Sipilän hallituksen strateginen ohjelma 29.5.2015. Hallituksen julkaisusarja 10/2015. Edita Prima 2015. Saatavissa: http://valtioneuvosto.fi/documents/10184/1427398/Ratkaisujen+Suomi_FI_YHDISTETTY_netti.pdf/801f523e-5dfb-45a4-8b4b-5b5491d6cc82 [käyty 26.1.2018].

Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). COM (2017) 10 final. Bryssel 10.1.2017. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52017PC0010&qid=1525328653778&from=FI [käyty 20.3.2018].

Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Digitaalisten sisämarkkinoiden strategia Euroopalle. COM (2015) 192 final. Bryssel 6.5.2015. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1517828385049&uri=CELEX:52015DC0192 [käyty 5.2.2018].

Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Digitaalisten sisämarkkinoiden strategian täytäntöönpanon väliarviointi. Yhdennetyt digitaaliset sisämarkkinat kaikille. COM (2017) 228 final. Bryssel 10.5.2017. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1517829434967&uri=CELEX:52017DC0228 [käyty 5.2.2018].

Komission tiedonanto Euroopan parlamentille ja neuvostolle. Vahvempi suoja, uudet mahdollisuudet – komission ohjeet yleisen tietosuoja-asetuksen suorasta soveltamisesta 25. toukokuuta 2018 lähtien. COM (2018) 43 final. Bryssel 24.1.2018. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1522066139198&uri=CELEX:52018DC0043 [käyty 26.3.2018].

Finanssivalvonta Standardi 2.4. Asiakkaan tunteminen – rahanpesun ja terrorismin rahoittamisen estäminen. Määräykset ja ohjeet. Saatavissa http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/2.4.std6.pdf [käyty 5.4.2018].

Muut lähteet:

Ailisto, Heikki(toim.) – Collin, Jari(toim.) – Juhanko, Jari(toim.) – Mäntylä, Martti(toim.) – Ruutu, Sampsa(toim.) – Seppälä, Timo(toim.) – Halén, Marco – Hiekkanen, Kari – Hyytinen, Kirsi – Kiuru, Eeva – Korhonen, Heidi – Kääriäinen, Jukka – Parviainen, Päivi – Talvitie, Jaakko: Onko Suomi jäämässä alustatalouden junasta? Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 19/2016. Valtioneuvoston kanslia 20.4.2016. Saatavissa: http://tietokayttoon.fi/documents/10616/2009122/19_Onko+Suomi+j%C3%A4%C3%A4m%C3%A4ss%C3%A4+alustatalouden+junasta.pdf/5e1f46ed-415c-4763-a530-633309eafb77?version=1.0 [käyty 23.5.2018].

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) loppumietintö. Oikeusministeriön julkaisu 8/2018. Helsinki 2018. Saatavissa: http://julkaisut.valtioneuvosto.fi/handle/10024/160626 [käyty 24.5.2018].

Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. Sisäasiainministeriön julkaisuja 32/2010. Helsinki 2010. Saatavissa: http://julkaisut.valtioneuvosto.fi/handle/10024/79876 [käyty 6.2.2018].

IDC: EMC Digital Universe with Research & Analysis by IDC. The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. April 2014. Saatavissa: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm [käyty 20.3.2018].

Kansallisen palveluarkkitehtuurin toteuttamisohjelma (KaPA) 2014 – 2017. Loppuraportti. Valtiovarainministeriön julkaisu 7/2018. Saatavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160710/VM_07_2018.pdf?sequence=1&isAllowed=y [käyty 9.4.2018].

Katakri 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Saatavissa: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointity-okalu_viranomaisille.pdf [käyty 6.4.2018].

Pankkien Tupas -tunnistuspalvelun tunnistusperiaatteet. V 2.0c. 2.12.2013. Finanssialan Keskusliitto. Saatavissa: http://www.finanssiala.fi/maksujenvalitys/Sivut/Sahkoinen-tunnistaminen.aspx [käyty 9.4.2018].

Porvoo Group. The international Porvoo Group supports the deployment of electronic identity in Europe. Saatavissa: https://eevertti.vrk.fi/en/porvoo-group [käyty 29.5.2018].

Suomen Asianajajaliitto. Hyvää asianajajatapaa koskevat ohjeet (2.10.2012/540) B 05.1 Tietoturvallisuusohje ja B 05.2 Tietoturvaopas. Saatavissa: Asianajoalan tietopankki Aada https://www.asianajajaliitto.fi/asianajajaliitto/tieto-pankki_aada?s=693&type=1&text_search=&search= [käyty 13.4.2018].

Sähköisen asioinnin tietoturvallisuus -ohje. Valtiovarainministeriön julkaisuja 25/2017. Julkisen hallinnon ICT. Helsinki 2017. Saatavissa: https://www.vah-tiohje.fi/web/guest;jsessio-nid=68E518A8E63C00825110DFEA34762E154294F56A70D14BF3094942445110C47EDB54130EE4EC215D1944CE [käyty 6.4.2018].

Valtiovarainministeriö. Tietohallinnon ohjaus -sivusto. Saatavissa: http://vm.fi/tietohal-linnon-ohjaus [käyty 24.5.2018].

Viestintävirasto. *Ajankohtaista 2018*. TUPAS-tunnistamista käyttäviltä asiointipalve-luilta edellytetään muutoksia. Julkaistu 10.4.2018. Saatavissa: https://www.viestintavi-rasto.fi/viestintavirasto/ajankohtaista/2018/tupas-tunnistamistakayttaviltaasiointipalve-luiltaedellytetaanmuutoksia.html [käyty 10.4.2018].

Liikenne- ja viestintäministeriö. Tiedote 7.5.2018. Yhteiskunnan keskeisten palvelujen tietoturvallisuutta kasvattavat lakimuutokset voimaan. Saatavissa: https://www.lvm.fi/-/yhteiskunnan-keskeisten-palvelujen-tietoturvallisuutta-kasvattavat-lakimuutokset-voi-maan-971405 [käyty 8.5.2018].

Reinboth, Susanna: Auer-urkinnasta syytetyt poliisit oikeudessa. Helsingin Sanomat 6.9.2016 s. A13. Helsinki 2016.

Oikeustapaukset:

KKO 2016:73

KKO 2014:86

KHO 2017:19

KHO 2016:216

KHO 8.1.2010, taltionumero 15, diaarinumero 1568/1/09

LYHENTEET:

art.	artikla
EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
EU	Euroopan unioni
EUVL	Euroopan unionin virallinen lehti
EYVL	Euroopan yhteisöjen virallinen lehti
FIVA	Finanssivalvonta
HE	hallituksen esitys
ICT	Information and Communication Technology, suom. tieto- ja viestintäteknologia
KHO	Korkein hallinto-oikeus
KKO	Korkein oikeus
LiVM	Liikenne- ja viestintävaliokunnan mietintö
PeVL	Perustuslakivaliokunta
SEU	Euroopan unionista tehty sopimus
STM	Sosiaali- ja terveysministeriö
USA	Amerikan Yhdysvallat
ViVi	Viestintävirasto
VM	Valtiovarainministeriö
VnA	Valtioneuvoston asetus
vp	valtiopäivät
VRK	Väestörekisterikeskus
VTJ	väestötietojärjestelmä

1 Johdanto

1.1 Tausta

Elämme informaatiorikkaassa maailmassa. Voidaan ehkä puhua jopa informaatiokeskeisestä maailmankuvasta, sillä siinä määrin data ja informaatio ohjaavat niin tiedettä, taloutta, politiikkaa kuin lähes kaikkea yksilöiden toimintaa ja inhimillisen elämän osa-alueita. Datan määrä on kasvanut räjähdysmäisesti ja tutkimusyhtiö *IDC* arvioi datan määrän maailmassa vuonna 2020 saavuttavan 44 zettatavun lukeman.[1] Data on raaka-aineena tietojärjestelmissä ja tietokannoissa. Tästä raaka-aineesta voidaan luoda erilaisia tietotuotteita ja informaatioyhteiskunnan palveluita lukuisiin tarpeisiin. Dataa ja siitä edelleen jalostettua informaatiota hyödynnetään monin eri tavoin sekä yksityisellä että julkisella sektorilla. Informaatiota hyödynnetään viranomaisten omaa toimintaa koskevassa päätöksenteossa sekä yksittäisen kansalaisen kannalta häntä koskevassa hallinnollisessa päätöksenteossa. Edelleen tietotuotteita käytetään yksityisen sektorin liiketoiminnassa joko päätöksenteon tukena tai omien palvelutuotteiden valmistamisessa. Informaation taloudellista merkitystä ei voi aliarvioida.

Tietoverkkojen ja niiden välityksellä käytettävien palveluiden käytöstä on tullut elämäämme määrittävä tekijä. Tietoverkoista ovat riippuvaisia sekä yksilöt että organisaatiot. Tietoverkkoinfrastruktuurista on tullut kriittinen elementti, ja esimerkiksi *van Dijk* kutsuukin nyt elämäämme aikakautta tietoverkkojen aikakaudeksi.[2] Hän pitää myös digitalisaatiota keskeisenä yhdistävänä rakenteellisena tekijänä, tosin kuvaten sen melko suppeasti vain viestinvälityksen muuttumisena analogisesta digitaaliseksi.[3] Esimerkiksi tutkimusyhtiö *Gartner* määrittelee sanastossaan digitalisaation (engl. digitalization) prosessiksi, jossa hyödyntämällä digitaalista teknologiaa muutetaan liiketoimintamalleja uusien tuottojen ja arvonlisäyksen mahdollistamiseksi.[4]

---

[1] https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm .
[2] *van Dijk* 2012, s. 2.
[3] *van Dijk* 2012, s. 50.
[4] Ks. http://www.gartner.com/it-glossary/digitalization .

Juridisessa mielessä tietoverkkoympäristö on kaikkea muuta kuin ongelmaton.[5] Tämä käy hyvin ilmi esimerkiksi siitä laajasta sääntelykokonaisuudesta, joka koskee sähköisiä palveluita eri muodoissaan. Tähän kokonaisuuteen voidaan lukea kuuluvaksi niin henkilötietojen suojaa, sähköistä tunnistamista ja allekirjoittamista, kuin lukuisat muutkin informaatiohallintoa ja -infrastruktuuria koskevat säädökset.

Digitalisaation edistäminen on huomioitu meillä Suomessa pääministeri *Sipilän* hallitusohjelmassa, jossa yhtenä kärkihankkeista on julkisten palveluiden digitalisointi ja palveluiden rakentaminen käyttäjälähtöisiksi. Ylätason toimenpiteinä tavoitteen konkretisoimiseksi ohjelmassa esitetään digitaalisen liiketoiminnan kasvuympäristön rakentaminen, säädösten sujuvoittaminen, kokeilukulttuurin käyttöönotto sekä johtamisen ja toimeenpanon parantaminen.[6] On kuitenkin todettava, että vaikka tavoitteet tällä tasolla on määritelty, toteutus tapahtuu lähinnä lainsäädännön ja finanssipolitiikan keinoin.

Eurooppa on kokonaisuudessaan jäänyt USA:n varjoon digitaalisten palveluiden kehittämisessä ja tuottamisessa. Lähes kaikki merkittävät ja laajasti käytetyt kuluttajaverkkopalvelut, lukuun ottamatta viranomaisasiointia, ovat lähtöisin USA:sta ja se on myös näitä palveluita tuottavien yritysten kotipaikka. Toisaalta esimerkiksi sähköinen pankkiasiointi ei ole monissakaan maissa kehittynyt Suomeen verrattavalle tasolle.

Euroopan Komissio (jäljempänä myös komissio) on asettanut keskeiseksi tavoitteeksi digitaalisten sisämarkkinoiden[7] luomisen julkaisussaan *Digitaalisten sisämarkkinoiden strategia Euroopalle*. Komission mukaan nämä markkinat luovat runsaasti mahdollisuuksia innovointiin, talouskasvuun ja työllisyyteen. Digitaalisilla sisämarkkinoilla tarkoitetaan tässä yhteydessä markkinoita, joilla tavarat, ihmiset ja palvelut liikkuvat vapaasti. Lisäksi ihmiset ja yritykset voivat kansallisuudestaan tai sijaintipaikastaan riippumatta saada käyttöönsä korkeatasoisen kuluttajan- ja tietosuojan sekä terveen kilpailun ehdoin

---

[5] *Ponka* 2013, s. 18.
[6] Ratkaisujen Suomi, s. 26–27.
[7] Sisämarkkinoiden toteuttaminen Euroopan unionissa perustuu SEU-sopimuksen 3(3) artiklaan, jonka mukaan *Unioni toteuttaa sisämarkkinat. Se pyrkii Euroopan kestävään kehitykseen, jonka perustana ovat tasapainoinen talouskasvu ja hintavakaus, täystyöllisyyttä ja sosiaalista edistystä tavoitteleva erittäin kilpailukykyinen sosiaalinen markkinatalous sekä korkeatasoinen ympäristönsuojelu ja ympäristön laadun parantaminen. Se edistää tieteellistä ja teknistä kehitystä.* Ks. EUVL C 202 7.6.2016, s. 17.

toteutettuja verkkopalveluita. Digitaalisten sisämarkkinoiden perustaksi tarvitaan verkkopalveluita, jotka suojelevat kuluttajien perusoikeuksia, kuten oikeutta yksityisyyteen ja henkilötietojen suojaan. Samalla näiden palveluiden tulisi olla varmoja, luotettavia, nopeita ja kohtuuhintaisia. Komission mukaan verkkoalustoilla on yhä keskeisempi merkitys niin sosiaalisessa kuin taloudellisessa elämässä. Alustat keräävät ja hallinnoivat merkittävää määrää dataa asiakkaistaan ja datan määrä kasvaa eksponentiaalisesti. Ongelmia aiheuttavat esimerkiksi avoimuuden puute liittyen alustojen keräämiin tietoihin, läpinäkymätön hinnoittelu ja alustojen omien palveluiden haitallinen edistäminen kilpailijoita mahdollisesti syrjivällä tavalla.[8] Nykyisin puhutaan yhä enemmän *alustataloudesta*. Alustatalouden perusideana on digitaalisiin alustoihin tukeutuva liiketoimintamalli, joka on saavuttanut merkittävän tai jopa määräävän markkina-aseman. Alustatalouden liiketoimintamallille tyypillisiä piirteitä ovat kiinteiden investointien vähäinen tarve, yksikkökustannusten alhaisuus ja ennen kaikkea datan käyttöön perustuvat algoritmipohjaiset toimintamallit.[9]

Digitaalisten sisämarkkinoiden toteuttaminen edellyttää selkeää ja vakaata oikeudellista ympäristöä. Vakaa ympäristö edistää innovointia, torjuu markkinoiden pirstaloitumista ja antaa kaikille toimijoille mahdollisuuden hyötyä markkinoista oikeudenmukaisin ja tasapuolisin ehdoin.[10]

Sähköisen hallinnon osalta komissio toteaa, että sähköiset viranomaispalvelut ovat olennaisia kansalaisille ja yrityksille niin kustannustehokkuuden kuin laadun parantamisen näkökulmasta. Kansalaisten tai yritysten ja viranomaisten väliset yhteydet ovat kuitenkin hajallaan ja tehtävää riittää esimerkiksi rajat ylittävän yhteentoimivuuden parantamiseksi.[11]

Tieto- ja viestintäteknologian kehittyminen on osaltaan monipuolistanut ja toisaalta monimutkaistanut viranomaisten hallintotoimintaa. Palvelusuuntautuneen sähköisen hallinnon asiakkaat ovat tietoisempia oikeuksistaan ja velvollisuuksistaan suhteessa julkiseen

---

[8] COM (2015) 192 final, s. 3–12.
[9] *Ailisto et al*. 2016, s. 15.
[10] COM (2017) 228 final, s. 3.
[11] COM (2015) 192 final, s. 17.

hallintoon. Oikeusvarmuuden toteuttaminen sähköisessä hallinnossa edellyttääkin ennakoivaa otetta juridisten näkökulmien tunnistamisessa, olipa kyseessä sitten suurelle käyttäjämäärälle tarkoitettujen sähköisten palveluiden tai viranomaisten omien sähköisten asiankäsittelyjärjestelmien kehittäminen.[12]

Sähköinen tunnistaminen ja allekirjoittaminen ovat keskeinen osa nykyaikaisen informaatiohallinnon infrastruktuuria. Suomessa sähköinen tunnistaminen on kehittynyt pääasiassa yksityisen sektorin toimijoiden vuoksi, lähinnä verkkopankkien yleistyttyä 1990-luvulla ja siitä eteenpäin. Niin kutsuttujen pankkitunnisteiden leviämisen ansiosta – ja valtion kuluttajille tarjoamien varteenotettavien vaihtoehtojen[13] puuttuessa – niiden käyttämisestä on tullut arkipäiväisen sähköisen tunnistamisen *de facto* -standardi. Toisaalta tämä on voinut aiheuttaa ongelmia henkilöille, joilla ei esimerkiksi henkilökohtaisten taloudellisten ongelmien tai oikeustoimikelpoisuuden puuttumisen vuoksi ole ollut mahdollista saada pankkien myöntämiä tunnistusvälineitä.

1.2 Tutkimusala

Oikeusinformatiikka määritellään oikeustieteelliseksi tutkimus- ja opetusalaksi, jossa tutkimus ja opetus keskittyvät oikeuden ja informaation sekä oikeuden ja tietotekniikan välisiin suhteisiin. Näissä suhteissa ilmenevät oikeudelliset sääntely- ja tulkintakysymykset kuuluvat oikeusinformatiikan alaan. Nämä oikeusinformatiikan käsittelemät sääntely- ja tulkintakysymykset ulottuvat samalla monille perinteisen systematiikan mukaisille oikeustieteen alueille. Lisäksi oikeusinformatiikalle on ominaista tieteidenvälisyys.[14]

---

[12] *Magnusson Sjöberg et al.* 2011, s. 360.
[13] Vahvan sähköisen tunnistamisen välineenä on tarjoilla ollut myös *sähköinen henkilökortti*, joka ei kuitenkaan ole tunnistusvälineenä saavuttanut pankkitunnisteisiin verrattavaa asemaa. Ks. tästä esim. *Korhonen* 2016, s. 307–310.
[14] *Saarenpää* 2016, s. 67–84.

Oikeusinformatiikalle tyypillisiä tutkimusaiheita ovat nykyään riskien tunnistaminen, lainsäädännön muutostarpeet, informaation yhteiskunnallinen merkitys, tietojärjestelmien ja -verkkojen käyttömahdollisuudet sekä oikeudelliset tietovarannot.[15] Oikeusinformatiikkaan kuuluvan informaatio-oikeuden keskeisiä tutkimuskohteita ovat yksityisyys, yksityiselämän suoja ja henkilötietojen suoja.[16]

Systemaattisessa katsannossa henkilötietojen suoja on ensisijaisesti osa siviilioikeuteen kuuluvaa persoonallisuusoikeutta. Kyse on identiteettimme suojasta henkilötietoja käsiteltäessä. Tietosuojalainsäädäntö on kuitenkin ollut keskeisimpiä oikeusinformatiikan lainopillisia tutkimusaiheita.[17]

Sähköinen tunnistaminen ja allekirjoittaminen kuuluvat informaatio- ja tietotekniikkaoikeuden perinteisiin aihealueisiin, vaikka sähköinen tunnistaminen on noussut erityisesti esiin vasta viime vuosina. *Laineen* mukaan teknisen luonteensa ja moniulotteisuutensa vuoksi sähköistä tunnistamista voidaan pitää vaativana aiheena. Tähän vaikuttavat myös tietoteknisten sovellusten nopea kehittyminen sekä kaupallisten ja oikeudellisten käytäntöjen mahdollinen poikkeaminen toisistaan.[18] *Korjan* mielestä oikeusinformatiikan ja persoonallisuusoikeuden piirissä voidaan jo puhua niin sanotun tunnisteoikeuden erityiskysymyksistä.[19] Nimi- ja tunnisteoikeus ovat keskeinen osa persoonallisuusoikeutta ja niissä lähdetään siitä, että on oikeudellisesti tärkeää kyetä tunnistamaan yksilö yhteiskunnassa. Nimioikeus liittyy läheisesti perusoikeuksiin ja nimikulttuuriin. Sen keskeiset kysymykset koskevat sitä, miten nimestä voidaan päättää ja miten se voidaan yksilöidä ja säilyttää tai miten sitä voidaan muuttaa. Tunnisteoikeus osana uudempaa persoonallisuusoikeutta liittyy yksilön luotettavaan tunnistamiseen sekä yksilön integriteettiin ja anonymiteettiin. Tunnisteoikeuden tarkoittamat tunnistetiedot eivät nimestä poiketen ole yleensä julkisia eikä niitä käsitellä julkisesti. Henkilötunnus on esimerkki yksilöivästä tunnistetiedosta.[20]

---

[15] *Saarenpää* 2016, s. 95.
[16] *Korja* 2016, s. 30.
[17] *Saarenpää* 2016, s. 75.
[18] *Laine* 2014, s. 612.
[19] *Korja* 2016, s. 5.
[20] *Saarenpää* 2013, s. 79–93.

Oikeusinformatiikan merkitystä oikeuden yleistieteenä lisää erityisesti yhteiskunnassa jatkuvasti lisääntyvä oikeudellistuminen, joka on seurausta oikeusvaltion vahvistumisesta. Oikeudellistuminen merkitsee sääntelyn määrällistä lisääntymistä, oikeudellisen käsitteistön määrän kasvua ja oikeusperiaatteiden muuttumista. Myös oikeudellisia kysymyksenasetteluja on jouduttu muuttamaan yhteiskunnan teknologisen kehityksen myötä. Yhä useammista informaatioon, tietojenkäsittelyyn ja viestintään liittyvistä asioista säädetään ja on säädettävä laissa. Lakisääteisyyden vaatimus seuraa eurooppalaisista perusoikeuksista, kuten henkilötietojen suojasta, yksityisyydestä ja sananvapaudesta. Keskeisenä lainsäädännöllisenä perusperiaatteena on ihmisoikeuksiin perustuvien perusoikeuksien kunnioittaminen.[21]

Oikeudellisesta näkökulmasta katsottuna yhä useampia yhteiskunnan toimintoja tulee arvioida erilaisina informaatioprosesseina ja oikeuksien toteuttaminen nähdään näiden informaatioprosessien koosteena. Yksi oikeusinformatiikan keskeisistä tarkastelukohteista on nimenomaan yhteiskunnan informaatioprosessien juridinen arviointi ja analysointi. Tämän päivän informaatiohallinto koostuu useista eri tasoilla säännellyistä informaatioprosesseista. Perinteisen hallinnollisen päätöksenteon ja fyysisesti tarjottavien palveluiden ohella nykyajan hallintoprosessit ovat vahvasti sidoksissa informaation käsittelyyn tietojärjestelmissä sekä informaation välittämiseen tietoverkoissa. Euroopan unionin puitteissa puhutaan vakiintuneesti verkkoyhteiskunnan oikeudellisesta viitekehyksestä (legal framework), joka on seurausta tietokoneiden, tietojärjestelmien ja tietoverkkojen merkityksen muuttumisesta. Näiden muutosten seurauksena myös oikeudellinen kysymyksenasettelu muuttuu.[22]

Oikeusinformatiikka toteuttaa omalta osaltaan oikeudellisen elämän riskianalyysia ja sen perustehtävänä on muutosten tunnistaminen ja hallinta. Uusien riskien tunnistamisesta aiheutuu uusia oikeustieteellisiä, lainsäädännöllisiä ja lakiteknisiä haasteita. Esimerkiksi tietoturvallisuus on oikeusinformatiikan tutkima aihepiiri, jota ei kuitenkaan ole riittävästi ja yhtenäisesti säädelty.[23]

---

[21] *Saarenpää* 2016, s. 77–80.
[22] *Saarenpää* 2016, s. 79–136.
[23] *Saarenpää* 2016, s. 82–271.

