Tietosuojavaltuutetun sosiaali- ja terveysalan toimijoihin kohdistama ohjaus ja valvonta

Lapin yliopisto
Oikeustieteiden tiedekunta
Maisteritutkielma
Hallinto-oikeus
Eila Pennala
Kevät 2025

Lapin yliopisto
Tiedekunta: Oikeustieteiden tiedekunta
Työn nimi: Tietosuojavaltuutetun sosiaali- ja terveysalan toimijoihin kohdistama ohjaus ja valvonta
Tekijä/-t: Eila Pennala
Koulutusohjelma/oppiaine: OTM, Hallinto-oikeus
Työn laji: Pro gradu -tutkielma/Maisteritutkielma _x_ Lisensiaatintutkimus__
Sivumäärä, liitteiden lukumäärä: XI + 83
Vuosi:2025

Tiivistelmä:

Tutkielma tarkastelee sosiaali- ja terveydenhuollon tietosuojaa Suomessa hyvän tietojenkäsittelytavan ja tietosuojavaltuutetun roolin kautta. Tutkielmassa selvitetään alalla tapahtuneita tietosuojaloukkauksia, tietosuojavaltuutetun antamaa ohjausta sekä käytettyjä korjaavia toimivaltuuksia, jotta hyvinvointialueet voivat hyödyntää kertyneen opin. Metodina käytettiin empiiristä oikeustutkimusta analysoimalla 56 tietosuojavaltuutetun Finlexissä julkaistua henkilötietolain ja tietosuoja-asetuksen mukaista kannanottoa.

Tulokset osoittavat, että tietosuojarikkomuksia tapahtui kaikissa käsittelyn vaiheissa. Syinä oli usein teknisiä tai inhimillisiä virheitä tai vanhentuneiden ohjeiden soveltamista. Yleisiä puutteita havaittiin erityisesti tietojen minimoinnissa, turvallisessa käsittelyssä, rekisteröidyn tarkastusoikeuden toteuttamisessa, automatisoidussa päätöksenteossa ja ilmoitusvelvollisuuden toteuttamisessa.

Tietosuojavaltuutetun ohjaus oli henkilötietolain aikana usein kannanottoja organisaatioiden kysymyksiin, kun tietosuoja-asetuksen mukaiset tapaukset keskittyivät korjaaviin toimiin, jotka sisälsivät teknistä ohjausta, viittauksia ohjeisiin tai vaihtoehtoisia toimintatapoja lainmukaiseen henkilötietojen käsittelyyn. Käytetyt korjaavat toimivaltuudet olivat useimmin huomautus ja määräys saattaa käsittely lainmukaiseksi. Vakavimmissa tapauksissa käytettiin hallinnollista seuraamusmaksua.

Räikeää huolimattomuutta tai välinpitämättömyyttä esiintyi vähän. Jatkossa hyvinvointialueiden on tärkeää huomioida aiemmista tapauksista erityisesti ilmoitusvelvollisuus, automaattinen päätöksenteko ja tietojen minimointivaatimus.

Avainsanat: tietosuoja, tietosuojavaltuutettu, yleinen tietosuoja-asetus, GDPR, tietosuojalaki, korjaavat toimivaltuudet

_x_ Tutkielma ei sisällä muita kuin tekijän/tekijöiden omia henkilötietoja.

Sisällys

Lähteet

Kirjalliset lähteet

Andreasson, Ari; Koivisto, Juha & Ylipartanen, Arto: Tietosuojakäsikirja johdolle. 2. uudistettu laitos. 3. painos. Tallinna 2016.

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

Husa, Jaakko; Mutanen, Anu & Pohjolainen, Teuvo: Kirjoitetaan juridiikkaa. Hämeenlinna 2010.

Hyppönen, Mikko: Internet. Helsinki 2021.

Häyhä, Juha (toim.): Minun metodini. Porvoo 1997.

Järvinen, Petteri: Yrityksen tietoturvaopas. Viro 2022.

Järvinen, Petteri: Digiajan tietosuoja. Helsinki 2022.

Kess, Kaija: Itsemääräämisoikeus sosiaali- ja terveydenhuollossa. Helsinki 2023.

Kleemola, Maija: Henkilötietolain merkitys sosiaali- ja terveydenhuollon asiakastietojen käsittelyssä. Teoksessa: *Pahlman, Irma* (toim.) Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa. Helsinki 2010. s. 37–58.

Koillinen, Mika: Henkilötietojen suoja itsenäisenä perusoikeutena. Julkaisussa: Oikeus 2/2013 s. 171–193.

Koillinen, Mika: Hallinnolliset seuraamukset tietosuojan sanktiomekanismina. Defensor Legis N:o 4/2016, s.570–586.

Korhonen, Rauno: Perusrekisterit ja henkilötietojen suoja. Informaatio-oikeudellinen tutkimus yksityisyyden suojasta yhteiskunnan perusrekisteritietojen käsittelyssä. Rovaniemi 2003.

Korkea-aho, Emilia: Empiirisen oikeustutkimuksen käytäntö. Teoksessa Lindfors, Heidi (toim.) Empiirinen tutkimus oikeustieteessä. Helsinki 2004. s.81–90.

Korpisaari, Päivi; Pitkänen, Olli & Warma-Lehtinen, Eija: Uusi tietosuojalainsäädäntö. Liettua 2018.

Korpisaari, Päivi; Pitkänen, Olli & Warma-Lehtinen, Eija: Tietosuoja. Keuruu 2022. 2. uudistettu painos.

Kuusikko, Kirsi: Neuvonta hallinnossa. Helsinki 2000.

Lehtonen, Lasse; Lohiniva-Kerkelä, Mirva & Pahlman Irma: Terveysoikeus. Helsinki 2015.

Lehtonen, Lasse; Lohiniva-Kerkelä, Mirva & Pahlman, Irma: Terveysoikeus. 2. uudistettu painos. Helsinki 2024.

Lehtonen, Lasse: Potilaan yksityisyyden suoja. Suomalaisen lakimiesyhdistyksen julkaisuja A-sarja N:o 230. Vammala 2001.

Leppänen, Pasi; Sorvettula, Johanna & Valli-Lintu, Auli: Hyvinvointialue: Järjestäminen, hallinto ja Talous. Helsinki 2024.

Lindroos-Hovinheimo, Susanna: Henkilötietojen suoja EU-oikeudessa – yksityisyyttä yhteisön kustannuksella? Lakimies 1/2018, s. 52–74.

Lindström, Amanda; Murto, Liisa & Uuskallio, Assi. Asiakastietojen Käsittely Sosiaali- Ja Terveydenhuollossa. Edilex Lakitieto, ilmoitettu julkaisuaika: 2025.

Liuha, Roope: Tietosuoja-asetuksen mukaisten hallinnollisten seuraamusmaksujen määrääminen yritykselle. Pro gradu, Lapin yliopisto, Oikeustieteiden tiedekunta. 2022

Lohiniva-Kerkelä, Mirva: Johdanto. Teoksessa: Lehtonen, Lasse; Lohiniva-Kerkelä, Mirva; Pahlman, Irma: Terveysoikeus. 2. uudistettu painos. Helsinki 2024.

Lång, Jukka & Taka, Anni-Maria: Tietosuoja-asetuksen soveltaminen käytännössä – Katsaus ensimmäiseen vuoteen. Julkaisussa: Data, viestintä ja sääntely. Viestintäoikeuden vuosikirja 2018. Toim. Päivi Korpisaari. Helsinki 2019. s. 55–74.

Miettinen, Tarmo: Mikä tekee tutkimuksesta tieteellisen? s. 3–16.Teoksessa: Miettinen, Tarmo (toim.): Oikeustieteellinen opinnäytetyö. Joensuun yliopiston oikeustieteellisiä julkaisuja. 2. painos. Joensuu 2006.

Myllynpää, Arja: Potilasasiakirjoihin liittyvät valvontaviranomaisten kannanotot. Teoksessa: Palhman, Irma: Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa. Helsinki 2010. s. 159–190.

Mäenpää, Olli: Yleinen hallinto-oikeus: Liettua 2017.

Mäenpää, Olli: Hallinto-oikeus. Liettua 2018.

Mäenpää, Olli: Hallinto-oikeus. 3. uudistettu painos. Helsinki 2023.

Mäenpää, Olli: Hallinto-oikeus ja hyvän hallinnon takeet. Keuruu 2024.

Niemivuo, Matti: Uusi aluehallinto – Hyvinvointialueista maakuntaitsehallintoon? Turenki 2022.

Paaso, Ilpo: 4.6. Lääkintäoikeus. Teoksessa: *Urpo, Kangas*: Oikeustiede Suomessa 1900–2000. Juva 1998. s. 401–405.

Paasonen Jyri & Luomala Mikko: Tietosuojan viranomaisvalvonnan ja seuraamusjärjestelmän kehitys – tarkastelussa tietosuojavaltuutetun ja seuraamuskollegion päätöksiä vuosilta 2018–2022. Defensor legis 1/2024 s. 40–66.

Pahlman, Irma: Johdanto. Teoksessa: Pahlman, Irma (toim.) Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa. Helsinki 2010. s. 11–12.

Pahlman, Irma: Asiakirjajulkisuus ja tietosuoja sosiaali- ja terveydenhuollossa. Helsinki 2007.

Posio Sirpa: Yksityisyyden suoja sosiaalihuollossa. Suomalaisen lakimiesyhdistyksen julkaisuja A-sarja N:o 283. Vammala 2008.

Rautiainen, Pauli, Aura Kostiainen, Visa Kurki, Niko Soininen & Tapio Määttä: Oikeus Ja Sen Tutkiminen. Tampere 2023.

Saarenpää, Ahti (toim.); Pöysti, Tuomas (toim.); Sarja, Mikko; Still, Vivec &; Balboa-Alcoreza, Ruxandra: Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Helsinki 1997.

Saarenpää, Ahti: Oikeusinformatiikka. Teoksessa Oikeus tänään – osa I, toim. *Marja-Leena Niemi*. Lapin yliopiston oikeustieteellisiä julkaisuja, sarja C 64 s. 67–273, Rovaniemi, 2016.

Saarenpää, Ahti & Riekkinen, Juhana: Oikeusinformatiikan perusteet. Rovaniemi 2023.

Schnabel, Christoph: Privacy and data protection in EC telecommunications law. Teoksessa: EC competition and telecommunications law. Koenig, Bartosh, et al. (toim.). Second Edition. Kluwer Law International 2009.

Tuori, Kaarlo & Kotkas, Toomas: Sosiaalioikeus. 5. uudistettu painos. Liettua 2016.

Tuori, Kaarlo & Kotkas, *Toomas*: Sosiaalioikeus. 6. uudistettu painos. Helsinki 2023.

Tuori, Kaarlo: 4.5 Sosiaalioikeus. Teoksessa: *Kangas, Urpo* (toim.): Oikeustiede Suomessa 1900–2000. Juva 1998. s. 397–401.

Tötterman Magnus: Tietosuoja-asetuksen vaikutus terveydenhuollon ammattihenkilöiden välisiin potilastietojen siirtoihin. Pro gradu -tutkielma, Helsingin yliopisto 2020.

Vanto, Jarno J.: Henkilötietolaki käytännössä. Helsinki 2011.

Voutilainen, Tomi: Oikeus tietoon - informaatio-oikeuden perusteet. Keuruu 2019.

Voutilainen, Tomi & Kurvinen Evgeniya: Asiakas- ja potilastietojen käsittelyn sääntely. Helsinki 2024.

Ylipartanen, Arto: Tietosuoja terveydenhuollossa. Potilaan asema ja oikeudet henkilötietojen käsittelyssä. 3. uudistettu painos. Tallinna 2010.

Internet lähteet

Hirvonen, Ari; Mitkä metodit? Opas oikeustieteen metodologiaan. Helsinki 2011. s. 22. https://www2.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf Luettu 6.6.2022.

Hyvän tiedonhallintatavan määritys, VM:n työryhmämuistioita 11/2000 https://portti.kansallisarkisto.fi/fi/arkistoalan-sanasto/hyv%C3%A4-tiedonhallintatapa Luettu 20.5.2025

Leponen, Marko: Uusi, huolestuttava ilmiö – rikolliset kohdistavat Vastaamo-tietovuodon uhreihin raukkamaisia rikoksia. Poliisi, blogit. Julkaistu: 11.2.2022. Saatavissa: https://poliisi.fi/blogi/-/blogs/uusi-huolestuttava-ilmio-rikolliset-kohdistavat-vastaamo-tietovuodon-uhreihin-raukkamaisia-rikoksia Luettu 17.3.2022.

THL https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/mita-tiedonhallinta-on- Luettu 20.5.2025.

Tieteen termipankki; Tietosuoja. 10.3.2020. Saatavissa: https://tieteentermi-pankki.fi/wiki/Avoin_tiede:tietosuoja Luettu 25.4.2022.

Tieteen termipankki; Tietosuoja. 18.9.2019. Saatavissa: https://tieteentermipankki.fi/wiki/Oikeus-tiede:tietosuoja Luettu 25.4.2022.

Tietosuojavaltuutetun nettisivut, Tietosuoja. Saatavissa: https://tietosuoja.fi/tietosuoja Luettu 1.6.2022.

Tietosuojavaltuutetun toimiston toimintakertomus 2022. K 14/2023 vp. Saatavissa: https://tieto-suoja.fi/documents/6927448/169954657/TSV+Toimintakertomus+2022.pdf/74eca5fa-bc1d-77ef-1a0e-b81df6bb0c5e/TSV+Toimintakertomus+2022.pdf?t=1690784877980 Luettu 18.4.2024.

Virallislähteet

HE 31/2023 Hallituksen esitys eduskunnalle laiksi Oikeushallinnon erityisviranomaiset -virastosta ja siihen liittyviksi laeiksi

HE 246/2022 Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen käsittelystä sekä siihen liittyviksi laeiksi

HE 241/2020 Hallituksen esitys eduskunnalle hyvinvointialueiden perustamista ja sosiaali- ja terveydenhuollon sekä pelastustoimen järjestämisen uudistusta koskevaksi lainsäädännöksi sekä Euroopan paikallisen itsehallinnon peruskirjan 12 ja 13 artiklan mukaisen ilmoituksen antamiseksi

HE 145/2022 Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi

HE 30/2020 Hallituksen esitys eduskunnalle yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn yleissopimuksen muuttamisesta tehdyn pöytäkirjan hyväksymiseksi ja voimaansaattamiseksi sekä laeiksi tietosuojalain ja henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain 1 ja 54 §:n muuttamisesta

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

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

HE 33/1994 Hallituksen esitys Eduskunnalle terveydenhuollon ammattihenkilöitä koskevaksi lainsäädännöksi

Valiokuntien lausunnot ja mietinnöt

Perustuslakivaliokunnan lausunto PeVL 14/2018 vp – HE 9/2018 vp (Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi)

Muut lausunnot ja mietinnöt

Eu:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö 2017, Oikeusministeriön mietintöjä ja lausuntoja 35/2017

Oikeustapaukset

KHO/KKO

KHO 8.2.2006, taltionumero 230, dnro 6/3/04

Ylimmät laillisuusvalvojat EOA ja OKA

Tietosuojavaltuutetun ja apulaistietosuojavaltuutetun ratkaisut

Julkaistut

Tietosuoja-asetuksen mukaiset

ATSV/29/2020 Henkilötunnuksen sisältävien automatisoitujen tekstiviestien lähetys terveydenhuollossa

ATSV 6629/163/21 Oikeus tutustua magneettikuviin maksutta

ATSV 9707/152/19 Rekisteröidyn oikeus tutustua tietoihinsa ja oikeuden puutteellinen toteutus

ATSV TSV/3/2019 Henkilön tunnistaminen terveydenhuollon sähköisessä ajanvarausjärjestelmässä

ATSV 4022/171/22 Arkaluonteisten henkilötietojen asianmukainen suojaaminen ja henkilötietojen turvallinen käsittely

ATSV 9492/153/22 Rekisteröidyn oikeuksien käyttäminen alaikäisen lapsen puolesta

ATSV 6482/186/2020 Automatisoitujen yksittäispäätösten syntyminen ennakoivan terveydenhuollon työkalussa

ATSV 5546/163/2019 Henkilötietojen käsittelyn turvallisuus ajanvarausjärjestelmässä

ATSV 3895/83/22 Potilastietojen käsittely ennaltaehkäisyn ja ennakoinnin tarkoituksissa sekä automatisoidut yksittäispäätökset

ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä

ATSV 6602/161/2021 Koronarokotustietojen käytettävyys ja tietoturvaloukkauksesta ilmoittaminen

ATSV 1150/161/2021 Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen

ATSV 6132/151/19 Potilaan tarkastusoikeuden toteuttaminen terveydenhuollossa röntgen- ja magneettikuvien osalta

ATSV 6745/163/18 Potilastietojen käsittely ammatillista kehittymistä varten hoitosuhteen päätyttyä

TSV 3096/161/21 Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi

TSV 8235/154/18 Asiakkaan pyyntö henkilötietojen poistosta ja henkilötietojen käsittelyperuste

TSV 5242/157/2018 Tietojen luovuttaminen sosiaali- ja terveydenhuollosta kuljetuspalveluille kuljetusten järjestämistä varten

TSV 5036/183/2019 Henkilötietojen rekisterinpitäjästä ja käsittelijästä

TSV 28/523/2018 Jäljennösten saaminen sosiaalihuollon asiakastiedoista

TSV 2691/171/19 Henkilötietoasiakirjoja sisältävän postipaketin katoaminen

Henkilötietolain mukaiset

TSV 235/41/2017 Asiakas tai hänen laillinen edustajansa voi vaatia asiakasta koskevien rekisteritietojen korjaamista

TSV 2540/41/2014 Lähiomaisen oikeudesta saada täysi-ikäistä kehitysvammaista koskevia salassa pidettäviä tietoja

TSV 1565/41/2012 Kotihoidon tietojen käsittelystä

TSV 1044/41/2012 Sosiaalihuollon asiakastietojen ja terveydenhuollon potilastietojen käsittelystä palveluohjauksessa

TSV 590/41/2012 Asiakkaalle tarjottavista sähköisen asioinnin palveluista

TSV 2296/451/2012 Lääkereseptin kopiointi tai sen tietojen tallettaminen asiakasrekisteriin toimeentulotukea haettaessa

TSV 2655/41/2011 Oikeudesta kerätä ja tallettaa potilaiden arkaluonteisia henkilötietoja

TSV 539/451/2011 Kameravalvonta perhekodissa

TSV 1820/452/2006 Yksityisvastaanoton potilaskortisto kuolinpesässä

TSV 1475/41/2009 Sähköpostin ja tekstiviestien käyttäminen terveydenhuollossa

TSV 1674/451/2009 Vastaanottotoimintansa pois siirtävien vuokralaishammaslääkäreiden oikeus ottaa mukaansa potilasrekisterit

TSV 2128/41/09 Sosiaalipalvelujen tarpeen kartoitusta ja ennakollista lastensuojeluilmoitusta koskevien henkilötietojen käsittelystä

TSV 2044/41/2009 Teknisen käyttöyhteyden avaaminen sivistystoimelle sosiaalitoimen toimeentulotukitietoihin