Muuttuvassa yhteiskunnassa tapahtuva oikeuden ja yhteiskunnan suhteen tutkimus kuuluu oikeusinformatiikan yleiseen osaan. Sen piirissä tutkitaan esimerkiksi yhteiskunnan oikeudellisesti merkittävää kehitystä, informaatioinfrastruktuuria ja oikeudellisen informaation merkitystä yhteiskunnassa. Oikeusinformatiikan erityinen osa jaetaan puolestaan oikeudelliseen tietojenkäsittelyyn, oikeudellisen informaation tutkimukseen, informaatio-oikeuteen sekä tietotekniikkaoikeuteen, joista erityisesti kahden viimeksi mainitun välinen rajanveto on kuitenkin epäselvää. Lisäksi käsitteenä on yleistynyt ICT-oikeus (Information and Communication Technology Law).[24]

Tietoverkkojen ja informaatiomarkkinoiden kehittymisen myötä informaatio-oikeus on muodostunut oikeusinformatiikan merkittäväksi osa-alueeksi. Yksityisyys, henkilötietojen suoja, julkisuus, teletoiminta, viestintä, sähköinen kaupankäynti ja tietoturvallisuus ovat kysymyksiä, joita eurooppalaisessa katsannossa pidetään informaatio-oikeuden piiriin kuuluvina. Huomioitavaa on myös se, ettei informaatio-oikeutta voida enää pitää vain teoreettisena viitekehyksenä, vaan teknisen kehityksen myötä sen tulkintoja tarvitaan niin lainsäätämisessä, laintulkinnassa kuin oikeudellisessa ratkaisutoiminnassa ja ohjauksessa.[25]

Voutilaisen mukaan yleinen kysymyksenasettelu oikeusinformatiikkaan lukeutuvassa tutkimuksessa voi koskea esimerkiksi sitä, millaisia reunaehtoja lainsäädäntö asettaa tietojenkäsittelyprosesseille ja informaatioteknologian käytölle sekä millaisia seurannaisvaikutuksia lainsäädännön asettamilla vaatimuksilla on teknologisille tuotteille tai tietojenkäsittelylle.[26] *Pöystin* mukaan oikeusinformatiikan antama lisäarvo onkin ennen kaikkea erilaisten näkökulmien yhdistämisessä ja kyvyssä esittää uusia kysymyksiä.[27]

1.2.1 Informaatio-oikeuden normeista

Oikeusinformatiikan lähestymistapa on monioikeudellinen ja ongelmakeskeinen. Monioikeudellisella tässä yhteydessä tarkoitetaan sitä, että esimerkiksi sähköisen asioinnin

---

[24] *Saarenpää* 2016, s. 99–131.
[25] *Pöysti* 1999, s. 366–370.
[26] *Voutilainen* 2009, s. 14.
[27] *Pöysti* 1999, s. 360.

lainsäädännön kehittyminen on saanut aikaan sääntelyvaikutuksia monilla perinteisillä oikeudenaloilla kuten hallinto-, kauppa-, persoonallisuus-, sopimus-, rikos- ja vahingonkorvausoikeudessa. Uutta sääntelyä on vaatinut myös tietoturvallisuuden ja yksityisyyden suojan huomioiminen.[28]

Informaatio-oikeudellisilla normeilla säännellään useita kohteita. Näitä ovat esimerkiksi informaation käyttäjien ja toisaalta informaatiosubjektien oikeudet ja velvollisuudet sekä toisaalta itse informaatioon ja informaatiomarkkinoihin liittyvät institutionaaliset asiat. Nämä puolestaan jakautuvat ensinnä yksilöiden institutionaalisiin suojasäännöksiin ja toiseksi informaatiomarkkinoita ja informaatioinfrastruktuuria koskeviin säännöksiin. Institutionaalisilla suojasäännöksillä tarkoitetaan yksilöiden oikeuksia ylläpitäviä, valvovia tai muulla tavoin turvaavia instituutioita ja organisaatioita koskevia normeja. Nämä normit perustavat kyseisiä instituutioita tai ohjaavat niiden menettelytapoja. Esimerkkinä voidaan mainita tietosuojavaltuutettua koskevat normit henkilötietolainsäädännössä.[29]

Yhtenä keskeisenä sääntelyperiaatteena on teknologianeutraalisuus. Tällä tarkoitetaan yleisesti sitä, ettei lainsäädännössä tule pääsääntöisesti säännellä yksittäisen teknologisen ilmiön hyödyntämistä tai asettua jonkin kilpailevan teknologian puolelle tai sitä vastaan esimerkiksi kieltämällä se.[30] Toisaalta huomiota tulisi kiinnittää siihen, että lainsäädännön uudistamisessa keskityttäisiin laajempiin kokonaisuuksiin. Tällä hetkellä teknologisen kehityksen aikaansaamat lainsäädännön muutokset ovat usein pistemäisiä ratkaisuja esimerkiksi tekijänoikeuden, sopimusoikeuden tai vaikkapa tunnistamis- ja maksamissääntelyn alueilla.[31]

Informaatio-oikeudelliselle sääntelymallille on ominaista, että lainsäädännön tasolla on annettu puitteet ja suunta toimenpiteille, joihin viranomaisten on ryhdyttävä. Näiden toimenpiteiden tuloksena syntyy *soft law* -tyyppistä sääntelyä, johon vaikuttavat osaltaan

---

[28] *Korhonen* 2016, s. 276–277.
[29] *Pöysti* 1999, s. 375–376.
[30] *Saarenpää* 2016, s. 223.
[31] *van Dijk* 2012, s. 139. Toisaalta teknologinen kehitys on saanut aikaan laajempia perusoikeuslähtöisiä sääntelyuudistuksia. Henkilötietojen suojan perusoikeutta toteuttava EU:n yleinen tietosuoja-asetus on esimerkkinä kattavasta henkilötietojen käsittelyä koskevasta sääntelystä. Ks. tästä jäljempänä jakso 3.

myös kansalliset ja kansainväliset standardit.[32] Soft law voi sisältää erilaisia viranomaisten laatimia suosituksia, lausuntoja, tiedonantoja tai toimintaohjeita. Näillä ei kuitenkaan ole oikeudellista sitovuutta. Soft law:lla voi olla tulkinnallista vaikutusta säädösten soveltamisessa ja sillä pyritään epävirallisesti vaikuttamaan eri toimijoiden käyttäytymiseen. Myös erilaisilla käytännesäännöillä, suuntaviivoilla, ohjeilla ja valmisteluasiakirjoilla voi olla ohjaava vaikutus lainsäädännön soveltamiseen.[33]

1.3 Tutkimustehtävä

Käsillä oleva tutkielma on laadittu osana professori *Rauno Korhosen* ohjaamaa oikeusinformatiikan notaari- ja maisteritutkielmaprojektia. Projektin teemana on ollut *Oikeusinformatiikan ajankohtaisia kysymyksiä*. Ylätason tutkimusaiheena on ollut henkilötietojen suoja. Sähköinen tunnistaminen sekä yleisemmin sähköisen identiteettimme käyttäminen liittyvät vahvasti henkilötietojen suojaan. Kysymys on yksilön oikeusturvasta, kun hänen sähköistä identiteettiään, eli häntä koskevia tietoja käytetään sähköisen hallinnon prosesseissa[34].

Tämän tutkimuksen aiheena on sähköinen tunnistaminen osana tietosuoja- ja tietoturvallisuussääntelyä informaatiohallinnossa. Sähköistä tunnistamista voidaan pitää yhtenä keskeisimmistä informaatiohallinnon palveluista. Lisäksi sillä on merkittävä rooli myös yksityisen sektorin palveluissa. Tietoturvallisuuden näkökulmasta sähköinen identiteetti ja tunnistaminen liittyvät olennaisesti tarkasteltavaan kokonaisuuteen, identiteetin hallinnan ja pääsynvalvonnan ollessa kaksi merkittävää tietoturvallisuuden prosessia.

Tutkimuksen lähtökohtana tarkastellaan sähköisen hallinnon, tai kuten jäljempänä esitetään, informaatiohallinnon oikeudellisia perusteita ja reunaehtoja. Yksi näistä perusteista on tietoturvallisuus, jota käsittelen omana kokonaisuutenaan. Pääasiallisena tutkimustehtävänä on selvittää sähköistä tunnistamista koskevan lainsäädännön sisältöä. Kyseinen lainsäädäntö on ollut viime vuosina muutostilassa erityisesti EU-tasoisessa sääntelyssä

---

[32] *Voutilainen* 2006, s. 42.
[33] *Mäenpää* 2017, s. 189.
[34] *Voutilainen* 2009, s. 7.

tapahtuneiden muutosten vuoksi, jonka puitteissa on esitelty rajat ylittävän sähköisen tunnistamisen käsite. Tästä säädetään nykyisin asetuksella, jota yleisesti kutsutaan *eIDAS-asetukseksi* (Euroopan parlamentin ja neuvoston asetus N:o 910/2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta[35], jäljempänä eIDAS-asetus). Asetuksen voimaantulo on muuttanut myös kansallista lainsäädäntöämme. Tutkimustehtävän voi tiivistää kysymysmuotoon. Miten sähköistä tunnistamista säännellään keskeisenä informaatiohallinnon palveluna ja osana tietoturvallisuuden kokonaissääntelyä?

EU:n tietosuojaa koskevan sääntelyuudistuksen vuoksi ja kotimaisen sääntelyn ollessa parasta aikaa muutoksen kohteena, en käsittele tietosuojasääntelyä tai siihen kohdistuvia muutoksia muutoin kuin yleisellä tasolla ja siinä laajuudessa kuin se varsinaisen tutkimusaiheen kannalta on olennaista. Tutkimuksen laajuuden rajaamiseksi tässä tutkimuksessa ei tarkemmin käsitellä biometristä tunnistamista, vaikka se voidaankin lukea osaksi sähköistä tunnistamista. Samasta syystä tutkimuksen ulkopuolelle on rajattu sähköistä allekirjoittamista koskeva uudistunut sääntely sekä valtuutusta ja puolesta asiointia koskevat kysymykset, jotka liittyvät läheisesti sähköiseen tunnistamiseen ja asiointiin.

1.4 Tutkimusmetodi

Voimassa olevan oikeuden tulkinta on aina sidottu aikaan, paikkaan ja yhteiskunnalliseen tilanteeseen. Kirjoitettu laki edustaa säätämisajankohdan yhteiskunnallisia ja poliittisia näkemyksiä. Toisin sanoen se kertoo siitä, mitä on pidetty säätämisen arvoisena ja yhteiskunnallisesti merkittävänä asiana.[36]

Viimeaikainen sääntelyn lisääntyminen sähköisen asioinnin ja viestinnän aloilla, josta esimerkiksi *Korhonen* käyttää normitulvan[37] käsitettä, puolustaa perinteisen lainopin me-

---

[35] EUVL L 257, 28.8.2014, s. 73.
[36] *Korja* 2016, s. 19. Ks. myös *Aarnio* 2006, s. 107–109, jonka mukaan oikeus on dynaaminen prosessi, ei suljettu systeemi eikä toisaalta itseään muuttava. Muutosajurit tulevat ulkopuolelta ja ne voivat olla taloudellisia, kulttuurisia tai ne voivat liittyä yhteiskuntasuhteisiin. *Aarnio* näkee Euroopan yhdentymisen tällaisena muutosajurina.
[37] *Korhonen* 2016, s. 275.

todin, oikeusdogmatiikan, käyttämistä tässä tutkimuksessa. Keskeinen tavoite on näin ollen voimassa olevan oikeuden sisällön tutkiminen ja selvittäminen. Oikeusdogmatiikka osaltaan määrittää oikeusjärjestyksen sisältöä. Systematisoinnin avulla jäsennetään normimassaa yleisellä ja abstraktilla tavalla, käyttäen apuna oikeudellisia teorioita.[38]

Aarnio puhuu oikeudellisesta dimensiosta. Moderni yhteiskunta oikeudellistuu, ja sekä normien määrä että intensiteetti kasvavat. Tähän on viitattu myös *holhousyhteiskunnan* käsitteellä.[39]

Oikeussääntöjen tulkinta ja soveltaminen ei ole yksiselitteinen, tiettyjä sääntöjä noudattava prosessi. Siksi Aarnion mukaan oikeustieteen metodi on ennen kaikkea näkökulma oikeuteen. Käytännöllinen ja teoreettinen lainoppi ovat vuorovaikutussuhteessa toisiinsa. Näillä tarkoitetaan oikeussääntöjen sisällön selvittämistä eli tulkintaa ja oikeussääntöjen systematisointia. Voidaan puhua myös lainopin praktisesta ja teoreettisesta ulottuvuudesta.[40] Lainoppi ei nykyään ole pelkästään sääntöjen tutkimista vaan tutkinnan kohteena ovat myös oikeusperiaatteet. Eri oikeusperiaatteiden sovittaminen yhteen edellyttää aina oikeusnormien tulkintaa. Lainopin avulla kuvataan voimassa olevaa oikeutta, ja siksi sitä voidaan kutsua deskriptiiviseksi tieteeksi.[41]

Oikeudellisessa ratkaisutoiminnassa on olennaista, että juridisesti mahdollisten tulkintavaihtoehtojen joukosta voidaan osoittaa käytettävissä olevat relevantit vaihtoehdot. Nämä vaihtoehdot voidaan osoittaa nimenomaan oikeuslähdeopin avulla. Näin voidaan tunnistaa se, mikä yksittäistapauksessa on oikeudellisesti relevanttia.[42]

Lainopissa voidaan kritisoida vallitsevia oikeudellisia käytäntöjä tai oikeusnormeja, mutta kritiikin on lähdettävä voimassaolevasta oikeudesta käsin. Tämä tarkoittaa, että kriittiset tulkintakannanotot tulee perustaa esimerkiksi perus- ja ihmisoikeuksiin tai oi-

---

[38] *Aarnio* 2006, s. 96–97.
[39] *Aarnio* 2006, s. 95.
[40] *Aarnio* 2006, s. 237–238.
[41] *Hirvonen* 2011, s. 22–25.
[42] *Aarnio* 2006, s. 307.

keusperiaatteisiin. Lainopin tutkimusmenetelmät eivät ole eksakteja kuten luonnontieteissä. *Hirvosen* mukaan tarjoilla ei ole myöskään sellaista lainopin metodisäännöstöä, jota seuraamalla välttämättä päädyttäisiin oikeaan tulkintaan, oikeudenmukaiseen punnintaan tai perusteltuun systematisointiin.[43]

Tutkimuksen kohdetta joudutaan sen oikeudellisen luonteen vuoksi lähestymään oikeusjärjestystä läpileikkaavalla tavalla, ottaen huomioon esimerkiksi informaatio- ja hallintooikeudelliset näkökulmat. Voutilainen nimittää tällaista tutkimuksellista lähestymistapaa oikeusjärjestyskeskeiseksi lainopiksi. Tyypillistä oikeusinformatiikan alaan kuuluvalle tutkimukselle on, että sen rakenneosana on yhteiskunnan muutoksista lähtöisin oleva ongelmakeskeisyys.[44] Myös *Bygrave* toteaa, että kaikkien tärkeiden näkökulmien huomiointi edellyttää perinteisen oikeusdogmatiikan menetelmän sulauttamista muihin menetelmiin, kuten erilaisten menettelytapaohjeiden arviointiin.[45]

Voutilaisen mukaan se, että tutkimuksella on sidokset sekä oikeustieteen traditioon että oikeusinformatiikan lähitieteisiin[46] ja tutkimuksessa myös hyödynnetään edellä mainittujen aineistoa, tekee siitä oikeusinformatiikan alaan kuuluvan.[47]

1.5 Tutkimuksen rakenne

Rakenteeltaan tämä tutkimus jakautuu 7 pääjaksoon, joissa johdantojakson 1 jälkeen käsitellään informaatiohallintoa ja sähköistä asiointia jaksossa 2, henkilötietojen suojaa jaksossa 3, tietoturvallisuutta jaksossa 4, sähköistä tunnistamista jaksossa 5 sekä tunnistusvälineiden oikeudetonta käyttöä ja niihin liittyvää oikeuskäytäntöä jaksossa 6. Tutkimuksen johtopäätökset esitetään jaksossa 7.

---

[43] *Hirvonen* 2011, s. 50–53.
[44] *Voutilainen* 2009, s. 11–12.
[45] *Bygrave* 2002, s. 10–11.
[46] *Voutilainen* viittaa näillä lähitieteillä tietojenkäsittelytieteeseen, kognitiotieteeseen, informaatiotieteisiin sekä näitä lähellä oleviin muihin tieteisiin.
[47] *Voutilainen* 2009, s. 14.

2 Informaatiohallinto ja sähköinen asiointi

2.1 Sähköisestä hallinnosta informaatiohallintoon

Hallintoa, jossa hallintotoiminta hyödyntää tietotekniikkaa tai kyseinen toiminta ja sen järjestäminen tapahtuu kokonaisuudessaan tietotekniikan avulla, voidaan kutsua sähköiseksi hallinnoksi.[48] (ruots. e-förvaltning, engl. e-government) Sähköisen hallinnon käsitettä ei tule ymmärtää suppeasti siten, että se käsittäisi ainoastaan kansalaisten mahdollisuuden asioida viranomaisten kanssa tietoverkon välityksellä sähköisiä asiointipalveluita käyttäen, vaan laajasti käsittäen hallinnon koko sisäisen toiminnan ja prosessit. Tässä laajassa käsityksessä tarkasteltuna sähköisen hallinnon kehittymistä ei voida pitää uutena asiana, vaan se on pohjoismaisella tasolla alkanut jo 1960-luvulla.[49] Sähköisen hallinnon käsitettä on kuitenkin pidetty liian teknisluonteisena. Yleistymässä onkin sähköisen hallinnon sijaan *informaatiohallinnon* käsite.[50] Informaatiohallintoa ei voida pitää vain sähköisen hallinnon seuraavana kehitysasteena, vaan se on täydentävä näkökulma. Se ohjaa tarkastelemaan informaatiovirtoja ja sitä, miten, missä ja milloin ne muuttuvat sekä mitä nämä muutokset tarkoittavat julkisen sektorin toimintojen kannalta. Sähköisen hallinnon osalta keskityttiin ennen kaikkea kysymyksiin informaatioteknologian mahdollisista käyttötarkoituksista hallinnon tehokkuuden, kustannussäästöjen ja palveluiden lisäämisen näkökulmista.[51] Sähköistä hallintoa ei ole määritelty lainsäädännössämme. Voutilainen kuvaa sähköiseksi hallinnoksi viranomaistoimintaa, joka hyödyntää sähköisen hallinnon rakenneosia hallinnon eri prosesseissa.[52]

Euroopan unionin tasolla sähköisen hallinnon palveluita kehitetään eri jäsenvaltioissa, mutta palveluiden yhteentoimivuutta haittaa niiden kehittäminen eristyksissä. Komission mukaan viranomaispalveluiden sähköistäminen on keskeistä kansalaisille ja yrityksille tarjottavien palveluiden kustannustehokkuuden ja laadun näkökulmasta.[53] Komission

---

[48] *Voutilainen* 2006, s. 29.
[49] *Magnusson Sjöberg et al*. 2011, s. 268.
[50] *Korhonen* 2016, s. 276.
[51] *Mayer-Schönberger & Lazer (ed.)* 2007, s. 5–12.
[52] *Voutilainen* 2009, s. 40.
[53] COM (2015) 192 final, s. 16–17.

mukaan sähköisen hallinnon palveluiden tarjoaminen ja käyttäminen tuovat etuja kansalaisille, yrityksille ja julkishallinnolle sekä avaavat mahdollisuuksia erityisesti sähköistä allekirjoitusta hyödyntäville palveluille. Digitaaliset palvelut mahdollistavat viranomaispalveluiden nopeamman, täsmällisemmän ja tehokkaamman tarjoamisen.[54]

Informaatiohallinnon rakenneosia ovat sähköiset asiointipalvelut, asianhallintajärjestelmät, viranomaisten operatiiviset järjestelmät ja niiden taustajärjestelmät sekä tietoverkot.[55] Informaatiohallinnon toimintoja ja prosesseja toteutettaessa asiaa voidaan tarkastella joko substantiivisesta tai funktionaalisesta näkökulmasta. *Substantiivisessa* näkökulmassa tavoitteena on toteuttaa perinteisen fyysisen ympäristön toimenpide (esimerkiksi tunnistaminen tai allekirjoittaminen) ja sen ominaisuudet sähköisessä ympäristössä mahdollisimman hyvin, käytännössä vastaten täysin perinteistä menettelyä. *Funktionaalisessa* näkökulmassa puolestaan keskitytään oikeudellisesti merkittäviin tehtäviin, joita tietyt ominaisuudet palvelevat ja nämä ominaisuudet toteutetaan sähköiselle ympäristölle parhaiten soveltuvalla tavalla. Tästä kaikesta on seurauksena se, että sähköinen ja perinteinen menetelmä voivat merkittävästikin poiketa toisistaan.[56] Nykyisessä vuorovaikutteisessa verkkoympäristössä ei ole Laineen mukaan tarpeen simuloida paperimaailman prosesseja, vaan asiat voidaan tehdä kulloinkin sähköiseen ympäristöön parhaiten sopivalla tavalla.[57]

2.1.1 Informaatioinfrastruktuuri

Toimivan ja hyvän informaatiohallinnon perusedellytyksenä ovat laadukkaat sääntely- ja teknologiaympäristöt. Harvaan asutussa maassa, kuten Suomessa, on järkevää tuottaa sähköisiä palveluita kansalaisille. Palveluiden sähköistämistä tai nykytermein digitalisointia voidaan perustella sekä taloudellisilla että ekologisilla syillä. Käytännön esimerkkinä pitkälle sähköistetystä ja automatisoidusta massaluonteisesta palvelusta on verotus. Verohallinto onkin ollut maassamme yksi julkishallinnon edelläkävijöistä verotuksen prosessien ja sähköisen asioinnin kehittämisessä.

---

[54] COM (2017) 228 final, s. 4–19.
[55] *Voutilainen* 2009, s. 40.
[56] *Ponka* 2013, s. 20–21.
[57] *Laine* 2014, s. 619.

Yhteiskunnan viestinnän sekä informaation hallinnan ja käsittelyn järjestämistä teknisesti, taloudellisesti ja organisatorisesti kuvataan *informaatioinfrastruktuurin* käsitteellä. Mukaan luetaan myös edellä mainittujen asioiden järjestämiseksi tarvittavat ja käytettävät välineet sekä rakenteet. Kysymys on yhteiskunnan sisäisestä kokonaisvaltaisesta järjestelystä, joka teknisessä mielessä pitää sisällään kaikki laitteet ja ohjelmistot, jotka mahdollistavat viestinnän ja informaation käsittelyn. Teknisten komponenttien ohella mukaan luetaan myös eri toimintojen henkilöllinen järjestäminen.[58] Informaatioinfrastruktuurin sääntelyssä ei ole enää kysymys vain erilaisten hallinnollisten määräysten antamisesta. Se on muodostunut omaksi sääntelyn kohteekseen, jolle on ominaista kansainvälisyys, tekninen konvergenssi, kilpailu, käyttäjien oikeudet sekä tietoturvallisuuden uhkatekijät. Tämä kehitys näkyy esimerkiksi asiaa koskevien EU-tasoisten säädösten lisääntymisenä.[59]

Viranomaisten operatiivisista järjestelmistä ei pääasiassa ole säädetty lailla, vaan sääntely perustuu joko rekistereitä tai viranomaisen tehtäviä koskeviin säännöksiin. Käytännössä toimialasidonnaisuus on johtanut siihen, ettei yhteisiä palveluita voida kehittää ilman lainsäädännön kehittämistä ja valtioneuvoston ohjausta[60]. Yhtenä ongelmana on, että rekisterilainsäädäntöä on kehitetty julkisuuslain (Laki viranomaisen toiminnan julkisuudesta 21.5.1999/621, jäljempänä myös JulkL) perusteella, joka on vahvasti asiakirjalähtöinen. Tästä seuraa tilanteita, joissa rekistereissä oleva sinänsä julkinen tieto ei ole kuitenkaan saatavilla tai sen käyttöä kontrolloidaan joskus tarpeettomasti lainsäädännöllisin estein.[61]

---

[58] *Pöysti* 1999, s. 378.
[59] *Saarenpää* 2016, s. 205.
[60] Keskeinen merkitys julkisen tietohallinnon ohjauksessa on julkisen hallinnon tietohallinnon neuvottelukunnalla (JUHTA). JUHTA:sta säädetään tietohallintolain (L julkisen hallinnon tietohallinnon ohjauksesta, 10.6.2011/634) 5 §:ssä ja sen tehtävistä tarkemmin em. lain nojalla annetussa valtioneuvoston asetuksessa (VnA julkisen hallinnon tietohallinnon neuvottelukunnasta annetun valtioneuvoston asetuksen muuttamisesta 129/2016). JUHTA on ministeriöiden ja kunnallishallinnon pysyvä yhteistyö- ja neuvotteluelin, joka tukee tietohallinnon strategista ohjaamista ja koordinointia sekä edistää julkisten palveluiden saatavuutta, tehokkuutta ja laatua. Ks. tarkemmin VM, Tietohallinnon ohjaus -verkkosivusto.
[61] *Voutilainen* 2014, s. 34–39.

Tietohallinnollisesta näkökulmasta katsottuna julkishallinnon ICT-toiminnoille on viime vuosina ollut leimallista voimakas keskittäminen. Esimerkiksi valtionhallinnon toimialariippumattomien ICT-palveluiden tuotanto on keskitetty Valtion tieto- ja viestintätekniikkakeskukseen (Valtori), josta säädetään laissa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (30.12.2013/1226). Vuoden 2017 lopussa päättyi myös VM:n asettama Kansallisen palveluarkkitehtuurin (KaPA) toteuttamisohjelma.[62] KaPA -ohjelman tuloksena säädettiin erikseen laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (29.6.2016/571, jäljempänä KaPAL). KaPAL:ssa säädetään lisäksi tukipalveluiden tuotanto- ja käyttövastuista (2 luku), henkilö- ja muiden tietojen käsittelystä palvelutuotannossa (3 luku), tukipalveluja ja niiden käyttöä koskevista vaatimuksista (4 luku) sekä palveluiden ohjauksesta (5 luku). Merkittävä osa tukipalveluiden järjestämisvastuusta on säädetty Väestörekisterikeskukselle (VRK).

Hallituksen esityksessä katsottiin, ko. palveluista on tarpeen säätää lailla, koska kyseisillä palveluilla on merkittävä ja välitön vaikutus hallinnossa asioivan oikeusturvaan ja asioinnin sujuvuuteen ja koska tukipalveluita käytetään suoraan sähköisten asiointipalveluiden tukipalveluina. Merkittävänä kannanottona valtionhallinnon tietojärjestelmäkehittämisen sujuvoittamisen puolesta voidaan pitää hallituksen esityksen mainintaa siitä, että kansallisen palveluarkkitehtuurin niin sanotut jatkuvat palvelut perustuvat jatkossa avoimen lähdekoodin ratkaisuihin ja avoimiin rajapintoihin. Tällä halutaan vaikuttaa esimerkiksi kehittäjäyhteisötoiminnan edistämiseen.[63] Tämän uuden ajattelumallin mukaisesti kansalliseen palveluarkkitehtuuriin kuuluvan palveluväylän (tiedonvälityskanava) tekninen toteutus on tehty yhteistyössä Viron kanssa ja käyttöön on otettu siellä kehitetty avoimeen lähdekoodiin perustuva ohjelmisto, joka Virossa[64] tunnetaan nimellä X-Road[65].

---

[62] Ohjelman tiedot ks. http://valtioneuvosto.fi/hanke?tunnus=VM140:02/2013 [käyty 9.4.2018].
[63] HE 59/2016 vp, s. 16–19.
[64] Suomen informaatiohallinnon palveluita verrataan usein Virossa toteutettuihin palveluihin, mikä ei mielestäni ole täysin perusteltua. Viron itsenäinen hallintokulttuuri on hyvin nuori ja sähköisiä palveluita on voitu siellä kehittää ns. puhtaalta pöydältä, ilman hallintohistorian ja esimerkiksi olemassa olevan arkkitehtuurin huomiointia. Suomessa on puolestaan hallinnon palveluilla ja prosesseilla ollut joskus pitkäkin, lainsäädännön ja toimivallanjaon sisältävä historia kauan ennen niiden saattamista sähköiseen muotoon.
[65] Ks. https://e-estonia.com/solutions/interoperability-services/x-road/ [käyty 16.4.2018].

van Dijk toteaa osuvasti, että viime kädessä verkon käyttäjät ratkaisevat sen, mitkä palvelut jäävät elämään. Ei ole lainkaan varmaa, että jokin nykyisistä suurista toimijoista[66] olisi sitä myös jatkossa. Asiakkaiden, siis käyttäjien, rooli on noussut keskiöön.[67] Vaikka tämä koskettaakin ensi sijassa yksityisen sektorin tuottamia verkkopalveluita, ei tämä oikeuta julkista sektoria jättämään asiakaslähtöisyyttä huomioimatta palveluiden kehittämisessä.