TSV 1773/49/2009 Sosiaalihuollon asiakastietojen ja potilastietojen käsittelystä sosiaalihuollossa

TSV 423/49/2009 Viranomainen ei saa asiakkaan suostumuksellakaan lähettää salassa pidettäviä asiakastietoja suojaamattomassa sähköpostissa

TSV 285/41/2009 Käyttöoikeudet päihdeklinikan A-klinikkalehden tietoihin

TSV 90/41/2009 Sosiaalihuollon etuuksien pankkiin maksun yhteydessä ilmenevät tiedot

TSV 617/41/2008 Henkilötietojen siirtäminen palvelujen järjestämisvastuun siirtyessä esimerkiksi uudelle kunnalle

TSV 1504/41/2007 Sairaaloiden ilmoitukset Kelalle hoitotukea ja vammaistukea saavista potilaista

TSV 1567/41/2007 Tietojen luku- ja kirjoitusoikeus ylikunnallisessa sosiaalipäivystyksessä

TSV 567/41/2007 Lastensuojeluilmoitusten käsittelystä sosiaalitoimistossa

TSV 150/49/2007 Isäntäkuntamalli ja rekisterinpitäjä sekä asiakastietojen siirtäminen palvelujen järjestämisvastuun siirtyessä

TSV 1330/523/2006 Sivullisella ei ole tarkastusoikeutta potilasrekisteritietoihin

TSV 1782/41/2004 Huumausainetestitodistuksen toimittaminen työterveyshuollosta suoraan työnantajalle

TSV 702/49/2004 Kameravalvonta nuorisokodissa

TSV 1245/45/2001 Työntekijän/potilaan suostumus tietojen luovuttamiseen työnantajalle

TSV 982/45/2001 Asiakkaan tiliotteen pyytäminen toimeentulotukea myönnettäessä

TSV 80/45/1998 Potilasrekisteritietojen luovuttaminen

TSV 403/45/2001 Alaikäisen potilasrekisteritietojen tarkastusoikeus

TSV 2798/1/00 Tarkastusoikeuden osittainen epääminen

TSV 163/41/2001 Terveydenhuollon eri toimintayksiköiden potilasrekisteritietojen tallettaminen samaan ulkopuolisen palveluntuottajan ylläpitämään tietokantaan

TSV 1196/523/2000 Tarkastusoikeus asiantuntijalääkäreiden nimiin

TSV 36/523/2001 Henkilötietolain soveltaminen asiakirjapyyntöön

TSV 287/45/1998 Täysi-ikäisen pojan lastensuojelutietojen tarpeellisuus perhehoitosopimusta tehtäessä

TSV 1035/45/2000 Potilasasiakirjoissa olevien tietojen poistaminen

TSV 925/41/2000 Telefaxin käyttö potilasasiakirjojen lähettämisessä

Ei julkaistut

TSV 2546/41/2008

1 Johdanto

1.1 Tutkielman aihe ja lähtökohdat

Tässä tutkielmassa tarkastellaan sosiaali- ja terveydenhuollon tietosuojaa ja sen toteutumista tietosuojavaltuutetun julkaistun ratkaisukäytännön avulla. Tietosuoja on tärkeä, mutta jokseenkin abstrakti asia siihen saakka, kunnes se pettää ja konkreettiset seuraukset tulevat näkyviksi. Henkilötietojen ja erityisesti sosiaali- ja terveydenhuollossa käsiteltävien arkaluonteisiksi[1] luokiteltavien henkilötietojen päätyminen ulkopuolisille tai tuhoutuminen on vakava uhka sekä yksittäiselle rekisteröidyille, eli sosiaali- ja terveydenhuollon asiakkaalle, että rekisterinpitäjälle.

Tutkielman aihe on ajankohtainen, sillä tuoreessa muistissa on vielä paljon julkisuudessa ollut Psykoterapiakeskus Vastaamon tapaus vuodelta 2020. Tapaus oli varoittava ja hyvin ikävä esimerkki siitä, miten vakavia seurauksia[2] voi olla, jos tietosuoja pettää sosiaali- ja terveysalan palveluja antavassa yksikössä. Tapauksessa psykoterapiapalveluita tarjoavan yrityksen huonosti suojattuihin asiakastietoihin tehtiin tietomurto, jonka yhteydessä varastettuja tietoja käytettiin asiakkaiden kiristykseen ja lopulta ne vuodettiin Tor-verkkoon. Tällaisia vaaroja sosiaali- ja terveydenhuollon asiakastietojen sähköinen käsittely voi aiheuttaa.

Tutkielman aiheen ajankohtaisuutta ja kiinnostavuutta lisää myös tietosuojasääntelyn muutokset. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (EU:n tietosuoja-asetus**)** tuli sovellettavaksi vuonna 2018. Tietosuoja-asetusta on siis vuoden 2024 loppuun mennessä sovellettu noin 6 vuotta, minkä vuoksi tietosuojavaltuutetun soveltamiskäytäntöä on kertynyt sen verran, että aineiston tarkastelu on mahdollista rajata yksittäiseen sektoriin: sosiaali- ja terveydenhuoltoon. Tutkielmaan tuo kiinnostavuutta myös se, että tietosuojavaltuutetun toiminta muuttui jonkin verran

[1] Henkilötietolaissa käytettiin termiä arkaluonteinen henkilötieto esimerkiksi sosiaali- ja terveydenhuollon asiakas ja potilastiedoista. Tietosuoja-aseuksessa (artikla 9) ja tietosuojalaissa (6 §) kyseisistä tiedoista käytetään termiä *erityisiin henkilötietoryhmiin* kuuluvat tiedot.

[2] Rikolliset ovat poliisin mukaan käyttäneet Vastaamon tietomurrossa vuodettuja henkilötietoja erilaisissa rekisteröinneissä ja edelleen on vaara siitä, että tietoja voidaan käyttää esimerkiksi tilauspetosten tekemiseen. Leponen, 2022. Poliisi blogit. Vastaamo tapauksen oikeudenkäynnin yhteydessä uhreja puolustanut juristi puolestaan kertoi, että tietomurron uhreja on päätynyt itsemurhaan tietomurron ja kiristyksen vuoksi. Ks. YLE Uutiset: Vastaamo-uhrien juristi: Ihmisiä on päätynyt itsemurhaan tietomurron ja kiristyksen takia. 1.3.2024. https://yle.fi/a/74-20077270

tietosuoja-asetuksen voimaantulon myötä, kun se sai muun muassa asetuksen 58 artiklan 2 kohdan mukaiset korjaavat toimivaltuudet tilanteisiin, joissa reksiterinpitäjän toiminta on ollut tietosuoja-asetuksen vastaista.

Luottamuksellisuus on avainasemassa sosiaali- ja terveydenhuollossa, jossa esimerkiksi potilassuhteessa potilaat kertovat oireista, vaivoista ja muista asioistaan luottamuksellisesti sosiaali- ja terveydenhuollon ammattilaisille.[3] Ongelmat ja puutteet tietosuojassa rapauttavat luottamusta, joka on sosiaali- ja terveydenhuollon perusta. Ilman luottamusta ja luottamuksellisia tietoja hyvää hoitoa ja sosiaalipalveluja on mahdoton toteuttaa. Kuitenkin sähköiset asiakas- ja potilastietojärjestelmät ovat edelleen haavoittuvia ja toimintatavoissa sekä henkilökunnan osaamisessa on aina parantamisen varaa. Tässä tutkielmassa tarkastellaan sosiaali- ja terveydenhuollon tietosuojaa tietosuojavaltuutetun ratkaisujen kautta ja selvitetään millaista neuvontaa ja ohjausta sosiaali- ja terveysalalla on viime vuosina tietosuojavaltuutetun mukaan tarvittu.

Tutkielman ajankohtaisuutta lisää myös se, että sosiaali- ja terveysalalla on juuri tehty yksi Suomen historian suurimmista hallinnollisista uudistuksista, kun sosiaali- ja terveyspalvelujen kokonaisuudistuksen vuoksi palvelujen järjestämisvastuu siirtyi vuoden 2023 alussa kunnilta hyvinvointialueille. Tämän hallinnollisen uudistuksen vuoksi on hyvä aika tarkastella alan tietosuojaohjausta kokonaisuutena ja miettiä voiko aiemmista asioista oppia jotain ja välttää virheitä tulevaisuudessa.

1.2 Tutkimusongelma, tavoitteet ja rajaukset

Tutkielmassa selvitetään millaista ohjausta ja neuvontaa tietosuojavaltuutettu on sosiaali- ja terveysalaan kohdistanut tietosuoja-asioissa ja millaista hyvää tietojenkäsittely tapaa se on sillä luonut ja ylläpitänyt. Tutkielmassa tarkastellaan sosiaali- ja terveydenhuollon tietosuojaa ja sen ongelmakohtia tietosuojavaltuutetun sosiaali- ja terveysalaan kohdistaman ohjaus- ja ratkaisukäytännön kautta ja hyväntietojenkäsittelytavan käsitteen avulla. Tarkastelussa ovat tietosuojavaltuutetun ratkaisut ja kannanotot[4] vuosilta 1999–2024. Annettua ohjausta ja

[3] Ks. lisää Ylipartanen 2010, s. 23–24. Lisäksi myös Lohiniva-Kerkelän 2015, s. 25–27, mukaan hyvä hoitosuhde on terveydenhuollon henkilöstön onnistuneen toiminnan edellytys.

[4] Jatkossa käytetään näistä molemmista yleisnimitystä *tapaus*. Sillä lainsäädäntömuutoksen myötä 25.5.2018 tietosuoja-asetuksesta tuli suoraan sovellettavaa oikeutta, myös tietosuojavaltuutetun ratkaisujen luonne muuttui kannanottoista ja ohjausmaisesta ratkaisuiksi yksittäisen rekisterinpitäjän tapauksissa, joten tapaus kuvaa näitä molempia, ellei ole tarpeen korostaa tapauksen merkitystä nimenomaan ratkaisuna tai kannanottona.

havaittuja ongelmakohtia tarkastellaan kokonaisuutena myös hyvinvointialueiden näkökulmasta.

Koska tutkimuksen aineisto on varsin pitkältä aikaväliltä ja lainsäädäntö on sen aikana muuttunut. Vuosina 1999–2018 on ollut voimassa henkilötietolaki (523/1999) ja toukokuusta 2018 lähtien on ollut voimassa EU:n yleinen tietosuoja-asetus. Lisäksi kansallinen tietosuojalaki (1050/2018) on tullut voimaan vuoden 2019 alusta. Tämä on huomioitu myös tutkimusongelmaa määriteltäessä ja tutkielmassa tarkastellaankin tapauksia osittain jaoteltuina sen mukaan, kumman lainsäädännön aikana ne on annettu, että sen mukaan millaisiin tietosuojan vaarantumistilanteisiin ne liittyvä.

Tutkimuskysymykset pohjautuvat sekä henkilötietolain 38 §:ssä säädettyihin tietosuojavaltuutetun tehtäviin ja saman lain 40 §:n mukaiseen tietosuojavaltuutetun velvollisuuteen edistää hyvää tietojenkäsittelytapaa ja pyrkimykseen estää lainvastaisen menettelyn jatkaminen, että tietosuoja-asetuksen artikloissa 55–59 säädettyihin valvontaviranomaisen tehtäviin.[5] Toisin sanoen tietosuojaperusoikeuden toteutumista tarkastellaan tietosuojavaltuutetun ratkaisujen valossa.[6]

Yhtenä tutkimuskysymyksenä on selvittää, mikä hyvässä tiedonkäsittelytavassa on epäonnistunut tai ollut vaarassa epäonnistua, kun tietosuojavaltuutettu on antanut ohjausta sosiaali- ja terveysalaan liittyvissä asioissa. Tutkielmassa tarkastellaan tapauksia, joissa hyvä tiedonkäsittelytapa on selvästi pettänyt, mutta myös tapauksia, joissa se on ollut vaarassa pettää, sillä molemmista löytyy vastauksia kysymykseen, mitkä asiat sosiaali- ja terveysalalla ovat olleet ongelmallista tietosuoja-asioissa tarkastelussa olevalla ajanjaksolla. Käänteisesti tutkimuskysymys vastaa kysymykseen: mikä ei ole ollut hyvän tietojenkäsittelytavan mukaista sosiaali- ja terveydenhuollon tietosuojassa.

Tutkielmassa tarkastellaan myös tietosuojavaltuutetun sosiaali- ja terveydenhuollon rekisterinpitäjiin kohdistamia tietosuoja-asetuksen 58 artiklan 2 kohdan mukaisia korjaavia toimi-

[5] Erityisesti 57 artiklan 1 kohdan a ja b alakohdat: tietosuojavaltuutetun tehtäviin kuuluu tietosuoja-asetuksen täytäntöönpano ja sen soveltamisen valvominen sekä yleisen tietoisuuden edistäminen henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista. Ks. myös tietosuoja-asetuksen johdannon kohta 122.

[6] Vastaavasti esim. Kaija Kees on tarkastellut asiakkaan ja potilaan itsemääräämisoikeuteen liittyviä perusoikeuksia ihmisoikeustoimielinten ratkaisujen ja tarkastusten valossa kirjassaan Itsemääräämisoikeus sosiaali- ja terveyden huollossa, 2023, joka tosin ei ole tutkimus, vaan koonti aihepiirin ratkaisuista ja kannanotoista.

valtuuksia**.** Kiinnostuksen kohteena on erityisesti se mitä toimivaltuuksia tietosuojavaltuutettu on käyttänyt ja millaisissa tapauksissa niille on ollut tarvetta. Voiko toimivaltuuksien käytöstä tehdä johtopäätöksiä esimerkiksi ongelmien vakavuudesta, piittaamattomuudesta, toistuvuudesta tai yhteistyöhaluttomuudesta?

Tutkielmassa selvitetään lisäksi aiemman ohjaus- ja ratkaisukäytännön perusteella mitä hyvinvointialueiden tulee erityisesti ottaa huomioon tietosuojakysymyksissä, kun sosiaali- ja terveyspalvelujen järjestämisvastuu siirtyi niille. Tutkielmassa kootaan yhteen tietosuojaan liittyviä yksittäisiä tilanteita ja kokonaisuuksia, joihin sosiaali- ja terveysalalla on ollut aiemmin tarpeen kiinnittää huomiota ja jotka jatkossa tulisi pystyä välttämään.

Henkilötietojen suojaamiseen liittyy erilaisia suojakeinoja, kuten rikosoikeudelliset keinot, henkilötietolainsäädäntö, hallinnolliset ja vahingonkorvausoikeudelliset suojakeinot, markkinat suojakeinona sekä tietoturva ja teknologia. Rikoslain 38 luvussa säädetään salassapitorikoksesta, viestintäsalaisuuden loukkauksesta, tietomurrosta ja tietosuojarikoksesta.[7] Yleisesti sosiaali- ja terveysalalla tietosuojaan liittyvät rikokset ovat usein liittyneet työntekijän uteliaisuudesta tekemiin rekisteritietojen urkkimisiin. Usein tällaisissa tapauksissa urkitut tiedot ovat koskeneet urkkijan työtoverin henkilörekisteritietoja, esimerkiksi potilastietoja.[8] Tässä tutkielmassa vakaviakin tietosuojarikkomuksia tarkastellaan tietosuojavaltuutetun tehtävien ja toimivaltuuksien kautta, joten rikosoikeudelliset kysymykset rajautuvat tutkielman ulkopuolelle.

1.2.1 Metodien yhdistelmä

Tutkielmassa tarkastellaan tietosuojavaltuutetun aiempaa ratkaisukäytäntöä ja antamaa ohjausta ja neuvontaa. Metodologiesti tutkielma ei istu puhtaasti minkään oikeustieteen metodiin, vaan tutkielmassa käytetään eri metodien yhdistelmää. Tällainen metodologinen kirjavuus ei ole poikkeuksellista oikeustieteellisessä tutkimuksessa.[9] Tutkielmassa käytetään pääosin empiiristä ja osittain myös lainopillista tutkimusotetta, mutta tutkimuksen metodi ei ole puhtaasti näitä kumpaakaan.

Koska tutkielman aineistona käytetään sekä lainsäädäntöä että tietosuojavaltuutetun julkaistuja kannanottoja ja ratkaisuja ja tutkielmassa tarkastellaan tietosuojan vaarantumistilanteita,

[7] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 22–24.
[8] Andreasson, Koivisto ja Ylipartanen 2016, s.53.
[9] Ks. lisää oikeustieteen metodeista ja niiden moninaisuudesta mm. Häyhä 1997.

käytettyjä toimivaltuuksia ja ohjauksen sisältöä ja muotoa, metodi on pohjimmiltaan empiirinen. Aineistoa tarkastellaan sekä osin määrällisesti että osin laadullisesti. Oikeuslähteinä tietosuojavaltuutetun ratkaisut eivät ole sitovaa oikeuskäytäntöä, mutta niiden sisällöstä saadaan kuitenkin empiiristä tietoa siitä, millaista oikeus käytännössä on sosiaali- ja terveydenhuoltoon liittyvissä tietosuojakysymyksissä. Tutkielma ei kuitenkaan ole puhdasta määrällistä oikeustutkimusta, sillä aineisto (56 tapausta) on liian suppea, jotta siitä voisi tehdä määrällisen tutkimuksen vaatimukset täyttäviä johtopäätöksiä. Lisäksi aineisto on Finlexissä julkaistua ratkaisukäytäntöä, joten se on mennyt tutkielman tekijästä riippumattoman seulan läpi, eikä siten sovellu myöskään kovin syvään laadulliseen tarkasteluun. Joten tutkimuksen aineisto ei ole kaikilta osin riittävän edustava ja yleistettävissä ollakseen puhdasta empiiristä tutkimusta. Aineisto on silti monipuolinen ja kiinnostava tutkimuskohde.

Empiirinen oikeustutkimus jakautuu kuvailevaan ja selittävään tutkimukseen. Kuvailevan tutkimuksen tarkoitus on mitä- ja miten -kysymyksillä rakentaa tutkittavasta ilmiöstä yleiskuva. Tämä vaatii riittävän kattavan ja luotettavan aineiston. Selittävä oikeustutkimus taas vastaa miksi -kysymyksiin ja siinä tutkitaan ilmiötä, josta on jo olemassa riittävän kattava käsitys. [10] Tässä tutkielmassa tutkimusote on kuvaileva ja kuten edellisestä luvusta käy ilmi, vastaa mikä ja mitä -kysymyksiin sosiaali- ja terveydenhuollon tietosuoja riskeistä, tietosuojavaltuutetun antamasta ohjauksesta ja käyttämistä toimivaltuuksista.

Empiirisen oikeustutkimuksen laadullista puolta on myös kuvattu pyrkimyksenä luoda ensikäden käsitys satunnaistetusta ilmiöstä esimerkiksi konkurssista tai ulosotosta ja esittämään tämän muodostetun käsityksen muille.[11] Tässä tutkielmassa tarkasteltava ilmiö on tietosuojavaltuutetun sosiaali- ja terveysalaan kohdistama neuvonta ja ohjaus.