2.1.2 Sähköinen asiointi

Yleisellä tasolla sähköisestä asioinnista viranomaisen kanssa Suomessa säädetään laissa sähköisestä asioinnista viranomaistoiminnassa (24.1.2003/13, jäljempänä AsiointiL). Lakia sovelletaan *hallintoasian, tuomioistuinasian, syyteasian ja ulosottoasian sähköiseen vireillepanoon, käsittelyyn ja päätöksen tiedoksiantoon, jollei muualla laissa toisin säädetä* (2 §). Lakia sovelletaan myös muussa viranomaistoiminnassa soveltuvin osin, ei kuitenkaan poliisi- tai esitutkinnassa (2.3 §). Laki antaa hyvin yleisluontoiset ohjeet sähköisestä asioinnista viranomaistoiminnassa ja siinä säädetäänkin viranomaisen velvollisuuksista sähköisten asiointipalveluiden järjestämisessä (2 luku), sähköisten viestien lähettämisestä viranomaiseen (3 luku), päätösasiakirjojen sähköisestä allekirjoittamisesta ja tiedoksiannosta (4 luku) sekä erinäisistä muista asioista, kuten koneellisesta allekirjoituksesta ja sähköisten asiakirjojen arkistointivelvollisuudesta (5 luku).

AsiointiL 1 §:ssä säädetään, että lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa edistämällä sähköisten tiedonsiirtomenetelmien käyttöä.

Asioinnissa keskeisiä ovat hallinnon asiakkaan ja asianosaisen käsitteet. Hallinnon asiakas on viranomaispalvelun hakija, saaja tai käyttäjä ja käsite tulee ymmärtää laajasti.[68] Asianosaisen käsite on määritelty julkisuuslaissa, jonka 11 §:n mukaan *hakijalla, valittajalla sekä muulla, jonka oikeutta, etua tai velvollisuutta asia koskee (asianosainen), on*

---

[66] *van Dijk* viittaa yleisesti tunnettuihin suuryrityksiin kuten Apple, Google, Facebook ja Microsoft.
[67] *van Dijk* 2012, s. 93.
[68] *Mäenpää* 2017, s. 253.

oikeus saada asiaa käsittelevältä tai käsitelleeltä viranomaiselta tieto muunkin kuin julkisen asiakirjan sisällöstä, joka voi tai on voinut vaikuttaa hänen asiansa käsittelyyn.

Sähköisellä asiointipalvelulla tarkoitetaan asiakkaan näkymää viranomaisen palveluun ja siihen liittyvään informaatioon. Asiointipalveluun kuuluvia yksittäisiä toimintoja voivat olla tunnistautuminen, lomakkeen täyttäminen, allekirjoittaminen ja lähettäminen.[69]

2.2 Hallinto-oikeudelliset periaatteet ja hyvä informaatiohallinto

Perustuslain (11.6.1999/731, jäljempänä PL) 21.1 §:n mukaisesti *jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi.* Kyseessä on myös hyvän informaatiohallinnon perustan luova säännös.

Lakisidonnaisuuden periaate (PL 2.3 §) edellyttää, että viranomainen huomioi toiminnassaan perus- ja ihmisoikeudet sekä hallinnon oikeusperiaatteet. Käytännön toiminnassa viranomaisten kannalta merkitystä saavat erityisesti yhdenvertaisuus- ja julkisuusperiaate, yksityiselämän ja kotirauhan suoja sekä elinkeinon ja ammatin harjoittamisen vapaus. Julkiseen toimintaan kohdistuvana perusoikeutena keskeinen merkitys on hyvällä hallinnolla ja asianmukaisella menettelyllä. Lakisidonnaisuuden vaatimus hallinnossa on soveltamisalaltaan yleinen sekä asiallisesti että organisatorisesti ja sen alaan kuuluu myös julkisen hallintotehtävän hoitaminen.[70]

Hyvän hallinnon perusoikeussäännöksen vaatimukset materialisoituvat hallintolaissa (6.6.2003/434, jäljempänä HallL), jonka 2 luvussa säädetään hyvän hallinnon takeena toimivista hallinnon oikeusperiaatteista (6 §), palveluperiaatteesta ja palvelun asianmukaisuudesta (7 §), neuvontavelvollisuudesta (8 §), hyvän kielenkäytön vaatimuksesta (9 §) sekä viranomaisten välisestä yhteistyöstä (10 §). Hallinnon oikeusperiaatteet koskevat

---

[69] *Korhonen* 2016, s. 276.
[70] *Mäenpää* 2017, s. 139–140.

kaikkea hallinnon toimintaa riippumatta sen muodosta ja sisällöstä. Silloin kun hallintotehtävää hoitaa joku muu kuin viranomainen, on hallinnon oikeusperiaatteilla tärkeä ohjaava merkitys. Erilaiset sopimukset koskien julkisten palvelutehtävien hoitoa ovat yleistyneet. Tätä ei voida sinällään pitää toimivallan lakiperustaisuuden vaatimuksen vastaisena menettelynä, kun sopimustoimivalta on määritelty laissa. Viranomaisen tehtävien hoitamista voidaan määritellä sopimustoimin silloin, kun kysymys ei ole varsinaisesta julkisen vallan käyttämisestä.[71]

Yksityisoikeudellinen sääntely koskee kasvavassa määrin myös viranomaistoimintaa, esimerkiksi sopimusoikeuden ja asiakkaiden suojan osalta. Lisäksi viestintä- ja informaatio-oikeudellisella sääntelyllä on lisääntyvää merkitystä ja ne sisältävät sekä yksityis- että julkisoikeudellisia elementtejä. Julkisten ja yksityisten palveluiden samankaltaisuus ja yhtäläisyys ovat osaltaan madaltaneet julkisen ja yksityisen rajaa. Yhtiöittäminen, yksityistäminen, kilpailuttaminen ja ostopalvelut ovat hyvinvointivaltion keskeisiä piirteitä. Julkishallinnon ei ole tarpeen itse tuottaa kaikkia palveluita tai määrätä kaikista sääntelyn yksityiskohdista. Hallinnon toimintamuotoja voidaan määritellä väljemmin ja yksityisoikeudelliset toimet ovatkin yleisiä. Toisaalta useat palvelut voivat olla sekä julkisen että yksityisen sektorin vastuulla.[72] Monien ICT-palveluiden osalta näin onkin, sillä yhä useammin palvelun teknisestä tuottamisesta julkisella sektorilla vastaa yksityinen informaatioteknologia-alan yritys. Vanhan sanonnan mukaisesti vastuuta ei kuitenkaan voi ulkoistaa. Tietojärjestelmän tai -palvelun omistavalla viranomaisella on viime kädessä vastuu palvelusta ja sen toimivuudesta, vaikka se hankkisi jonkin palvelun tai palvelukomponentin markkinoilta. Sopimusnäkökulmasta voidaan todeta, että vaikka julkisia hankintoja on lailla säännelty varsin yksityiskohtaisesti, ovat kuitenkin julkisia hankintoja koskevat sopimukset yksityisoikeudellisia[73].

Hyvän hallinnon vaatimukset ulottuvat myös informaatiohallintoon. Laajassa mielessä näihin vaatimuksiin kuuluvat asianmukaisesti järjestetty asiakirjahallinta, tietoturvalli-

---

[71] *Mäenpää* 2017, s. 144–280.
[72] *Mäenpää* 2017, s. 8–22.
[73] *Mäenpää* 2017, s. 62.

suus, laadukkaat asiointipalvelut, viranomaisten tietovarantojen hyvä julkisuus- ja salassapitorakenne sekä tehokkaat ohjelmistotuotantomenetelmät.[74] Tietoturvallisuuden hallinnan on oltava integroitu osa laadukkaaseen toimintaan pyrkivää hyvää hallintoa.[75] Palvelukohtainen tietoturvallisuuden arviointi on osa asianmukaisesti järjestettyä hyvää informaatiohallintoa.[76]

Informaatiohallintoa määrittävät sitä koskeva lainsäädäntö ja lain nojalla annetut muut säännökset sekä erilaiset määräykset, suositukset ja ohjeet. Nämä yhdessä tapaoikeudellisten periaatteiden kanssa luovat hyvän informaatiohallinnon oikeudelliset perusteet. Hallinnon asiakkaan näkökulmasta hyvä informaatiohallinto ilmenee sähköisten asiointipalveluiden hyvänä toimintana, asioiden nopeana ja virheettömänä käsittelynä sekä ohjeiden ja päätösten selkeytenä.[77] Viranomaisen tulee noudattaa julkisuuslaissa määriteltyä *hyvää tiedonhallintatapaa* ja myös viranomaisen tietojärjestelmien ja tietojenkäsittelyn on tätä tuettava. Keskeisenä tavoitteena hyvässä tiedonhallintatavassa on tiedon laadun säilyttäminen. Tässä tapauksessa tiedon laatuun luetaan erityisesti tiedon saatavuus, käytettävyys, eheys sekä suojaaminen.[78]

2.2.1 Hyvä tiedonhallintatapa

Hyvä tiedonhallintatapa määritellään säädöstasolla julkisuuslaissa. Sen 18 §:n mukaan viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä. Lainkodassa on lisäksi esitetty luettelo niistä toimenpiteistä, joita viranomaiselta vähintään edellytetään hyvän tiedonhallintatavan toteuttamiseksi.

---

[74] *Voutilainen* 2009, s. 44.
[75] *Pöysti* 2002, s. 245.
[76] *Voutilainen* 2009, s. 206.
[77] *Voutilainen* 2009, s. 147.
[78] *Mäenpää* 2017, s. 369.

Lainvalmisteluaineiston mukaan luetteloa ei tule tulkita tyhjentäväksi. Luettelossa ei tuoda julki kaikkia viranomaiselle asetettuja velvoitteita hyvän tiedonhallintatavan edistämiseksi vaan sisältö määräytyy, kuten hallituksen esityksessä todetaan, ajan sekä esiin tulevien tilanteiden mukaan. Viranomaisten tietoaineistoihin kohdistuu erilaisia intressejä, kuten asiakirjan julkisuus ja salassapito, arkistointi, henkilötietojen suoja, tietojen käyttörajoitukset sekä tietoturvallisuus. Nämä on haluttu liittää yhteen hyvän tiedonhallintatavan käsitteellä.[79]

Voutilainen tiivistää hyvän tiedonhallintatavan sisältöä siten, että sen ytimessä ovat viranomaisen toiminnan ja julkisten tietovarantojen tietoturvallisuudesta huolehtiminen sekä tietoon liittyvien oikeuksien huomioiminen. Lisäksi hyvän tiedonhallintatavan asettamia vaatimuksia ovat viranomaisen tietojärjestelmien rakenteellinen julkisuus sekä viranomaisen henkilöstön toimiminen hyvän tiedonhallintatavan edellyttämällä tavalla.[80] Saarenpää kuvaa kyseistä lainkohtaa yhdeksi verkkoyhteiskunnan periaatteellisesti merkityksellisimmistä julkisen sektorin säännöksistä.[81]

3 Henkilötietojen suoja

3.1 Tiedollinen itsemääräämisoikeus

Yksityiselämän suojaamisessa on lähtökohtana yksilön oikeus elää ilman ulkopuolisten, esimerkiksi viranomaisten, aiheetonta tai mielivaltaista puuttumista hänen elämäänsä.[82]

Bygrave jakaa tietosuojalainsäädännön syntymiseen vaikuttaneet tekijät kolmeen: teknologiseen ja organisatoriseen kehitykseen, näiden kehittymisen aiheuttamiin pelkoihin sekä oikeudellisiin tekijöihin. Erityisen keskeistä on ollut eri organisaatioiden tallentamien henkilötietojen määrän kasvu sekä tietojen kerääminen suuriin keskitettyihin tieto-

[79] HE 30/1998 vp, s. 76.
[80] *Voutilainen* 2006, s. 61.
[81] *Saarenpää* 2016, s. 139.
[82] *Korja* 2016, s. 115.

varastoihin. Bygraven mukaan on jatkuvasti enemmän todistusaineistoa siitä, että merkittävä osa kerätystä tiedosta ei ole riittävän oikeaa, tarkkaa, täydellistä tai yleensä relevanttia tietojen käsittelyn tarkoitukseen nähden.[83]

Yleisen itsemääräämisoikeuden yksi elementti on *tiedollinen itsemääräämisoikeus*. Yksilöllä on oikeus olla yhteiskunnassa yksin niin halutessaan. Perinteisen fyysisen yksityisyyden rinnalle on verkkoyhteiskunnassa noussut tiedollinen yksityisyys, jota perusoikeusnäkökulmasta tuetaan oikeuksilla luottamukselliseen viestintään ja henkilötietojen suojaan. Meillä tulee olla oikeus itse määritellä yksityisyytemme rajat ja siten myös digitaalinen identiteettimme kuuluu tiedollisen itsemääräämisoikeutemme piiriin.[84] Yksilöllä on itsemääräämisoikeutensa perusteella oikeus päättää itseensä kohdistuvista toimenpiteistä, omista tiedoistaan ja itseään koskevista asioista.[85]

Tiedollinen itsemääräämisoikeus yhdistetään siis henkilötietojen suojaan. Yksilöllä tulee olla mahdollisuus vaikuttaa siihen kuka, miten ja missä hänen henkilötietojaan käsittelee. Nyky-yhteiskunta asettaa erilaisia tarpeita henkilötietojen käsittelylle. Tietoja on käsiteltävä hyvinvointivaltion palveluiden tuottamisessa, väestön hallinnoinnissa ja kaupankäynnissä. Toiminta esimerkiksi ilman terveydenhuollon rekistereitä tai sähköisiä maksuvälineitä olisi tehotonta. Yhteiskunnassa toimiminen edellyttääkin sitä, että yksilö luopuu osasta yksityisyyttään. Tämä puolestaan nostaa henkilötietojen suojan keskiöön kysymykset siitä, millä ehdoilla henkilötietoja voidaan käsitellä ja miten kerättyjä tietoja voidaan luovuttaa tai yhdistellä.[86] Käytännössä ilman henkilötietojen suojaa ei voida tehokkaasti toteuttaa nykyajan informaatiohallinnon prosesseja.

Perusoikeutemme henkilötietojen suojaan on yksi tärkeimmistä oikeushyvistä, mutta samalla yksi loukatuimmista.[87] Digitaalisessa maailmassa yksityisyyden suojan kokonaisuuden turvaamat oikeudet linkittyvät toisiinsa. Jokaisella yksilöllä on tietoja, joita tämä

---

[83] *Bygrave* 2002, s. 93–95.
[84] *Saarenpää* 2016, s. 216.
[85] *Korja* 2016, s. 99.
[86] *Neuvonen* 2014, s. 59–60.
[87] *Saarenpää* 2016, s. 75.

ei halua julkisuuteen tai muiden tietoon tarpeettomasti ja jokaisella on fyysinen piiri, jota suojataan ulkopuolisten häirinnältä.[88]

Tieteen ja teknologian kehittyminen voivat tuoda perustuslailliselle yksityiselämän suojalle uusia uhkatekijöitä, joihin ei lainsäädännön keinoin pystytä ennalta varautumaan. Yksityiselämän perustuslaillinen suoja ulottuu kuitenkin tällaisten ennakoimattomien muutosten mahdollisesti aiheuttamaan puuttumiseen yksityiselämään.[89]

3.2 Henkilötietojen suoja ihmis- ja perusoikeutena

Demokraattinen oikeusvaltio perustuu keskeisiin valtiosääntöperiaatteisiin, kuten demokratiaan ja perusoikeuksiin. Demokraattisessa oikeusvaltiossa ennalta asetetut normit määrittelevät yksilöiden oikeudet, velvollisuudet ja vastuut, jotka toteutetaan yhtäläisesti ja tehokkaasti. Henkilötietojen suojan keskeinen tehtävä on järjestää ne puitteet, joiden mukaan on sallittua käsitellä henkilötietoja.[90]

Yksi merkittävimmistä Suomea velvoittavista kansainvälisistä ihmisoikeussopimuksista on *Euroopan ihmisoikeussopimus* (SopS 18-19/1990, jäljempänä EIS). Tämän sopimuksen noudattamista jäsenvaltioissa valvoo Euroopan ihmisoikeustuomioistuin (EIT). EIT:n oikeuskäytännön velvoittavuus on vahva. Sen päätöksissä esitetyt oikeudelliset arviot ja johtopäätökset ovat oikeudellisesti sitovia viranomaisen päätöksenteossa. Kysymyksessä on Suomea sitovien kansainvälisten velvoitteiden sisältöä koskevien tulkintojen noudattaminen.[91]

EIS 8 artiklassa säädetään jokaisen oikeudesta nauttia yksityis- ja perhe-elämän kunnioitusta. Artiklan 1 kohdan mukaisesti jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Artiklan 2 kohdan mukaan viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen

---

[88] *Neuvonen* 2014, s. 243.
[89] *Korja* 2016, s. 217.
[90] *Korja* 2016, s. 117–408.
[91] *Mäenpää* 2017, s. 181.

turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojelemiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi. Lainkohdasta voi tehdä huomion, että vaikka ensimmäinen kohta on kirjoitettu varsin ehdottomaan muotoon, sallii jälkimmäinen kuitenkin useita poikkeamisperusteita.

Vuonna 2009 voimaan tulleella *Lissabonin sopimuksella* (2007/C 306/01, Euroopan Unionista tehdyn sopimuksen ja Euroopan Yhteisön perustamissopimuksen muuttamisesta)[92] muutettiin Euroopan unionin perustamissopimuksia ja samalla EU:n perusoikeuskirjalle annettiin sama oikeudellinen arvo kuin perustamissopimuksilla on. Lissabonin sopimuksella EU sai myös oikeushenkilöllisyyden[93].

Euroopan unionin perusoikeuskirjassa (2012/C 326/02)[94] turvataan kahdessa erillisessä artiklassa sekä yksityis- ja perhe-elämää että henkilötietojen suojaa. Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. 8 artiklan mukaisesti jokaisella on oikeus henkilötietojensa suojaan. Lisäksi artiklassa säädetään, että tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on lisäksi oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada ne oikaistuksi. 8 artiklan 3 kohdassa säädetään edelleen, että sääntöjen noudattamisen valvonnasta vastaa riippumaton viranomainen.

Euroopan unionin toiminnasta tehdyn sopimuksen (2012/C 326/01, SEUT-sopimus)[95] 16 artiklassa on vahvistettu, että jokaisella on oikeus henkilötietojensa suojaan. 16 artiklan 2 kohdassa säädetään toimivallasta henkilötietojen suojan osalta siten, että Euroopan parlamentti ja neuvosto antavat säännökset tavallisessa lainsäätämisjärjestyksessä. Kyseisestä menettelystä säädetään SEUT-sopimuksen 294 artiklassa[96].

---

[92] EUVL C 206, 17.12.2007.
[93] *Neuvonen* 2013, s. 35.
[94] EUVL C 326, 26.10.2012, s. 391.
[95] EUVL C 326, 26.10.2012, s. 55.
[96] EUVL C 326, 26.10.2012, s. 173–175.

Kansallisella tasolla PL 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Lainkohdan mukaisesti henkilötietojen suojasta säädetään tarkemmin lailla.

Usein kuulee käytävän keskustelua omien henkilötietojen omistamisesta. Tätä kysymystä ei voi kuitenkaan suoraan rinnastaa tiedolliseen itsemääräämisoikeuteen. Eurooppalaisen käytännön mukaisesti henkilötietojen suoja on perusoikeus, eikä perusoikeuden luovuttaminen ole mahdollista. Näin ollen henkilötietojen suoja asettaa valtiolle turvaamisvelvoitteen, joka lainsäädännön kautta heijastuu yksityisten välisiin suhteisiin. Omistajuusnäkökulma henkilötietoihin on lähinnä yhdysvaltalaisen historiallisen kehityksen tulos. USA:ssa nimittäin on yksityisyyden suojan lähtökohdaksi otettu vahingonkorvausoikeus ja malli, jossa vahingonkorvausta voidaan hakea sen seurauksena, että henkilön yksityiseen piiriin on tunkeuduttu oikeudettomasti. Yksityisyyden perustuslaillinen suoja siis puuttuu. Puutteellista yksityisyyden suojaa paikataan määrittelemällä henkilötiedot omaisuudeksi ja soveltamalla loukkauksiin vahingonkorvauslakia. Euroopassa yksityisyyden suojalla on vahva valtiosääntö- ja perusoikeuskytkentä ja tämän vuoksi yksityisyyden suojan käsittäminen omaisuutena on ongelmallista.[97]

3.3 Henkilötietojen suoja Euroopan unionissa

EU-lainsäädäntöön kuuluvia unionin säädöksiä ovat asetukset, direktiivit ja päätökset. Tärkeimmät materiaaliset oikeuslähteet hallintotoiminnan kannalta ovat asetukset ja direktiivit, mutta myös päätöksiin voi sisältyä sovellettavia normeja. Unionin lainsäädännön tulkintaa ja soveltamista täsmentää myös sitä koskeva oikeuskäytäntö, jota ei kuitenkaan voida soveltaa samalla tavoin kuin yksittäisiä normeja. Oikeuskäytäntö ohjaa joustavammin ja yleisemmällä tasolla EU-oikeuden toimeenpanoa. Kun arvioidaan materiaalisia säännöksiä koskevaa oikeuskäytäntöä, on huomioitava kulloinkin ratkaistun tapauksen erityispiirteet.[98]

---

[97] *Neuvonen* 2014, s. 68–69.
[98] *Mäenpää* 2017, s. 127.

Asetuksia käytetään oikeustilan yhtenäistämiseen aloilla, joilla unionilla on yksinomainen tai laaja toimivalta. Tällaisia ovat erimerkiksi kilpailun valvonta ja arvonlisäverotus. Asetuksia ei saateta kansallisesti voimaan, vaan niistä tulee osa jäsenvaltion oikeutta heti voimaantulon jälkeen. Asetuksen säännöksillä on välitön oikeusvaikutus kansallisissa oikeusjärjestyksissä, joka ulottuu niin viranomaisten ja yksityisten välisiin suhteisiin kuin yksityisten oikeussubjektien välisiin suhteisiin. Viranomaiset soveltavat asetuksia sellaisinaan. *Direktiivejä* käytetään jäsenvaltioiden lainsäädäntöjen lähentämiseen aloilla, joilla kansallinen päätöksentekovalta on laaja. Tällaisia ovat erimerkiksi viestinnän sääntely ja työelämä. Direktiivi määrittelee puitteet ja tavoitteet, jotka jäsenvaltion on toteutettava. Miten tavoitteet yksityiskohtaisesti toteutetaan, on jäsenvaltion päätösvallassa. Oikeusvaikutusten saamiseksi kansallisessa järjestelmässä direktiivit implementoidaan, eli saatetaan osaksi kansallista oikeusjärjestystä. Mikäli kansallinen voimassa oleva lainsäännös ei jo vastaa direktiivin asettamia vaatimuksia, tämä edellyttää yleensä lainsäädäntötoimenpiteitä.[99]

Henkilötietojen suojasta tällä tasolla säädettiin aikaisemmin direktiivillä, josta yleisesti käytetään nimitystä *henkilötietodirektiivi* (Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta)[100]. Henkilötietodirektiivi oli voimassa vuodesta 1995 lähtien ja se on kansallisesti saatettu voimaan henkilötietolailla (22.4.1999/523, jäljempänä HetiL).

3.3.1 Yleinen tietosuoja-asetus

Henkilötietojen suojan sääntelyn uudistamista valmisteltiin EU:ssa varsin pitkään. Vuosien valmistelutyön jälkeen annettiin keväällä 2016 asetus, joka korvaa henkilötietodirektiivin ja on asetuksena jäsenvaltioissa suoraan sovellettavaa oikeutta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta

[99] *Mäenpää* 2017, s. 128–129.
[100] EYVL L 281, 23.11.1995, s. 31.

liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), jäljempänä tietosuoja-asetus tai asetus)[101]. Asetus tuli voimaan 24.5.2016 ja sitä aletaan soveltaa siirtymäajan päätyttyä 25.5.2018. Asetus tunnetaan maailmalla yleisesti sen englanninkielisestä nimestä johdetulla lyhenteellä GDPR (*General Data Protection Regulation*).

EU hyväksyi *tietosuojakehyksen* merkittävän uudistuksen. Tietosuojakehys[102] muodostuu yleisestä tietosuoja-asetuksesta ja niin sanotusta *poliisidirektiivistä* (Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta).[103] Yleisen tietosuoja-asetuksen tavoitteena on esitellä yhdenmukainen oikeudellinen kehys, jonka mukaisia sääntöjä sovelletaan yhdenmukaisesti ja josta koituisi siten hyötyä EU:n sisämarkkinoiden kehitykselle. Tavoitteena on lisäksi taata tasapuoliset toimintaedellytykset kaikille EU:n markkinoilla toimiville yrityksille.[104]

Keskeisenä lähtökohtana tietosuoja-asetuksessa on ollut rekisteröidyn oikeuksien parantaminen. Näitä tavoitteita toteutetaan muun muassa säännöksillä sisäänrakennetusta ja oletusarvoisesta tietosuojasta, vahvemmista yksilöiden oikeuksista (kuten oikeus tulla unohdetuksi[105]), yksilöiden paremmista mahdollisuuksista hallita omia henkilötietojaan ja siirtää niitä järjestelmästä toiseen, vahvemmasta suojasta tietoturvaloukkauksia vastaan, tilivelvollisuusperiaatteesta (*accountability*) sekä tietosuojaviranomaisten mahdollisuudesta määrätä hallinnollisia sakkoja rekisterinpitäjille ja henkilötietojen käsittelijöille niiden toimittua vastoin asetuksessa säädettyä.[106]

---

[101] EUVL L 119, 4.5.2016, s. 1–88.
[102] Tietosuojakehykseen voitaneen jatkossa lukea kuuluvaksi myös valmisteilla oleva EU:n sähköisen viestinnän tietosuoja-asetus (nk. ePrivacy-asetus). Ks. myös jakso 4.5.
[103] EUVL L 119, s. 89–131.
[104] COM (2018) 43, s. 1–2.
[105] Oikeus tulla unohdetuksi ei voi tietenkään olla ehdoton. Rekisteröity ei voi esimerkiksi vaatia tietojaan poistettavaksi tapauksissa, joissa niiden säilyttämisestä, usein määräajaksi, on säädetty erikseen. Tällaisia tiedon tallennus- ja säilytysvelvollisuuksia on säädetty mm. teleoperaattoreille, finanssialan toimijoille sekä sosiaali- ja terveydenhuollon alalla.
[106] COM (2018) 43, s. 2–4.

Vastuullisuuden tai vastuutettavuuden (accountability) käsitteellä tarkoitetaan edellä mainitun tilivelvollisuuden lisäksi sitä, että tietojen käyttämisestä tai muuttamisesta jää jälki, jonka perusteella voidaan jälkikäteen selvittää, ketkä tietoja ovat käsitelleet. Käsitteellä voidaan tarkoittaa organisaatiotasolla myös sitä, että organisaatio itse osoittaa menettelevänsä lain säännösten ja hyvän tiedonhallintatavan mukaisesti. Asetuksessa korostetaan nimenomaan vastuutettavuutta ja tarkastettavuutta, joita on pidettävä aktiivisempana toimintana kuin pelkkää lainmukaisuutta (*compliance*).[107]

Asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa (2(1) art.). Asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei (3(1) art.).

Asetuksen mukaan *henkilötiedoilla* tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella (4(1)(1) art.). *Neuvosen* mukaan henkilötieto on sinällään teknologianeutraali[108] käsite. Se kattaa kaikenlaiset tiedot, joista yksin tai yhdistelemällä luonnollinen henkilö on yksilöitävissä. Henkilötietoja ovat esimerkiksi kameravalvontatallenteet tai ajoneuvon rekisteritunnus.[109]

Henkilötietojen käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä,

---

[107] *Pitkänen et al.* 2013, s. 216.
[108] Ks. myös *Saarenpää* 2016, s. 92, jonka mukaan uusi lainsäädäntömme on jo pitkään ainakin periaatteessa, ollut teknologianeutraalia, eli se ei ole sisältänyt juurikaan tietoteknisiä ilmaisuja.
[109] *Neuvonen* 2014, s. 74.

jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista (4(1)(2) art.).

Asetuksen mukaan *rekisterillä* tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu (4(1)(6) art.). Rekisteri muodostuu samassa käyttöyhteydessä olevista tiedoista, eivätkä tietojen sijainti tai merkitsemistapa ole ratkaisevia. Mikä tahansa kokonaisuus, joka koostuu henkilöiden tiedoista, on rekisteri.[110] *Rekisterinpitäjällä* tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti (4(1)(7) art.). Asetuksessa tarkoitetaan *henkilötietojen käsittelijällä* luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (4(1)(8) art.).

Kaiken kaikkiaan tietosuoja-asetus on säädöksenä varsin laaja, sisältäen 173-kohtaisen johdanto-osan ja 99 artiklaa alakohtineen. Asetuksen laajuuden vuoksi sitä ei ole mielekästä käydä yksityiskohtaisesti läpi tässä tutkimuksessa, vaan jäljempänä keskityn tutkimuksen aihepiirin kannalta keskeisiin säännöksiin.

3.4 Kansallinen sääntely

3.4.1 Henkilötietolaki yleislakina ja erityislainsääntö

Aiemmin mainitun henkilötietodirektiivin voimaansaattamisen lisäksi perustuslaillinen lainsäädäntötoimeksianto (PL 10 §) toteutettiin Suomessa HetiL:lla. Lain tarkoituksena

[110] *Neuvonen* 2014, s. 75.

on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (1 §). HetiL on henkilötietojen käsittelyä koskeva yleislaki ja sitä sovelletaan, jollei muualla laissa toisin ole säädetty (2.1 §). Lakia sovelletaan niin henkilötietojen automaattiseen käsittelyyn kuin muunkin tyyppiseen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa (2.2 §).

Kotimaisen erityislainsäädännön määrää tietosuojan alalla voidaan pitää merkittävänä. Lisäksi lainsäädäntömme sisältää runsaan määrän säädöksiä, joissa viitataan nykyiseen HetiL:iin. HetiL:a täydentävästi henkilötietojen suojasta on säädetty ainakin seuraavissa säädöksissä:

- laki viranomaisen toiminnan julkisuudesta (21.5.1999/621)
- laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (21.8.2009/661)
- laki yksityisyyden suojasta työelämässä (13.8.2004/759)
- luottotietolaki (11.5.2007/527)
- tietoyhteiskuntakaari[111] (7.11.2014/917, 1.6.2018 alkaen nimeltään Laki sähköisen viestinnän palveluista)
- laki henkilötietojen käsittelystä poliisitoimessa (22.8.2003/761)
- laki terveydenhuollon valtakunnallisista henkilörekistereistä (9.6.1989/556)
- laki potilaan asemasta ja oikeuksista (17.8.1992/785)
- laki verotustietojen julkisuudesta ja salassapidosta (30.12.1999/1346)

Korhonen on todennut, ettei erityislainsäädännön suuri määrä ole välttämättä hyvä asia ja se saattaa rapauttaa tietosuojan uskottavuutta. Joka tapauksessa se hämärtää tietosuojan yleislakien eli henkilötietolain ja julkisuuslain asemaa ja merkitystä. Ongelmia voi siten syntyä määriteltäessä yleislakien ja erityislakien välisten säännösten suhteita.[112]

---

[111] Tietoyhteiskuntakaarta lain nimenä voidaan pitää jo lähtökohtaisesti harhaanjohtavana, sillä kyseisessä säädöksessä säädetään hyvin rajatusta määrästä informaatiohallintoa ja -infrastruktuuria koskevia asioita.
[112] *Korhonen* 2003, s. 297.

3.4.2 Tietosuojalakiesitys

EU:n tietosuoja-asetuksen myötä kotimainen lainsäädäntö on parasta aikaa muutostyön kohteena. Keväällä 2018 hallitus on antanut eduskunnalle esityksen EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Esityksessä ehdotetaan säädettäväksi uusi tietosuojalaki, joka sisältäisi täydentävät ja täsmentävät säännökset tietosuoja-asetukseen nähden. Samalla esitetään kumottavaksi HetiL sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta.[113] Tietosuojalain säätämisessä on kysymys tietosuoja-asetuksen salliman kansallisen liikkumavaran käyttämisestä tietyissä asioissa.

Lakiesityksen mukaisesti tietosuojalaissa säädettäisiin lain tarkoituksesta ja soveltamisalasta (1 luku), henkilötietojen käsittelyn oikeusperusteesta eräissä tapauksissa (2 luku), valvontaviranomaisesta (3 luku), oikeusturvasta ja seuraamuksista (4 luku) sekä tietojenkäsittelyn erityistilanteista[114] (5 luku).[115]

Vaikka lakiesitystä ei ole tarkoitus tässä käydä tarkemmin läpi, voidaan todeta, että seurannaisvaikutuksena muutoksia aiheutuu myös edellä mainittuun erityislainsäädäntöön ja muihin lakeihin, jotka sisältävän viittauksia nykyiseen HetiL:iin. Käytännön esimerkkinä tästä kehityksestä voidaan mainita sosiaali- ja terveydenhuollon alalla meneillään oleva säädöshanke, jonka tavoitteena on yhtenäistää sosiaali- ja terveydenhuollon asiakas- ja henkilötietojen käyttöä ohjaava lainsäädännön kokonaisuus sekä saattaa säädökset vastaamaan tietosuoja-asetuksen vaatimuksia.[116]

---

[113] HE 9/2018 vp, s. 1.
[114] Erityistilanteilla tarkoitetaan henkilötietojen käsittelyä journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten.
[115] HE 9/2018 vp, s. 129–136.
[116] HE 159/2017 vp, s. 1.

4 Tietoturvallisuus

4.1 Tietoturvallisuus oikeusvaltiossa

Nykyisessä verkkoyhteiskunnassa *tietoturvallisuus* on yhteiskunnallisesti, tietoteknisesti ja oikeudellisesti merkittävä asia, jonka kriittinen merkitys on otettava vakavasti toiminta- ja sääntelyongelmana. Tietoverkkojen käyttämisestä jää pääsääntöisesti aina jälkiä. Tämän vuoksi salassapitosäännöksin ja tietoturvallisuustoimenpitein on tuettava anonymiteetin toteutumista informaatiohallinnossa.[117] Tietosuoja, henkilötietojen suoja ja tietoturvallisuus sekoitetaan usein käsitteellisesti toisiinsa. Tietosuojassa on kysymys informaatiota koskevista aineellisista normeista, joihin nähden tietoturvallisuus on välineellinen asia. Oikeudellisessa merkityksessä tietoturvallisuus muodostuu normeista, jotka koskevat informaation luottamuksellisuuden, eheyden, aitouden sekä käytettävyyden suojaamista.[118] Myös tietosuojan käsitettä voidaan pitää osittain harhaanjohtavana, sillä tietosuojalainsäädännön tavoitteena ei ole suojata tietoja sinänsä vaan yksilöitä ja heidän perusoikeuksiaan, erityisesti henkilötietojen väärinkäyttöä vastaan.[119]

PL 7.1 §:n mukaisesti *jokaisella on oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen. Råman* näkee tietoturvallisuuden niin tärkeänä osana yksilöiden toimintaa ja oikeuksien käyttöä verkkoyhteiskunnassa, että se voidaan lukea yhdeksi kyseisen lainkohdan suojaamista oikeuksista.[120]

---

[117] *Saarenpää* 2016, s. 67–239.
[118] *Korhonen* 2016, s. 362–363.
[119] *Korja* 2016, s. 116. *Korja* käyttää tässä yhteydessä jopa niin voimakasta termiä kuin ”informaatioväkivalta”.
[120] *Råman* 2006, s. 819.

Tietoturvallisuus on paljon enemmän kuin asetusten ja ohjeiden tasoinen tekninen tai ainoastaan rikosoikeudellinen kysymys. Saarenpää luonnehtiikin tietoturvallisuutta eräänlaiseksi *metaperusoikeudeksi*[121]. Ilman tietoturvallista informaatioinfrastruktuuria verkkoyhteiskunta ei toimi demokraattisen oikeusvaltion edellytysten mukaisesti.[122] Siten tietoturvallisuus on edellytyksenä toimivalle informaatioinfrastruktuurille ja se mahdollistaa perusoikeuksien turvallisen käytön tietoverkoissa.[123]

Käytännön toimijat tarkastelevat tietoturvallisuutta osana organisaation toimintaa sen palveluiden ja tuotteiden turvallisuuden kautta. Oikeustieteen harjoittajan näkökulmasta kyse on taas yksilön oikeuksien ja yhteiskunnan toimintojen turvaamisesta ja näiden välisestä tasapainosta. Oikeusperiaatteena tietoturvallisuus on kuitenkin vielä selkiytymätön. Tietoturvallisuus on oikeudellisesta näkökulmasta erityisesti perusoikeuksiemme taustalla vaikuttava ylempitasoinen periaate, metaperiaate.[124]

Oikeusvaltion käsitteeseen sekä perusoikeusajatteluun sisältyy ajatus oikeuden tehokkaasta toteutumisesta, mihin myös tietoturvallisuus liittyy. Siksi oikeuden kiinnostuksen kohteena ovat nykyaikainen infrastruktuuri ja tekniset ratkaisut. Ne määrittävät ympäristön, jossa oikeuksia toteutetaan. Hyvin järjestettyinä ne edistävät oikeuksien toteutumista ja huonosti järjestettyinä voivat asettaa esteitä oikeuksiin pääsylle. Tekninen tietoturvallisuus luo edellytyksiä oikeuksien tehokkuudelle, eli oikeusvarmuuden toteutumiselle. Oikeusvarmuus on lakiin perustuvaa ennustettavuutta ja hyväksyttävyyttä. Siten oikeudellinen tietoturvallisuus luo edellytyksiä oikeusvarmuudelle. Tietoturvallisuus on informaation ja tiedon käsittelyn tavoitetila ja se on muuttunut välttämättömästä teknisestä edellytyksestä oikeudellisen sääntelyn päämääräksi ja tavoitteeksi.[125]

---

[121] Ks. myös *Pöysti* 2002, s. 242, jonka mukaan tietoturvallisuus metaoikeutena on oikeudellinen rakenne, joka kuvaa yksittäisen lain säännöksen taustalla olevia arvoja ja tavoitteita, joiden tulee vaikuttaa myös lain tulkintaan ja hallinnon käytäntöihin.
[122] *Saarenpää* 2016, s. 123.
[123] *Råman* 2006, s. 819.
[124] *Råman* 2006, s. 818.
[125] *Pöysti* 2002, s. 240–242.

Tietoturvallisuuden selkeänä lähtökohtana tulee olla yksilöiden suojaaminen myös muilta kuin valtiovallan taholta tulevilta loukkauksilta, sillä yksilön ja hänelle palveluita tarjoavan tahon välillä ei vallitse yhdenvertainen asema ja ilman selkeitä sääntöjä tämä asetelma saattaa uhata yksilöiden perusoikeuksien toteutumista.[126] Hyvän hallinnon periaate edellyttää, että tietoturvallisuus on integroitu osaksi hallinnon menettelyitä ja perustoimintaa.[127]

Viranomaistoiminta on informaatio- ja teknologiakeskeistä ja siten riippuvaista teknisten laitteiden sekä ohjelmistojen toimivuudesta. Viranomaisen velvollisuutena on huolehtia toimintansa tietoturvallisuudesta. Erityisesti sähköisten palveluiden osalta tietoturvallisuuden tavoitteena on lisätä hallinnon asiakkaiden luottamusta hallinnon toimivuuteen. Tietoturvallisuudella varmistetaan myös viranomaisen lainmukainen toiminta tietojenkäsittelytoiminnassa. Suppeasti katsottuna tietoturvallisuus palvelee informaatiohallinnossa kahta tarkoitusta. Ensinnä sen avulla varmistetaan yksilön oikeus saada esteettä julkisia tietoja ja toiseksi turvataan yksilön oikeus tiedolliseen yksityisyyteen, kun kyseessä ovat salassa pidettävät tiedot.[128] Tietoturvallisuus olisi kuitenkin ymmärrettävä laaja-alaisesti kaikkeen organisaation informaation kokoamiseen, hyödyntämiseen ja muuhun käsittelyyn sekä kaikkiin prosesseihin ja johtamiseen liittyvänä asiana.[129]

Tietoturvallisuus ja tietosuoja ovat vuorovaikutussuhteessa keskenään. Tietoturvallisuuden toteuttamisessa voi nousta esiin kysymyksiä, joihin tietosuojan tulisi antaa vastauksia. Kysymyksessä voi olla esimerkiksi arvio jonkin tietoturvatoimenpiteen vaikutuksesta tietosuojaan. Toisaalta voi olla kysymys siitä, että tietoturvan nimissä tehtävä seurantamenettely tietojärjestelmässä olisi mahdollisesti laillistettu tietosuojaloukkaus perustuslaillista henkilötietojen suojaa kohtaan.[130]

---

[126] *Råman* 2006, s. 822.
[127] *Pöysti* 2002, s. 238–239.
[128] *Voutilainen* 2006, s. 109–118.
[129] *Pöysti* 2002, s. 234.
[130] *Voutilainen* 2009, s. 199.

4.2 Tietoturvallisuusperiaatteet

Tietoturvallisuuden sanotaan olevan yhtä aikaa paradigma, filosofia ja ajattelutapa.[131] Tietoturvallisuuden perusajatuksena on, että jälkiteollisessa yhteiskunnassa organisaatioiden tärkein omaisuuserä on tieto, joka halutaan pitää luotettavasti, nopeasti, oikeassa muodossa ja oikeiden henkilöiden saatavilla. Sähköisessä kaupankäynnissä ja julkisyhteisöjen sähköisessä asioinnissa puolestaan on tärkeää, että tietojärjestelmät pystyvät luotettavasti ja aukottomasti kertomaan, kuka tai ketkä ovat luoneet järjestelmässä olevat tiedot. Klassisesti tietoturvallisuus määritellään tiedon arvoon perustuen. Tällöin tietoturvallisuus muodostuu tiedon luottamuksellisuudesta, käytettävyydestä ja eheydestä.[132]

Tiedon luottamuksellisuudella (*confidentiality*) tarkoitetaan sitä, että tietojärjestelmän tiedot ovat vain niiden henkilöiden käytettävissä, joilla on niihin oikeus. Tiedon käytettävyydellä (*availability*) tarkoitetaan sitä, että tarvittavat tiedot ovat saatavilla tietojärjestelmästä oikea-aikaisesti ja oikeassa muodossa. Tiedon eheydellä (*integrity*) puolestaan tarkoitetaan sitä, että tietojärjestelmän tiedot ovat paikkansa pitäviä eivätkä sisällä tahallisia tai tahattomia virheitä.[133]

Tietojen luottamuksellisuutta pyritään suojaamaan käyttäjätunnuksin ja salasanoin sekä esimerkiksi suojaamalla tiedot salakirjoituksella. Salakirjoitus sopii hyvin erityisesti arkaluontoisten tai erityisen arvokkaiden tietojen suojaamiseen. Tietojen käytettävyydestä pyritään huolehtimaan siten, että tietojärjestelmien laitteet ja ohjelmistot olisivat riittävän tehokkaita ja mahdollisimman hyvin soveltuvia kuhunkin tietojenkäsittelytarpeeseen. Tehokkuuden näkökulmasta pyritään myös siihen, että tietojen käsittely olisi mahdollisimman automatisoitua. Tietojen eheyden turvaamiseen pyritään ennen kaikkea ohjelmistoteknisin ratkaisuin. Ohjelmistoissa voidaan käyttää erilaisia syötteen tarkistuksia ja tiedonsiirroissa varmistussummia tai tiivisteitä.[134] Nykyisin viitataan yhä useammin siihen, että tietojen tulisi olla salattuja sekä niiden ollessa tallennettuna (data at rest) että siirrettäessä tietoja (data in transit).

---

[131] *Rhodes-Ousley* 2004, s. 21.
[132] *Hakala et al.* 2006, s. 4.
[133] *Hakala et al.* 2006, s. 4.
[134] *Hakala et al.* 2006, s. 4–5.

Informaatio voi muuttua tietojenkäsittelyprosessissa tai tietoliikenteessä tapahtuneiden virheiden vuoksi. Tällöin muutos kohdistuu nimenomaan tiedon eheyteen, joka kertoo tiedon alkuperäisyydestä. Tiedon eheyden varmistamiseen tähtäävät toimenpiteet varmistavat, että tieto on sen syntymisen tai luomisen jälkeen samassa muodossa, ilman muutoksia, jossa se oli tietyllä ajanhetkellä. Eheyden varmistaminen edellyttää myös jäljitettävyyttä. On kyettävä todentamaan, mitä tietylle tiedolle on tehty, kuka sen on tehnyt ja milloin. Hallinnollisessa prosessissa tiedon eheys toteuttaa oikeusvarmuusfunktiota. Eheydellä todennetaan tällöin hallintopäätöksen sisällöllinen muuttumattomuus päätöksen tekemisen ja jonkin hyväksymistoimenpiteen jälkeen.[135] Hyväksymistoimenpiteenä voi toimia esimerkiksi sähköinen allekirjoittaminen.

Laajemmassa tietoturvallisuuden määritelmässä on edellisten lisäksi huomioitu myös tiedon kiistämättömyys sekä pääsynvalvonta. Kiistämättömyydellä (*non-repudiation*) tarkoitetaan sitä, että tietojärjestelmässä olisi kyky luotettavalla tavalla tunnistaa järjestelmän käyttäjän henkilötiedot. Tavoitteena on, että riittävällä tavalla voidaan varmistua tiedon alkuperästä tai esimerkiksi väärinkäytöstapauksissa vahvistaa tietojen luvaton käyttö. Kiistämättömyys pyritään varmistamaan käyttämällä salausmenetelmiin liittyviä tunnistusmekanismeja, kuten älykortteja tai biometrisiä tunnisteita. Pääsynvalvonnalla (*access control*) rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä sekä estetään ulkopuolisia käyttämästä luvatta organisaation tietojärjestelmiä. Mikäli pääsynvalvontaa ei ole hoidettu asianmukaisesti, myös tietojen eheys ja luottamuksellisuus voivat vaarantua.[136]

4.3 Tietoturvallisuuden osa-alueet

Organisaation kokonaisturvallisuus muodostuu fyysisestä turvallisuudesta ja tietoturvallisuudesta. Fyysisen turvallisuuden suojelukohteena ovat organisaation henkilöstö ja omaisuus. Vastaavasti tietoturvallisuuden suojelukohteena on organisaation tietopääoma.[137] Tietoturvallisuuden kohteena viranomaistoiminnassa ovat tietojenkäsittelytoimintojen turvaaminen, asiakirjajulkisuus, salassapito ja tietosuoja.[138] Henkilötietolain

[135] *Voutilainen* 2009, s. 200–201.
[136] *Hakala et al.* 2006, s. 5–6.
[137] *Hakala et al.* 2006, s. 14.
[138] *Voutilainen* 2009, s. 198.

ja julkisuuslain asettamia velvoitteita toteutetaan teknisin tietoturvallisuustoimenpitein ja kyseiset säädökset määrittävät myös toimenpiteiden toteuttamisen ja laadun arviointikriteerejä.[139]

Tietoturvallisuus jaetaan yleisesti useampaan osa-alueeseen, joita ovat:

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöstöturvallisuus
- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus.[140]

Hallinnollisen turvallisuuden tavoitteena on turvata tietoturvallisuuden kehittäminen ja johtaminen. Myös yhteydenpito sekä sisäisiin että ulkoisiin turvallisuustoimijoihin kuuluu tähän osa-alueeseen. Tärkeänä osana hallinnollista tietoturvallisuutta ovat lainsäädännön ja yksityisoikeudellisten sopimusten vaikutusten arviointi organisaation tietoturvakäytäntöihin.[141]

Fyysisen turvallisuuden tavoitteena on suojata rakennuksen eri tiloja sekä niihin sijoitettuja laitteita ulkoisilta uhilta, kuten ympäristövahingoilta tai tulipalolta. Henkilöstöturvallisuuteen kuuluvat toimenpiteet, joilla varmistetaan tietojärjestelmien käyttäjien toimintakyky ja toisaalta rajataan käyttäjien mahdollisuudet käyttää heille kuulumattomia tietoja ja tietojärjestelmiä. Tietoaineistoturvallisuuteen kuuluvat ne toimenpiteet, jotka toteutetaan tietojen säilyttämiseksi, varmistamiseksi, palauttamiseksi ja tuhoamiseksi. Myös manuaalisen tietojenkäsittelyn avulla käsiteltävät aineistot kuuluvat aineistoturvallisuuden piiriin. Ohjelmistoihin liittyvät turvallisuusasiat kuuluvat nimensä mukaisesti ohjelmistoturvallisuuden piiriin. Ohjelmistoturvallisuuteen kuuluu ohjelmistojen testaaminen,

---

[139] *Pöysti* 2002, s. 239.
[140] *Hakala et al.* 2006, s. 10–12.
[141] *Hakala et al.* 2006, s. 10–11.

jolla pyritään varmistumaan ohjelmistojen soveltuvuudesta suunniteltuun käyttötarkoitukseen, ohjelmistojen yhteentoimivuudesta ja toiminnan luotettavuudesta sekä virheettömyydestä. Ohjelmistoversioiden sekä -lisenssien hallinta kuuluvat myös tähän osa-alueeseen.[142]

Tietoliikenneturvallisuuden piirissä huolehditaan siitä, että käytetyt tiedonsiirtoratkaisut ovat turvallisia.[143] Tietoliikenteen häirinnän valvonta ja estäminen ovat myös keskeisiä tietoturvatoimia.[144]

Huolimatta esitetystä jaottelusta mainitut osa-alueet ovat osin päällekkäisiä. Joka tapauksessa kaikkien osa-alueiden yhteisenä tavoitteena on tiedon luottamuksellisuuden, käytettävyyden, eheyden, kiistämättömyyden ja pääsynhallinnan toteuttaminen.[145] Tietoturvallisuus voidaan toisaalta jakaa myös strategiseen, taktiseen ja operatiiviseen tasoon. Strategiselle tasolle kuuluvat organisaation turvallisuusstrategia ja tavoitteet sekä turvallisuuskulttuurin edistäminen organisaatiossa. Taktiselle tasolle kuuluvat strategiaan pohjautuvat konkreettiset suunnitelmat ja vastuiden jakaminen sekä konkreettisten toimenpiteiden arviointi ja seuranta. Operatiiviselle tasolle puolestaan kuuluu jokapäiväinen toiminta, ylemmillä tasoilla päätettyjen toimenpiteiden implementointi sekä käytännön teknisten ratkaisujen toteuttaminen.[146]

4.4 Riskienhallinta

Tietoturvallisuus on perusteettoman riskinoton vastakohta ja osa *riskienhallintaa*. Sen avulla pyritään ennakolta varautumaan häiriötilanteisiin ja ehkäisemään niiden muuttuminen vahingoiksi. Oikeudellisessa tietoturvallisuusajattelussa tämä ilmenee esimerkiksi rekisterinpitäjälle säädetyllä huolellisuusvelvoitteella. Toteutuessaan tietoturvallisuusriskit ovat yhä useammin taloudellisia vahinkoja sekä toiminnallisia ja laillisuusongelmia

[142] *Hakala et al.* 2006, s. 11–12.
[143] *Hakala et al.* 2006, s. 12.
[144] *Pitkänen et al.* 2013, s. 216.
[145] *Hakala et al.* 2006, s. 12.
[146] *Jansen & Skagestein* 2005, s. 75–76.

aiheuttavia. Riskienhallinnan kokonaisuuden järjestäminen ja vastuu siitä kuuluu organisaation johdolle.[147] Riskienhallinnan avulla tunnistetaan organisaation toimintaan kohdistuvia uhkia ja riskejä. Samalla se on osa tietoturvallisuuden hallintaa ja kehittämistä organisaatiossa.[148] EU:n tietosuoja-asetuksen myötä on myös tietosuojariskien hallinta syytä ottaa osaksi organisaation riskienhallintaprosessia.[149]

Riskienhallinta on prosessi, jossa tunnistetaan riskejä, vähennetään niiden todennäköisyyttä ja vaikutuksia hyväksyttävälle tasolle sekä ylläpidetään saavutettua tasoa. Tietoturvariskien hallinnalla pyritään toteuttamaan turvatoimien yhdistelmä, joka varmistaa käsiteltävän tiedon riittävän suojaustason sekä saa aikaan tasapainon käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä.[150]

Tietoturvallisuuteen liittyvien projektien tärkein analyysi on riskianalyysi, jossa pyritään löytämään tietojärjestelmään kohdistuvat riskitekijät ja uhkakuvat. Tavoitteena on luokitella havaitut riskit tarkoituksenmukaisesti luottamuksellisuus-, käytettävyys- ja eheysriskeihin. Olennaisena osana analyysiin kuuluu myös riskien realisoitumisen seurauksien arviointi sekä toiminnan jatkuvuuden että taloudellisten vaikutusten osalta.[151] Tietoturvallisuusriskejä arvioitaessa voidaan mahdollisia riskejä jaotella todennäköisiin, melko todennäköisiin ja epätodennäköisiin tai toisaalta suuria, keskisuuria ja pieniä vahinkoja aiheuttaviin. Tällaisella jaottelulla sekä tietoturvallisuusriskien taloudellisten vaikutusten arvioinnilla voidaan saada kuva siitä, millaisten riskien torjuntaan on syytä erityisesti panostaa.[152]

---

[147] *Pöysti* 2002, s. 247–262.
[148] *Andersson* 2018, s. 2.
[149] *Hanninen et al*. 2017, s. 16.
[150] HE 59/2016 vp, s. 59.
[151] *Hakala et al.* 2006, s. 25.
[152] *Pitkänen et al.* 2013, s. 220–221.