Lisäksi kuten suurimmassa osassa oikeustieteellisistä tutkimuksista[12], myös tässä tutkielmassa yhtenä metodina on lainoppi eli oikeusdogmatiikka. Lainopin tarkoitus on tulkita ja systematisoida voimassa olevaa oikeutta.[13] Lainopissa tehdään tulkintakannanottoja voimassa olevasta oikeudesta. Lainopin avulla pyritään vastaamaan tutkimuskysymykseen, joka on muodostettu kysymysmuotoon: miten oikeuslähteeseen X sisältyvää normilausetta Y pitäisi tulkita, vallitsevaan tuomarinideologiaan tukeuduttaessa. [14] Lainoppi muodostuu

[10] Rautiainen, Kostiainen, Kurki, Soininen & Määttä 2023, s. 241–242.
[11] Korkea-aho 2004, s. 84.
[12] Ks. Husa, Mutanen & Pohjolainen 2010. s. 20.
[13] Ks. Hirvonen 2011. s. 22.
[14] Ks. Rautiainen, Kostiainen, Kurki, Soininen & Määttä 2023, s. 129.

oikeuslähde, tulkinta- ja argumentaatio-opeista ja se on keskeisin suuntaus oikeustieteen tutkimuksessa. Lainoppi puolestaan voidaan jakaa käytännölliseen ja teoreettiseen lainoppiin. Käytännöllisellä lainopilla tarkoitetaan tutkimustapaa, joka tuottaa tulkintasuosituksia lainsoveltajille. Sen avulla yritetään löytää tulkintasuosituksia erityisesti lakitekstin epäselvyyksiin, monimerkityksellisiin sanoihin, ristiriitoihin ja aukkoihin.[15]

Tutkielmassa tarkastellaan, miten tietosuojavaltuutettu on toteuttanut sille laissa annettua tehtävää edistää hyvää tiedonkäsittelytapaa tai yleistä tietoisuutta ja ymmärrystä henkilötietojen käsittelystä. Tutkielmassa on myös tarkoitus systemaattisesti tuoda esille hyväntiedonkäsittelytavan sisältöä tai käänteisesti sitä, mikä ei kuulu hyvään tiedonkäsittelytapaan. Eli mitä sisältöä hyvä tietosuoja sosiaali- ja terveydenhuollossa tarkoittaa säädösten, säännösten, lainvalmisteluaineiston ja laillisuusvalvontakäytännön perusteella.

Oikeushistoriallisessa tutkimuksessa tutkitaan nimenomaan oikeusnormien tai oikeudellisen ajattelun kehitystä ja sen avulla tuotetaan tietoa jo menneen ajan oikeudesta, jota sellaisenaan ei enää ole olemassa. Oikeushistoriallisessa tutkimuksessa voidaan myös tarkastella sitä kehitystä, joka on johtanut tiettyjen voimassa olevien oikeudellisten sääntöjen syntyyn.[16] Tutkielmassa voi siis myös nähdä joitain oikeushistoriallisia piirteitä, sillä tapauksia katsotaan noin 20 vuotta taaksepäin, eikä kaikkien tapausten perusteena ollut lainsäädäntö ole enää samankaltaisena voimassa. Oikeushistoriallinen näkökulma, jossa tutkitaan, millaista oikeus oli, ei kuitenkaan ole tutkielman päätarkoitus, vaan tarkoituksena on etsiä tietosuojavaltuutetun valvontakäytännöstä asioita, jotka voivat olla hyödyllisiä tulevaisuudessa.

Oikeustieteellisen tutkimukseen liittyy usein ainakin pieni oikeusvertaileva osa tai katsaus yleensä lähinnä pohjoismaiden vastaavaan sääntelyyn tai oikeuskäytäntöön, koska ne ovat oikeusjärjestykseltään ja kulttuuriltaan kotimaista järjestelmäämme lähimpänä ja siksi vertailu niihin on sekä helppoa että yleensä myös hedelmällistä. Tässä tutkielmassa oikeusvertaileva osuus on aiheen laajuuden ja monitahoisuuden sekä EU sääntelyn aiheuttaman oletetun yhdenmukaisuuden vuoksi rajattu ulkopuolelle.

[15] Ks. Rautiainen, Kostiainen, Kurki, Soininen & Määttä 2023, s. 135–136.
[16] Ks. Husa, Mutanen & Pohjalainen 2010, s. 21.

1.2.2 Aineisto

Tutkielman aineistona on Finlex tietokannassa julkaistu tietosuojavaltuutetun sosiaali- ja terveysalaan liittyvä ratkaisukäytäntö vuosilta 1999–2024. Tällaisia tapauksia, joissa henkilötietojen rekisterinpitäjä on sosiaali- ja terveysalan toimija ja rekisteröity on sosiaali- ja terveysalan asiakas tai potilas, on yhteensä 56 Lainsäädännöstä erityisen tarkastelun kohteena ovat EU:n tietosuoja-asetus, tietosuojalaki, henkilötietolaki ja sosiaali- ja terveydenhuollon asiakastietolaki ja lainvalmisteluaineistosta HE 9/2018 vp Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, HE 96/1998 vp Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi, HE 246/2022 Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen käsittelystä sekä siihen liittyviksi laeiksi.

Tietosuojavaltuutettu on julkaissut vuodesta 1999 alkaen ratkaisujaan Finlexissä, mutta kaikilta vuosilta ei ole julkaistu välttämättä yhtään sosiaali- ja terveysalaan liittyvää ratkaisua. Tietosuojalainsäädäntö on muuttunut tarkastelujakson aikana muun muassa tietosuoja-asetuksen ja tietosuojalain tultua voimaan. Aineistossa on 20 tietosuoja-asetuksen mukaista ja 36 henkilötietolain mukaista tapausta. Tietosuoja-asetuksen mukaisia päätöksiä tarkastellaan tarkemmin, kuin aiempia jo kumotun henkilötietolain mukaisia ratkaisuja ja kannanottoja. Tutkielman ulkopuolelle rajautuu kuolleiden henkilöiden henkilötietojensuoja, koska tietosuoja-asetuksen johdanto-osan 27 kohdan mukaan asetusta ei sovelleta vainajan henkilötietoihin, eikä siitä ole kansallisesti säädetty toisin.

Tietosuojavaltuutetun ratkaisut ja kannanotot kuuluvat oikeuslähteinä oikeuslähdeopin mukaan sallittujen oikeuslähteisiin, jotka yleensä määritellään sisältävän oikeustieteen, oikeushistorialliset, oikeusvertailevat ja reaaliset argumentit sekä arvot ja arvostukset. Näihin oikeuslähteisiin lakia sovellettaessa voi vedota, mutta sivuuttamista ei tarvitse erikseen perustella.[17] Tietosuoja-asetus, tietosuojalaki sen sijaan kuuluvat vahvasti velvoittaviin oikeuslähteisiin ja tutkielmassa tarkastellut hallituksen esitykset heikosti velvoittaviin oikeuslähteisiin. Tietosuojavaltuutettu yhtenä valvontaviranomaisena[18] tuottaa laillisuusvalvontakäytän-

[17] Ks. Husa, Mutanen ja Pohjolainen 2010, s. 33. Lisäksi hallintotoiminnan oikeuslähteistä ks. esimerkiksi Mäenpää 2017, s. 111–118.
[18] Muita sosiaali- ja terveydenhuollon palvelujen valvontaviranomaisia ovat eduskunnan oikeusasiamies, valtioneuvoston oikeuskansleri, Valvira ja aluehallintovirastot. Voutilainen & Kurvinen 2024, s. 23.

töä ohjaamaan sosiaali- ja terveydenhuollon palvelujen tuottamista ja menettelyjä, jotka liittyvät esimerkiksi tiedonsaantioikeuden toteutumiseen tai asiakirjojen laatimiseen liittyvien säännösten tulkintaan.[19]

Tutkielmassa käytetään tietosuojavaltuutetun ratkaisuista ja kannanotoista käytetään selkeyden ja luettavuuden vuoksi yleiskäsitettä *tapaus*. Pääosin tietosuoja-asetuksen mukaiset tapaukset ovat tietosuojavaltuutetun tekemiä ratkaisuja yksittäisessä asiassa ja henkilötietolain mukaiset tapaukset ovat useammin kannanottoja. Tutkielmassa ei myöskään erotella tekstin tasolla, onko kyse tietosuojavaltuutetun vai apulaistietosuojavaltuutetun ratkaisusta, ellei sillä ole erityistä merkitystä tapauksen lopputuloksen tai muun erityisen seikan kannalta. Apulaistietosuojavaltuutetun ratkaisut on kuitenkin eroteltu lähdeluettelossa (s. VIII) lyhennettä ATSV käyttäen erotuksena tietosuojavaltuutetun ratkaisusta TSV[20].

1.3 Tutkimuksen viitekehys ja rakenne

1.3.1 Aiempi tutkimus ja kirjallisuus

Yleisesti tietosuojasta, henkilötietojen suojasta ja tietoturvasta on viime vuosina kirjoitettu paljon. Tietosuojalainsäädäntö on vuosien aikana muuttunut paljon ja erityisesti tietosuoja-asetuksen valmistelun ja voimaantulon aikaan on kirjoitettu useita erilaisia tietosuojaan liittyviä teoksia. Kehittyvä teknologia ja sen myötä muuttuva lainsäädäntö on luonut tarpeen kirjoittaa sekä yleisiä teoksia tietosuojasta, että sektorikohtaisia kirjoja ja erilaisia oppaan tapaisia teoksia. Kattava tietosuojaan liittyvä oikeustieteellinen julkaisu on *Päivi Korpisaaren, Olli Pitkäsen ja Eija Warma-Lehtisen* kirjoittama Tietosuoja, joka on ilmestynyt vuonna 2022[21]. Kirjassa käydään läpi tietosuoja-asetus sekä kansallinen tietosuojalaki.

Tietosuojaa perusoikeutena ja sen periaatteita käsitellään teoreettisemmin pääasiassa vanhemmissa teoksissa, jotka ovat osa 1990-luvulta. Tietojen suojaamisen periaatteet ja ydin eivät kuitenkaan ole pohjimmiltaan muuttuneet, vaikka teknologia on keittynyt ja sähköiset

[19] Voutilainen & Kurvinen 2024, s. 23.
[20] TSV lyhennettä käytetään *Tieteellisten seurain valtuuskunnasta*, joten kyseistä lyhennettä ei käytetä tässä tutkielmassa tarkoittamaan tietosuojavaltuutettua muulloin kuin tapausten diaarinumeroiden yhteydessä, joka vaikuttaa olevan sekä tietosuojavaltuutetun toimiston itsensä käytäntö uusimmissa ratkaisuissa esim. TSV/29/2020 että joissain oikeustieteellisissä kirjoissa käytetty lyhenne, mm. Korpisaari, Pitkänen ja Warma-Lehtinen 2022 ja Voutilainen & Kurvinen 2024.
[21] Korpisaari, Pitkänen ja Warma-Lehtinen 2022.

järjestelmän yleistyneet, joten tutkielmassa käytetään myös vanhempia lähteitä. Vanhemmassa kirjallisuudessa esimerkiksi *Rauno Korhosen* väitöskirjassa Perusrekisterit ja henkilötietojen suoja käsitellään tietosuojan historiaa ja perusteita informaatio-oikeuden näkökulmasta.[22] *Ahti Saarenpään ja Tuomas Pöystin* toimittama Tietoturvallisuus ja laki – Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä on tutkimusraportti, jossa muun muassa analysoidaan tietoturvallisuuden sääntelytarpeita ja sääntelyssä käytettävissä olevia sääntelymalleja ja normityyppejä.[23]

Tietosuojavaltuutetusta ja sen harjoittamasta tietosuojaan liittyvästä valvonnasta on kirjoitettu verraten vähän ja suurin osa kirjoituksista on pääasiassa artikkeleita. Tietosuojavaltuutetun tehtävistä ja toimialasta on kirjoitettu osana henkilötietolaista kertovaa oikeuskirjallisuutta, mutta tietosuojavaltuutetun ratkaisukäytännön tarkastelu on vähäistä. Esimerkiksi *Arto Ylipartanen* viittaa muutamiin tietosuojavaltuutetun kannanottoihin kirjassaan Tietosuoja terveydenhuollossa[24], mutta niitä ei tarkastella erityisen syvällisesti. Tietosuojavaltuutetusta viranomaisena ei ole erillistä tutkimusta, mutta sen tehtäviä ja tekemiä kannanottoja kyllä sivutaan useissa tietosuojaa käsittelevissä kirjoissa. *Päivi Korpisaari, Olli Pitkänen ja Eija Warma-Lehtinen* kuvaavat kirjassa *Uusi tietosuojalainsäädäntö* tietosuoja-asetuksen artiklat valvontaviranomaisesta.[25] Kirjasta on myös uudistettu painos nimeltä: Tietosuoja, joka mainittiin jo aiemmin. *Tomi Voutilaisen* oppikirjaksi ja käsikirjaksi suunnattu teos Oikeus tietoon, Informaatio-oikeuden perusteet kuvaa kattavasti tietosuoja-asetuksen ja tietosuojalain tietosuojavaltuutettua koskevat pykälät ja artiklat.[26] [27]

Sosiaali- ja terveysalan tietosuojakysymyksiä on oikeuskirjallisuudessa käsitelty erityisesti terveysalan näkökulmasta. Kovin tuoretta alaan liittyvää kirjallisuutta ei kuitenkaan ollut tutkielmaa aloitettaessa, mikä myös osaltaan puolsi tutkielman aihetta. Tutkielmaprosessin aikana julkaistiin kuitenkin *Tomi Voutilaisen ja Evgeniya Kurvisen* teos Asiakas- ja potilastietojen käsittelyn sääntely.[28]

---

[22] Korhonen 2003.
[23] Saarenpää (toim.) & Pöysti (toim.) 1997.
[24] Ks. esimerkiksi Ylipartanen 2010, s. 89, 94 ja 96.
[25] Korpisaari 2018, s. 425–460.
[26] Voutilainen 2019, s. 595–607.
[27] Tietoa tietosuojavaltuutetun toimistosta ja sen toiminnasta löytyy myös jonkin verran hallituksen esityksissä sekä tietosuojavaltuutetun verkkosivuilta ja tietosuojavaltuutetun toimiston omista toimintakertomuksista.
[28] Voutlainen & Kurvinen 2024.

Sirpa Posion väitöskirjasta Yksityisyyden suoja sosiaalihuollossa, joka selvittää sosiaalihuollon asiakkaan yksityisyyden suojaa, tämän suojan sisältöä, tarkoitusta, rajoja sekä rajoituksia.[29] Terveydenhuollon tietosuojaa koskeva *Arto Ylipartasen* kirja Tietosuoja terveydenhuollossa käy potilaan näkökulmasta läpi rekisterinpitäjän hyvää henkilötietojen käsittelytapaa.[30] Terveysoikeudesta ovat kirjoittaneet myös *Lasse Lehtonen, Mirva Lohiniva-Kerkelä ja Irma Pahlman* Terveysoikeus[31] kirjassaan. Lisäksi on mainittava potilaan yksityisyyden suojaan liittyen *Lasse Lehtosen* väitöskirja Potilaan yksityisyyden suoja[32].

Irma Pahlman on puolestaan toimittanut 2010-luvun taitteessa kaksi sosiaali- ja terveysalan tietosuojaan liittyvää teosta, jotka käsittelevät tietosuojaa, tiedonsaantioikeutta ja asiakirjajulkisuutta ja salassapitokysymyksiä sosiaali- ja terveysalalla: Asiakirjajulkisuus ja tietosuoja sosiaali- ja terveydenhuollossa[33] sekä Asiakastietojen käsittely, salassapito ja asiakkaan tiedonsaantioikeus sosiaali- ja terveydenhuollossa.[34] *Ari Andreassonin, Juha Koiviston ja Arto Ylipartasen* kirjoittamassa kirjassa Tietosuojakäsikirja johdolle, sosiaali- ja terveydenhuollon tietosuojakysymyksiä käytetään esimerkkeinä yritysmaailmaan. *Kaija Kessin* Itsemääräämisoikeus sosiaali- ja terveydenhuollossa kirja on julkaistu vuonna 2023 ja siinä käsitellään asiakkaan ja potilaan itsemääräämisoikeutta sosiaali- ja terveydenhuollossa.

Hyvinvointialueuudistuksesta ovat kirjoittaneet *Matti Niemivuo*: Uusi aluehallinto – Hyvinvointialueista maakuntaitsehallintoon?[35] *ja Pasi Leppänen, Johanna Sorvettula ja Auli Valli-Lintu*: Hyvinvointialue, järjestäminen, hallinto ja talous.

Artikkelit ja opinnäytteet. *Jyri Paasonen ja Mikko Luomalan* artikkeli Tietosuojan viranomaisvalvonnan ja seuraamusjärjestelmän kehitys – tarkastelussa tietosuojavaltuutetun ja seuraamuskollegion päätöksiä vuosilta 2018–2022 on yksi tätä tutkielmaa lähinnä oleva viimeaikainen artikkeli.[36] *Susanna Lindroos-Hovinheimon* artikkeli Henkilötietojen suoja EU-oikeudessa – yksityisyyttä yhteisön kustannuksella?[37] tarkastelee tietosuojaa kriittisesti, mutta hyvin yleisesti. *Mikael Koillinen* taas on kirjoittanut hallinnollisista seuraamuksista

[29] Posio 2008.
[30] Ks. Ylipartanen 2010. Kirja
[31] Lehtonen, Lohiniva-Kerkelä ja Pahlman 2015 ja 2024.
[32] Lehtonen 2001.
[33] Pahlman 2007.
[34] Pahlman 2010.
[35] Niemivuo 2022.
[36] Paasonen & Luomala 2024, s. 40–66.
[37] Lindroos-Hovinheimo 2018, s. 52–74.

tietosuojan sanktiomekanismina.[38] Aiheeseen liittyvistä opinnäytetöistä (Pro gradu -tutkielmat) mainitsemisen arvoisia ovat *Magnus Töttermanin* tutkielma*:* Tietosuoja-asetuksen vaikutus terveydenhuollon ammattihenkilöiden välisiin potilastietojen siirtoihin[39] ja *Roope Liuhan* tutkielma: Tietosuoja-asetuksen mukaisten hallinnollisten seuraamusmaksujen määrääminen yritykselle[40]

1.3.2 Tutkielman sijoittuminen oikeustieteessä

Tämän tutkielman aihe sijoittuu julkisoikeuden alalle, koska siinä tarkastellaan julkisen viranomaisen, tietosuojavaltuutetun, toimintaa. Tutkielma on myös helppo sijoittaa hallinto-oikeuden piiriin. Hallinto-oikeudellisessa tutkimuksessa kohteena ovat hallinto-oikeudelliset oikeusnormit, oikeusperiaatteet, oikeuskäytäntö ja oikeussuhteet. Tutkimus on kiinnostunut myös käytännöstä, jossa hallinto-oikeuden normeja sovelletaan ja joissa hallinto-oikeudelliset oikeussuhteet muodostuvat.[41] Hallinto-oikeuden lisäksi tutkielmassa sivutaan hallinnollisten päätösten kohteena olevien sosiaali- ja terveysalan toimijoiden kautta myös sosiaali- ja terveysoikeutta, sekä tietosuojakysymysten osalta oikeusinformatiikkaa ja informaatio-oikeutta.