4.5 Tietoturvallisuuden sääntely

Lainsäädäntö ei ole ainoa, eikä aina edes oikea keino tietoturvallisuuden edistämiseksi yhteiskunnan tasolla. *Eriksen* jaottelee mahdolliset toimenpiteet fyysisiin, organisatorisiin, taloudellisiin, pedagogisiin ja normatiivisiin.[153]

Tietoturvallisuudesta ei ole säädetty yhtenä lain tasoisena säädöksenä voimassa olevassa lainsäädännössämme.[154] Tietoturvallisuutta koskeva sääntely on hajautunut lukuisiin eri lakeihin ja sääntely on asia- tai palvelukohtaista. Vuonna 2010 tuli voimaan kuitenkin niin sanottu tietoturvallisuusasetus (valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010, jäljempänä TtA). TtA 1 §:n mukaisesti siinä *säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.* Soveltamisalan määrittelystä voidaan huomata, että nimestään huolimatta tietoturvallisuusasetus on vahvasti asiakirjasidonnainen ja siinä säädetäänkin erityisesti viranomaisen asiakirjojen turvallisuusluokittelusta sekä luokitellun aineiston käsittelystä (3-4 luku). Tietoturvallisuudella tarkoitetaan TtA:n mukaan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä (3.1 § 2 kohta). Saarenpään mukaan TtA on askel kattavampaan tietoturvallisuussääntelyyn ja tietoturvallisuusperiaatteen korostamisen suuntaan[155].

EU:n tasolla tietoturvallisuutta suoraan tai välillisesti koskevan sääntelyn määrä on viime vuosina lisääntynyt. Siihen voidaan lukea kuuluvaksi tässä tutkimuksessa mainittavien tietosuojakehyksen ja eIDAS-asetuksen lisäksi ainakin niin sanottu NIS-direktiivi[156] sekä valmisteilla oleva sähköisen viestinnän tietosuoja-asetus[157] (nk. ePrivacy-asetus). Sekä

---

[153] *Eriksen* 2005, s. 27.
[154] Ajatus tietoturvallisuuden yleislaista ei ole uusi. Sitä ovat esittäneet *Saarenpää et al*. tutkimusraportissaan Tietoturvallisuus ja laki jo vuonna 1997. Ks. *Saarenpää et al*. 1997, s. lxxiii.
[155] *Saarenpää* 2016, s. 218.
[156] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. EUVL L 194 s. 1–30.
[157] COM (2017) 10 final, s. 1–37.

NIS-direktiivi että tietosuoja-asetus tulevat jatkossa lisäämään organisaatioiden riskienhallintavelvoitteita.[158] NIS-direktiivin kansallinen voimaansaattaminen on vaatinut muutoksia lukuisiin lakeihin, joissa direktiivin asettamat tietoturvallisuusriskien hallintaa ja poikkeamien ilmoittamista koskevat velvoitteet on saatettu osaksi toimialakohtaista lainsäädäntöä.[159] Laajuutensa vuoksi näitä ei voida kuitenkaan tarkemmin käsitellä tässä esityksessä.

Tietoturvallisuuden sääntelykokonaisuuteen kuuluvat olennaisena osana kansainväliset standardit ja erilaiset toimialaohjeistukset. Keskeisimpiä lainsäädännön perusteella annettuja tietoturvallisuusohjeita ovat valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) antamat ohjeet sekä kansainväliset tietoturvastandardit, kuten ISO 19977 ja ISO 27001.[160] Kansainväliset standardit voidaan jakaa *de jure* -standardeihin, jotka ovat viralllisten standardointilaitosten (esim. International Organization for Standardization, ISO[161]) hyväksymiä, julkaistuja ja niiden sisältö perustuu useiden toimijoiden yhteistyöhön sekä toisaalta *de facto* -standardeihin, jotka ovat kehittyneet erilaisten käytäntöjen vakiintumisen myötä, eikä niillä ole muodollista hyväksymisprosessia.[162] Toisen tyyppisenä esimerkkinä toimialakohtaisesta ohjeistuksesta voidaan mainita Suomen Asianajajaliiton asianajotoimintaa koskevat säädökset ja ohjeet. Nämä sisältävät asianajotoimintaa harjoittaville osana muuta ohjeistusta tietoturvaoppaan ja tietoturvallisuusohjeen. Näissä annetaan yleisiä ohjeita asianajotoiminnan tietoturvallisesta järjestämisestä ja turvallisesta sähköisestä viestinnästä asiakkaan kanssa.[163]

Lainsäädännön asettamien tietoturvallisuutta koskevien vaatimusten välittämisestä käytännön palvelutoimintaan voidaan esimerkkinä mainita tietoturvallisuuden arviointiin tarkoitetut työkalut, kuten kansallinen turvallisuusarviointikriteeristö (Katakri), jonka ensimmäinen versio valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjel-

---

[158] *Andersson* 2018, s. 10.
[159] Ks. https://www.lvm.fi/-/yhteiskunnan-keskeisten-palvelujen-tietoturvallisuutta-kasvattavat-lakimuutokset-voimaan-971405 [käyty 8.5.2018].
[160] *Voutilainen* 2009, s. 205.
[161] Ks. www.iso.org .
[162] *Voutilainen* 2009, s. 111.
[163] Ks. Asianajoalan tietopankki Aada.

maa. Katakrin uusin versio on julkaistu vuonna 2015. Katakri on tarkoitettu auditointityökaluksi tapauksissa, joissa arvioidaan viranomaisorganisaation kykyä suojata salassa pidettävää tietoa. Katakrin sisältämät vaatimukset nousevat suoraan lainsäädännöstä, kuten TtA:sta, eikä se sinällään aseta tietoturvallisuudelle itsenäisiä, uusia vaatimuksia. Arviointikriteeristö on jaettu kolmeen pääjaksoon, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen tietoturvallisuus.[164]

Kaiken kaikkiaan tietoturvallisuutta toteutetaan useissa eri säädöksissä ja ennen muuta tietoturvallisuus on osa hyvän informaatiohallinnon vaatimusta, joka voidaan johtaa PL:n hyvän hallinnon perusoikeussäännöksestä (21 §) ja JulkL:n hyvää tiedonhallintatapaa koskevasta 18 §:stä. Tietoturvallisuussääntelyllä, vaikka se hajautunutta onkin, toteutetaan myös muita perusoikeuksia kuten oikeutta turvallisuuteen (PL 7 §), henkilötietojen suojaan ja luottamukselliseen viestintään (PL 10 §).

4.5.1 Henkilötietojen käsittelyn turvallisuus

Keskeinen osa henkilötietojen suojaa on henkilötietojen turvallinen käsittely.[165] Käsiteltäessä henkilötietoja hallintotoiminnassa on noudatettava tietosuojaa koskevia velvoitteita ja rajoituksia. Henkilötietojen suoja ja luottamuksellisen viestin salaisuus kuuluvat PL 10 §:n suojan alaan. Yksityiselämän suojan toteuttaminen hallinnossa ja julkisissa palveluissa edellyttää esimerkiksi yksityiselämää koskevien tietojen salassapitoa. Vastaavasti henkilökohtaisen viestinnän eri muodot on suojattu hallinnolliselta valvonnalta suojaamalla luottamuksellinen viestintä.[166]

Edellä mainittujen tietosuojalainsäädäntöä koskevien muutosten vuoksi, keskityn tässä käymään läpi, mitä tietosuoja-asetuksessa säädetään henkilötietojen käsittelyn[167] turvallisuudesta.

---

[164] KATAKRI 2015, s. 2–3.
[165] *Pitkänen et al.* 2013, s. 215.
[166] *Mäenpää* 2017, s. 103–104.
[167] Henkilötietojen käsittelystä sähköisen tunnistamisen osalta ks. jakso 5.6.1.

Tietosuoja-asetuksen mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (5(1)(f) art.). Tietosuoja-asetuksessa henkilötietojen *tietoturvaloukkauksella* tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin (4(1)(12) art.).

Asetuksen mukaan rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta, paitsi jos tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä (33(1)(1) art.). Myös henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoon (33(1)(2) art.). Lainkohdassa mainitun ilmoituksen tulee sisältää vähintään kuvaus henkilötietojen tietoturvaloukkauksesta, tietosuojavastaavan nimi ja yhteystiedot, kuvaus tietoturvaloukkauksen todennäköisistä seurauksista sekä toimenpiteet, joita rekisterinpitäjä on ehdottanut tai toteuttanut tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi (33(1)(3 a-d) art.). Henkilötietojen tietoturvaloukkauksesta on asetuksen mukaan ilmoitettava myös rekisteröidylle silloin, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Ilmoitus tulee tehdä ilman aiheetonta viivytystä (34(1)(1) art.). Ilmoitusta ei kuitenkaan tarvitse tehdä, jos jokin 34(1)(3) artiklan a-c alakohdissa mainituista edellytyksistä täyttyy, eli esimerkiksi se, että tiedot on salattu. Myös valvontaviranomainen voi vaatia laissa tarkoitetun ilmoituksen tekemistä (34(1)(4) art.). Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet (33(1)(5) art.).

5 Sähköinen tunnistaminen

5.1 Sähköinen identiteetti

Nykyinen yhteiskuntamme on taloudellinen ja sosiaalinen informaation markkinapaikka, joka rakentuu tiedon omistamiselle, käsittelylle, varastoimiselle, manipulaatiolle ja siirtämiselle. Merkittävä osa tästä tiedosta sisältää henkilötietojamme, joiden perusteella meidät voidaan tunnistaa. Eri organisaatioilla on hallussaan suuret määrät tietoa, joka lisää riskiä siihen, että tietoja voi päätyä vääriin käsiin joko tietojen haltijalta tai siirrettäessä tietoja tietosubjektin ja tietojen käsittelijän välillä. Myös tunnistaminen on muuttunut verkkoyhteiskunnassa. Tunnistaminen ei usein tapahdu suoraan, vaan tunnistaudumme käyttämällä jotakin sellaista, joka välittää identiteettimme palveluntarjoajalle. Tällaisia identiteettimme välittäviä tietoja ovat esimerkiksi salasanat, asiakastunnukset ja pääsyavaimet. Näiden avulla pääsemme käsittelemään verkkopankissa tietoja, jotka koskevat henkilökohtaista talouttamme. Edellä mainitut tekijät altistavat tietomme identiteettivarkauksille ja erilaisten identiteettiä välittävien tietojen lisääntyvä käyttö lisää puolestaan tietojen kalastelua verkossa (*phishing*), jonka tarkoituksena on saada käyttöön henkilötietojamme.[168]

Verkkoyhteiskunta ja informaatiohallinto rakentuvat verkossa tapahtuvan kommunikoinnin ja asioinnin varaan. Tämän vuoksi digitaalisesta identiteetistä on tullut eräänlainen välttämättömyys. Oikeudellisesti katsottuna identiteetti ei ole yksiselitteinen asia. Identiteetti ja identifiointi ovat eri asioita, eikä kyse ole ainoastaan yksilön tunnistamisesta. Tunnistamiseen tarvittava informaatio on yleensä vähäisempi kuin informaatio, jota tarvitaan koko identiteetin muodostamiseen.[169]

Digitalisoituminen on johtanut myös henkilön identiteetin digitalisoitumiseen.[170] Tiedollisen itsemääräämisoikeutemme puitteissa meillä voi olla useita erilaisia identiteettejä

[168] *Murray* 2013, s. 390–391.
[169] *Korja* 2016, s. 124.
[170] *Korja* 2016, s. 173.

suhteessa eri organisaatioihin.[171] Digitaalisessa ympäristössä identiteetti on ongelmallinen käsite, sillä siihen fyysisessä maailmassa liittyvät ominaisuudet, kuten persoonalliset ja sosiaaliset piirteet eivät ole käytössä.[172] Henkilön sähköiseen identiteettiin kuuluvan yksilöivän ominaisuuden tulee olla ainutlaatuinen tieto tai ominaisuus, joka on yhdistettävissä vain tiettyyn henkilöön.[173] Sähköisessä muodossa olevat henkilön toimintaa tietyssä tilanteessa kuvaavat tiedot kuuluvat myös sähköiseen identiteettiin.[174] Korja toteaa persoonallisuuden suojaan viitaten, että yksilön oikeudella identiteettiin tulee olla perusoikeustasoinen suoja, vaikka PL:ssa ei näin suoraan säädetäkään.[175]

Sähköistä identiteettiä tulee verkkoyhteiskunnassa pitää tärkeänä käsitteenä, sillä sen avulla tehdyt toimet voidaan kohdistaa tietyn henkilön oikeudelliseen kelpoisuuteen. Sähköinen identiteetti mahdollistaa yksilön oikeudellisesti luotettavan toiminnan tietoverkossa.[176]

Kysymys sähköisestä identiteetistä ei rajoitu vain sähköistä tunnistamista koskeviin kysymyksiin. Muutoin kuin laissa säädetyissä tilanteissa voimme tiedollisen itsemääräämisoikeutemme pohjalta määritellä ne tekijät, joista identiteettimme muodostuu. Voimme siten erilaisissa verkkoyhteisöissä toimia määrittelemämme identiteetin puitteissa. Tämän identiteetin käyttämiselle rajana on lähinnä se, ettemme käytä toisen henkilön identiteettiä, eli syyllisty rikoslaissa (19.12.1889/39, jäljempänä RL) tarkoitettuun identiteettivarkauteen. Identiteetin käyttö ei myöskään voi loukata toisen yksilön kunniaa.[177]

Oikeushenkilöllä ei aikaisemmin voinut olla itsenäistä sähköistä identiteettiä. Sen oikeudellinen toimintakyky voitiin toteuttaa vain sitä edustavan luonnollisen henkilön kautta. Näin ollen luotettavassa sähköisessä asioinnissa oikeushenkilön sähköinen identiteetti oli luonnollisen henkilön sähköisen identiteetin ominaisuus ja sen avulla voitiin varmistaa

---

[171] *Saarenpää* 2016, s. 217.
[172] *Korja* 2016, s. 120–121.
[173] *Voutilainen* 2009, s. 240.
[174] *Voutilainen* 2008, s. 3.
[175] *Korja* 2016, s. 207.
[176] *Korja* 2016, s. 175–178.
[177] *Saarenpää* 2016, s. 234.

oikeushenkilön puolesta toimivan kelpoisuus.[178] eIDAS-asetuksen yksi selkeä muutos on se, että vahvan sähköisen tunnistamisen tunnistusväline voidaan nyt myöntää myös oikeushenkilölle, eli sille voi muodostua oma digitaalinen identiteetti.[179] Joka tapauksessa digitaalisen identiteetin osalta voidaan todeta, että hyvän tiedonhallintatavan ja tietoturvallisuusvaatimusten täyttämiseksi on palveluntarjoajien huolehdittava asianmukaisten identiteetin-, pääsynhallinta ja käyttövaltuushallintaprosessien järjestämisestä.

5.1.1 Biometrinen tunnistaminen

Digitaalinen teknologia vaikuttaa kulttuuriimme ja sen myötä myös oikeuskulttuuriin, oikeuden sisältöön ja tulkintaan. Teknologinen kehitys oikeuskulttuurissa näkyy esimerkiksi siten, että tiettyä teknologista ratkaisua esitetään jonkin yhteiskunnallisen tai oikeudellisen ongelman ratkaisuna. Tämä näkyy vaikkapa biometrisen tunnistamisen esittämisenä ratkaisuna henkilön tunnistamista koskeviin ongelmiin.[180]

Biometrisellä tunnistamisella tarkoitetaan yleisesti henkilön tunnistamista jonkin fysiologisen ominaisuuden tai käyttäytymispiirteen perusteella. Biometrinen tunnistaminen on yksi modernin verkkoyhteiskunnan keskeisistä toimintamalleista, jonka avulla tavoitellaan varmuutta, tehokkuutta ja kevyempää hallintoa. Samalla kun biometrinen tunnistaminen antaa tehokkaamman keinon yksilön tunnistamiselle verrattuna nykyisiin ratkaisuihin, kyseisen teknologian käyttö mahdollistaa myös yksilöiden tehokkaan valvonnan ja seurannan yhteiskunnassa. Keskeiseksi kysymykseksi nouseekin rajojen luominen biometrisen tunnistamisen teknologian käyttämiselle, jotta voidaan välttää väärinkäytöksistä mahdollisesti johtuvia oikeudenloukkauksia.[181]

Biometrinen tunnistaminen perustuu informaatioon, joka saadaan suoraan tai välillisesti ihmisruumiista. Ihmisruumis muunnetaan digitaaliseksi koodiksi, jonka avulla saadaan

---

[178] *Voutilainen* 2008, s. 9.
[179] HE 74/2016 vp, s. 13.
[180] *Korja* 2016, s. 56–57.
[181] *Korja* 2016, s. 4–452.

tietoa ihmisen yksilöllisistä piirteistä ja jonka avulla yksilö on tunnistettavissa.[182] Tietosuoja-asetuksen mukaan *biometrisillä tiedoilla* tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa (4(1)(14) art.). Julkisessa hallinnossa biometristä tunnistamista hyödynnetään esimerkiksi oleskelulupakortissa, johon tallennetaan kortinhaltijan biometrisiä tunnistetietoja.[183]

5.1.2 Identiteettivarkaus

Kun jotakin identiteettitietoa kerätään oikeudettomasti, puhutaan yleiskielessä identiteettivarkauksista. Kerättyä identiteettitietoa käytetään oikeudetta rikoshyödyn hankkimiseksi tai muutoin tavalla, josta aiheutuu vahinkoa[184] identiteetin oikealle haltijalle. Henkilöllisyysvarkaus on identiteettivarkauden osajoukko, jossa teon kohteena on nimenomaan henkilötieto.[185] Identiteettivarkaudesta säädetään RL 38:9a §:ssä. Sen mukaan, *joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon*.

Identiteettivarkauksilla tarkoitetaan perinteisesti varastettujen asiakirjojen, kuten henkilö- ja ajokorttien tai passien avulle tehtyjä väärennys- tai petosrikoksia. Toisena henkilönä esiintymistä yksityiselle ei ollut myöskään säädetty rangaistavaksi ennen nykyistä

---

[182] *Korja* 2016, s. 87–88.
[183] *Korja* 2016, s. 156.
[184] Vahinkoa voidaan aiheuttaa vaikkapa esiintymällä toisena henkilönä tai tekemällä toisen henkilön tiedoilla ns. valeprofiili sosiaalisen median palveluissa (esim. Facebook, Twitter). Sosiaalisen median palveluissa ei yleisesti ole käytössä vahvan sähköisen tunnistamisen menetelmiä, eikä palveluun syötettyjä tietoja välttämättä varmenneta millään tavalla. Ks. myös *Soininen* 2017, s. 87, jonka mukaan tietoverkkoympäristön anonymiteetistä johtuen jo pelkkä toisen nimimerkin tai hahmon (avatar) oikeudeton käyttäminen voi täyttää identiteettivarkauden tunnusmerkistön.
[185] Identiteettiohjelman loppuraportti, s. 47–48.

identiteettivarkauden kriminalisointia.[186] Vaikka identiteettivarkaus on kriminalisoitu itsenäisenä tekona vasta hiljattain, eivät identiteettiin kohdistuneet teot aiemminkaan jääneet sääntelyn ulkopuolelle. Identiteettivarkauden kaltaiset teot saattoivat tulla rangaistavaksi esimerkiksi väärän henkilötiedon antamisena (RL 16:5), rekisterimerkintärikoksena (RL 16:7) tai petoksena (RL 36:1).

5.2 Tunnistaminen käsitteenä

Käytännön syyt ovat viime vuosina nostaneet sähköistä tunnistamista koskevan keskustelun pintaan. Aikaisemmin painopiste on selkeästi ollut sähköisessä allekirjoittamisessa. Sähköisen tunnistamisen keskeiset ongelmat liittyvät tasapainoon oikeusvarmuuden ja joustavuuden välillä. Sääntely on kuitenkin sähköistä allekirjoittamista yleisluontoisempaa ja teknologian suhteen neutraalimpaa, osin siksi, että sähköisen tunnistamisen piirissä ei ole toistaiseksi löytynyt yhtä ylivoimaista, sähköistä allekirjoittamista vastaavaa teknologiaa.[187]

Tunnistaminen on toimenpide tai prosessi, jossa identiteetti luodaan tai esitetään toiselle. Tietojärjestelmien näkökulmasta tunnistamisella yhdistetään tietoja tiettyyn henkilöön. Tietoverkossa toimittaessa on tärkeää yksilöidä henkilöt, eli erottaa yksilöt toisistaan. Tunnistaminen mahdollistaa henkilölle hänen oikeudellisen identiteettinsä käyttämisen ja sen seurauksena henkilön tekemien oikeudellisten toimenpiteiden arviointi kohdistuu oikein.[188] Fyysisessä ympäristössä henkilö voidaan tunnistaa vertaamalla viranomaisen myöntämässä virallisessa henkilötodistuksessa olevia tunnistetietoja läsnäolevaan henkilöön tai hänen ominaisuuksiinsa. Tällaisia tietoja voivat olla esimerkiksi henkilön valokuva, jota voidaan verrata hänen ulkoisiin ominaisuuksiinsa tai henkilön allekirjoitus, jota verrataan aiemmin tallennettuun vertailukappaleeseen.[189]

---

[186] Identiteettiohjelman loppuraportti, s. 53.
[187] *Ponka* 2013, s. 111.
[188] *Korja* 2016, s. 82–83.
[189] *Ponka* 2013, s. 59.

Yleisesti henkilöllisyyttä osoittavan asiakirjan käyttö tunnistamisessa perustuu siihen, että sen myöntänyttä viranomaista kohtaan tunnetaan luottamusta sekä siihen, että asiakirjan väärentäminen on eri keinoin pyritty estämään.[190] Suomessa virallisia henkilöllisyyden osoittavia asiakirjoja ovat passilaissa (21.7.2006/671) säädetty passi sekä henkilökorttilaissa (25.8.2016/663) säädetty henkilökortti. Laissa säädetyistä passin ja henkilökortin myöntämisestä vastaa poliisi, joka myös tunnistaa henkilön luotettavasti myöntämisprosessin aikana. Prosessin tuloksena poliisi myöntää hakijalle turvallisuudeltaan korkeatasoisen todistuksen henkilöllisyydestä.[191]

Poliisin myöntämän ajokortin roolista tunnistamisasiakirjana on käyty paljon keskustelua vuosien mittaan. Suomessa poliisin myöntämän ajokortin tehtävänä on osoittaa ajo-oikeuden olemassaolo, eikä se ole henkilöllisyyttä osoittava asiakirja. Tästä huolimatta ajokorttia käytetään runsaasti mainitussa tarkoituksessa esimerkiksi pankkien, teleoperaattorien ja postin palveluissa.[192] Ajokortin käyttämistä tunnistamisessa on epäilemättä lisännyt sen levinneisyys sekä se, että se sisältää yleisesti tunnistamisessa käytettäviä tietoja, kuten valokuvan ja henkilötunnuksen.

Palveluntarjoajan näkökulmasta sähköinen tunnistaminen perustuu siihen, että sillä on hallussaan joitakin yksilöintitietoja, joiden avulla käyttäjä tunnistetaan. Joissakin tapauksissa palveluntarjoajalla ei ole mainittuja yksilöintitietoja, vaan tunnistus tapahtuu kolmannen luotetun osapuolen avulla siten, että luotettu osapuoli välittää palveluntarjoajalle henkilön yksilöintiin liittyvät tiedot ja varmentaa käyttäjän henkilöllisyyden omassa tunnistuspalvelussaan. Sähköisessä tunnistamisessa onkin usein kysymys henkilötietojen luovuttamisesta palveluntarjoajalta toiselle.[193]

Monet toimijat, kuten esimerkiksi teleoperaattorit puhelimitse tapahtuvassa asiakaspalvelussaan pyytävät käyttäjältä henkilötunnuksen ilmoittamista tunnistamisen ja yksi-

---

[190] *Korhonen* 2016, s. 303.
[191] Identiteettiohjelman loppuraportti, s. 31.
[192] Identiteettiohjelman loppuraportti, s. 31.
[193] *Voutilainen* 2014, s. 70.

löimisen tarpeisiin. Tällaista menetelmää ei voida pitää kovin luotettavana. Henkilötunnuksen käyttäminen tunnistamiseen ei vastaa digitaalisen verkkoyhteiskunnan tunnistustarpeita, vaan tulisi käyttää vahvoja sähköisen tunnistamisen menetelmiä[194].

Sähköinen tunnistaminen viittaa tunnistuksessa käytettävään menetelmään, kun sähköinen identiteetti taas henkilöön liittyvään informaatioon. Tällaisen informaation tulee olla koneellisesti käsiteltävää, yksilöllistä ja ainutlaatuista ja nämä tavoitteet voidaan saavuttaa esimerkiksi käyttämällä tietojen salausta ja siten, että tietoja on vaikea väärentää. Tästä näkökulmasta Korja arvelee biometristen tunnisteiden tulevan jatkossa kiinteäksi osaksi yksilön sähköistä identiteettiä, vaikka niitä ei tulisi pitää ensisijaisena vaihtoehtona niiden käyttöön sisältyvien riskien vuoksi. Riskinä on esimerkiksi tunnisteen joutuminen vääriin käsiin.[195]

Sähköisen tunnistamisen hyödyntämiseen liittyviä palveluita kutsutaan yleisesti tunnistamisinfrastruktuuriksi. Sen yksi päätehtävä on yhdistää luotettavasti toisiinsa sähköiset välineet ja näitä välineitä käyttävien henkilöiden tiedot.[196] Keskeisiä käsitteitä ovat *avoin ja suljettu infrastruktuuri*. Avoin järjestelmä on nimensä mukaisesti kaikille avoin, kun suljettuun järjestelmään ei kolmansilla osapuolilla ole pääsyä. Suljetusta järjestelmästä voidaan esimerkkinä mainita pankkien Tupas-järjestelmä. Avoimessa järjestelmässä kuka tahansa voi luottaa annettuun varmenteeseen tai tehtyyn tunnistukseen, vaikka osapuolilla ei olisi mitään aikaisempaa suhdetta toisiinsa. Suljettu järjestelmä puolestaan perustuu vahvasti sopimussuhteeseen tai -suhteisiin ja edellyttää osapuolilta liittymistä tietyn infrastruktuurin osaksi. Mikäli osapuoli ei ole osana suljettua järjestelmää, eivät sen tunnistus- tai allekirjoituspalvelut luonnollisesti ole käytettävissä. Suljetun infrastruktuurin etuna voitaneen pitää sitä, että osapuolet voivat sopia osapuolten oikeuksista ja velvollisuuksista, kun avoimessa järjestelmässä tämä on vaikeaa. VRK:n kansalaisvarmenne on ainoa Suomessa käytössä oleva avoimeen järjestelmään perustuva palvelu.[197]

---

[194] *Korja* 2016, s. 85.
[195] *Korja* 2016, s. 175–176.
[196] *Ponka* 2013, s. 85.
[197] *Ponka* 2013, s. 412–516.