Sosiaalioikeuteen, itsenäisenä oikeudenalana, kuuluvat oikeusnormit, joilla säännellään sosiaaliturvaa. Sosiaaliturva puolestaan jakautuu toimeentuloturvaan ja sosiaali- ja terveydenhuoltoon.[42] Sosiaalioikeus on oikeustieteessä sijoitettu sekä hallinto-oikeuden että työoikeuden tutkintovaatimuksiin.[43] Sosiaalioikeutta pidetään kuitenkin nykyään itsenäisenä oikeudenalana, vaikka sen läheistä yhteyttä hallinto-oikeuteen ei voi kiistää ja sitä onkin luonnehdittu ja kutsuttu hyvinvointivaltion hallinto-oikeudeksi tai sosiaalihallinto-oikeudeksi taikka pidetty yhtenä erityishallinto-oikeuden alana. Sosiaalioikeuden oikeudenalaan katsotaan kuuluvan erityisesti sosiaali- ja terveyshallinnon toimivaltaan, menettelyyn ja toimintaan kuuluvat oikeudelliset asiat.[44]

Sosiaalioikeuden tapaan myös terveysoikeus on ollut perinteisesti hankalaa sijoittaa oikeustieteen systematiikkaan. Sekin on nähty osana hallinto-oikeutta, jolloin on keskitytty lähinnä

[38] Ks. Koillinen 2016.
[39] Magnus Tötterman 2020.
[40] Liuha, Roope 2022.
[41] Mäenpää 2023, s.41–42.
[42] Ks. Tuori & Kotkas 2023, s.1–4.
[43] Tuori 1998, s. 397–398. Sosiaalihuollon lainsäädäntö on katsottu kuuluvan hallinto-oikeuteen, kun taas eläkelainsäädännöllä on läheinen yhteys työoikeuteen. Ks. Tuori & Kotkas 2016, s. 2–8.
[44] Ks. Tuori & Kotkas 2023, s. 4–5 ja Mäenpää 2017

terveydenhuollon palvelujen tuottamiseen ja ammattihenkilöiden asemaan sekä alaan kohdistuvaan valvontaan. Vastuukysymysten osalta suhteessa potilas – terveydenhuollon ammattihenkilö, on taas nähty rikosoikeudellisesta näkökulmasta. Myös vahingonkorvausoikeus tulee kysymykseen, kun puhutaan hoitosuhteessa tapahtuneista vahingoista. Terveydenhuoltoon liittyviä normistoja on sijoitettu viime aikoina myös sosiaalioikeuden oikeudenalaan.[45] Raja sosiaalihuollon ja terveydenhuollon välillä ei ole kovin selkeä, oikeudellisessa eikä käytännöllisessä mielessä ja sitä on myös tarkoituksellisesti madallettu viimevuosina sosiaali- ja terveydenhuollon integraation yhteydessä.[46] Sosiaali- ja terveyshuollossa on kuitenkin myös eroavaisuuksia, joiden vuoksi niitä on välillä tarkastella erillään.

Tutkielmassa ei kuitenkaan tarkastella sosiaali- ja terveysoikeudellisia oikeuskysymyksiä vaan sosiaali- ja terveydenhuollon asiakkaan tietosuojaperusoikeuden toteutumista käytännön tasolla. Joten tutkielman aihe ulottuu tietosuojakysymysten myötä myös informaatio-oikeuden oikeudenalle. Informaatio-oikeus omana oikeudenalanaan koskee viranomaisten tuottamaan, käsittelemään ja välittämään informaatioon liittyviä oikeudellisia kysymyksiä.

Henkilötietojen suojan on katsottu kuuluvan ensisijaisesti siviilioikeuteen ja sen alla persoonallisuusoikeuteen, joka on sen kiistatonta ydinaluetta. Samaan aikaan tietosuojalainsäädäntö on oikeusinformatiikan vakiintuneimpia lainopillisia tutkimusaiheita.[47] Informaatio-oikeuteen kuuluvia yleisiä periaatteita ovat: oikeus tietoon, viestintään, tiedolliseen itsemääräämiseen, informaation vapauteen, informaation kulun vapauteen ja tietoturvaan.[48]

Tämä tutkielma tietosuojavaltuutetun sosiaali- ja terveydenhuollon tietosuojaan kohdistamista ratkaisuista sijoittuu siis oikeustieteessä usean eri perinteisen oikeudenalan välimaastoon. Tutkielman aihepiiri ulottuu tietosuojaperusoikeuden kautta alueille, joissa on sosiaali- ja terveysoikeudellisia, informaatio-oikeudellisia ja hallinto-oikeudellisia piirteitä. Tutkielman sijoittuminen monen oikeudenalan välimaastoon osoittaa, että oikeudenalajaottelua ei aina ole mahdollista tehdä kovin tarkkarajaisesti ja että moderni oikeustiede on hyvin monialaista. Hyvä tietosuoja osana sosiaali- ja terveyhdenhuoltoa yhdistää tapaukset ja oikeudenalat tässä tutkielmassa mielekkääksi tutkittavaksi kokonaisuudeksi.

---

[45] Ks. lisää mm. Lohiniva-Kerkelä 2024, s. 37–39.
[46] Tuori & Kotkas 2023, s. 31. Lisäksi mm. laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) jonka 1 §:n mukaan lain tarkoituksena on yhdenmukaistaa asiakastietojen käsittelyä sosiaali- ja terveydenhuollossa sekä sosiaali- ja terveyspalveluita järjestettäessä ja toteutettaessa.
[47] Saarenpää & Riekkinen 2023, s.10.
[48] Saarenpää 2016, s. 213.

2 Tietosuoja ja tietosuojalainsäädäntö

2.1 Käsitteet

Hyvän tietojenkäsittelytavan käsitettä, joka mainittiin mm. henkilötietolain 40 §:ssä, ei enää sellaisenaan käytetä EU:n tietosuoja-asetuksessa eikä kansallisessa tietosuojalaissa. Pykälän mukaan tietosuojavaltuutetun tuli edistää hyvää tietojenkäsittelytapaa[49]. Tietosuojavaltuutetun tehtävistä säädetään tietosuoja-asetuksen artikloissa 55–59[50]. Tietosuoja-asetuksen 57(1)(b) artiklan mukaan valvontaviranomaisen [tietosuojavaltuutettu] on edistettävä yleistä tietoisuutta ja ymmärrystä [henkilötietojen] käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista. Vaikka tietosuoja-asetuksen voimaantulon jälkeen ei lainsäädännössä enää mainita erikseen hyvää tietojenkäsittelytapaa, sen voidaan ajatella kattokäsitteenä sisältävän tietosuojaan liittyvät yleiset periaatteet. Tietosuojavaltuutetun tehtävänä on siis ollut edistää hyvää tiedonkäsittelytapaa ja nykyään tehtävä on tiivistettynä edistää yleistä tietoisuutta ja ymmärrystä.

Tietosuojaan liittyy paljon abstrakteja käsitteitä, joiden merkitys ei aina ole itsestään selvä. Siksi tietosuojaan liittyvissä laeissa on usein määritelty käytettyjä käsitteitä lain alussa olevissa yleisissä säännöksissä.[51] Lisäksi tietosuojasta ja esimerkiksi sen asemasta perusoikeutena on kirjoitettu oikeuskirjallisuudessa runsaasti. [52] Esimerkiksi Rauno Korhonen on väitöskirjassaan avannut pohjoismaista henkilötietojen suojaan ja tietosuojaan liittyvää käsitteistöä ja sen eroavaisuuksia.[53]

Käsite *tietosuoja* määritellään Tieteen termipankissa ihmisten yksityisyyden suojelemiseksi ja yksilöä koskevien tietojen suojaamiseksi oikeudettomalta käytöltä, kun henkilötietoja käsitellään.[54] Oikeustieteen näkökulmasta tietosuoja on määritelty Tieteen termipankissa ”*henkilötietojen käsittelyä koskevien vaatimusten noudattaminen henkilöiden yksityiselämän ja*

[49] Saarenpää & Riekkinen 2023, s. 87:
[50] Kansallinen henkilötietolaki viittaa tietosuojavaltuutetun tehtäviä ja toimivaltuuksia koskevassa 14 §:ssä tietosuoja-asetuksen artikloihin 55–59. Tietosuojavaltuutetulla on 14 §:n mukaan myös muita tässä tai muussa laissa säädettyjä tehtäviä ja toimivaltuuksia. Tietosuojavaltuutettu esimerkiksi edustaa Suomea Europan tietosuojaneuvostossa ja akkreditoi tietosuoja-asetuksen 43 artiklassa tarkoitetun sertifiointielimen.
[51] Esimerkiksi: henkilötietolaissa 3 §:ssä on määritelty muun muassa 1) henkilötieto, 2) henkilötietojen käsittely ja 4) rekisterinpitäjä. Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä on säädetty lain 3 §:ssä mm. 3) asiakasasiakirja, 12) omatietovaranto ja 15) tiedonhallintapalvelu.
[52] Ks. esim. Koillinen 2012; Schnabel 2009, s. 509; Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 8–25.
[53] Korhonen 2003, s. 129–149.
[54] Tieteen termipankki; Tietosuoja Saatavissa: https://tieteentermipankki.fi/wiki/Avoin_tiede:tietosuoja

yksityisyyden suojaamiseksi."[55] Tietosuojan käsite liittyy myös läheistesti yksityisyyden suojaan, koska tietosuojan kohteena ei ole tietojen konkreettinen suojaaminen, vaan yksittäisen ihmisen yksityisyys. Sosiaali- ja terveysalalla tämä tarkoittaa esimerkiksi luottamuksellista potilassuhdetta, potilaan itsemääräämisoikeutta tai potilaan sosiaalisia suhteita.[56]

Yksityisyyden suojan käsite taas sisältyy jo perustuslakiin. Perustuslain 10 § yksityiselämän suojasta säädetään: *Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla*. Vaikka perustuslaissa henkilötietojen suoja asemoidaan yksityiselämän osa-alueen tavoin, oikeuskirjallisuudessa sitä pidetään kuitenkin laajempana.[57] Yksityisyyden suojaa on kuvattu esimerkiksi ikään kuin suojaavana kehänä, jossa suoja heikkenee, mitä kauemmaksi henkilöä itseään koskevista asioista siirrytään.[58] Tällaisen kehäajattelun ytimessä, eli kaikkein suojatuimpia, ovat yksilön terveyteen ja sairauteen liittyvät tiedot.[59] Sosiaali- ja terveydenhuollossa käsiteltävät tiedot ovat juuri näitä.

Itse käsitettä *yksityisyys* ei ole lainsäädännössä erikseen määritelty, mutta sen on kuvattu sisältävän muun muassa seuraavat perustuslailliset oikeudet:

- *oikeuden järjestää yksityiselämänsä ilman perusteetonta ulkopuolista puuttumista*
- *oikeuden tietää itseään koskevien tietojen käsittelystä ja käsittelyn tarkoituksesta*
- *oikeuden tulla arvioiduksi oikeiden ja tarpeellisten tietojen perusteella*
- *oikeuden vaikuttaa ja päättää itseään koskevien tietojen käsittelystä, ellei sitä ole rajoitettu lainsäädännöllä*
- *oikeuden viestinnän luottamuksellisuuteen mm. potilas-lääkäri-suhteessa*.[60]

Tietoturva puolestaan on käsitteenä määritelty jo 1981 voimaan tulleessa Euroopan neuvoston yleissopimuksessa yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä[61] henkilötietojensuojan perusperiaatteeksi. Se määritellään velvollisuudeksi suo-

[55] Tieteen termipankki; Tietosuoja Saatavissa: https://tieteentermipankki.fi/wiki/Oikeustiede:tietosuoja
[56] Ks. Ylipartanen 2010, s. 24.
[57] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 8–9, myös henkilötiedot, jotka eivät kuulu yksityiselämään, voivat tulla turvatuksi henkilötietoina, esimerkiksi tieto työtehtävästä tai työpaikasta.
[58] Lehtonen 2001, s. 193 ja Pahlman 2010, s. 20.
[59] Ks. Pahlman 2010, s. 20.
[60] Andreasson, Koivisto ja Ylipartanen 2016, s.32.
[61] Euroopan neuvoston sopimussarja ETS N:o 108. Käytetään myös nimitystä "tietosuojayleissopimus" ks. esimerkiksi HE 30/2020 vp s. 3.

jella henkilötietoja vahingossa tai tahallaan tehdyltä tuhoamiselta, katoamiselta, muuttamiselta, levittämiseltä tai luvattomalta tiedostoon pääsyltä.[62] Tietoturva voidaan ajatella tietosuojakäsitteen alla olevaksi astetta teknisemmäksi ja konkreettisemmaksi käsitteeksi, vaikka sanat turva ja suoja ovatkin suomen kielessä synonyymit. Tietoturvasta kannattaa huomata se, että on siis tietosuojan toteuttamiskeino ja sen tarkoituksena on suojata tietoaineistot ja tietojärjestelmät. Tietoturvalla tarkoitetaan esimerkiksi organisatorisia tai teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys, järjestelmien käytettävyys ja rekisteröidyn oikeuksien toteutuminen.[63]

Tietoturva ja tietosuoja muistuttavat käsitteinä paljon toisiaan, mutta suojan *kohde ja tarkoitus* ovat erilaiset. Esimerkiksi yrityksen tietoturvaa ajateltaessa, tietoturvan tarkoituksena on yrityksen *toiminnan* turvaaminen, kun taas tietosuojan kohteena on henkilötiedot eli *ihminen ja hänen yksityisyytensä*.[64] Tietoturvan ja tietosuojan eroa on selkeytetty myös kuvaamalla tietoturva ensisijaisesti tiedon integriteetin (eheyden) säilyttämiseen tähtäävää teknistä suojelua. Tietosuoja puolestaan nähdään perinteisesti sen estämisenä, että yksityisyyttä loukkaavan tietoon pääsisi joku ulkopuolinen oikeudettomasti käsiksi. Täysin selkeää rajaa näiden käsitteiden välillä ei kuitenkaan ole nähty. [65]

Henkilötieto käsitteenä on laaja ja merkityksellinen, että se on nähty tarpeelliseksi määritellä sekä jo kumotussa henkilötietolaissa, että EU:n tietosuoja-asetuksessa. Tietosuoja-asetuksen 4 artiklan 1 kohdan mukaan henkilötiedolla tarkoitetaan: ”*kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja*”. Kohdassa määritellään tunnistettavissa oleva henkilö sellaiseksi luonnolliseksi henkilöksi, joka voidaan tunnistaa erityisesti tunnistetietojen avulla. Tällaisia tunnistetietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto tai yksi tai useampi henkilölle tunnusomainen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä. Lisäksi tunnistaminen voi tapahtua joko suoraan tai epäsuorasti. Tämä monipolvinen määritelmä on yksinkertaistettu toteamalla, että kyse on aina henkilötiedoista, jos tietojen perusteella voidaan saada selville henkilö, jota ne koskevat[66].

[62] Myös Vanto 2011, s. 15.
[63] Tietosuojavaltuutetun internetsivut, Tietosuoja. Saatavissa: https://tietosuoja.fi/tietosuoja
[64] Järvinen 2022, s. 25.
[65] Ks. HE 94/1993 kohta 1.12.1.1.
[66] Muun muassa: Hanninen ym. 2017, s. 18.

Henkilötiedon käsiteen sisällön on nähty jo ennen tietosuoja-asetusta olevan mahdollisimman laaja ja sen keskeisimpänä tekijänä on pidetty henkilön *tunnistettavuutta* kyseisen tiedon perusteella. Henkilötietoja ovat siten myös esimerkiksi henkilötunnus, sormenjälki, tietokoneen tai päätelaitteen IP-osoite, auton rekisterinumero, päätelaitteen asetettu evästetiedosto, internetselailuhistoria, valokuva, paikannustieto, sähköpostiosoite, takuukortti, kaupan bonushistoria tai katuosoite, kunhan tämä tieto voidaan jotenkin tunnistaa tiettyä henkilöä koskevaksi.[67]

Henkilötiedon käsitteen on katsottu tietosuoja-asetuksen voimaan tulon jälkeen paremminkin laajentuneen kuin kaventuneen sen aiemmasta merkityksestä[68]. Tästä syystä käsitteen kehittyminen ei ole ongelma tämän tutkielman kannalta, vaan henkilötietolain mukaista oikeuskäytäntöä voidaan tarkastella vielä tietosuoja-asetuksen voimaantulon jälkeenkin käsitteen laajentuminen huomioon ottaen. Lisäksi jo henkilötietolain voimassa ollessa muistutettiin siitä, että henkilötietojen käsittelyyn liittyen ei ole syytä katsoa määritelmiä kapeasti, vaan että sääntelyn on tarkoitus kattaa kaikki sellainen henkilötietojen käsittely, jota nimenomaisesti ei ole rajattu lain soveltamisalan ulkopuolelle.[69] Henkilötiedon käsitteen määrittelyssä on lisäksi otettu uuden teknologian tuomat tunnistamiskeinot huomioon.[70] Tämä jonkin asteinen käsitteen joustavuus tai laaja-alaisuus on ymmärrettävää koska, että informaatioteknologia on aina kehittynyt nopeasti ja sääntelyn on sen vuoksi tarpeellista olla muun muassa tekniikkaneutraalia.

Huomioitavaa on myös se, että koska henkilötiedon käsite määritellään luonnollisen henkilön käsitettä käyttäen, kyse on silloin vain eläviä henkilöitä koskevasta tiedosta. [71] Tämä mainitaan myös tietosuoja-asetuksen johdanto-osan kohdassa27, jonka mukaan asetusta ei sovelleta kuolleita henkilöitä koskeviin tietoihin.[72]

---

[67] Vanto 2011, s. 22–23.
[68] Korpisaari, Pitkänen & Warma-Lehtinen 2018, s. 49–50.
[69] Esimerkiksi Vanto 2011, s. 22.
[70] Korpisaari, Pitkänen & Warma-Lehtinen 2018, s. 49–50.
[71] Korpisaari, Pitkänen & Warma-Lehtinen 2018, s. 49–50.
[72] Kohdassa annetaan kuitenkin jäsenvaltioille mahdollisuus säätää kuolleiden henkilöiden henkilötietojen käsittelystä kansallisesti, mutta tätä mahdollisuutta ei Suomessa ole käytetty. Korpisaari ja kumppanit kirjoittavat, että aiemmin myös vainajien tietoja on jollain tasolla suojeltu, mutta suojan määrä on vähentynyt sitä mukaa, kun aikaa kuolemasta on kulunut ja suoja on ollut ”pistemäistä ja tapauskohtaista” Tietosuoja-asetuksen voidaan katsoa supistavan vainajien henkilötietojen suojaa ja Korpisaari ja kumppanit pohtivat voiko henkilörekisteririkoksesta enää tuomita henkilöä, joka lukee kuolemantapaukseen liittyviä yksityiskohtia esim. poliisin rekisteristä, vaikka henkilön työtehtävät eivät antaisi syytä tarkastella tietoja. Korpisaari, Pitkänen & Warma-Lehtinen 2018 s. 50–51.

Muita käsitteitä. Tietosuojalainsäädännön yhteydessä määritellään usein myös paljon muita käsitteitä. Esimerkiksi vanhassa henkilötietolain 3 §:ssä määriteltiin (kohdissa 1–9) muun muassa käsitteet *henkilötietojen käsittely, henkilörekisteri, rekisteröity, rekisterinpitäjä, sivullinen* ja *suostumus*. EU:n tietosuoja-asetuksessa määritelmiä on huomattavasti enemmän ja sen 4 artiklassa määritellään yhteensä 26 eri käsitettä, joita asetuksessa käytetään. Näistä esimerkiksi **rekisterillä** (kohta 6) tarkoitetaan mitä tahansa tietojoukkoa, joka sisältää jäsenneltyjä henkilötietoja ja josta tietyin perustein on saatavissa tiedot. Tietojoukko voi olla keskitetty, hajautettu tai jaettu toiminnallisin tai maantieteellisin perustein. **Rekisterinpitäjällä** (kohta 7) puolestaan tarkoitetaan sellaista luonnollista henkilöä, oikeushenkilöä, viranomaista tai muuta elintä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Tietosuoja-asetuksessa määritellyistä käsitteistä on huomioitava se, että niistä ei ole mahdollista säätää kansallisesti eri tavalla[73].

2.2 Tietosuoja-asetus ja tietosuojalaki

Tietosuoja-asetus Euroopan unionin *tietosuoja-asetus* eli Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (tietosuoja-asetus), annettiin 27.4.2016 ja sitä alettiin soveltaa 25.5.2018. Henkilötietojen suoja on hajaantunut hyvin moniin eri säädöksiin eri hallinnonaloilla.[74] Tietosuoja-asetus voimaantullessaan lisäsi sääntelyä ollen suurilta osin päällekkäinen tuolloin voimassa olleen henkilötietolain kanssa. Perustuslakivaliokunnan kannan mukaan tietosuoja-asetus sisältää riittävän yksityiskohtaista sääntelyä ja henkilötietojen suojasta tulisikin siten säätää jatkossa tietosuoja-asetuksen ja kansallisen yleislain nojalla. Kansallista erityislainsäädäntöä puolestaan tulisi välttää ja käyttää kansallista sääntelyä vain tilanteissa, joissa se on sekä sallittua että välttämätöntä henkilötietojen suojaamiseksi.[75] Tietosuoja-asetuksen turvaama henkilötietojen suoja on siis ensisijaista.[76]

[73] Korpisaari, Pitkänen & Warma-Lehtinen 2018, s. 49. Samoin: Eu:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö 2017, Oikeusministeriön mietintöjä ja lausuntoja 35/2017, s. 49.
[74] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 2–3. Kirjassa viitataan selvitykseen, jonka mukaan tietosuojaan liittyvää sääntelyä oli tietosuoja-asetuksen voimaan tullessa noin 800 säädöksessä.
[75] Ks. PeVL 14/2018 vp, s. 4; PeVL 2/2018 vp, s. 5 ja Korpisaari, Pitkänen, Warma-Lehtinen 2022, s. 10–11.
[76] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 10–11.

Tietosuoja-asetusta on kuvattu periaatelähtöiseksi sääntelyksi.[77] Asetuksen yksityiskohtaisten artiklojen (99 artiklaa) ja johdanto-osan kohtien (173 kohtaa) taustalla vaikuttaa vahvasti henkilötietojen käsittelyn asetuksessa säädetyt periaatteet. Asetusta voikin kritisoida siitä, ettei siitä saa käytännössä tarkkoja ohjeita ja suuntalinoja sääntelyn noudattamiselle ja tulkinnalle. Abstraktisti muotoiltu asetus hankaloittaa sen soveltamista ja tekee siitä *vaikeasti hallintaan otettavaa sääntelyä*.[78] Toisaalta ehdottomien sääntöjen korvaaminen ohjaavilla periaatteilla lisää rekisterinpitäjän toimintavapautta, kun tämä voi vapaammin valita toimintatavan periaatteiden sallimissa rajoissa. Tietosuoja-asetus on kokonaisuutena myös sen verran vaikeaselkoinen ja monimutkainen, että sen periaatteiden tunteminen helpottaa myös koko asetuksen tulkintaa.[79]

Periaatteet. Tietosuoja-asetuksen 5 artiklassa luetellut periaatteet henkilötietojen käsittelyn *lainmukaisuudesta, kohtuullisuudesta ja läpinäkyvyydestä, käyttötarkoitussidonnaisuudesta, tietojen minimoimisesta* ja *täsmällisyydestä, säilytyksen rajoittamisesta* sekä *käsittelyn eheydestä ja luottamuksellisuudesta* ovat tärkeimpiä tietosuoja-asetuksen tulkintaa ohjaavia periaatteita. Myös riskiperustainen lähestymistapa, on tietosuoja-aseuksen keskeinen periaate. Sitä ei ole erikseen määritelty asetuksessa, mutta se sisältyy useampaan eri artiklaan (mm. 25 artikla sisäänrakennetusta ja oletusarvoisesta tietosuojasta ja 32 artikla käsittelyn turvallisuudesta).[80]

Tietosuoja-asetuksen 5 artiklan 1 kohdan a) alakohdassa säädetyllä *henkilötietojen käsittelyn lainmukaisuudella* tarkoitetaan sitä, että rekisterinpitäjän harjoittamalle henkilötietojen käsittelylle tulee löytyä lainmukainen peruste. Tietosuoja-asetuksessa tällaisia käsittely perusteita ovat: rekisteröidyn antama suostumus, sopimuksen täytäntöönpano, rekisterinpitäjän lakisääteisen velvoitteen noudattaminen, elintärkeiden etujen suojaaminen, yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen sekä oikeutettujen etujen toteuttaminen.[81]

---

[77] Ks. Lång ja Taka 2018, s. 56. Ja heidän viittaamana Kuner, Christoffer – Svantesson, Dan Jerker B. – Cate, Fred H. – Lynksey, Orla – Millard, Christopher: The language of data privacy law (and how it differs from reality). International Data Privacy Law 2016, Vol. 6 No. 4, s. 259–260; De Hert, Paul: Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection. European Data Protection Law Review (EDPL) 2017, Vol. 3 No. 2, s. 160–179.
[78] Ks. Lång ja Taka 2018, s 56–57.
[79] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 28.
[80] Ks. lisää Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 30–35.
[81] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 28–29.

5 artiklan 1 (a) kohdassa säädetään myös *kohtuullisuuden periaatteesta*, jolla voidaan tarkoittaa myös reiluutta (fairness), tämän mukaan rekisterinpitäjän on huomioitava rekisteröidyn etu ja odotukset ja oltava käyttämättä tietoja väärin.[82] *Läpinäkyvyyden* periaatteella sen sijaan tarkoitetaan rekisteröidyn oikeutta tietää, häntä koskevien henkilötietojen sisällöstä, käytöstä, keräämisestä ja muusta käsittelystä. Läpinäkyvyydellä tarkoitetaan myös henkilötietojen käsittelyyn liittyvän informoinnin saatavuutta ja selkeyttä.[83]

Käyttötarkoitussidonnaisuudesta säädetään alakohdassa b) ja sillä tarkoitetaan sitä, että henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Myöhempi alkuperäisten käsittelytarkoitusten kanssa yhteensopimaton käsittely on kielletty. *Tietojen minimoinnin periaatteesta* säädetään alakohdassa c) ja sen mukaan käsiteltävien henkilötietojen tulee olla asianmukaisia ja olennaisia sekä rajoittua siihen, mikä on niiden käyttötarkoitukseen nähden tarpeellista. Periaate velvoittaa rekisterinpitäjää määrittelemään käsittelyn tarkoituksen.

Henkilötietojen *täsmällisyydestä* säädetään alakohdassa d) ja sen mukaan henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Rekisterinpitäjän on myös varmistettava (kohtuullisin toimenpitein), että epätarkat ja virheelliset henkilötiedot oikaistaan tai poistetaan. *Säilytyksen rajoittamisen periaatteen* mukaan (alakohta e) kerättyjen henkilötietojen säilytysajan tulee olla mahdollisimman lyhyt ja säilyttämisperusteen päättymisen jälkeen tiedot tulee poistaa. Säilytysaika koskee tietoja, jotka ovat muodossa, josta rekisteröidyn voi tunnistaa. Pidempiaikaisessa säilytyksessä tilastointi ja tutkimus- tai arkistointitarkoitukseen säädetään enemmän 89 artiklassa.

Eheyden ja luottamuksellisuuden periaatteesta henkilötietojen käsittelyssä säädetään alakohdassa f), jonka mukaan henkilötietoja on käsiteltävä sellaisella tavalla, joka varmistaa tietojen asiamukaisen turvallisuuden, suojaamisen luvattomalta ja lainvastaiselta käsittelyltä sekä häviämiseltä, tuhoutumiselta tai vahingoittumiselta, jotka tapahtuvat vahingossa. Näiden varmistamiseksi on käytettävä asianmukaisia teknisiä tai organisatorisia toimia.

[82] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 29.
[83] Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s. 29.

Tietosuoja-asetuksen rekisteröidyn oikeudet eivät muuttaneet paljon Suomessa jo käytössä ollutta sääntelyä. Uusia oikeuksia sen sijaan ovat rekisteröidyn mahdollisuus saada itseään koskevia tietoja sähköisesti ja tietojen siirto toiseen järjestelmään.[84]

Osoitusvelvollisuuden mukaan rekisterinpitäjä vastaa siitä, että edellä kuvattuja periaatteita on noudatettu, ja sen on pystyttävä myös se osoittamaan (myös jälkikäteen). Periaate toteutetaan esimerkiksi dokumentoimalla toimenpiteitä sekä laatimalla vaikutustenarviointi ja mahdolliset muut arvioinnit sekä asetuksen edellyttämät käsittelytoimia koskevat selosteet ja sopimukset.[85]

Tietosuojalaki Kansallinen henkilötietojen suojan sääntely on hajautunut useisiin eri säädöksiin ja yksittäisiin säännöksiin eri laeissa ja niitä on myös valmisteltu eri hallinnonaloilla.[86] Tietosuoja-asetuksen voimaantullessa vuonna 2018 tietosuojasääntelyä on laskettu olleen noin kahdeksassasadassa säädöksessä.[87] Tämä ja tietosuojakäsitteen abstraktius huomioon ottaen ei ole ihme, että tietosuojasääntely voi vaikuttaa vaikeasti hahmotettavalta.

EU:n Tietosuoja-asetusta täydentävä kansallinen tietosuojalaki (1050/2018) tuli voimaan 1.1.2019. Lain tarkoituksena on täsmentää ja täydentää tietosuoja-asetusta ja sen soveltamista (1 §). Samalla kumottiin Lailla henkilötietolaki ja laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Tietosuojalaki säädettiin henkilötietojen sääntelyn yleislaiksi, mutta koska sitä sovelletaan rinnakkain tietosuoja-asetuksen kanssa, se ei ole itsenäinen ja kattava sääntelykokonaisuus. Tietosuojalaki mahdollistaa poikkeamisen siitä erityislainsäädännöllä tietosuoja-asetuksen kansallisen harkintamarginaalin mahdollistamissa rajoissa.[88]

Tietosuojalain valmistelussa on pyritty muotoilemaan laki ja sen säännökset niin, että sen ja tietosuoja-asetuksen välille ei syntyisi ristiriitaa. Tulkinnanvaraisuutta saattaa kuitenkin aiheuttaa tilanteet, joissa sektorikohtainen lainsäädäntö ei ole tietosuoja-asetuksen mukaiseksi päivitetty.[89] Sosiaali- ja terveydenhuollon tietosuojasääntelyssä tallainen päivitys on tehty

[84] Andreasson, Koivisto ja Ylipartanen 2016, s.12.
[85] Korpisaari, Pitkänen & Warma-Lehtinen 2022, s. 109–111.
[86] Korpisaari, Pitkänen & Warma-Lehtinen 2022, s. 3.
[87] Korpisaari, Pitkänen & Warma-Lehtinen 2018, s.1–9.
[88] HE 9/2018 vp s.1.
[89]Tällaista ristiriitaa saattoi syntyä aikana, jolloin tietosuoja-asetus oli jo suoraan sovellettavaa oikeutta, mutta kansallista tietosuojalakia ei ollut vielä säädetty ja voimassa oleva tietosuojan yleislaki oli vielä henkilötietolaki, jota ei ollut päivitetty tietosuoja-asetuksen kanssa yhteensopivaksi. Toki myös tällöin etusija soveltamisessa oli tietosuoja-asetuksella. Ks. Korpisaari, Pitkänen & Warma-Lehtinen 2022, s 752.

hiljattain kokoamalla sektorikohtainen tietosuojasääntely samaan lakiin (Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä(703/2023).

Tietosuojalaissa säädetään muun muassa henkilötietojen käsittelyn oikeusperusteesta (4–7 §), erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelystä (4 §), tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettavasta ikärajasta (5 §), valvontaviranomaisesta (8–20 §), oikeusturvasta (21–26 §) sekä tietojenkäsittelyn erityistilanteista (35–38 §).[90]

Tietosuojalaissa säädetään tietosuoja-asetuksen edellyttämästä valvontaviranomaisesta, sen perustamisesta, pätevyydestä ja kelpoisuusehdoista tehtävään. Valvontaviranomaiseen liittyen kansallisesti tietosuojalaissa säädetään myös sen jäsenten nimittämiseen liittyvistä seikoista sekä valvontaviranomaisen jäsenten toimikauden kestosta (oltava väh. neljä vuotta). Suomessa tietosuojaviranomaiselle ei aiemmin kuulunut rangaistuksenomaisten seuraamusten määrääminen, vaikka muilla hallinnonaloilla vastaavia toimivaltuuksia seuraamusmaksujen määräämiseen onkin kansallisesti jo ollut. [91]

Tietosuojalaissa säädetään kansallisesti hieman toisin kuin tietosuoja-asetuksessa muun muassa hallinnollisesta seuraamusmaksusta (tietosuoja-asetuksessa hallinnollinen sakko) 24 §. Tietosuoja-asetuksen 83 artiklan mukaisen hallinnollisen sakon määrää Suomessa seuraamuskollegio, jonka muodostavat tietosuojavaltuutettu ja apulaistietosuojavaltuutetut. Kollegion puheenjohtajana on tietosuojavaltuutettu, se on päätösvaltainen kolmijäsenisenä ja päätökset tehdään esittelystä. 24 §:n 4 momentissa säädetään tahot, joille seuraamusmaksua ei voi määrätä, mm. valtion ja kunnan viranomaisille tai eduskunnan virastoille. [92]

Tietosuojavaltuutetun toimistolla on myös asiantuntijalautakunta, joka on sen sisäinen asiantuntijaelin (12 §). Asiantuntijalautakunta poikkeaa aiemmasta tietosuojalautakunnasta, sillä se ei ole päätoiminen vaan se kokoontuu tarvittaessa eikä sillä ole muodollista päätösvaltaa kuten tietosuojalautakunnalla oli henkilötietolain mukaan.[93]

[90] HE 9/2018 vp s.1.
[91] Paasonen & Luomala 2024, s. 43–44 ja HE 9/2018 vp, s. 8. Tietosuoja-asetuksen voimaantulo ennen tietosuojalain säännöksiä tietosuojavaltuutetusta kansallisena valvontaviranomaisena, aiheutti eräänlaisen välivaiheen, jolloin tietosuoja-asetuksen mukaisille seuraamuksille ei ollut toimivaltaista viranomaista niitä määräämään.
[92] Korpisaari, Pitkänen & Warma-Lehtinen 2022, s. 517.
[93] Paasonen & Luomala 2024, s. 45–46.

2.3 Kumottu henkilötietolaki

Henkilötietolaki (523/1999) tuli voimaan kesäkuun alussa vuonna 1999. Henkilötietolailla kumottiin tuolloin voimassa ollut henkilörekisterilaki (471/1987), joka puolestaan oli tullut voimaan 1.1.1988. Henkilötietolain säätämisen yhteydessä saatettiin kansalliseen lainsäädäntö vastaamaan Euroopan parlamentin ja neuvoston direktiivin (95/46/EY) yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta[94] (jatkossa tietosuojadirektiivi) sisältöä.[95] Henkilötietojen käsittelyn sääntelyn ja tietosuojadirektiivin yhteensovittamisen lisäksi henkilötietolakia säädettäessä otettiin huomioon myös 1995 voimaan tullut perusoikeusuudistus.[96]

Myös henkilötietolaki oli tietosuojaa koskeva yleislaki, jota yleislakien tapaan sovellettiin silloin, kun erityislainsäädännössä ei toisin säädetty. Lain yleisiä periaatteita sovellettiin myös erityislain tullessa kyseeseen ja erityisesti silloin, jos erityislaissa ei ollut lainkaan säädelty jotain tiedonkäsittelyn aluetta.[97] Henkilötietojen käsittelyn tekniikat olivat nopeassa kehityksessä jo henkilörekisterilain voimassaolon aikana, joten hyväksi havaittu tietotekniikkaneutraalisuus pidettiin henkilötietolakia säädettäessä ennallaan ja uudet säännökset pyrittiin kirjoittamaan niin, että niiden sanamuoto ei olisi sidottu tietynlaiseen tekniikkaan.[98] Tämä voidaan myös katsoa yhdeksi yleislain piirteeksi, jonka tarkoitus oli mahdollistaa lain soveltaminen sellaisissakin tilanteissa, joita ei vielä sen säätämisen aikaan ollut osattu ottaa huomioon.

Kumotun henkilötietolain toisessa luvussa säädettiin henkilötietojen käsittelyä koskevista yleisistä periaatteista, joita ovat huolellisuusvelvoite (5§), henkilötietojen käsittelyn suunnittelu (6§) ja käyttötarkoitussidonnaisuus (7§).[99] Henkilötietojen käsittelyn yleisistä edellytyksistä säädettiin puolestaan lain 8 §:ssä. Pykälässä oli 9 kohdan luettelo sallituista henkilötietojen käsittelyperusteista, joihin kuuluivat muun muassa 1) rekisteröidyn yksiselitteisesti antama suostumus, 2) sopimus, 3) käsittely tarpeen elintärkeän edun suojaamiseksi, ja

[94] Kyseisestä direktiivistä on käytetty sekä nimitystä henkilötietodirektiivi että tietosuojadirektiivi. mm Korhonen 2003, s. 126.
[95] HE 96/1998 Hallituksen esitys eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi sisälsi muutoksia myös lakiin tietosuojalautakunnasta ja tietosuojavaltuutetusta sekä rikoslain 38 lukuun.
[96] HE 96/1998 vp s. 1 ja 24.
[97] Korhonen 2003, s. 156.
[98] Ks. HE 96/1998 vp s. 23.
[99] Tässä tutkielmassa ei käsitellä henkilötietolain mukaisia yleisiä periaatteita tämän tarkemmin, koska tutkielma kuitenkin painottuu enemmän tietosuoja-asetuksen mukaiseen valvontakäytäntöön ja sääntelyyn. Henkilötietolain mukaisista periaatteista ks. lisää: Vanto 2011 tai terveydenhuollon näkökulmasta Ylipartanen 2010.

4) käsittelystä säädetään laissa tai se johtuu rekisterinpitäjän laissa säädetyn tehtävän tai velvoitteen suorittamisesta.