5.3 Lainsäädäntö

Suomessa ei oltu ennen vuotta 2009 säädetty sähköisestä tunnistamisesta, ainoastaan sähköisestä allekirjoittamisesta (Laki sähköisistä allekirjoituksista 24.1.2003/14). Uuden, sähköistä tunnistamista koskevan lain säätämisellä pyrittiin saamaan aikaan toimivat sähköisen tunnistamisen markkinat, joiden lähtökohtana ovat tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu.[198] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista tuli voimaan 1.9.2009.

EU:ssa rajat ylittävästä sähköisestä tunnistamisesta säädetään asetuksella, jota yleisesti kutsutaan eIDAS-asetukseksi. Asetuksella pyritään varmistamaan sisämarkkinoiden asianmukainen toiminta ja takaamaan sähköisen tunnistamisen menetelmien ja luottamuspalveluiden tietoturvan riittävän korkea taso (1 art.). eIDAS-asetuksen voimaantulo on aiheuttanut useita muutoksia kansalliseen lainsäädäntöömme ja tällä hetkellä Suomessa sähköisestä tunnistamisesta säädetään laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (7.8.2009/617, jäljempänä SäTuL).

5.3.1 SäTuL

SäTuL mukaisesti kyseisessä laissa säädetään *vahvasta sähköisestä tunnistamisesta* sekä *tunnistuspalveluiden tarjoamisesta* palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille (1.1 §). Laissa säädetään eIDAS-asetuksen säännösten noudattamisen valvonnasta ja annetaan mainittua asetusta täydentäviä säännöksiä (1.2 §). Lakia sovelletaan EU:n komissiolle ilmoitettaviin rajat ylittäviin tunnistusjärjestelmiin vain, jollei eIDAS-asetuksesta muuta johdu (1.3 §).

Lakia ei sovelleta lainkaan yhteisön sisäiseen tunnistamiseen käytettävien palveluiden tarjontaan eikä yhteisöön, joka käyttää omaa tunnistusmenetelmäänsä omien asiakkaiden tunnistamiseen omissa palveluissaan (1.4 §). Tätä on perusteltu sillä, että organisaatioiden sisäisten käyttäjien suojan tarve on vähäisempi kuin markkinoilta tunnistusvälineensä

[198] HE 36/2009 vp, s. 29.

hankkivalla kuluttajalla.[199] Käytännössä siis organisaatioiden sisäiset tunnistamisjärjestelmät eivät kuulu lain soveltamisalaan.

Huomionarvoista on, että laki koskee ainoastaan *vahvaa sähköistä tunnistamista*. Monissa verkkopalveluissa on yleisesti käytössä niin sanottu *heikko sähköinen tunnistaminen*, joka perustuu usein esimerkiksi käyttäjätunnuksen ja salasanan yhdistelmään[200]. Heikkoa sähköistä tunnistamista käyttävät verkkopalvelut eivät kuitenkaan jää muulla tavoin sääntelyn ulkopuolelle. Esimerkiksi tietoturvallisuutta, tietosuojaa ja muu sähköistä viestintää koskeva sääntely kattaa myös kyseiset palvelut. Esimerkkinä heikon tunnistamisen tarpeellisuudesta on kuvattu koulumaailman alle 15-vuotias, joka ei välttämättä saa vielä vahvaan sähköiseen tunnistamiseen tarvittavaa tunnistusvälinettä, mutta jolla on tarve tunnistautua koulutehtäviä tehdäkseen sähköiseen oppimisympäristöön[201]. Vahvaa sähköistä tunnistamista hyödyntävät palvelut ovat jakaantuneet pääosin pankki- ja vakuutuspalveluihin, julkisen hallinnon palveluihin sekä muihin yksityisen sektorin palveluihin.[202] Hallituksen esityksessä on arvioitu näiden tunnistusvälineiden käytön lisääntyvän myös verkkokaupankäynnissä.[203] Toistaiseksi verkkokauppojen tunnistaminen on perustunut pitkälti heikkoon sähköiseen tunnistamiseen ja käyttäjän itse antamiin tietoihin, kuten osoitetietoihin. Tietoja ei yleensä varmenneta millään tavoin, esimerkiksi vertaamalla niitä VTJ:n tietoihin. Osasyynä voivat olla tietojen varmistamiseen liittyvät kustannukset. Mainitun kaltainen menettely saattaa osaltaan mahdollistaa väärinkäytökset ja petosrikokset verkkokaupoissa.

SäTuL:ssa tarkoitetaan *vahvalla sähköisellä tunnistamisella* sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää

---

[199] HE 36/2009 vp, s. 40.
[200] Heikon sähköisen tunnistamisen turvallisuutta eri verkkopalveluissa on haluttu parantaa ottamalla käyttöön niin sanottu *two factor authentication* (2FA) -menetelmä, jossa käyttäjätunnuksen ja salasanan syöttämisen jälkeen kirjautujan palveluun rekisteröitymisen yhteydessä ilmoittamaan matkapuhelinnumeroon lähetetään tekstiviestinä kirjautumisen lisävahvistuksena käytettävä koodi. Kyseinen menettely ei kuitenkaan muuta tilannetta lain tarkoittamaksi vahvaksi sähköiseksi tunnistamiseksi. Menettely ei esimerkiksi perustu luotettavaan ensitunnistamiseen (ensitunnistamisesta ks. jakso 5.5).
[201] HE 59/2016 vp, s. 38.
[202] HE 272/2014 vp, s. 3.
[203] HE 74/2016 vp, s. 5.

eIDAS-asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset (2.1 § 1 kohta). SäTuL:ssa käytetty *tunnistusvälineen* määritelmä (2.1 § 2 kohta) on teknologianeutraali. Se kuvaa mitä tahansa fyysisessä, sähköisessä tai tiedollisessa muodossa olevaa asiaa, josta tunnistusväline muodostuu. Väline voi siten olla esimerkiksi varmenne ja sen käyttämiseen tarvittava PIN-koodi, käyttäjätunnuksen ja vaihtuvan salasanan yhdistelmä tai sormenjäljen ja PIN-koodin yhdistelmä.[204]

Tunnistusvälityspalvelun tai tunnistusvälineen tarjoajaa kutsutaan *tunnistuspalvelun tarjoajaksi* (2.1 § 3 kohta). *Tunnistusvälineen tarjoaja* on palveluntarjoaja, joka tarjoaa tai laskee liikkeelle vahvan sähköisen tunnistamisen tunnistusvälineitä yleisölle sekä tarjoaa tunnistusvälinettään tunnistusvälityspalvelun tarjoajalle välitettäväksi luottamusverkostossa (2.1 § 4 kohta). *Tunnistusvälityspalvelun tarjoajalla* tarkoitetaan palveluntarjoajaa, joka välittää vahvan sähköisen tunnistamisen tunnistustapahtumia sähköiseen tunnistukseen luottavalle osapuolelle (2.1 § 5 kohta). *Tunnistusvälineen haltija* on luonnollinen henkilö ja oikeushenkilö, jolle tunnistuspalvelun tarjoaja on sopimukseen perustuen antanut tunnistusvälineen (2.1 § 6 kohta).

eIDAS-asetuksen aiheuttamien muutosten vuoksi SäTuL koskee siis varsinaisesti vahvaa sähköistä tunnistamista ja tunnistuspalveluiden tarjoamista. Sähköisestä allekirjoituksesta ja sähköisistä luottamuspalveluista säädetään mainitussa asetuksessa.[205]

5.3.2 Luottamusverkosto

Luottamusverkostolla tarkoitetaan ViVi:oon ilmoituksen tehneiden tunnistuspalvelun tarjoajien verkostoa (SäTuL 2.1 § 10 kohta). Luottamusverkosto on toimintamalli, jossa sekä sähköisen palvelun käyttäjällä että palvelun tarjoajalla on niin sanottu luotettu kolmas osapuoli, joka palvelutilanteessa yhdistää luotettavalla tavalla tuntemattomat osapuolet.

[204] HE 74/2016 vp, s. 24.
[205] HE 74/2016 vp, s. 22.

Silloin, kun käyttäjä- ja palveluntarjoajaryhmiä kolmansine osapuolineen on useita, kysymyksessä on luottamusverkosto.[206] Luottamusverkostosta säädetään valtioneuvoston asetuksella (10.3.2016/169, valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta).

Luottamusverkostossa tunnistusvälineen tarjoajan tulee tarjota tunnistusvälinettään tunnistuksen välityspalveluiden tarjoajille. Lisäksi tämä voi tarjota omaa tunnistusvälinettään luottaville osapuolille oman tunnistuksen välityspalvelun kautta, jolloin se toimii myös tunnistusvälityspalvelun tarjoajan roolissa. On huomattava, että tilanne, jossa palvelun tarjoaja käyttää vahvan sähköisen tunnistamisen menetelmiä omien asiakkaidensa tunnistamiseen, ei kuulu SäTuL:n soveltamisalaan. Lain soveltamisalaan kuuluu tilanne, jossa kyseinen toimija tarjoaa samaa menetelmää toiselle vahvaan sähköiseen tunnistamiseen luottavalle osapuolelle, kuten esimerkiksi pankit toimivat.[207]

Luottamusverkoston käsite on erotettava luottamuspalvelusta, jolla tarkoitetaan eIDAS-asetuksessa esimerkiksi sähköisestä allekirjoituksesta ja sähköisistä aikaleimoista koostuvia palveluita.[208]

5.4 Varmuustasot ja todennusmenetelmät

Jokainen tunnistus- tai allekirjoitusjärjestelmä on korkeintaan niin turvallinen, kuin yksittäisen välineen käyttöönottoon liittyvät tunnistusprosessit sekä tietojen tarkistaminen.[209] Sähköisen tunnistamisen menetelmän *varmuustasolla* tarkoitetaan käytettävän menetelmän luotettavuutta esitetyn henkilöllisyyden toteamisessa. Mitä korkeampi varmuustaso on, sitä todennäköisemmin asiointipalveluun kirjautuva henkilö tosiasiassa on henkilö, jolle tietty henkilöllisyys ja siihen liitetyt tunnistusvälineet on osoitettu.[210]

---

[206] HE 272/2014 vp, s. 10–11.
[207] HE 74/2016 vp, s. 25.
[208] HE 272/2014 vp, s. 5.
[209] *Ponka* 2013, s. 86.
[210] Sähköisen asioinnin tietoturvallisuus -ohje, s. 54.

Sähköisen tunnistamisen järjestelmien varmuustasoista säädetään eIDAS-asetuksen 8 artiklassa. *Matala varmuustaso* tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa rajallisen luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää henkilöllisyyden väärinkäytön tai muuttamisen riskiä (8(2)(a) art.). *Korotettu varmuustaso* tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa merkittävän luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää merkittävässä määrin henkilöllisyyden väärinkäytön tai muuttamisen riskiä (8(2)(b) art.). *Korkea varmuustaso* tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa korkeamman luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta kuin korotetun varmuustason omaava sähköisen tunnistamisen menetelmä ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on estää henkilöllisyyden väärinkäyttö tai muuttaminen (8(2)(c) art.).

eIDAS-asetuksen mukaan komission tuli viimeistään 18 päivänä syyskuuta 2015 täytäntöönpanosäädöksillä vahvistaa tekniset vähimmäiseritelmät, -standardit ja -menettelyt sähköisen tunnistamisen menetelmien matalan, korotetun ja korkean varmuustason määrittelemiseksi (8(3) art.). *Varmuustasoasetuksella* tarkoitetaan komission kyseisen lainkohdan nojalla antamaa täytäntöönpanoasetusta[211].

Varmuustasoasetuksen mukaisesti ilmoitetun sähköisen tunnistamisen järjestelmän puitteissa myönnettyjen sähköisen tunnistamisen menetelmien matala, korotettu ja korkea

[211] Komission täytäntöönpanoasetus (EU) 2015/1502, annettu 8 päivänä syyskuuta 2015, teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti. EUVL L 235 s. 7–20.

varmuustaso on määritettävä käyttäen asetuksen liitteessä esitettyjä eritelmiä ja menettelyjä (1(1) art.). Kyseisen liitteen tekniset eritelmät ja määrittelyt ovat varsin yksityiskohtaisia. Jokaisen kokonaisuuden kohdalla on lueteltu erikseen edellytykset, joiden tulee täyttyä matalan, korotetun tai korkean varmuustason osalta. Nämä kokonaisuudet ovat rekisteröinti, sähköisen tunnistamisen menetelmien hallinta, todentaminen sekä hallinto ja organisointi. Tässä tutkimuksessa ei ole syytä käydä läpi jokaista teknistä erittelykohtaa, mutta niiden noudattaessa samaa kaavaa, voidaan esittää viitteeksi *todentamismekanismia* koskeva kohta[212]:

Varmuustaso	Tarvittavat osatekijät
Matala	1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen. 2. Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella. 3. Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkeampaa perustasoa (”enhanced-basic”), voi heikentää todentamismekanismeja.
Korotettu	Taso ”matala” lisättynä seuraavalla: 1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista. 2. Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen (”moderate”), voi heikentää todentamismekanismeja.
Korkea	Taso ”korotettu” lisättynä seuraavalla: Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea (”high”), voi heikentää todentamismekanismeja.

[212] Varmuustasoasetus, Liite 1, kohta 2.3.1.

Kotimaisten sähköisen tunnistamisen järjestelmien vaatimusten osalta viitataan SäTuL:ssa monin osin varmuustasoasetukseen. Näin on esimerkiksi edellä mainittujen varmuustasojen osalta. Sähköisen tunnistamisen järjestelmälle asetettavista vaatimuksista säädetään SäTuL 8.1 §:ssä. Vaatimukset voidaan tiivistää siten, että sähköisen tunnistamisen järjestelmässä käytettävän tunnistusmenetelmän on perustuttava SäTuL 17 tai 17a §:n mukaiseen ensitunnistamiseen (1 kohta), tunnistusmenetelmällä on voitava yksiselitteisesti tunnistaa tunnistusvälineen haltija (2 kohta), tunnistusmenetelmällä on voitava varmistua siitä, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä (3 kohta), tunnistusmenetelmä täyttää vähintään varmuustasoasetuksen korotetulle varmuustasolle säädetyt edellytykset (4 kohta) ja tietoturvallisuuden hallinnasta on huolehdittu samoin korotetun varmuustason edellytysten mukaisesti (5 kohta).

Tunnistusmenetelmässä on käytettävä *vähintään kahta* laissa mainituista todentamistekijöistä. Laissa säädetyt *todentamistekijät* ovat:

- tiedossa oloon perustuva todentamistekijä, jonka henkilön on osoitettava olevan tiedossaan
- hallussapitoon perustuva todentamistekijä, jonka henkilön on osoitettava olevan hallussaan
- luontainen todentamistekijä, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen (SäTuL 8a.1 §).

Tiedossa oloon perustuva todentamistekijä voi olla esimerkiksi salasana, joka henkilöllä on tiedossaan. Hallussapitoon perustuva todentamistekijä voi olla esimerkiksi avainlukulista, sirukortti tai mobiilivarmenne. Luontainen todentamistekijä puolestaan perustuu johonkin henkilön fyysiseen ominaisuuteen, kuten sormenjälkeen.[213] SäTuL:n määritelmät vastaavat varmuustasoasetuksen liitteen 1 määritelmiä.

[213] HE 74/2016 vp, s. 28–29.

5.5 Ensitunnistaminen

Ensitunnistamisella tarkoitetaan tunnistusvälineen hakijana olevan luonnollisen henkilön henkilöllisyyden todentamista tai oikeushenkilön oikeushenkilöllisyyden todentamista ennen välineen myöntämistä.[214] Tunnistusvälineen liikkeeseenlaskun yhteydessä tehtävällä ensitunnistamisella on keskeinen merkitys vahvan sähköisen tunnistamisen luotettavuudelle. Ensitunnistaminen tarvitsee pääsääntöisesti tehdä vain yhden kerran.[215] Henkilöllisyyden todentamisen perusteella voidaan hakijalle myöntää tunnistusväline, johon liitetään vähintään sellaiset henkilön yksilöivät tunnistetiedot, joilla käyttäjän henkilöllisyys voidaan sähköisesti todentaa. Lisäksi tällainen tunnistusväline on voitava ketjuttaa uusien sähköisten tunnistusvälineiden luomiseksi.[216] Salassapitosäännösten estämättä on tunnistuspalvelun tarjoajalla oikeus saada teknisen käyttöyhteyden avulla poliisin hallintoasiain tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta (SäTuL 7 b §).

Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. Lisäksi henkilöllisyyden varmentaminen voi perustua julkisen tai yksityisen tahon aiemmin muuhun tarkoitukseen kuin vahvan sähköisen tunnistusvälineen myöntämiseen käyttämään menettelyyn, jonka Viestintävirasto hyväksyy menettelyä koskevien säännösten tai viranomaisvalvonnan perusteella tai 28 §:n 1 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella (SäTuL 17.1 §). Vastaavasti tunnistusvälineen hakijana olevan oikeushenkilön ilmoitettu henkilöllisyys tulee varmentaa yritys- ja yhteisörekistereistä tai siten, että vähintään oikeushenkilön henkilöllisyyden todistamista ja varmentamista koskevat sähköisen tunnistamisen varmuustasoasetuksen liitteen 2.1.3 korotetulle varmuustasolle säädetyt vaatimukset täyttyvät (17 a §).

---

[214] HE 74/2016 vp, s. 26.
[215] HE 36/2009 vp, s. 42.
[216] HE 272/2014 vp, s. 12.

Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia (SäTuL 17.2 §). Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen tekee poliisi. Poliisin tekemästä ensitunnistamisesta tunnistusvälineen hakijalle aiheutuva kustannus on julkisoikeudellinen suorite. Suoritteen maksullisuudesta säädetään valtion maksuperustelaissa[217] (SäTuL 17.3 §). Esimerkiksi pankissa asiakkaan henkilöllisyyden todentaminen on dokumentoitava ja arkistoitava niin, että jälkikäteen voidaan osoittaa, mihin tietoihin tunnistaminen perustuu ja kuka tunnistamisen on tehnyt.[218]

SäTuL:a on muutettu siten, että nykyään on mahdollista niin sanottu ensitunnistamisen ketjuttaminen. Muutos tarkoittaa sitä, ettei vahvan sähköisen tunnistamisen välinettä enää tarvitse hakea henkilökohtaisesti. Fyysistä ensitunnistamista ei tarvita, mikäli käyttäjällä on jo vahva sähköinen tunnistusväline. Uutta tunnistusvälinettä voi hakea myös sähköisesti ja ensitunnistukseen luottava tunnistuspalvelun tarjoaja saa käyttöönsä toisen tunnistuspalvelun tarjoajan tekemän ensitunnistuksen, mutta vastaa myös tunnistamisen mahdollisesta virheellisyydestä.[219] Kun tunnistusvälineen tarjoaja lähettää tiedon tekemästään ensitunnistamisesta toiselle tunnistusvälineen tarjoajalle, jotta tämä voisi myöntää sähköisen tunnistusvälineen, se saa periä oikeudenmukaisen ja kohtuullisen korvauksen (SäTuL 17.5 §).

Valtaosa vahvan sähköisen tunnistamisen ensitunnistamisista on toteutettu pankkien toimesta.[220] Eduskunnan liikenne- ja viestintävaliokunta on esittänyt huolensa ensitunnistamisen hinnoittelusta sekä siitä, että käytännössä pankeilla on sähköisten tunnisteiden osalta monopoliasemaan rinnastettava asema.[221]

---

[217] Valtion maksuperustelaki, 21.2.1992/150.
[218] Tupas tunnistusperiaatteet, s. 10.
[219] HE 272/2014 vp, s. 13.
[220] LiVM 17/2017 vp, s. 3.
[221] LiVM 18/2016 vp, s. 4.

5.6 Tunnistaminen asiointipalveluissa

Korja esittää tunnistamiseen liittyen osuvasti kolme keskeistä kysymystä. Missä tilanteissa henkilö on tarpeen tunnistaa sähköisessä asioinnissa, mitä tunnistusmenetelmiä tulisi käyttää missäkin tilanteessa ja onko asiakkaalla oikeus asioida sähköisissä asiointipalveluissa anonyymisti?[222] Saarenpään mukaan asiointi informaatiohallinnossa tulee rakentaa turvatun anonymiteetin varaan. Tämän mukaisesti anonyymin asioinnin vaiheesta siirrytään kansalaisen niin halutessa tunnistettavuuden vaiheeseen. Turvatun anonymiteetin mukaan palvelun hyödyntäjästä ei jää anonyymin asioinnin vaiheessa ilman pakkokeinosäännöksiä hyödynnettäviä tietoja järjestelmiin. Ensisijaisena ratkaisuna tulisi kuitenkin olla mainittujen tietojen välitön poistaminen järjestelmästä.[223]

Sähköisen identiteetin hyödyntäminen on yksi peruselementeistä julkisen hallinnon sähköisen asioinnin järjestämisessä. Asiointitapahtuman yhteydessä henkilö voidaan tunnistaa tietyksi henkilöksi sähköiseen identiteettiin kuuluvien tietojen avulla. Näiden tietojen avulla henkilö voidaan profiloida tai tietoja voidaan analysoida tiettyä käyttötarkoitusta, kuten päätöksentekoa varten. Täysin ongelmatonta henkilön sähköinen tunnistaminen ei kuitenkaan ole. Sähköinen tunnistaminen luo tapahtumana yhden lisäelementin asiointitapahtumaan ja voi hankaloittaa palveluiden käyttöä etenkin siinä tapauksessa, ettei henkilöllä ole käytössään tarvittavaa tunnistusvälinettä.[224]

Yleislainsäädännön tasolla ei ole säädetty henkilön tunnistamisesta asiointitilanteissa. HallL 16 §:n mukaan viranomaiselle toimitettavassa asiakirjassa on mainittava lähettäjän nimi ja tarvittavat yhteystiedot asian hoitamiseksi.[225] Lisäksi erityislainsäädäntöön sisältyy tunnistamista koskevia säännöksiä.[226] Valtionhallinnon asiointipalvelussa luotettava käyttäjien yksilöinti ja sähköinen tunnistaminen on toteutettava silloin, kun palvelussa käsitellään ei-julkista tietoa, palvelussa on mahdollista laittaa vireille asioita, joilla on huomattava oikeudellinen tai taloudellinen merkitys taikka silloin kun asiointipalvelun

[222] *Korja* 2016, s. 87.
[223] *Saarenpää* 2016, s. 164.
[224] *Voutilainen* 2008, s. 4–23.
[225] *Voutilainen* 2014, s. 61.
[226] HE 59/2016 vp, s. 6–7.

anonyymiin käyttöön liittyy ilmeinen riski haitanteosta.[227] Tunnistautumista voidaan edellyttää myös silloin, kun asiointipalvelussa päästään katselemaan asianosaisjulkisuuden piiriin kuuluvia tietoja.[228] Lähivuosina sosiaali- ja terveyspalveluihin arvioidaan tulevan runsaasti sähköisiä asiointipalveluita, joissa tarvitaan vahvaa sähköistä tunnistamista. Kyseisissä palveluissa käsitellään usein salassa pidettäväksi luokiteltuja henkilötietoja yksilöiden terveyteen tai toimeentuloon liittyen. Tämä edellyttää tehokasta tapaa tunnistaa luotettavasti sekä palveluita käyttävät asiakkaat että heidän tietojaan käsittelevät henkilöt.[229]

Sähköinen tunnistautuminen verkkopalveluihin toimii yleisimmin siten, että käyttäjälle ilmoitetaan tunnistamisen tarpeesta ja tämän jälkeen käyttäjä valitsee omaan pankkiinsa osoittavan linkin ja hänet siirretään kyseisen pankin tunnistusjärjestelmään. Tämän jälkeen käyttäjä tunnistautuu pankkitunnuksin ja hänelle ilmoitetaan, mitkä häntä koskevat tiedot välitetään alkuperäisen palvelun tarjoajalle. Usein kyseessä on nimen ja henkilötunnuksen välittäminen. Hyväksyttyään näiden tietojen siirtämisen käyttäjä siirretään takaisin alkuperäisen palveluntarjoajan palveluun tunnistettuna käyttäjänä.[230]

Aiemmin mainittu KaPA -toteuttamisohjelma aiheutti muutoksia myös julkishallinnon sähköisessä tunnistamisessa. KaPAL:ssa säädetään tukipalveluksi[231] luonnollisen henkilön tunnistuspalvelu, joka tunnistaa julkisen hallinnon sähköisiä palveluita käyttävän luonnollisen henkilön SäTuL:ssa tarkoitetun tunnistuspalvelun tarjoajan palvelua käyttäen, hallinnoi tunnistustapahtumaa sekä luovuttaa VTJ:stä henkilön yksilöintiä koskevat tiedot käyttäjäorganisaatiolle (3 § 1 mom. 4 kohta). KaPA -ohjelman osana olleen sähköinen tunnistusmalli -hankkeen päätyttyä uusi suomi.fi -tunnistuspalvelu on korvannut

[227] Sähköisen asioinnin tietoturvallisuus -ohje, s. 45.
[228] *Voutilainen* 2009, s. 268.
[229] HE 74/2016 vp, s. 6.
[230] *Ponka* 2013, s. 225.
[231] Tukipalvelulla tarkoitetaan kyseissä laissa *sähköisen asioinnin tukipalvelua, jota käyttäjäorganisaatio käyttää asiointipalvelunsa tai muun sille kuuluvan tehtävän taikka sen tarjoaman palvelun tukena* (2.1 § 1 kohta).

tunnistamisen osalta hallinnon päällekkäiset ratkaisut, eli Tunnistus.fi- ja Vetuma -palvelut vuoden 2017 loppuun mennessä.[232] Suomi.fi -tunnistus on julkishallinnon asiointipalveluiden yhteinen tunnistuspalvelu, josta vastaa VRK.[233] Kansalliseen tunnistusratkaisuun liittyvien sopimusten hallinta keskitettiin VRK:een. Tällä tavoitellaan kustannussäästöjä sekä sopimushallinnan yksinkertaistamista vähentämällä tunnistuspalvelun tarjoajien kanssa tehtävien sopimusten määrää 1500 kappaleesta noin kymmeneen.[234]

5.6.1 Henkilötietojen käsittely

Tunnistuspalvelun ja sähköisiin allekirjoituksiin liittyvän varmennepalvelun yhteydessä henkilötietojen käsittelyn on todettu olevan välttämätöntä. Henkilöt on kyettävä erottamaan toisistaan, jotta palvelut voidaan luotettavasti toteuttaa. Käytännössä tämä tarkoittaa henkilötunnuksen käsittelyä.[235]

SäTuL:n mukaan tunnistuspalvelun tarjoaja saa käsitellä tunnistusvälineen liikkeelle laskemisessa, palvelun ylläpidossa sekä tunnistustapahtuman toteuttamisessa tarvittavia henkilötietoja HetiL 8.1 §:n 1 ja 2 kohdassa säädetyillä perusteilla. Tässä yhteydessä henkilötietoja käsitellään siis rekisteröidyn yksiselitteisesti antaman suostumuksen perusteella tai rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä. Luottamuspalveluja tarjoava varmentaja saa samoilla perusteilla käsitellä varmenteen myöntämisessä ja ylläpidossa tarvittavia henkilötietoja sekä kerätä henkilötietoja henkilöltä itseltään (6.1 §). Tunnistusvälityspalvelun tarjoajalla on oikeus tunnistuksen välityspalvelua tarjotessaan luovuttaa henkilötietoja sähköiseen tunnistukseen luottavalle osapuolelle, jos luottavalla osapuolella on lain perusteella oikeus käsitellä henkilötietoja (6.2 §). Muussa tapauksessa henkilötietoja saa käsitellä ainoastaan rekisteröidyn yksiselitteisen suostumuksen perusteella (6.3 §). Henkilötietojen käsittelystä noudatetaan täydentävästi, mitä säädetään 19 ja 24 §:ssä sekä HetiL:ssa (6.5

---

[232] Kansallisen palveluarkkitehtuurin toteuttamisohjelma (KaPA) 2014 – 2017 loppuraportti, s. 39.
[233] https://www.suomi.fi/sivu/tietoa-tunnistuksesta .
[234] HE 59/2016 vp, s. 22–25.
[235] HE 26/2009 vp, s. 47.

§). Oletettavaa on, että jatkossa myös SäTuL:n sääntely muutetaan vastaamaan tietosuoja-asetuksen sääntelyä, ainakin henkilötietojen käsittelyperusteiden osalta.

Tunnistuspalvelun tarjoajan ja luottamuspalveluja tarjoavan varmentajan tulee tarkastaessaan hakijan henkilöllisyyden vaatia hakijaa ilmoittamaan henkilötunnuksensa. Tunnistuspalvelun tarjoaja ja luottamuspalveluja tarjoava varmentaja saavat käsitellä henkilötunnusta rekistereissään SäTuL 6.1 §:ssä mainitussa tarkoituksessa. Henkilötunnuksen saa sisällyttää tunnistusvälineeseen tai varmenteeseen, jos välineen tai varmenteen tietosisältö on ainoastaan sellaisen tahon saatavilla, jolle se on välttämätöntä palvelun toteuttamiseksi. Henkilötunnus ei saa olla saatavissa julkisesta hakemistosta (6.4 §).

Viranomaistoiminnassa henkilöiden yksilöinti tapahtuu pääasiassa henkilötunnuksen avulla ja se onkin käytössä kaikissa vahvan sähköisen tunnistamisen palveluissa. Kun yksilöintitietona oleva henkilötunnus luovutetaan sähköiseen asiointipalveluun kirjautumisen yhteydessä, tarvitaan tähän tunnistettavan henkilön yksiselitteinen suostumus. Henkilötunnusta ei voida kuitenkaan automaattisesti käyttää yksilöintitietona. Sen käyttämiselle pitää olla asian hoitoon ja käsittelyyn liittyvä funktionsa. Pääasiassa henkilötunnusta voidaan viranomaisessa käsitellä ilman rekisteröidyn suostumusta, sillä henkilötunnuksen käsittely viranomaisessa perustuu lakiin. Kun sähköisen asiointipalvelun tarjoaja on vastaanottanut henkilön yksilöintitiedot, henkilötunnuksen käsittelyvastuu siirtyy sille.[236]

Tunnistusvälineen tarjoajan ja luottamuspalveluja tarjoavan varmentajan on hankittava ja päivitettävä luonnollisten ja oikeushenkilöiden tiedot suoraan väestötietojärjestelmästä sekä yritys- ja yhteisörekistereistä (SäTuL 7 ja 7a §).

5.7 Tunnistuspalvelun tarjoajat ja tunnistusvälineet

Tunnistuspalveluita voi tarjota toimija, joka täyttää SäTuL 9 §:ssä säädetyt edellytykset ja tekee ViVi:lle 10 §:ssä säädetyn kirjallisen ilmoituksen ennen toiminnan aloittamista.

---

[236] *Voutilainen* 2014, s. 70–72.

Tunnistuspalvelun tarjoaja voi laskea liikkeelle loppukäyttäjille tarkoitettuja tunnistusvälineitä tai se voi edelleen välittää toisen tunnistuspalvelun tarjoajan tekemiä käyttäjien tunnistustapahtumia. Palvelun tarjoaja voi toimia myös molemmissa näistä rooleista. Sähköisten tunnisteiden myöntäjiä velvoittavat useat eri säädökset. Myönnettäessä pankkitunnisteita on huomioitava esimerkiksi luottolaitoksiin, rahanpesun estämiseen ja perusmaksutileihin liittyvä kotimainen ja EU-tasoinen sääntely. Sähköiseen tunnistamiseen perustuvat palvelut sekä niissä tehtävät taloudelliset tai oikeudelliset toimet poikkeavat merkittävästi toisistaan. Tämän vuoksi sääntelyn piiriin kuuluvilta tunnistuspalveluiden tarjoajilta edellytetään yhtenäistä luotettavuuden perustasoa.[237] Vahvojen sähköisten tunnistuspalveluiden tuottajia ovat tällä hetkellä pankit, matkaviestinyritykset ja Väestörekisterikeskus.[238] Teleoperaattoreiden tarjoama mobiilivarmenne sekä VRK:n tarjoama kansalaisvarmenne eivät ole saavuttaneet merkittävää asemaa sähköisen tunnistamisen markkinoilla.[239]

Sähköisen tunnistamisen tunnistusvälineen myöntämisestä säädetään SäTuL 20 §:ssä. Tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä kirjallisesti. Sopimus voidaan tehdä myös sähköisesti, jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla. Tunnistuspalvelun tarjoajan tulee kohdella asiakkaitaan syrjimättä ja tunnistusvälineiden hakijoita tasapuolisesti sopimuksen tekemisen yhteydessä (20.1 §). Sopimus voi olla voimassa toistaiseksi tai määräaikaisesti. Tunnistusvälineellä voi olla oma voimassaoloaikansa, joka on lyhyempi kuin sopimuksen tekemisen yhteydessä (20.2 §). Tunnistusväline myönnetään aina luonnolliselle henkilölle tai oikeushenkilölle. Luonnollisen henkilön ja oikeushenkilön tunnistusvälineiden kytkös on toteutettava sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.1.4 mukaisesti. Tunnistusvälineen on oltava henkilökohtainen. Tunnistusvälineeseen voidaan tarvittaessa liittää tieto siitä, että tunnistusvälineen haltija voi tapauskohtaisesti myös edustaa toista luonnollista henkilöä tai oikeushenkilöä (20.3 §). Kuluttajien oikeuksien turvaamiseksi on säädetty, että

[237] HE 272/2014 vp, s. 5–11.
[238] HE 74/2016 vp, s. 5.
[239] HE 272/2014 vp, s. 3.

sellainen sopimusehto, joka poikkeaa lain säännöksistä kuluttajan vahingoksi, on mitätön, ellei SäTuL:ssa toisin säädetä (3 §).

On huomattava, että sähköinen tunnistamistoiminta on pääosin yksityisten toimijoiden hoitamaa. Perustuslain mukaisesti julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle (PL 124 §). PeVL:n mukaan tunnistamiseen liittyvät palvelut nähdään nykyään pääasiassa liiketaloudellisina ja niiden luonne on siinä määrin etääntynyt julkiseen hallintotehtävään liitettävistä ominaisuuksista, että toimintaa ei ole pidettävä julkisena hallintotehtävänä.[240]

Suomessa vahvan sähköisen tunnistamisen tunnistusvälineiden tuottamiselle ja jakelulle on valittu markkinaehtoinen malli. Tunnistusvälineen hankinnasta ja käytöstä aiheutuvat kulut tulevat välinettä käyttävän kansalaisen maksettavaksi[241].

Julkisten ja yksityisten palveluiden sähköistyessä yhä enemmän on tunnistusvälineiden saatavuus keskeistä ihmisten tasa-arvon kannalta. Tämä voi aiheuttaa myös ongelmia, sillä toimiminen ja palveluiden käyttö digitaalisessa toimintaympäristössä vaikeutuu, mikäli henkilöllä ei ole käytössään tarvittavia sähköisiä tunnisteita tai tunnistusvälineitä.[242] Sähköisen tunnistamisen välineet ovat käyttäjälleen usein maksullisia ja liittyvät tiettyyn palvelukokonaisuuteen, kuten pankkipalveluihin.[243] Liikenne- ja viestintävaliokunta kantoi huolta kansalaisten epätasa-arvoisesta asemasta sähköisten tunnistusvälineiden saamisen kannalta ja totesi, että ongelmaan tulee etsiä aktiivisesti ratkaisua kansalaisten yhdenvertaisuuden turvaamiseksi ja yhteiskunnasta syrjäytymismahdollisuuksien vähentämiseksi.[244]

---

[240] PeVL 16/2009 vp, s. 2–3.
[241] HE 272/2014 vp, s. 3.
[242] *Korja* 2016, s. 87.
[243] HE 74/2016 vp, s. 8.
[244] LiVM 17/2017 vp, s. 3.

Yhden sähköisen tunnistusvälineen laajamittainen käyttö on Voutilaisen mukaan tietosuojaongelma, sillä tässä tapauksessa yksi avain antaa laajamittaisen pääsyn henkilön sähköiseen identiteettiin jopa yhdellä tunnistuskerralla. Ratkaisuna hän näkee sen, että henkilön tietoihin pääsy olisi hajautettu useammalle tunnistusvälineelle.[245] Käytännössä tällaiseen tilanteeseen ei ole päästy, vaan vahvassa sähköisessä tunnistamisessa laajamittaisesti käytetyt pankkitunnisteet avaavat tarvittaessa pääsyn niin henkilön taloudellisiin tietoihin kuin suurimpaan osaan viranomaispalveluita. Voutilaisen mainitseman tietosuojaongelman ei voi siten katsoa poistuneen tai edes rajoittuneen.

5.7.1 Pankkitunnisteet

Finanssialalla toimivat yritykset, kuten rahoitus- ja vakuutuslaitokset ovat velvollisia tunnistamaan asiakkaansa lainsäädännön ja sitä täydentävien viranomaismääräysten perusteella. Läsnäolevan asiakkaan henkilöllisyyden todentaminen asiakassuhdetta perustettaessa perustuu viranomaisen antamaan, voimassa olevaan henkilöllisyysasiakirjaan. Mikäli asiakassuhde perustetaan niin, ettei asiakas ole henkilökohtaisesti läsnä, tulee käytössä olla menetelmät, joilla henkilöllisyys voidaan todentaa luotettavasti. Esimerkkinä etätunnistamisen osalta viitataan siihen, että henkilöllisyyden todentaminen perustuu SäTuL:ssa tarkoitettuun vahvan sähköisen tunnistamisen välineeseen.[246]

Tunnistuspalveluita tarjoavat pankkitoimijat eivät ole käytännössä hyväksyneet toisten tunnistuspalveluiden tarjoajien tunnistusvälineitä. Verkkopankkitunnukset on tehty pääasiassa pankkien omien asiakkaiden tunnistamista varten. Käyttäjän kannalta tästä on seurannut se, että hän on tarvinnut useita eri tunnistusvälineitä ollessaan esimerkiksi usean eri pankin asiakas. Sopimuksellisesti asia on ollut myös haasteellinen, sillä sähköisten palveluiden tarjoaja on joutunut käytännössä tekemään sopimuksen kaikkien eri tunnistuspalveluiden tarjoajien kanssa, mikäli tämä on halunnut mahdollistaa eri tunnistusvälineiden käyttämisen palvelussaan.[247]

---

[245] *Voutilainen* 2009, s. 325.
[246] FIVA Standardi 2.4, s. 21–22.
[247] HE 272/2014 vp, s. 9.

Hallituksen esityksessä todettiin, että tunnistusvälinemarkkinoiden tilannetta ei voida pitää kilpailu- ja kuluttajanäkökulmasta tarkoituksenmukaisena, eikä tunnistusvälinemarkkinoiden markkinaehtoista kehitystä ole tapahtunut. Vahva sähköinen tunnistaminen perustuu pääosin tilinkäyttövälineiksi tarkoitettuihin pankkitunnisteisiin, jotka ovat sidoksissa asiakkuuteen ja usein liittyvät johonkin muuhun palveluun oheispalveluna. Ongelmaksi on nähty se, että sähköisten palveluiden tarjoajilla ei ole ollut tosiasiallista mahdollisuutta kilpailuttaa sähköisen tunnistamisen palveluita eikä kontrolloida tunnistamisesta aiheutuvia kustannuksia. Kustannuksia aiheutuu tietenkin myös tunnistuspalveluiden tarjoajille. Niitä aiheutuu esimerkiksi uuden tunnistusvälineen luomisesta jo olemassa olevalla tunnistusvälineellä, tunnistusvälineen jakelusta ja käyttämisestä sekä tunnistusvälineiden tarjoamiseen liittyvästä infrastruktuurista.[248]

Pankit kehittävät edelleen aktiivisesti omia tunnistusmenetelmiään. Suomessakin on otettu käyttöön menetelmiä, joissa perinteisesti osaksi pankkitunnisteita kuulunut, tunnistautujan hallussa ollut avainluku- tai muu pääsyavainluettelo on korvattu älypuhelimeen asennettavalla mobiilisovelluksella. Älypuhelinsovellus antaa käyttäjälle esimerkiksi tarvittavan pääsyavaimen. Yhä enemmässä määrin näihin sovelluksiin liitetään myös biometristen tunnisteiden, kuten sormenjälkien hyödyntämistä.

5.7.2 Tupas-tunnistuspalvelu

Suomessa finanssilaitosten käyttämä Tupas-tunnistuspalvelu on pankkien yhteisesti määrittelemä sähköiseen tunnistamiseen ja allekirjoittamiseen käytettävä palvelu, jota käytetään näihin toimintoihin palveluntarjoajien asiointipalveluissa. Tunnistamisessa käytettävien kiinteiden salasanojen ja tunnuslukujen lisäksi käytetään vaihtuvia tunnus- tai avainlukuja, jonka katsotaan täyttävän turvallisen tunnistustapahtuman kriteerit. Tupas-tunnistuspalvelun vastuuta on rajattu siten, että pankki huolehtii ainoastaan asiakkaan tunnistamisesta niin kuin palvelukuvauksessa on mainittu. Pankki ei kuitenkaan vastaa asiakkaan ja tunnistusta hyödyntävän kolmannen osapuolen välisen oikeustoimen sisällöstä ja sitovuudesta. Erilaisten sopimusten tekeminen verkossa on mahdollistettu siten, että asiakas

[248] HE 272/2014 vp, s. 9–14.

ja palveluntarjoaja voivat sopia Tupas-tunnisteen käyttämisestä osana sähköistä allekirjoitusta eri oikeustoimissa. Tupas-määrityksiä hallinnoi, kehittää ja ylläpitää Finanssialan keskusliitto.[249]

Pankkitunnuksista tehdään sopimus pankin ja tunnusten käyttäjän välillä. Tupas-tunnistusperiaatteiden mukaan ensimmäiset tunnukset on noudettava henkilökohtaisesti ja tässä yhteydessä asiakas tunnistetaan luotettavasti. Mikäli asiakkaalla on voimassa olevat tunnukset, voidaan uudet kertakäyttöiset tunnukset jatkossa lähettää asiakkaalle postitse.[250] Tupas-palvelua käyttävä asiakas antaa pankille suostumuksen palvelun käyttämisessä välttämättömien asiakastietojen välittämiseen palveluntarjoajalle.[251]

ViVi on vastikään ilmoittanut, että nykyinen Tupas-protokolla ei täytä uusia tietoturvallisuusvaatimuksia, eikä kyseistä protokollaa enää kehitetä näitä vaatimuksia vastaavaksi. ViVi:n mukaan yleisesti on saatavilla vaatimukset täyttäviä protokollia, joihin sisältyy tietoliikenteen sanomatason salaus, jolla parannetaan tunnistuspalvelun ja sähköisen asiointipalvelun rajapintojen turvallisuutta. Tämä kuitenkin edellyttää teknisiä muutoksia sekä tunnistuspalveluiden tarjoajien että asiointipalveluiden järjestelmiin. ViVi arvioi, että pankit toteuttavat tarvittavat muutokset omiin järjestelmiinsä. ViVi esittää, että pankkien tulisi tarjota uudet vaatimukset täyttävää rajapintaa asiointipalveluille alkuvuodesta 2019.[252]

5.8 Tunnistaminen erityislainsäädännössä

Useissa erityislain tasoisissa säädöksissä on säännöksiä liittyen vaatimuksiin asiakkaiden tai käyttäjien luotettavasta tunnistamisesta.

Laissa rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (28.6.2017/444) tarkoitetaan tunnistamisella asiakkaan henkilöllisyyden selvittämistä

---

[249] Tupas tunnistusperiaatteet, s. 4–6.
[250] Tupas tunnistusperiaatteet, s. 9.
[251] Tupas tunnistusperiaatteet, s. 10.
[252] Ks. https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2018/tupas-tunnistamistakayttaviltaasiointipalveluiltaedellytetaanmuutoksia.html [käyty 10.4.2018].

asiakkaan toimittamien tietojen perusteella (1:4.1:n 6 kohta). Henkilöllisyyden todentamisella tarkoitetaan asiakkaan henkilöllisyyden varmistamista luotettavasta ja riippumattomasta lähteestä peräisin olevien asiakirjojen tai tietojen perusteella (1:4.1:n 7 kohta). Lain soveltamisala on varsin laaja sisältäen esimerkiksi rahoitus- ja vakuutussektorin sekä asianajotoiminnan (1:2 §). Lain soveltamisalaan kuuluville toimijoille asetetaan velvollisuus asiakkaan tunnistamiseksi ja henkilöllisyyden todentamiseksi (3:2.1 §). Lisävelvollisuuksia asetetaan tunnistettaessa asiakasta, joka ei ole läsnä (etätunnistaminen). Tällöin on mahdollista käyttää asiakkaan henkilöllisyyden todentamiseen SäTuL:ssa tarkoitettua tunnistusvälinettä tai eIDAS-asetuksen 28 artiklassa tarkoitettua varmennetta taikka muuta tietoturvallista ja todisteellista tunnistamistekniikkaa (3:11 §).

Luotonhakijan henkilöllisyyden todentamisesta säädetään kuluttajansuojalain (20.1.1978/38) 7 luvun 15 §:ssä. Luotonantajan on ennen kuluttajaluottosopimuksen tekemistä todennettava luottoa hakevan henkilöllisyys huolellisesti. Jos henkilöllisyys todennetaan sähköisesti, luotonantajan on käytettävä tunnistusmenetelmää, joka täyttää SäTuL 8 §:ssä säädetyt vaatimukset (7:15.1 §). Jos luotonantaja on jo aiemmin todentanut kuluttajan henkilöllisyyden 1 momentissa tarkoitetulla tavalla, kuluttajan henkilöllisyys voidaan todentaa myös hänelle ensitunnistamisen jälkeen luodun henkilökohtaisen tunnisteen avulla (7:15.2 §).

Koska luottosuhteella on sekä taloudellista että oikeudellista merkitystä suhteen molemmille osapuolille, voidaan pitää tarkoituksenmukaisena, että luotonantajalla on velvollisuus tunnistaa hakijan henkilöllisyys huolellisesti. Niin kutsutuissa *pikaluotoissa* luoton myöntäminen tapahtuu tekstiviestin tai internetin välityksellä, eikä pikaluottoyhtiöillä ole fyysisiä asiakaspalvelupisteitä. Tämän vuoksi pikaluottotoimintaa koskevat nimenomaan asiakkaan sähköiseen tunnistamiseen liittyvät vaatimukset.[253]

[253] *Pönkä & Parkkali* 2010, s. 602–603.

5.9 Rajat ylittävä sähköinen tunnistaminen EU:ssa

eIDAS-asetus tuli voimaan 17.9.2014 ja sen soveltaminen alkoi 1.7.2016, lukuun ottamatta säännöksiä, joiden soveltamisesta oli säädetty siirtymäsäännöksin, kuten edellä käsiteltyjen varmuustasojen tarkemmasta määrittelystä. Sääntelyn tavoitteena on ollut sisämarkkinakehityksen edistäminen erityisesti sähköisen viranomaisasioinnin alueella. Asetuksen keskeinen tavoite on, että toisessa jäsenvaltiossa myönnetty komissiolle ilmoitettu (notifioitu) vahvan sähköisen tunnistamisen väline, hyväksytään asetuksen tarkoittamassa luottamusverkostossa automaattisesti myös toisessa jäsenvaltiossa ja sillä tehty sähköinen tunnistus hyväksytään automaattisesti toisessa jäsenvaltiossa (vastavuoroinen tunnustaminen). Tämä tarkoittaa käytännössä sitä, että yhden jäsenvaltion kansalainen voisi omilla tunnistusvälineillään tunnistautua toisen jäsenvaltion julkishallinnon sähköisiin palveluihin.

Asetusta sovelletaan *jäsenvaltion ilmoittamiin* sähköisen tunnistamisen järjestelmiin ja unioniin sijoittautuneisiin luottamuspalveluiden tarjoajiin (2(1) art.). Asetuksessa tarkoitetaan *sähköisellä tunnistamisella* prosessia, jossa käytetään tiettyä luonnollista henkilöä, oikeushenkilöä tai oikeushenkilöä edustavaa luonnollista henkilöä vastaavia yksilöiviä tunnistetietoja sähköisessä muodossa (3(1)(1) art.). *Sähköisen tunnistamisen menetelmällä* tarkoitetaan aineellista ja/tai aineetonta kokonaisuutta, joka sisältää henkilön tunnistetietoja ja jota käytetään verkkopalveluun liittyvään todentamiseen (3(1)(2) art.). *Henkilön tunnistetiedoilla* tarkoitetaan tietoja, jotka mahdollistavat luonnollisen henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön henkilöllisyyden toteamisen (3(1)(3) art.). *Sähköisen tunnistamisen järjestelmällä* tarkoitetaan sähköiseen tunnistamiseen liittyvää järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä myönnetään luonnollisille henkilöille, oikeushenkilöille tai oikeushenkilöä edustaville luonnollisille henkilöille (3(1)(4) art.). *Todentamisella* tarkoitetaan sähköistä prosessia, joka mahdollistaa luonnollisen henkilön tai oikeushenkilön sähköisen tunnistamisen tai sähköisessä muodossa olevien tietojen alkuperän ja eheyden vahvistamisen (3(1)(5) art.).

Kun julkisen sektorin elimen yhdessä jäsenvaltiossa tarjoaman verkkopalvelun käyttö edellyttää kansallisen oikeuden nojalla tai kansallisessa hallinnollisessa käytännössä säh-

köistä tunnistamista sähköisen tunnistamisen menetelmän ja todentamisen avulla, toisessa jäsenvaltiossa myönnetyt verkkopalveluiden käyttöön tarvittavat sähköisen tunnistamisen menetelmät on tunnustettava ensimmäisessä jäsenvaltiossa kyseisen verkkopalvelun osalta rajat ylittävää todentamista varten (6(1) art.) Edellyttäen, että sähköisen tunnistamisen menetelmä on myönnetty komission 9 artiklan mukaisesti julkaisemaan luetteloon sisältyvän sähköisen tunnistamisen järjestelmän puitteissa. Lisäksi sähköisen tunnistamisen menetelmän varmuustason tulee vastata varmuustasoa, joka on yhtä korkea tai korkeampi kuin asianomaisen julkisen sektorin elimen edellyttämä varmuustaso kyseiseen verkkopalveluun pääsemiseksi ensimmäisessä jäsenvaltiossa edellyttäen, että kyseisen sähköisen tunnistamisen menetelmän varmuustaso vastaa korotettua tai korkeaa varmuustasoa. Lisäksi asianomaisen julkisen sektorin elimen tulee soveltaa korotettua tai korkeaa varmuustasoa kyseisen verkkopalvelun käytön osalta (6(1)(a-c) art.). Julkisen sektorin elimet voivat hyväksyä verkkopalveluidensa rajat ylittävään todentamiseen myös matalan varmuustason sähköisen tunnistamisen järjestelmän, mikäli se sisältyy komission julkaisemaan luetteloon (6(2) art.). Komission julkaisema luettelo on saatavissa ajantasaisesti verkosta.[254]

Edellytyksistä sähköisen tunnistamisen järjestelmien ilmoittamiselle säädetään 7 artiklassa ja ilmoittamisesta 9 artiklassa. Ilmoitettuihin sähköisen tunnistamisen järjestelmiin liittyvistä vastuista säädetään 11 artiklassa. Jäsenvaltioiden yhteistyöstä sekä järjestelmien yhteentoimivuudesta puolestaan 12 artiklassa.

Jos ilmoitettuun sähköisen tunnistamisen järjestelmään tai 7(f) artiklassa tarkoitettuun todentamiseen liittyy loukkaus tai niiden jonkin osan turvallisuus on vaarantunut tavalla, joka vaikuttaa kyseisen järjestelmän rajat ylittävän todentamisen luotettavuuteen, ilmoittavan jäsenvaltion on viipymättä keskeytettävä tai peruutettava kyseinen rajat ylittävä todentaminen tai ne osat, joiden turvallisuus on vaarantunut ja ilmoitettava asiasta muille jäsenvaltioille ja komissiolle (10(1) art.). Loukkauksen tai turvallisuutta vaarantavan tekijän korjaamisesta on ilmoitettava komissiolle sekä koko järjestelmän peruuttamisesta,

[254] Ks. https://webgate.ec.europa.eu/tl-browser/#/ [käyty 19.4.2018].

mikäli mainittua vikaa ei ole korjattu kolmen kuukauden kuluessa alkuperäisestä keskeyttämisestä tai peruuttamisesta (10(2-3) art.).

Sähköisen tunnistamisen rajat ylittävässä toiminnassa tunnistamistietojen välittämisestä vastaa kansallinen solmupiste. Solmupisteen tarkoituksena on mahdollistaa se, että julkisen hallinnon organisaatiot voivat omissa asiointipalveluissaan huomioida toisen jäsenvaltion tunnistusvälinettä käyttävän asiakkaan.[255] Kansallisesta solmupisteestä vastaa Suomessa VRK. Jäsenmaiden välisessä sähköisessä tunnistamisessa ei välitetä maksuja.[256]

VRK osallistuu myös aktiivisesti sähköisen henkilöllisyyden kansainvälistä käyttöä edistävän, niin kutsutun *Porvoo-ryhmän*[257] toimintaan. Ryhmän pysyvä sihteeristö muodostuu VRK:n edustajista.