Tietojen laatuun liittyvät periaatteet (9 §) olivat tarpeellisuus ja virheettömyysvaatimukset. Pykälän mukaan k*äsiteltävien henkilötietojen tuli olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia* ja rekisterinpitäjän tuli huolehtia siitä, että se ei käsittele virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja. Tarpeellisuusvaatimuksen toteutumisen arvioinnissa oli oleellista, että henkilötietojen käsittelyn tarkoitus oli määritelty 6 §:n mukaisesti.[100]

Rekisterinpitäjän velvollisuudesta laatia henkilörekisteristä rekisteriseloste säädettiin henkilötietolain 10 §:ssä.[101] Kyseinen rekisteriseloste, oli pidettävä jokaisen saatavilla. Velvollisuudesta saattoi poiketa, j*os se on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi*. Jokaisen saatavilla -edellytys ei määritellyt, missä rekisteriselosteen tuli olla, mutta lähtökohtana oli, että sen tuli olla saatavilla rekisterinpitäjän toimipaikassa ja lisäksi, jos itse henkilörekisteri oli tietoverkossa, myös rekisteriselosteen tuli olla saatavilla verkossa.[102]

Arkaluonteisten henkilötietojen ja henkilötunnuksen käsittelystä säädettiin henkilötietolain luvussa 3 (11 §:ssä säädettiin arkaluonteisten henkilötietojen käsittelykiellosta ja 12 §:ssä säädettiin tähän pääsääntöön muun muassa sosiaali- ja terveysalaan liittyviä poikkeuksia) ja henkilötietojen käsittelystä erityisiä tarkoituksia varten luvussa 4. Lisäksi oikeudesta saada tieto ja henkilötietojen luovuttamisesta säädettiin julkisuuslaissa.

2.4 Sosiaali- ja terveysalan tietosuojalainsäädäntö ja sen erityispiirteet

2.4.1 Missä sosiaali- ja terveydenhuollon tietosuojasta säännellään?

Sosiaali- ja terveydenhuollosta yleisesti. Jos tietosuojasääntely on pirstaleista ja hajaantunut useisiin eri säädöksiin niin sosiaali- ja terveydenhuollon sääntelystä säädetään myös

[100] Ks. Vanto 2011, s. 53.
[101] Selosteesta oli löydyttävä: 1) rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot; 2) henkilötietojen käsittelyn tarkoitus; 3) kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä; 4) mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle; sekä 5) kuvaus rekisterin suojauksen periaatteista
[102] Ks. HE 96/1998 s. 43.

useissa eri laeissa. Yleensä ne voidaan jakaa sosiaalihuoltoa koskeviin lakeihin ja terveydenhuoltoa koskeviin lakeihin, joista on sekä omat yleislakinsa, että tarkempia erityislakeja eri sektoreita koskien. Tässä tutkielmassa ei ole tarpeen tarkastella tai luetella yksityiskohtaisemmin sektorikohtaisia lakeja.[103]

Yleislakeina sosiaali- ja terveydenhuoltoa koskevat keskeiset lait ovat sosiaalihuoltolaki (1301/2014) ja terveydenhuoltolaki (1326/2010). Sosiaalihuoltolakiin kuuluvat säännökset hyvinvoinnin ja terveyden edistämisestä, sosiaalipalveluista, sosiaalihuollon toteuttamisesta, palvelujen laadun varmistamisesta ja muutoksenhausta sosiaalihuoltoa koskeviin päätöksiin. Lain tarkoituksena on edistää ja ylläpitää hyvinvointia ja sosiaalista turvallisuutta; vähentää eriarvoisuutta ja edistää osallisuutta ja turvata asiakkaiden yhdenvertaiset palvelut (1§). Lisäksi tarkoituksena on painopisteen siirtäminen erityispalveluista yleispalveluihin ja viranomaistyön tiivistäminen. Terveydenhuoltolain säännökset koskevat puolestaan terveyden ja hyvinvoinnin edistämistä, perusterveydenhuoltoa ja erikoissairaanhoitoa. Lain tarkoituksena (2§) on edistää ja ylläpitää väestön terveyttä, hyvinvointia, työ- ja toimintakykyä sekä samoin kuin sosiaalihuoltolaissa, sosiaalista turvallisuutta; kaventaa terveyseroja, toteuttaa palveluja yhdenvertaisesti, laadukkaasti ja potilasturvallisesti ja lisätä asiakaskeskeisyyttä. Lisäksi samoin kuin sosiaalihuoltolaissa tiivistää viranomaisyhteistyötä. Kaikkia sosiaalihuollon palveluja koskevia yleisiä velvoitteita on säädetty myös laissa sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)[104] ja terveydenhuollon osalta laissa potilaan asemasta ja oikeuksista (78571992). Kyseisitä laeista tietosuojaa koskeva sääntely siirrettiin ja yhdistettiin vuoden 2024 alusta lakiin sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (70372023, asiakastieto-laki).

Myös **sosiaali- ja terveydenhuollon tietosuojasääntelyä** on useammassa eri laissa, vaikka sitä on lainsäädäntöuudistuksilla pyritty saamaan yhtenäisemmäksi. Sääntelyn, joka vaikuttaa asiakas- ja potilastietojen käsittelyyn ja tiedonhallintaan, on jaoteltu esimerkiksi 1) sosiaali- ja terveyspalvelujen järjestämistä koskevaan sääntelyyn, 2) tiedonhallinnan yleislainsäädäntöön, 3) palvelujen tuottamista koskevaan sääntelyyn, 4) asiakkaan ja potilaan asemaa

[103] Ks. sääntelystä lisää esim. Voutilainen & Kurvinen 2024, s. 27–62; Lehtonen, Lohiniva-Kerkelä & Pahlman 2024 tai Tuori & Kotkas 2023.
[104] Leppänen, Sorvettula & Valli-Lintu 2024, s. 48–49.

ja oikeuksia koskevaan sääntelyyn sekä 5) asiakas- ja potilastietojen tiedonhallintaa koskevaan sääntelyyn[105].

Tietosuojan yleislakeina edellä kuvattu yleinen tietosuoja-asetus sekä tietosuojalaki tulevat sovellettavaksi myös sosiaali- ja terveysalan asiakas- ja potilastietoihin, niiden keräämiseen, tallentamiseen, säilyttämiseen, luovuttamiseen ja muihin vastaaviin tilanteisiin. Näitä molempia sovelletaan sekä yksityisten että julkisten sosiaali- ja terveyspalvelujen reksiterinpitäjiin.[106] Lisäksi myös sosiaali- ja terveydenhuollossa viranomaistoiminnan tiedonhallinnan yleislakeja ovat julkisuuslaki, eli laki viranomaisen toiminnan julkisuudesta (621/1999), tiedonhallintalaki eli julkisen hallinnon tiedonhallinnasta annettu laki (906/2019) sekä arkistolaki (831/1994).[107] Myös hallintolaki (434/2003) ja sen viranomaistoimintaa ohjaavat yleiset periaatteet ohjaavat myös sosiaali- ja terveysalan toimijoita tietosuojaa ja sen toteutumista koskevissa asioissa.

Tämän tutkielman kontekstissa myös tietosuojalain edeltäjä, jo kumottu henkilötietolaki ja sen perustana oleva tietosuojadirektiivi, ovat olleet osan tapausten kohdalla tietosuojaa säänteleviä yleissäädöksiä ja tapauksia tarkastellaankin myöhemmin tähän yleislakijakoon perustuen erikseen henkilötietolain mukaisia tapauksia ja tietosuoja-asetuksen mukaisia tapauksia.

Asiakastietolaki. Sosiaali- ja terveydenhuollon hajanaista tietosuojasääntelyä muutettiin kokoamalla, yhdenmukaistamalla ja yksinkertaistamalla sitä kokonaan uuteen lakiin, laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (70372023, asiakastietolaki). Laki tuli voimaan 1.1.2024 lukuun ottamatta 102 §:n siirtymäsäännöksiä. [108] Lain tarkoitus on yhdenmukaistaa asiakastietojen käsittelyä sosiaali- ja terveydenhuollossa, palveluita järjestettäessä ja toteutettaessa (1 §). Lain säätämisen yhteydessä kumottiin sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki (784/2021), sosiaalihuollon asiakasasiakirjoista annettu laki (254/2015) sekä sellainen muissa laeissa oleva asiakas- ja potilastietoja koskeva sääntely, joka sisältyy uuteen lakiin (esim. potilaslain 13 § potilastietojen

[105] Ks. jaottelu: Voutilainen & Kurvinen 2024, s. 28–29.
[106] Voutilainen & Kurvinen 2024, s. 28–29. Soveltamisalasta säädetään tietosuojalain 2§:ssä ja tietosuoja-asetuksen 2 artiklassa.
[107] Voutilainen & Kurvinen 2024, s. 28–29.
[108] Ks. lisää mm. Lehtonen, Lohiniva-Kerkelä & Pahlman 2024, s. 227.

salassapidosta sekä sosiaalihuollon asiakaslain 11 § tietojen antamisesta asiakkaalle tai hänen edustajalleen). Asiakastietolaki on erityislaki, joten jos siinä säädetään toisin kuin tietosuojalaissa, sovellettavaksi tulevat asiakastietolain säännökset.[109]

Asiakastietolain avulla sosiaali- ja terveydenhuollon asiakastietojen ja -asiakirjojen keskeinen sääntely yhdistettiin ja koottiin samaan lakiin ja sillä myös päivitettiin sosiaali- ja terveydenhuollon käsittelyä koskeva sääntely yhteensopivaksi tietosuoja-asetuksen kanssa. Lisäksi sääntelyä yhdenmukaistettiin sosiaali- ja terveydenhuollon välillä. [110] Yhtenäistäminen näkyy muun muassa lain 3 § 1 momentin 3 kohdassa, jonka mukaan asiakastiedolla tarkoitetaan sekä terveydenhuollon potilasasiakirjoja että sosiaalihuollon asiakasasiakirjoja. Lisäksi myös asiakastietojen luovutustilanteita koskevaa sääntelyä tehtiin yksinkertaisemmaksi ja helpommaksi ymmärtää sekä ammattihenkilöille että sosiaali- ja terveydenhuollossa asioiville.[111] Yhtenäinen käsite asiakastiedosta vähentää säännösten määrää ja lisää yhtenäisyyttä, kun eri asiakirjoista ei tarvitse käyttää eri nimitystä.

Ennen vuotta 2024. Kuten jo edellä kerrottiin sosiaali- ja terveydenhuollon tietojenkäsittelyä yhtenäistävä asiakasasiakirjalaki tuli voimaan 1.1.2024. Ennen tätä uudistusta sosiaali- ja terveydenhuollon tietosuojasäännöksiä oli siis useammassa laissa. Myös tämän ajan lainsäädäntöä on syytä avata hieman, koska suurin osa tutkielmassa käytetystä aineistosta perustuu lainsäädäntöön ennen vuotta 2024.

Potilaslain (laki potilaan asemasta ja oikeuksista) 13 §:ssä[112] säädettiin potilasasiakirjoihin sisältyvien tietojen salassapidosta. Potilasasiakirjoihin sisältyvät tiedot olivat pykälän mukaan salassa pidettäviä ja niiden luovuttaminen ilman potilaan tai hänen laillisen edustajansa kirjallista suostumusta oli kiellettyä. Pykälän 3 momentissa säädettiin poikkeus, jonka mukaan tietoja voitiin antaa, jos laissa nimenomaisesti säädetty tiedon antamisesta tai saamisesta.

Sosiaalihuollon asiakaslain 11 ja 13 §:ssä tietojen antamisesta sosiaalihuollon asiakkaalle tai tämän edustajalle sekä asiakkaan informoinnista tietojen käsittelystä. Sittemmin 11 § on kumottu L:lla 14.4.2023/704 , joka tuli voimaan 1.1.2024. 13 §:n aiempi sisältö on kumottu samaisella lailla ja se sisältää nyttemmin viittaussäännöksen, jonka mukaan s*osiaalihuollon*

[109] Lehtonen, Lohiniva-Kerkelä & Pahlman 2024, s. 227.
[110] Lehtonen, Lohiniva-Kerkelä & Pahlman 2024, s. 228.
[111] Lehtonen, Lohiniva-Kerkelä & Pahlman 2024, s. 228.
[112] joka on kumottu Lailla sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)

asiakastietojen salassapidosta ja asiakastietojen käsittelystä sekä asiakasasiakirjojen laatimisesta ja säilyttämisestä säädetään sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetussa laissa (703/2023).

Reksiterinpitäjä. Sosiaali- ja terveydenhuollon asiakastietojen rekisterinpidosta säädetään asiakastietolain 3 luvussa. Sen 13 §:ssä säädetään asiakastietojen rekisterinpitäjästä julkisessa ja yksityisessä sosiaali- ja terveydenhuollossa sekä työterveyshuollossa. Julkisessa sosiaali- ja terveydenhuollossa asiakastietojen rekisterinpitäjä on palvelun järjestämisestä vastaava palvelunantaja, jos ei muualla säädetä toisin. Yksityisessä sosiaali- ja terveydenhuollossa puolestaan rekisterinpitäjä on se palvelunantaja, jonka kanssa asiakas on tehnyt sopimuksen palvelun toteuttamisesta. Työterveydenhuollossa rekisterinpitäjä voi olla palvelunantaja, jonka kanssa työnantaja on tehnyt sopimuksen työterveyshuoltopalveluiden toteuttamisesta tai työnantaja, joka järjestää itse työterveyshuollon.

Hyvinvointialueen sosiaali- ja terveydenhuollon asiakas- ja potilastietojen rekisterinpidosta säädetään sosiaali- ja terveydenhuollon järjestämislain 58 §:ssä. Pykälän mukaan hyvinvointialueen sosiaali- ja terveydenhuollon palveluiden järjestämisestä vastaava toimivaltainen viranomainen on tietosuoja-asetuksessa tarkoitettu rekisterinpitäjä niille asiakas- ja potilastiedoille, joita sen toiminnassa syntyy. Lisäksi rekisterinpitäjä vastaa niistä asiakas- ja potilastiedoista, jotka ovat siirtyneet sille kuntayhtymiltä ja kunnilta sote-uudistuksessa.[113]

2.4.2 Asiakas- ja potilastietojen tietosuojan erityispiirteitä

Sosiaali- ja terveydenhuollon asiakas- ja potilastietoihin, joita tässä tutkielmassa kutsutaan pääsääntöisesti uuden asiakaslain mukaisesti asiakastiedoiksi, liittyy monia erityisiä piirteitä, jotka tekevät sääntelystä monitahoista/kerroksellista. Tämä luku on selvyyden ja luettavuuden vuoksi kirjoitettu asiakaslain pohjalta, eikä tässä nosteta erikseen aiemman sääntelyn eroavaisuuksia, vaikka tutkielman aineisto sijoittuukin pääosin aikaan ennen asiakastietolain voimaantuloa. Tutkielman tarkoitus on kuitenkin tuoda aiempaa tietosuojakäytäntöä ohjeeksi tähän päivään, joten jäsentely tehdään voimassa olevan lainsäädännön pohjalta.

[113] Voutilainen & Kurvinen 2024, huomauttavat, että sosiaali- ja terveydenhuollon järjestämislain 58 §:n 1 momentin mukaan asiakas- ja potilastiedoista ja niiden käsittelystä säädetään sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetussa laissa, julkisuuslaissa ja tietosuojalaissa. Vastaava sääntely sisältyy Uusimaalain lain 25 §:n 3 momenttiin. Tästä voisi päätellä, että tiedonhallintalakia ei sovellettaisi asiakas- ja potilastietojen käsittelyyn. Heidän mukaansa ko. säännöksiä ei tule soveltaa kirjaimellisesti, vaan niitä tulee pitää ”*informatiivisina viittaussäännöksinä, joskin vajavaisina*”. s. 29

Sosiaali- ja terveydenhuollon asiakastietoihin liittyy monia tekijöitä, jotka tekevät siitä kiinnostavan kokonaisuuden.

Salassa pidettäviä. Sosiaali- ja terveydenhuollon asiakastietojen pysyvästä salassapidosta säädetään asiakastietolain 4 §:ssä. Säännös eikä sen sisältö ole uusi.[114] Salassapidolle on pitkät perinteen sillä jo Hippokrateen valassa, on ammattieettinen vakuutus: ”*Mikäli parannustyössäni tai sen ulkopuolella ihmisten parissa näen tai kuulen sellaista, mitä ei pidä levittämän, vaikenen ja pidän sen salaisuutena*”. Tämä salassapitovelvollisuus on säilynyt terveydenhuollon ammattietiikassa[115] ja se sisältö oli aiemmin kirjoitettuna myös potilaslakiin ja ammattihenkilölakiin. Voimassa olevassa lainsäädännössä sekä sosiaali- että terveydenhuollon ammattihenkilölaeissa on säännökset, jossa viitataan asiakastietolakiin, jossa salassapidosta säädetään (4 § ammattieettisistä velvollisuuksista sosiaalihuollossa ja 16 § Potilasasiakirjojen laatiminen ja säilyttäminen sekä niihin sisältyvien tietojen salassapito terveydenhuollossa).

Arkaluonteisia tai erityisiin henkilötietoryhmiin kuuluvia tietoja. Sosiaali- ja terveydenhuollon asiakas- ja potilastietoja kutsuttiin henkilötietolaissa (11 § kumottu) arkaluonteisiksi henkilötiedoiksi. Arkaluonteisia olivat muun muassa tiedot, jotka kuvasivat henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia (4 mom.) sekä henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia (6 mom.). Tietosuoja-asetuksessa eikä henkilötietolaissa ei käytetä käsitettä arkaluonteisuus, vaan tietosuoja-asetuksen terveyttä koskevat tiedot on erityisiä henkilötietoryhmiä koskevan 9 artiklan alla.