6 Tunnistusvälineiden oikeudeton käyttö

6.1 Sähköisen tunnistamisen turvallisuus ja tietojenkäsittelyrauha

Tiedon suojaaminen on kompleksinen prosessi. Tietoa suojataan luottamuksellisuuteen, eheyteen ja kiistämättömyyteen liittyvillä prosesseilla sekä pääsynvalvonnan[258] ja laitteisiin liittyvien fyysisten turvallisuustoimenpiteiden avulla. Mikään yksittäinen turvallisuusprosessi ei takaa täydellistä suojaa ja tiedon suojaamiseksi tulisikin käyttää useita eri

---

[255] HE 74/2016 vp, s. 17.
[256] HE 272/2014 vp, s. 6.
[257] *Porvoo-ryhmä* on nimensä mukaisesti, Porvoossa vuonna 2002 perustettu kansainvälinen, taloudellisesti ja poliittisesti riippumaton yhteistyöverkosto, jonka tehtävänä on tukea julkisen ja yksityisen sektorin sähköisen asioinnin kehittymistä ja sähköisen henkilöllisyyden yleistymistä Euroopassa. Ryhmän tehtävänä on lisäksi edistää tunnistusmekanismien vastavuoroista tunnustamista ja hyväksymistä eri maiden välillä sekä teknisten määritysten ja yhteensopivien varmenteiden käyttöönottoa. Ryhmän tavoitteena on kokoontua kahdesti vuosittain. Edellinen kokoontuminen oli toukokuussa 2017 Roomassa. Ks. lisätiedot ja työryhmän materiaalit https://eevertti.vrk.fi/en/porvoo-group [käyty 29.5.2018].
[258] Todettakoon, että viime vuosina erilaisiin viranomaisrekistereihin poliisihallinnon sekä sosiaali- ja terveydenhuollon aloilla kohdistuneet ns. *tietourkintatapaukset* eivät nähdäkseni ole johtuneet tunnistamiseen liittyvien tietoturvallisuuskontrollien puutteista vaan lähinnä ko. tekoihin syyllistyneiden henkilökohtaisista ratkaisuista. Kontrollien toimivuudesta kertoo myös se, että urkintaan liittyviä asioita on käsitelty rikosprosessissa ja rangaistu virkavelvollisuuden rikkomisena (esim. KKO 2014:86). Urkintatapauksista uutisointi ks. esim. Helsingin Sanomat 6.9.2016, s. A13.

prosesseja.[259] *Tietojenkäsittelyrauhalla* tarkoitetaan tietojenkäsittelyn loukkaamattomuutta.[260]

Tietotekniikkarikokset liittyvät aina tietojenkäsittelyprosessiin, jonka ominaispiirteenä on tietyntasoinen luottamuksellisuus ja yksityisyys. Tietotekniikkarikosten olennaisena elementtinä on siten näiden arvojen loukkaaminen. Tietotekniikkarikoksen määritelmän mukaisten tekojen kohteena, välikappaleena tai tekoympäristönä ovat tietojärjestelmät niihin kuuluvine laitteineen ja ne loukkaavat kaikki tietojenkäsittelyrauhaa, jonka *Pihlajamäki* rinnastaa kotirauhaan. Voidaan puhua myös tietojenkäsittelyn luottamuksellisuudesta. Suomen lainsäädäntö ei kuitenkaan nimenomaisesti tunne tietojenkäsittelyrauhan käsitettä. Tietotekniikkarikoksia koskevilla kriminalisoinneilla suojataan tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä, eli tietoturvallisuuden peruselementtejä.[261] Tietoturvallisuus on puolestaan laajempi käsite kuin tietojenkäsittelyrauha ja sitä toteutetaan myös hallinto- ja siviilioikeuteen kuuluvalla sääntelyllä. Tietojärjestelmän haltijalla on vastuu järjestelmän tietoturvallisuuden tasosta. Arvioitaessa sellaisten rikosten, kuten petos, maksuvälinepetos, väärennys, vahingonteko, luvaton käyttö tai yritysvakoilu, tietoteknistä ulottuvuutta, kohdistuu arviointi nimenomaan tietojenkäsittelyrauhan suojaan.[262]

Arvioitaessa sähköisen tunnistamismenetelmän turvallisuutta, *Ponka* nostaa esiin kolme keskeistä riskiä. Nämä ovat ensitunnistamisen epäonnistuminen, luomistietojen tai tunnistusvälineen joutuminen tunnistettavan hallusta vääriin käsiin sekä itse menetelmään, varmentajaan tai tunnistuspalvelun tarjoajaan taikka niiden toimintaan liittyvät puutteet.[263] Digitaalinen ja maantieteellisesti laaja ympäristö mahdollistavat sen, että väärinkäyttötilanteessa, jossa esimerkiksi tunnistusväline on joutunut vääriin käsiin, väärinkäyttötilanne voi kestää pitkään ennen havaitsemista ja välineen avulla voidaan tehdä suuri määrä erilaisia oikeustoimia. Näin mahdollisesti syntyneet vahingot, joissa voi olla luke-

[259] *Bragg* 2004, s. 174.
[260] *Pihlajamäki* 2004, s. 8.
[261] *Pihlajamäki* 2004, s. 21–121.
[262] *Pihlajamäki* 2004, s. 17–140.
[263] *Ponka* 2013, s. 320–321.

maton määrä vastapuolia, voivat olla myös arvomääräisesti suuria. Sähköisen tunnistamisen tai allekirjoittamisen oikeudellisesti merkittävä väärinkäyttö voi täyttää yleisimmin petoksen, väärennyksen tai tietomurron tunnusmerkistön.[264]

Tunnistusvälineen haltijalle on asetettu huolellisuusvelvoite, joka alkaa siitä hetkestä, kun tämä on vastaanottanut tunnistusvälineen. Tunnistusvälineen haltijan on käytettävä tunnistusvälinettä sopimuksen ehtojen mukaisesti ja säilytettävä tunnistusvälinettä huolellisesti (SäTuL 23.1 §). Tunnistusvälineen haltija ei saa luovuttaa tunnistusvälinettä toisen käyttöön (23.2 §). Tunnistusvälineen haltijan tunnistusvälineen oikeudetonta käyttöä koskevista vastuunrajoituksista säädetään SäTuL 27 §:ssä. Tunnistusvälineen haltija vastaa tunnistusvälineen oikeudettomasta käytöstä vain, jos hän on luovuttanut tunnistusvälineen toiselle (27.1 §:n 1 kohta), tunnistusvälineen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää (27.1 §:n 2 kohta) tai hän on laiminlyönyt ilmoittaa tunnistuspalvelun tarjoajalle tai sen ilmoittamalle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan (27.1 §:n 3 kohta).

Tunnistusvälineen haltija ei kuitenkaan vastaa tunnistusvälineen oikeudettomasta käytöstä siltä osin kuin tunnistusvälinettä on käytetty sen jälkeen, kun hän on ilmoittanut tunnistuspalvelun tarjoajalle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä (27.2 §:n 1 kohta), jos tunnistusvälineen haltija ei ole voinut tehdä ilmoitusta välineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan sen johdosta, että tunnistuspalvelun tarjoaja on laiminlyönyt 25 §:n 2 momentissa tarkoitetun velvollisuutensa huolehtia siitä, että tunnistusvälineen haltijalla on milloin tahansa mahdollisuus tehdä kyseinen ilmoitus (27.2 §:n 2 kohta) tai tunnistuspalvelua käyttävä palveluntarjoaja on laiminlyönyt 18 §:n 4 momentin tai 25 §:n 5 momentin mukaisen velvollisuutensa tarkastaa tunnistusvälineeseen liittyvän käyttörajoituksen olemassaolon tai tiedon välineen käytön estämisestä tai sulkemisesta (27.2 §:n 3 kohta).

---

[264] *Ponka* 2013, s. 424–464.

6.2 Tunnistamiseen ja tunnistusvälineisiin liittyvä oikeuskäytäntö

Vahvan sähköisen tunnistamisen tunnistusvälineisiin liittyviä vastuukysymyksiä on käsitelty tapauksessa *KKO 2016:73*. Siinä oli ratkaistavana tapaus, jossa henkilön B aviopuoliso C oli tämän tietämättä käyttänyt B:n pankkitunnisteita ja tunnistautunut niillä laissa tarkoitetulla vahvan sähköisen tunnistautumisen tavalla ja hakenut kuluttajaluottoa, joka oli hänelle myönnetty. B oli säilyttänyt pankkitunnisteitaan (sekä tunnistusvälinettä että tunnuslukuja) kotonaan paikassa, joka oli C:n tiedossa ja jossa perhe yleensä säilytti esimerkiksi saapuneita laskuja. Tapauksessa velkojana ollut A Oy vaati B:n velvoittamista suorittamaan maksamatta jääneen luoton. Käräjä- ja hovioikeudessa kanne oli hylätty. KKO katsoi, että B ei ollut luovuttanut mainittuja tunnisteita SäTuL 27 §:n 1 momentin 1 kohdassa tarkoitetulla tavalla. KKO:n mukaan B:n menettelyä oli kuitenkin pidettävä mainitun säännöksen 2 kohdan mukaisena huolimattomuutena, joka ei ollut vähäistä. B ei ollut ryhtynyt minkäänlaisiin toimenpiteisiin pitääkseen tunnistusvälineensä suojassa. Siten tunnistusvälineen oikeudeton käyttö johtui B:n huolimattomuudesta ja B oli velvollinen suorittamaan maksamatta olevan kuluttajaluoton A Oy:lle.

Tunnistusvälineiden saatavuuteen, ensitunnistamiseen ja mahdolliseen syrjintään näissä tilanteissa on annettu kaksi KHO:n ratkaisua. Ratkaisussa *KHO 2016:216* pankin ei todettu menetelleen yhdenvertaisuuslain (silloinen laki 20.1.2004/21, 1.1.2015 alkaen voimassa laki 30.12.2014/1325) vastaisesti tai siten, että sen käyttämät tunnistusperiaatteet olisivat olleet kohtuuttomia kantajan A kannalta. A:lle ei ollut myönnetty verkkopalvelutunnuksia, koska pankki ei ollut hyväksynyt ensitunnistamisessa A:n esittämiä Venäjän viranomaisen myöntämää passia tai ajokorttia, jonka Suomen poliisiviranomainen oli vaihtanut venäläisestä ajokortista suomalaiseksi. Mainittuja asiakirjoja ei ollut hyväksytty pankin noudattamissa ja Finanssivalvonnan ohjeiden[265] mukaan laadituissa tunnistusperiaatteissa kelvollisiksi tunnistamisasiakirjoiksi. KHO totesi tämän menettelyn olevan silloin voimassa olleen lain mukainen. A:lla, joka oli Venäjän kansalainen, olisi ollut mahdollisuus hankkia SäTuL:ssa tarkoitettu ensitunnistamiseen kelpaava asiakirja taikka antaa poliisin suorittaa ensitunnistaminen kyseisessä laissa tarkoitetulla tavalla.

---

[265] FIVA Standardi 2.4, luku 5.3.

Toiseen lopputulokseen päädyttiin ratkaisussa *KHO 2017:19*, jossa pankin katsottiin asettaneen henkilön T ilman asianmukaista perustetta eri asemaan muihin nähden. T oli hakenut verkkopankkitunnuksia ja esittänyt ensitunnistamisen yhteydessä Viron viranomaisen myöntämän passin henkilöllisyyttä todistavana asiakirjana. Pankki ei ollut tätä asiakirjaa kuitenkaan hyväksynyt vaan oli edellyttänyt lisäksi suomalaisen viranomaisen myöntämän tunnistusasiakirjan esittämistä. Pankki vetosi tässä yhteydessä muun muassa rahoitus- ja vakuutusneuvonta Fine:n[266] toisessa samankaltaisessa asiassa antamaan vastaukseen, jonka mukaan perusteluna kyseiselle menettelylle olisi ollut se, ettei ulkomaisesta passista käy ilmi suomalaista henkilötunnusta, eikä sitä voida varmistaa muutoin kuin suomalaisen viranomaisen myöntämästä tunnistusasiakirjasta. Lisäksi pankki vetosi rahanpesun ja terrorismin rahoituksen estämisestä annettuun lainsäädäntöön ja siihen, että Suomen ulkopuolelta tulevat henkilöt muodostavat korkeamman riskin. Tämän vuoksi se olisi edellyttänyt pankkitunnusten myöntämiseksi myös suomalaisen viranomaisen myöntämiä tunnistusasiakirjoja. KHO katsoi, että T:n esittämä passi olisi tullut hyväksyä laissa tarkoitetuksi tunnistusasiakirjaksi ja siten pankki oli menetellyt yhdenvertaisuuslain 6 §:n (nykyisin 8 §) vastaisesti.

Henkilötietojen lainmukaiseen käsittelyyn ja henkilöiden tunnistamiseen liittyy myös KHO:n ratkaisu niin sanotussa pikavippiasiassa (*KHO 8.1.2010*, taltionumero 15, diaarinumero 1568/1/09). Tapauksessa X Oy oli myöntänyt kuluttajaluottoja, eli niin sanottuja pikavippejä menettelyllä, jossa se vertasi lainanhakijan ilmoittamia henkilötietoja sen puhelinliittymän haltijan tietoihin, jonka liittymänumero oli lainahakemuksessa ilmoitettu. Mikäli tiedot olivat yhdenmukaiset, hakijan oletettiin olevan kyseisen liittymän haltija eikä muita varmistuksia tehty. Prosessissa ei käytetty mitään vahvan sähköisen tunnistamisen menetelmiä. Tietosuojalautakunta oli tietosuojavaltuutetun hakemuksen perusteella määrännyt X Oy:n muuttamaan pikaluottojen myöntämisessä käyttämäänsä luotonhakijoiden tunnistamistapaa siten, ettei väärää henkilöä voida rekisteröidä luoton hakijaksi. KHO hylkäsi X Oy:n valituksen ja pysytti hallinto-oikeuden päätöksen. Hallinto-oikeus katsoi perusteluissaan, että yhtiö oli menetellyt HetiL 5 §:n huolellisuusvelvoitteen sekä 9.2 §:n mukaisen virheettömyysvelvoitteen vastaisesti. Lisäksi katsottiin, että X

[266] Ks. www.fine.fi .

Oy:n käyttämä menettely ei täyttänyt lain 6 §:ssä henkilötietojen käsittelyn suunnittelulle asetettuja velvoitteita.

7 Lopuksi

7.1 Johtopäätökset

Edellä esitetyn perusteella voidaan todeta, että sähköisten asiointipalveluiden merkitys informaatiohallinnossa on edelleen kasvamassa. Maailman kehittyessä tietointensiivisemmäksi ja digitalisoitumiskehityksen tuloksena yhä useammat julkishallinnon palvelut tarjotaan tietoverkkojen välityksellä sähköisissä palvelukanavissa. On nähtävissä, että esimerkiksi sosiaali- ja terveyspalveluita koskevien muutosten myötä sähköinen asiointi lisääntyy kyseisellä alalla. Tämä puolestaan asettaa asiointipalveluille tietosuojaa ja -turvallisuutta koskevia vaatimuksia. Samalla tavoin kuin yhteiskunta yleensä, tarvitsee digitaalinen ympäristö toimiakseen säännöt, joilla taataan tietyt yksilöiden oikeudet ja asetetaan tietyt velvollisuudet. Olen kuitenkin samaa mieltä kuin Korhonen, jonka mukaan sähköisen asioinnin nopeaan kehittymiseen on vaikeaa varautua säädöstasolla siten, että voitaisiin ennakoida kaikki mahdollisesti esiin tulevat tietosuoja- ja tietoturvallisuusongelmat[267].

Informaatiohallintoa koskevan lainsäädännöllisen tai muun oikeudellisen materiaalin hallinta ei ole helppo tai suoraviivainen tehtävä. Säädösmateriaalin määrä on huomattava. Lisäksi tietyn asiakokonaisuuden, kuten henkilötietojen suojan osalta, sääntelyä on sekä yleis- että erityislainsäädännön tasolla. Myös lisääntyvä EU-tasoinen sääntely koskee yhä enemmän informaatiohallinnon eri prosesseja. Tämä on havaittavissa myös tässä tutkimuksessa käsiteltyjen tietoturvallisuuden ja sähköisen tunnistamisen alueilla. Informaatiohallinnon alueella Korhosen mainitsema normitulva näyttää siis yhä jatkuvan, joskin

[267] *Korhonen* 2016, s. 359.

sääntelyn painopisteen voi katsoa siirtyneen osittain EU-tasolle. Oikeusturvanäkökulmasta kehitystä voi arvostella, jos sen seurauksena yhä useampaan asiaan joudutaan jatkossa hakemaan oikeudellinen ratkaisu tai tulkinta EU-tuomioistuimesta[268].

Sääntelynäkökulmasta peruspohja hyvän informaatiohallinnon toteuttamiselle on olemassa. PL:ssa määritellyt perusoikeudet saavat konkreettisen sisältönsä niin HallL:n, AsiointiL:n ja julkisuuslain säännöksistä kuin muusta henkilötietojen suojaa, tietoturvallisuutta ja informaatioinfrastruktuuria koskevasta sääntelystä. Julkisuulain 18 §:n voi ymmärtää eräänlaisena hyvän informaatiohallinnon minimitason määrittäjänä. Selvää on, että informaatiohallintoa ei voida tyhjentävästi määritellä lainsäädännössä vaan avuksi tarvitaan myös muun tyyppistä sääntelyä, kuten erilaisia toimialaohjeita sekä parhaita käytäntöjä. Näenkin lainsäätäjän tärkeimpänä tehtävänä laadukkaiden ja kustannustehokkaiden sähköisten palveluiden turvaamisen. Tämä tulisi kuitenkin tehdä liiaksi rajoittamatta innovaatioita ja uusien palveluiden syntyä markkinoille.

Yksityisyyden suoja on, tai sen on oltava, keskeinen oikeushyvä digitaalisessa verkkoyhteiskunnassa. Palveluiden tarjoajien ja kehittäjien tulee kunnioittaa tätä oikeushyvää ja samaan tavoitteeseen näyttäisi tähtäävän myös uusi tietosuoja-asetus, sen ollessa vahvasti perusoikeuslähtöinen. Tietosuojan lisäksi tietoturvallisuus on hyvän informaatiohallinnon lähtökohta. Kuten edellä on esitetty, tietoturvallisuudella on keskeinen merkitys perusoikeuksiemme toteuttamisessa. Vaikka tietoturvallisuudesta ei nimenomaista perusoikeussäännöstä ole olemassa, sen voidaan niin sanottuna metaperusoikeutena katsoa toteuttavan perustuslaillisia oikeuksiamme turvallisuuteen, henkilötietojen suojaan sekä luottamukselliseen viestintään myös sähköisessä ympäristössä. Oikeudellisesta näkökulmasta tietoturvallisuus on edellytyksenä oikeuksiemme tehokkaalle toteuttamiselle informaatiohallinnossa. Tietoturvallisuus on lisäksi osa organisaation johdon vastuulle kuuluvaa riskienhallintaa.

---

[268] Samoin on todettu myös ns. *Tatti-työryhmän* mietinnössä, jonka mukaan yleisen tietosuoja-asetuksen tulkinnassa ja soveltamiskäytännön kehityksessä EU-tuomioistuimen rooli tulee olemaan merkittävä. Ks. Tatti-työryhmän mietintö 2018, s. 25.

Tietoturvallisuudesta ei ole säädetty johdonmukaisesti yhdessä laintasoisessa säädöksessä, ja kuten informaatiohallinnon kohdalla, myös tietoturvallisuutta koskevan säädösmateriaalin hallinta on haasteellista. Tietoturvallisuudesta on säädetty useissa laeissa asia- tai toimintokohtaisesti ja lisäksi tulee huomioida soft law -tyyppinen sääntely. Tietoturvallisuussääntelyyn voi laajassa mielessä lukea kuuluvaksi lähes kaikki tässäkin tutkimuksessa käsitellyt tai mainitut säädökset. Aiemmin käsitelty TtA on askel kokonaisvaltaisempaan tietoturvallisuuden sääntelyyn vähintään periaatetasolla. Näen, että jatkossa esimerkiksi TtA:ssa säädetyt keskeiset tietoturvallisuusvaatimukset (2 luku) voisivat olla nostettavissa lain tasolle.

Sähköisen asioinnin lisääntymisen myötä informaatiohallinnossa on huomioitava sähköisen tunnistamisen keskeinen rooli. Tähän rooliin nähden asiasta keskustelu, myös oikeustieteen piirissä, on ollut varsin vähäistä. Yhä keskeisemmäksi asian tekee se, että viime vuosina on keskusteltu paljon esimerkiksi sähköisen äänestämisen mahdollisuudesta. Sähköisen äänestämisen mahdollisesti toteutuessa vahvalla sähköisellä tunnistamisella on kriittinen merkitys. Yksi keskeisistä riskeistä sähköisessä äänestämisessä mielestäni liittyy juuri luotettavaan sähköiseen tunnistamiseen[269]. Lisäksi näen merkittäviä riskejä liittyen sähköisen identiteetin mahdolliseen väärinkäyttöön sekä ongelmaan, jota voidaan kutsua omakätisyyden ongelmaksi. Tarkoitan tällä sitä, että viime kädessä sähköisessä asioinnissa emme voi nykykeinoin varmistua siitä, kuka on tosiasiassa henkilö, joka suorittaa sähköisesti tunnistautuneena tietyn oikeustoimen. Sähköisen tunnistamisen jakautuessa heikkoon ja vahvaan sähköiseen tunnistamiseen, on jälkimmäinen näistä ainoa lakisääteinen sähköisen tunnistamisen muoto. Yleisemmin käytetty heikko sähköinen tunnistaminen ei kuulu SäTuL:n soveltamisalaan. Kuten edellä todetaan, heikkoa sähköistä tunnistamista käyttävät palvelut eivät jää kuitenkaan kokonaan sääntelyn ulkopuolelle. Tietoturvallisuuden näkökulmasta vahva sähköinen tunnistaminen on osa pääsynvalvonnan tietoturvallisuusprosessia ja toteuttaa erityisesti kahta aiemmin käsiteltyä tietoturval-

[269] Laajemmin katsottuna sähköisen äänestämisen toteuttamiseen liittyy myös lukuisia muita tietoturvallisuusuhkia. Näitä voivat olla esimerkiksi tietomurrot ja tietoliikenteen häirintä tai toisaalta vieraan valtion yritykset vaikuttaa äänestyskäyttäytymiseen tai -tuloksiin erilaisin informaatio-operaatioin.

lisuusperiaatetta, luottamuksellisuutta ja saatavuutta. Edellä esitetyt rajoitukset huomioiden ei ole syytä epäillä, ettei tämän hetken vahva sähköinen tunnistaminen takaisi oikeudellisesti arvioituna sähköiseen viranomaisasiointiin riittävää turvallisuustasoa.

Sähköisessä tunnistamisessa on kysymys sähköisen identiteettimme esittämisestä ja siihen liittyvien tietojen automaattisesta käsittelystä. Näin ollen kytkentä sähköisen tunnistamisen ja henkilötietojen suojan välillä on selvä. Sähköiseen identiteettiimme kohdistuu monenlaisia uhkia verkkoympäristössä. Identiteettivarkaus on yksi näistä. Vaikka uusi tietosuoja-asetus vahvistaa henkilötietojemme suojaa, se ei tarjoa suojaa identiteettivarkauden kohteeksi joutuneille henkilöille. Keskeisenä puutteena näen sen, ettei sääntelyssä huomioida riittävästi todellisen vahingonkärsijän asemaa. Vahingonkärsijän mahdollisuudeksi jää kenties siviilioikeudellisen vahingonkorvauskanteen tie, jota ei voida pitää optimaalisena oikeuksien tehokkaan toteutumisen kannalta. Monessa yhteydessä on arvioitu, että identiteettivarkaudet ovat jatkossa yhä tavanomaisempia. *De lege ferenda* -näkökulmasta olisikin pohdittava sitä, millaisin toimenpitein voidaan tulevaisuudessa torjua tai korjata identiteettivarkauksien yksilöille aiheuttamia haittoja.

Vahvan sähköisen tunnistamisen markkinoilla tosiasiallinen tilanne on se, että pankkitunnisteet ovat merkittävin tunnistamiseen käytettävä tunnistusväline. Pankkitunnisteisiin voi kuitenkin liittyä esimerkiksi saatavuuteen, laajuuteen ja kustannuksiin liittyviä ongelmia. Henkilö, joka ei voi taloudellisista syistä johtuen saada pankin palveluita ja tunnistusvälineitä käyttöönsä, ei välttämättä voi käyttää tunnistautumista vaativia sähköisiä viranomaispalveluita[270]. Tämä on ongelma etenkin yhdenvertaisuuden näkökulmasta. Tietoturvallisuuden näkökulmasta voidaan oikeutetusti kritisoida pankkitunnisteiden käytön laajuutta. Yksi tunniste avaa laajan pääsyn tunnisteen haltijan henkilötietoihin, mukaan luettuna taloudelliset tiedot. Yhden tunnistusvälineen käyttämiseen sisältyy siis merkittävä tietosuojariski. Jatkossa voi olla aihetta tutkia mahdollisuutta tarjota valtion toimesta jonkinlaista vähimmäistason vahvan sähköisen tunnistamisen välinettä henkilöille, joilla ei ole mahdollisuutta saada tunnistusvälinettä markkinaehtoisesti. Uudistunut lainsää-

[270] Tässä yhteydessä on kyse syrjäytymisriskistä, jolla tarkoitetaan tietotekniikan käytöstä aiheutuvaa kansalaisten eriarvoistumiskehitystä. Ks. *Saarenpää et al*. 1997, s. 38.

däntö ei näyttäisi toistaiseksi ratkaisevan tunnistusvälineiden saatavuuteen liittyviä ongelmia. Pankkitunnisteisiin liittyvä olennainen seikka on niiden yksityisoikeudellinen sopimusperusteisuus ja se, että tunnisteiden myöntämisessä ei ole kyseessä julkinen hallintotehtävä. Näin ollen prosessissa ei synny myöskään valituskelpoisia hallintopäätöksiä.

Lopulta vahvan sähköisen tunnistamisen rooli keskeisenä informaatiohallinnon palveluna voidaan tiivistää mielestäni kolmeen kohtaan, jotka ovat oikeusturva, asiointi sekä tietoturvallisuus. Oikeusturvanäkökulmasta vahva sähköinen tunnistaminen toteuttaa perusoikeuksia ja hallinnon asiakkaan oikeuksia. Asiointinäkökulmasta vahva sähköinen tunnistaminen saa aikaan lainsäädännössä määritettyjä oikeusvaikutuksia. Viimein vahva sähköinen tunnistaminen toteuttaa tietoturvallisuutta informaatiohallinnossa ja sähköisessä asioinnissa.