Sosiaali- ja terveydenhuollossa käsiteltävät tiedot ovat tyypillisesti hyvin henkilökohtaisia ja arkaluonteisia, joten koko asiakas- ja potilassuhteen perustana on oltava luottamuksellisuus ja salassapito. Tietosuojan ja tietoturvan merkitys korostuu erityisesti juuri tällaisten arkaluonteisten tietojen käsittelyssä.[116] Sosiaali- ja terveydenhuoltoon liittyy myös paljon eri toimijoita, joiden välillä asiakkaat ja potilaat ja heitä koskevat tiedot liikkuvat. Silloin kun

[114] Aiemmin sosiaalihuollon asiakastietojen salassa pidettävyydestä säädettiin sosiaalihuollon asiakaslain 14 §:ssä ja potilasasiakirjojen potilaslain 13 §:ssä.
[115] Pahlman 2010, s. 11.
[116] Pahlman 2010, s. 11.

lain sallimissa rajoissa arkaluonteista ja salassa pidettävää tietoa siirretään, ne eivät saa joutua asiaankuulumattomien ulkopuolisten saataville.[117]

Velvollisuus kirjata arkaluonteisia tietoja. Sosiaali- ja terveydenhuollossa käsiteltävien tietojen arkaluonteisuuden lisäksi on huomioitava, että niihin liittyy myös laissa säädettyjä velvollisuuksia asiakas- ja potilastietojen kirjaamisesta. Asiakastietolain 17 §:n mukaan kirjaamisvelvollisuus koskee asiakkaan palvelun ja potilaan hoidon järjestämistä, suunnittelua, toteuttamista, seurantaa ja valvontaa. Tietojen tulee olla tarpeellisia ja riittäviä. Kirjaamisella tarkoitetaan sitä, että asiakastiedot on kirjattava asiakas- ja potilasasiakirjoihin. Kirjaamisen tarkoituksena on, että kirjattujen tietojen perusteella asiakkaan tai potilaan saamista palveluista ja niiden sisällöstä ja palvelun tuottajasta saadaan selkeä ja yhtenäinen kuva, joka mahdollistaa palvelujen tuottamisen jatkumon yksittäisen asiakkaan tai potilaan kohdalla. Lisäksi kirjaamisen tarkoituksena on turvata tiedonkulkua, kun kirjatuista asiakas- ja potilasasiakirjoista tieto asiakkaan tai potilaan aiemmin saamista palveluista välittyy tehokkaasti eri ammattihenkilöiden ja toimintayksiköiden välillä ja palvelut voivat jatkua sujuvasti ja tehokkaasti ja ilman päällekkäisiä toimenpiteitä. Näistä syistä kirjaamisvelvollisuus lisää myös asiakas- ja potilasturvallisuutta. [118]

Kirjaamisvelvollisuus kohdistuu sosiaali- ja terveydenhuollon ammattihenkilöihin ja palvelujen antamiseen osallistuviin avustaviin henkilöihin (17 §). Asiakastietolain luvussa 4 säädetään asiakasasiakirjojen käsittelyä koskevat periaatteet sekä sosiaali- että terveydenhuollossa. Lain luvussa 5 säädetään potilasasiakirjoista ja luvussa 6 sosiaalihuollon asiakasasiakirjoista. Eli vaikka asiakasasiakirjoista säännelläänkin samassa laissa, on sosiaalihuollon asiakasasiakirjoilla ja potilasasiakirjoilla kuitenkin eroavaisuuksiakin, vaikka sääntelyä on pyritty yhdenmukaistamaan.

Sosiaalihuollossa kirjaamisvelvollisuus alkaa palvelunantajan saatua tiedon henkilön palveluntarpeesta ja tämä on ryhtynyt toteuttamaan sosiaalipalvelua (asiakastietolaki 37 §:n 1 mom.). Sosiaalihuollon asiakkuuden alkamisesta säädetään puolestaan sosiaalihuoltolain 34 §:n 2 momentissa.[119] *Potilasasiakirjoilla* ja niiden sisältämillä tiedoilla on merkitystä erilaisissa tilanteissa. Kirjaamisen tärkeys ja puutteellisen kirjaamisen riskit ovat näkyneen myös

[117] Pahlman 2010, s. 11.
[118] Voutilainen & Kurvinen 2024, s. 241–242.
[119] Ks. myös Voutilainen & Kurvinen 2024, s. 259.

laillisuus- ja oikeuskäytännössä. Potilasasiakirjoilla on merkitystä esimerkiksi potilaan tiedonsaantioikeuden näkökulmasta. Lisäksi potilasasiakirjojen kirjauksilla on merkitystä, jos jälkikäteen joudutaan arvioimaan, onko terveydenhuollon ammattihenkilöiden toiminta ollut asianmukaista tai onko hoidossa tapahtunut henkilövahinko korvattava potilasvahinkona.[120]

Henkilötietojen käsittely on välttämätöntä sosiaaliturvaan liittyvissä asioissa. Sosiaalisia etuuksia koskevaan päätöksen tekoon tarvitaan henkilötietoja, joiden pohjalta voidaan arvioida täyttääkö henkilö lain vaatimat edellytykset kyseisen palvelun myöntämiselle. Sosiaali- ja terveyshuollossa tosiasiallista hoitotoimintaakaan ei voi toteuttaa käsittelemättä asiakkaan terveydentilaan, sosiaalisen tilanteeseen ja muihin vastaavin seikkoihin liittyviä tietoja.

Luottamus. Salassa pidettävien, arkaluonteisten tietojen kirjaamiseen ja tallentamiseen liittyy läheisesti luottamuksellisuus. Esimerkiksi terveydenhuollon ammattihenkilöistä annetun lain (559/1994) 17 §:ssä säädetään, ettei terveydenhuollon ammattihenkilö saa ilmasta ilman lupaa yksityisen tai perheen salaisuutta, josta hän on työssään saanut tiedon.[121] Sosiaali- ja terveydenhuollossa luottamuksellisuus ei liity pelkästään asiakkaan tai potilaan yksityiselämän suojaan, henkilötietojen suojaan ja salassapitosäädöksiin, sillä luottamuksellisuus on edellytys huolto- tai hoitosuhteelle, jolla voidaan saavuttaa sotepalvelujen tavoitteet. Luottamuksellista hoitosuhdetta ei voi syntyä, ellei asiakas voi olla varma, että hänen ammattilaisille luovuttamansa ja näiden muualta saamat arkaluonteiset tiedot, eivät päädy sivullisille.[122]

Luottamuksellisuuteen liittyy siis sekä se, että arkaluonteisia tietoja on kerrottava ja tallennettava, että hoito- ja asiakassuhde voi syntyä ja toimia riittävän hyvin, mutta myös tietosuojan ulottuvuus. Henkilön, joka on kertonut arkaluonteisia tietoja, pitää pystyä henkilökunnan lisäksi luottamaan myös tietosuojaan ja siihen, ettei teknisten ja inhimillisten virheiden vuoksi tiedot päädy sitä kautta vääriin käsiin. Tietosuoja on siten oleellinen osa hyvää sosiaali- ja terveydenhuoltoa. Tämä on onneksi sosiaali- ja terveydenhuollossa tunnistettu ja

[120] Voutilainen & Kurvinen 2024, s. 296.
[121] Ks. myös Tuori ja Kotkas 2016, s. 726. jossa pohtivat luottamuksellisuutta hoito ja huoltosuhteessa. Lääkäreitä koskeva salassapitovelvollisuuden juuret ovat Hippokrateen valassa *”mikäli parannustyössäni tai sen ulkopuolella kuulen sellaista, mitä ei pidä levittämän, vaikenen ja pidän sen salaisuutena*”. Kyseistä periaatetta korostetaan myös nykyisissä lääkäreiden eettisissä säännöstöissä
[122] Tuori & Kotkas 2023, s. 743–762. Sosiaali- ja terveydenhuollon tietosuojasta, salassapidosta ja luottamuksellisuudesta. Myös HE 33/1994 vp, s. 34.

ala on ollut jopa edelläkävijä tietosuojaan liittyvissä kysymyksissä. Sillä esimerkiksi tietosuoja-asetuksen myötä voimaan tulleet säännökset esimerkiksi tietosuojavastaavasta, ovat olleet käytössä sosiaali- ja terveysalalla jo ennen tietosuoja-asetuksen voimaantuloa.[123]

Monet toimijat. Yksityinen ja julkinen sosiaali- ja terveyshuolto. Suomalaisen *terveydenhuoltojärjestelmän* perusteet ovat julkisen sektorin terveyden- ja sairaanhoidon järjestämisvastuussa. Terveydenhuollon palveluja kuitenkin tuottavat myös yksityisen sektorin toimijat itsenäisinä ammatinharjoittajina tai yritystoimintana. Terveydenhuoltoon liittyvä lainsäädäntö sen sijaan voidaan jakaa yksinkertaistaen palvelujen järjestämistä ja tuottamista; terveydenhuollon ammattihenkilöiden toimintaa; sekä potilaan asemaa ja oikeuksia koskevaan sääntelyyn.[124] Asiakastietolakia sovelletaan sekä yksityiseen, että julkiseen sote-toimintaan. Samoin myös yleistä tietosuoja-asetusta ja sitä täydentävää ja täsmentävää tietosuojalakia sovelletaan sekä yksityiseen että julkiseen sosiaali- ja terveydenhuoltoon.[125]

Hyvinvointialueuudistuksen jälkeen julkisen sosiaali- ja terveydenhuollon (ja pelastustoimen) tehtävät ovat hyvinvointialueiden lakisääteisiä tehtäviä. Tähän järjestämisvastuun sisältämät lakisääteiset tehtävät on säädetty hyvinvointialuelain 7 §:ssä ja järjestämislain 8 §:ssä. Palvelujen järjestämisen yleisistä edellytyksistä säädetään Sote-järjestämislain 4 §:ssä."[126] Hyvinvointialueilla on vaihtoehtoisia tapoja tuottaa lakisääteiset sosiaali- ja terveydenhuollon palvelut ja niistä säädetään hyvinvointialuelain 9 §:ssä. Pykälän mukaan hyvinvointialue voi tuottaa järjestämisvastuulleen kuuluvat palvelut omana toimintanaan itse, yhteistoiminnassa toisten hyvinvointialueiden kanssa, sopimusperusteisesti muilta palveluntuottajilta hankkimalla tai palvelusetelin avulla.[127]

Tilanteissa, joissa palveluntuottamiseen osallistuu useampia tahoja, tietojen liikkuminen eri toimijoiden välillä on tärkeää. Hyvinvointialue voi luovuttaa salassapitosäännösten estämättä sen asiakasrekisterissä olevia asiakastietoja, palveluntuottajalle, joka tuottaa hyvin-

[123] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) 20 § 4 mom "*jokaisella palvelujen antajalla, Kansaneläkelaitoksella ja Terveydenhuollon oikeusturvakeskuksella on oltava seuranta- ja valvontatehtävää varten tietosuojavastaava*"
[124] Lohiniva-Kerkelä 2024 s. 24–25.
[125] Voutilainen & Kurvinen 2024, s. 28.
[126] Leppänen, Sorvettula & Valli-Lintu 2024, s. 115.
[127] Leppänen, Sorvettula & Valli-Lintu 2024, s.171–172.

vointialueen järjestämisvastuulle kuuluvien sosiaali- ja terveydenhuollon palveluja. Luovutettavien asiakastietojen tulee olla välttämättömiä asiakkaan palvelun tuottamiseksi ja toteuttamiseksi, jotta niitä voidaan luovuttaa.[128]

Toinen hoitava taho. Sähköiset rekisterit ja arkistot ovat pakottaneet lainsäätäjän tasapainoilemaan sähköistymisen mahdollisuuksien ja sen vuoksi kasvavien tietosuojariskien välillä. Valtakunnalliset potilasrekisterit ja arkistot auttavat siinä, että potilastiedot ovat saatavilla siellä missä niitä tarvitaan, mutta se lisää tietosuojariskiä. Koska käytännössä tietojen käsittely ja rekisterinpito on pirstoutunutta, viimekädessä työntekijän vastuulle jää, että hän käyttää rekisterien käyttöoikeuksiaan oikein. Valvonta on yleensä jälkikäteistä. Käytännössä asiakastietojen urkkijan kiinnijäämisen riski on ollut pieni, sillä esimerkiksi suurten kaupunkien terveydenhuollon potilasrekisteritietojen lokimerkintöjä muodostuu päivittäin kymmeniä tuhansia, eikä niiden seuranta ja valvonta pistokoemaisesti riitä väärinkäytösten paljastamiseen. Tästä syystä valvonnan automatisointi on nähty tarpeelliseksi.[129]

Toiset viranomaiset. Sosiaali- ja terveysala ei sekään itsessään ole selvä ja tarkkarajainen kokonaisuus. Luonnollisten henkilöiden terveydentilaan ja sosiaalipalvelujen tarpeeseen liittyviä tietoja ei aina käsitellä vain yhdessä yksikössä, vaan tietoja siirretään ja jaetaan useiden eri toimijoiden kanssa eri säännösten perusteella. Tällaisia arkaluonteisia tietoja voidaan jakaa toisille viranomaisille kuten poliisille tai toiselle henkilöä hoitavalle yksikölle asiakkaan suostumuksella. Tietoja voidaan tarvita hoitavien yksikköjen lisäksi muun muassa kouluissa ja oppilaitoksissa, työterveyshuollossa, vakuutusyhtiöissä tai tutkimuslaitoksissa. Tässä tutkielmassa käsitellään kuitenkin perinteistä potilas ja asiakastyötä, jossa rekisteröitynä on potilas tai asiakas ja rekisterinpitäjänä palvelua tuottava yksikkö.

Lähiomaiset ja lailliset edustajat. Lisäksi sosiaali- ja terveydenhuollon tietosuojaan liittyy kysymyksiä tietojen luovuttamisesta potilaalle ja asiakkaalle itselleen tai tämän lailliselle edustajalle. Henkilö voi olla kyvytön päättämään asiakas- ja potilastietojensa luovuttamisesta muun muassa alaikäisyyden tai vaikka tajuttomuuden vuoksi. Sosiaali- ja terveydenhuollon asiakastietoihin kirjataan myös toisinaan tietoja muusta henkilöstä kuin rekisteröidystä itsestä (esimerkiksi lastensuojelussa huoltajaan liittyen). Myös tällaisia tilanteita tulee vastaan sosiaali- ja terveydenhuollon tietosuojakysymyksissä.

---

[128] Voutilainen & Kurvinen 2024, s. 279.
[129] Andreasson, Koivisto ja Ylipartanen 2016, s.54–55.

2.5 Hyvä tiedonkäsittelytapa ja hyvä tietosuoja

Hyvä tiedonkäsittelytapa ja hyvä tietosuoja. Kuten jo johdannossa kerrottiin tutkielman lähtökohtana, on tarkastella sosiaali- ja terveydenhuollon tietosuojaa henkilötietolain 40 §:n mukaisen hyvän tietojenkäsittelytavan kautta. Koska henkilötietolaki on kumottu, eikä sen 40 § ole voimassa olevaa oikeutta, eikä käsitettä ”hyvä tietojenkäsittelytapa” käytetä voimassa olevissa tietosuojalaissa tai tietosuoja-asetuksessa, käsitteen sanamuotoon ei ole tarpeen takertua. Hyvä tietojenkäsittelytapa perustuu kyllä henkilötietolain säännökseen, mutta sen voi katsoa lainsäädäntöuudistusten jälkeen tarkoittavan myös hyvää tietosuojaa. Hyvä tietojenkäsittelytapa on käsitteenä myös hyvin lähellä hyvää tiedonhallintatapaa, josta säädetään laissa julkisen hallinnon tiedonhallinnasta (906/2019 tiedonhallintalaki).

Hyvästä tiedonhallintatavasta säädettiin julkisuuslain 18 §:ssä, mutta se on sittemmin kumottu tiedonhallintalain säätämisen yhteydessä. hyvä tiedonhallintatapa oli silloin uusi ajatusmalli tiedonhallintaan, johon kuului myös tietoturvaa koskevia seikkoja, vaikkakin olivat hyvin yleisluonteisia. Tietoturva kuitenkin nähtiin osana hyvää tiedonhallintatapaa, vaikka sääntely kohdistui enemmän asiakirjojen käsittelyyn ja luokitteluun.[130]

Tiedonhallintalaki koskee hallintoviranomaisten tiedon ja asianhallintaa, tietoturvallisuutta sekä yleistä tiedonhallinnan ohjausta.[131] Lain 2 §:ssä määritellään tiedonhallinta *viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuviksi toimiksi ja tietoturvallisuustoimenpiteiksi viranomaisen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi*. Hyvä tiedonhallintatapa on muualla määritelty toimintatavaksi, jossa toiminta on korkeatasoista ja hyvälaatuista. Käsite liittyy hallinnon käsittelemiin asiakirjoihin, joihin hyvän laadun vaatimus erityisesti kohdistuu. Laadukkaiden asiakirjojen ominaisuuksia ovat käytettävyys, saavutettavuus, eheys, virheettömyys ja luottamuksellisuus.[132] Terveyden ja hyvinvoinninlaitos (THL) taas kuvaa sosiaali- ja terveydenhuollon tiedonhallinnan olevan ”*toiminnan, toimijoiden ja toimintamenetelmien tuottaman tiedon hallintaa*”, jossa tieto tulee kerätä, organisoida ja tallentaa siten,

[130] Saarenpää ja Riekkinen 2023, s. 87.
[131] Mäenpää 2024, s. 440.
[132] Hyvän tiedonhallintatavan määritys, VM:n työryhmämuistioita 11/2000 https://portti.kansallisarkisto.fi/fi/arkistoalan-sanasto/hyv%C3%A4-tiedonhallintatapa

että sitä voidaan käyttää tarkoituksenmukaisesti ja hallitusti. Kyse ei ole pelkästään teknisistä ratkaisuista, vaan myös organisaatioiden toiminnan ja tiedonkulun yhdistämisestä.[133]

Lähikäsite on myös *hyvä rekisteritapa*, joka on liitetty Suomen ensimmäinen henkilötietojen suojaa koskevaan lakiin: henkilörekisterilaki oli niin sanottu toisen polven tietosuojalaki, jossa merkittävää painoarvoa sai hyvä rekisteritapa. Tällä tarkoitettaan sitä, että rekisterinpitäjien tuli oma-aloitteisesti huomioida rekisterinpidossaan lainsäädännön tavoitteiden toteutuminen.[134] Tämä rekisterinpitäjien oma-aloitteisuus on viety tietosuoja-asetuksessa vielä pidemmälle osoitusvelvollisuusperiaatteen muodossa, jota kuvattiin aiemmin luvussa 2.2.

Ohjaus ja neuvontavelvollisuus. Tietosuojavaltuutetun tulee valvontatoimillaan ohjata sosiaali- ja terveydenhuollon toimijoita hyvään tietojenkäsittelytapaan tai hyvään tietosuojaan. Laissa viranomaisten toiminnan julkisuudesta (julkisuuslaki) 20 §:ssä säädetään viranomaisen velvollisuudesta tuottaa ja jakaa tietoa. Pykälän ensimmäisen momentin mukaan viranomaisella on lakisääteinen velvollisuus edistää toimintansa avoimuutta ja laadittava tarpeen mukaan esimerkiksi oppaita, tilastoja ja muita julkaisuja. Myös tietoaineistot viranomaisen palveluista, ratkaisukäytännöstä sekä yhteiskuntaoloista ja niiden kehityksestä viranomaisen toimialalla kuuluvat pykälän ensimmäisen momentin mukaan viranomaisen tiedontuottamis ja -jakamisvelvollisuuteen. Pykälän toisen momentin mukaan viranomaisella on myös velvollisuus tiedottaa sen toiminnasta ja palveluista sekä *yksilöiden ja yhteisöjen oikeuksista ja velvollisuuksista* sen toimialaan liittyvissä asioissa. Yleisön tiedonsaannin kannalta keskeisten asiakirjojen tai niitä koskevien luetteloiden on oltava saatavilla helposti käytettävissä olevilla keinoilla, kuten kirjastoissa, yleisissä tietoverkoissa tai muilla vastaavilla tavoilla.[135]

Tietosuojavaltuutetun on siis viranomaisena tuotettava ja jaettava tietoa toiminnastaan ja yksilöiden ja yhteisöjen oikeuksista ja velvollisuuksista tietosuojakysymyksissä. Sosiaali- ja terveysalaan liittyvässä ratkaisukäytännöstä tiedottamisessa tietosuojavaltuutetun on otettava huomioon julkisuunlain velvoite tiedottaa ja jakaa tietoa toiminnastaan, mutta myös huolehdittava, ettei tiedottaminen riko tietosuojasääntelyn ja yksityisyyden suojan periaatteita.

---

[133]THL https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/mita-tiedonhallinta-on-

[134] Korhonen 2003, s. 153.

[135] Ks. myös Mäenpää 2024, s. 410–411.

Tietosuojavaltuutetulla on myös neuvontavelvollisuus, joka perustuu hallintolain 8 §:ään. Viranomaisen antama neuvonta kuuluu hyvän hallinnon perusteisiin[136]. Neuvonnalla tarkoitetaan hallintoasioissa niiden vireillepanoon ja käsittelyyn liittyvää neuvontaa sekä asiakkaiden kysymyksiin ja tiedusteluihin vastaamista.[137] Vaikka neuvontavelvollisuus voi kuulostaa siltä, että viranomaisen on opastettava asiakasta toimialaan liittyvissä kysymyksissä, laissa säädetty neuvontavelvollisuus koskee kuitenkin lähinnä hallintoasian hoitamiseen liittyvää neuvontaa. Neuvonta velvollisuus ei ulotu asian käsittelyn sisältöön tai sen lopputuloksen arviointiin tai eri vaihtoehtojen kannattavuuteen asiakkaan kannalta. Viranomainen ei voi antaa taktisia tai asianajollisia ohjeita asiakkaalle.[138]

Tietosuojavaltuutetun kohdalla neuvonta velvollisuus on häilyvämpi, sillä sen aiempiin tehtäviin kuului myös neuvojen antaminen yksittäisissä tietosuojakysymyksissä. Vanhemmat tietosuojavaltuutetun julkaisemat ratkaisut ovatkin pääasiassa vastauksia joskus hyvin yksityiskohtaisiinkin tietosuojaan liittyviin kysymyksiin. Tällainen neuvonta on ongelmallista tietosuojavaltuutetun riippumattoman ja puolueettoman käsittelyn vaatimusten kannalta[139], sillä tietosuojavaltuutetulla on toimivalta määrätä myös hallinnollisia seuraamusmaksuja, joten olisi ongelmallista, jos se ensin antaa yksityiskohtaisia ohjeita toimintatavoista ja myöhemmin arvio antamiensa ohjeiden lainmukaisuutta. Tietosuojavaltuutetulla on myös velvollisuus antaa ratkaisuja niin sanotussa ennakkokuulemismenettelyssä, josta säädetään tietosuoja-asetuksen 36 artiklassa, mihin liittyy enemmän ohjauselementtejä kuin valvonta-asioiden käsittelyyn.

Tietosuojavaltuutettu siis toteuttaa velvollisuuttaan valvoa hyvää tiedonhallintatapaa tai hyvää tietosuojaa. Vaikka lainsäädännössä ei tällä hetkellä käytetä hyvä tiedonkäsittelytavan käsitettä, sen voi silti nähdä yläkäsitteenä, jonka alle myös tietosuoja-asetuksen yleiset periaatteet: lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus mahtuvat. Tietosuojavaltuutetulla on velvollisuus toimia hallintolain ja julkisuuslain mukaan ja pitää toimintansa ja neuvontansa avoimena. Tietosuojavaltuutetulla on ohjaus ja neuvontavelvollisuus tietosuoja-asioissa, mutta se ei voi noudattaa sitä liikaa sisällöllisissä kysymyksissä.

[136] Mäenpää 2024, s. 229.
[137] Mäenpää 2024, s. 229 ja Kuusikko 2000, s. 209–214. Ks. lisää myös Kuusikko 2000 s. 316–323.
[138] Mäenpää 2024, s. 229 ja Kuusikko 2000, s. 209–214. Ks. lisää myös Kuusikko 2000 s. 316–323.
[139] Mäenpää 2024, s. 230.

3 Tietosuojavaltuutettu

Tietosuojavaltuutettu on itsenäinen ja kansallinen viranomainen, joka valvoo tietosuojalainsäädännön noudattamista.[140] Tietosuojavaltuutettu toimii oikeusministeriön yhteydessä.[141] Yleisemmin tarkasteltuna tietosuojavaltuutettu on ns. julkinen asiamies, joka avustaa yksityistä henkilöä pääsemään oikeuksiinsa tietosuojakysymyksissä.

Tietosuojavaltuutetun toimisto perustettiin vuoden 1988 alussa samaan aikaan, kun silloinen henkilörekisterilaki (471/1987) tuli voimaan.[142] Tuolloin tietosuojavaltuutetun nimi tosin oli vielä tietosuoja-asiamies.[143] Tietosuojavaltuutetun tehtävistä oli säännöksiä myös (nyt kumotun) henkilötietolain 9 luvussa. Henkilörekisterilain ja henkilötietolain lisäksi tietosuojavaltuutetusta ja sen tehtävistä ja toimivallasta säädettiin erillisessä laissa tietosuojalautakunnasta ja tietosuojavaltuutetusta (474/1987), joka kumottiin myöhemmin saman nimisellä lailla 389/1994. Tietosuojalain korvattu henkilötietolain vuonna 2019 tietosuojavaltuutettua koskeva sääntely koottiin tähän uuteen lakiin ja myös laki tietosuojalautakunnasta ja tietosuojavaltuutetusta kumottiin.

3.1 Tehtävät valvontaviranomaisena

3.1.1 Tietosuoja-asetuksen mukaan

Tietosuoja-asetuksen luvun VI otsikko on *riippumattomat valvontaviranomaiset* ja sen artikloissa 51–59 säädetään valvontaviranomaisen asemasta, roolista, perustamista koskevista säännöistä, tehtävistä, toimivallasta ja valtuuksista. Tietosuoja-asetuksessa säädetään riippumattomista valvontaviranomaisista monikossa ”*yksi tai useampi riippumaton viranomainen*”. Valvontaviranomaisia voisi olla useitakin, mutta Suomessa asetuksen tarkoittamana tietosuojaviranomaisena toimii tietosuojavaltuutettu, josta säädetään tietosuojalain 8 §:ssä. Tietosuoja-asetuksen 51 artiklan 1 kohdan mukaan valvontaviranomainen *vastuussa tämän*

[140] Tietosuojavaltuutetun nettisivut, Tietosuoja.
[141] Vuoden 2025 alusta oikeusministeriön hallinnonalalla Oikeushallinnon erityisviranomaiset -virastossa. Ks. Laki oikeushallinnon erityisviranomaiset -virastosta (24/2024) ja HE 31/2023 s. 9, 53–54 ja 64.
[142] Andreasson, Koivisto ja Ylipartanen, 2016 s. 53. Huomaa lisäksi, että henkilörekisterilaki kumottiin 1.6.1999 voimaan tulleella henkilötietolailla, joka puolestaan kumottiin 2019 voimaan tulleella tietosuojalailla.
[143] HE 49/1986 vp s. 1 ja 75.

*asetuksen soveltamisen valvonnasta luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojaamiseksi käsittelyssä ja henkilötietojen vapaan liikkuvuuden helpottamiseksi unionis*sa.

Artiklassa 55(1) säädetään valvontaviranomaisen toimivallasta. Artiklan mukaan jokaisella valvontaviranomaisella on toimivalta omassa jäsenvaltiossaan tietosuoja-asetuksen mukaisesti annettujen tehtävien hoitoon ja valtuuksien käyttöön. Artiklan kohdassa kolme säädetään, ettei valvontaviranomaisilla ole toimivaltaa valvoa käsittelytoimia, joita tuomioistuimet suorittavat lainkäyttötehtäviensä yhteydessä. Tietosuoja-asetuksen johdanto-osan 122 kohdan mukaan valvontavaltuuksiin tulisi sisältyä rekisteröityjen valitusten käsittely, asetuksen soveltamista koskevat tutkimukset sekä tietoisuuden lisääminen henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista.

Tietosuojavaltuutetun valvontatoimet saatetaan yleensä vireille rekisteröityjen tekemien valituksien ja yhteydenottojen kautta tai reksiterinpitäjien itse tekemiin ilmoituksiin tapahtuneista tietoturvaloukkauksista. Lisäksi se suorittaa ennakollista valvontaa tietosuoja-asetuksen mukaisessa ennakkokuulemismenettelyssä (artikla 36). Esimerkiksi potilastietojärjestelmän hankinnassa on tehtävä vaikutustenarviointi. Jos siinä havaitaan riskejä tai epäselvyyksiä lainmukaisuudessa, rekisterinpitäjän tulee kuulla tietosuojavaltuutettua ennen käyttöönottoa. Tietosuojavaltuutettu voi antaa ohjausta riskien vähentämiseen tai käyttää muita ohjauskeinojaan. [144]

Tietosuoja-asetus on merkittävästi muuttanut ja monipuolistanut tietosuojavaltuutetun tehtäviä. Suomessa tietosuojaviranomaisena toimiva tietosuojavaltuutettu toimii tietosuojan yleisviranomaisena ja osallistuu laajasti henkilötietojen suojan toteutukseen sen eri vaiheissa. Lisäksi sen päätöksenteko-oikeudet ovat laajentuneet, mikä näkyy esimerkiksi siinä, että käsitettä "valvontaviranomainen" on laskettu käytettävän asetuksen johdanto-osassa ja eri artikloissa yhteensä 444 kertaa. Tietosuoja-asetuksen sääntely on myös selvästi aiempaa laajempaa ja tarkempaa.[145]

Tiedottaminen, ohjaus ja neuvonta ovat olleet tietosuojavaltuutetun toiminnan lähtökohtina senkin jälkeen, kun tietosuoja-asetus tuli voimaan, vaikka tietosuojavaltuutettu on nimetty

[144] Voutilainen & Kurvinen 2024, s.424.

[145] Saarenpää ja Riekkinen 2023, s. 234

asetuksessa *valvonta*viranomaiseksi. Ohjauksen perinteinen ensisijaisuus näkyy muun muassa tietosuojavaltuutetun verkkosivuilla rekisterinpitäjille ja rekisteröidyille suunnatuilla lukuisina käytännön ohjeina.[146] Tietosuojavaltuutetun toiminnan ohjauksellisuus näkyy myös Finlexissä julkaistuissa sosiaali- ja terveysalaan liittyvissä ratkaisuissa ja kannanotoissa. Niistä suurin osa on annettu yleisen ohjauksen muodossa (etenkin ennen tietosuoja-asetusta), vaikka niiden taustalla olisikin jokin yksittäinen tapaus. Tietosuojavaltuutettu antaa myös ratkaisuissaan ohjausta oikean lain soveltamisesta tai ohjeistaa kääntymään Sosiaali- ja terveysministeriön puoleen sellaisissa asioissa, joihin tietosuojavaltuutetulla ei ole toimivaltaa ja ne kuuluvat sosiaali- ja terveysministeriön hallinnonalaan.

3.1.2 Tietosuojalain mukaan

Tietosuojalaki. Kuten jo edellä todettiin, tietosuoja-asetuksen tarkoittama riippumaton valvontaviranomainen on Suomessa tietosuojavaltuutettu. Tietosuoja-asetuksen tarkoittamaksi tietosuojaviranomaisena jatkoi siis pienin rakenteellisin muutoksin oikeusministeriön yhteydessä jo toiminut tietosuojavaltuutettu.[147] Vuoden 2025 alusta tietosuojavaltuutetun toimisto siirtyi Oikeushallinnon erityisviranomaiset -virastoon, mutta toimii siis edelleen oikeusministeriön hallinnonalalla.[148]

Tietosuojalaissa säädetään, että tietosuojavaltuutetulla on toimisto, jossa työskentelee vähintään kaksi apulaistietosuojavaltuutettua ja tarpeellinen määrä tietosuojavaltuutetun tehtäväalaan perehtyneitä esittelijöitä ja lisäksi muuta henkilöstöä (9§). Kelpoisuusvaatimuksena tietosuojavaltuutetun tai apulaistietosuojavaltuutetun virkaan on oikeustieteen ylempi korkeakoulututkinto, jonka on oltava muu kuin kansainvälisen ja vertailevan oikeustieteen maisterin tutkinto. Lisäksi kelpoisuusvaatimuksena on hyvä perehtyneisyys henkilötietojen suojaa koskeviin asioihin ja käytännössä osoitettu johtamistaito (10§). Valtioneuvosto nimittää tietosuojavaltuutetun ja apulaistietosuojavaltuutetun viideksi vuodeksi kerrallaan (11§). Apulaistietosuojavaltuutettujen viroista säätäminen perustui tietosuojavaltuutetun kasvaneeseen työmäärään ja käytännön kokemuksiin. Tarkoituksena oli, että tietosuojavaltuutetun ratkaisu- ja puhevalta olisi mahdollista hajauttaa toimiston sisällä useammalle taholle. Tietosuojavaltuutetun toimiston käsittelemien asioiden määrä olikin nelinkertaistunut

[146] Saarenpää ja Riekkinen 2023, s. 234.
[147] Paasonen & Luomala 2024, s. 43–44 ja HE 9/2018 vp, s. 8.
[148] Ks. Laki oikeushallinnon erityisviranomaiset -virastosta (24/2024) ja HE 31/2023 s. 9, 53–54 ja 64.

vuoden 2000 jälkeen, ja myös yleisen tietosuoja-asetuksen myötä valtuutetun tehtävien määrän ennakoitiin edelleen kasvavan.[149]

Tietosuojavaltuutetun tehtävistä säädetään tietosuojalain 14 §:ssä. Pykälän 1 momentissa viitattaan valvontaviranomaisen toimivaltuuksista säädettävän tietosuoja-asetuksen 55–59 artikloissa. Lisäksi tietosuojavaltuutetulla on pykälän mukaan myös muita tehtäviä ja toimivaltuuksia, joista säädetään tietosuojalaissa ja muissa laeissa.[150] Pykälään sisältyy tietosuojavaltuutetun laaja yleistoimivalta ja tehtävät ja toimivaltuudet, jotka säädetään muissa laeissa.[151]

Tietosuojavaltuutetun tehtäviin ei kuulu 14 §:n toisen momentin mukaan valvoa valtioneuvoston oikeuskanslerin eikä eduskunnan oikeusasiamiehen toimintaa. Tämän rajauksen taustalla on perustuslakivaliokunnan lausunto, jonka mukaan tietosuojalain säännöksissä olisi ilmettävä, että ”*ylimpien laillisuusvalvojien valtiosääntöinen asema ja tehtävät ja laillisuusvalvonnan valtiosääntöinen kokonaisuus eivät mahdollista asteellisesti alemman tietosuojavaltuutetun ylimpiin laillisuusvalvojiin kohdistuvaa valvontaa*.”[152],[153]

Tietosuojalain 14 §:n 3 momentin mukaan tietosuojavaltuutettu edustaa Suomea Euroopan tietosuojaneuvostossa. Lisäksi tietosuojavaltuutettu akkreditoi tietosuoja-asetuksen 43 artiklassa tarkoitetun sertifiointielimen ja laatii eduskunnalle ja valtioneuvostolle vuosittain toimitettavan toimintakertomuksen (TSA 59 artikla). Lisäksi tietosuojalaissa säädetään tietosuojavaltuutetun päätöksenteosta (15 §). Asiat voivat tulla vireille rekisteröidyn aloitteesta, rekisterinpitäjän tai henkilötietojen käsittelijän toimesta, jonkun muun henkilön toimesta tai tietosuojavaltuutetun omasta aloitteesta. Edelleen tietosuojalaissa säädetään apulaistietosuojavaltuutettujen tehtävistä ja toimivaltuuksista (16 §) ja asiantuntijalautakunnan tehtävistä ja asioiden käsittelystä (17 §). Lautakunta antaa tietosuojavaltuutetun pyynnöstä lausuntoja henkilötietojen käsittelyä koskevan lainsäädännön soveltamiseen liittyvistä merkittävistä

[149] Paasonen & Luomala 2024, s. 43–44 ja HE 9/2018 vp, s. 93.
[150] Tietosuojavaltuutetulla voi olla tietosuoja-asetuksen 58 artiklan 6 kohdan mukaan myös kansallisesti säädettyjä muita kuin tietosuoja-asetuksen mukaisia valtuuksia
[151] Paasonen & Luomala 2024, s. 46–47. HE 9/2018 vp, s. 96–99.
[152] PeVL 14/2018 vp s.13–15.
[153] Saman 14 §:n kolmannessa momentissa säädetään tietosuojavaltuutetun Suomen edustamisesta Euroopan tietosuojaneuvostossa. Neljännessä momentissa säädetään tietosuojavaltuutetun tehtävästä akkreditoida tietosuoja-asetuksen 43 artiklassa tarkoitettu sertifiointielin. Viides momentti sisältää säädöksen tietosuojavaltuutetun tehtävästä laatia vuosittain tietosuoja-asetuksen 59 artiklassa tarkoitettu toimintakertomus, joka toimitetaan eduskunnalle ja valtioneuvostolle.

kysymyksistä. Erityisen korostunut merkitys asiantuntijalautakunnalla on, jos on kyse kansallisesta tietosuojalainsäädännön tulkinnasta.[154] Lisäksi säädetään tietosuojavaltuutetun tiedonsaanti ja tarkastusoikeudesta (18 §), yhteistyöstä kolmansien maiden valvontaviranomaisten kanssa (18a §), asiantuntijoiden käytöstä (19 §) ja virka-avusta (20 §).

3.1.3 Kumotun henkilötietolain mukaan

Henkilötietolain 9 luvussa säädettiin tietosuojavaltuutetusta ja tietosuojalautakunnasta. Luvun otsikko oli *Henkilötietojen käsittelyn ohjaus ja valvonta* ja sen pykälissä 38–46 säädettiin kyseessä olevien tietosuojaviranomaisten tehtävistä ja toimivallasta.

Tietosuojavaltuutettu. Tietosuojavaltuutetun tehtävä oli antaa henkilötietojen käsittelyyn liittyvää ohjausta ja neuvontaa sekä valvoa henkilötietojen käsittelyä henkilötietolain tavoitteiden toteuttamiseksi (38 § 1 mom). Lain 39 §:ssä säädettiin tietosuojavaltuutetun ja tietosuojalautakunnan tiedonsaanti ja tarkastusoikeuksista.[155]

Tietosuojavaltuutetun tuli edistää hyvää henkilötietojen käsittelytapaa, ja sen tuli ohjein ja neuvoin pyrkiä siihen, että rekisterinpitäjä tai rekisterinpitäjät eivät jatka tai uusi lainvastaista menettelyä. Tietosuojavaltuutetun oli tarvittaessa ”*saatettava asia tietosuojalautakunnan päätettäväksi tai ilmoitettava se syytteeseenpanoa varten”* (40§). Tietosuojavaltuutetulla oli velvollisuus ratkaista tarkastusoikeuteen tai tietojen korjaamiseen liittyvä asia, jonka rekisteröity oli saattanut sen käsiteltäväksi. Tietosuojavaltuutetulla oli myös toimivalta antaa reksiterinpitäjälle määräys rekisteröidyn tarkastusoikeuden toteuttamisesta tai tiedon korjaamisesta (2 mom.). Tietosuojavaltuutettu saattoi myös antaa myös tarkempia ohjeita siitä, miten henkilötietoja on suojattava niiden laittomalta käsittelyltä (3 mom.)

Tietosuojavaltuutetun kuulemisesta lainsäädäntö ja hallintouudistuksissa, jotka koskivat henkilöiden oikeuksien ja vapauksien suojaamista henkilötietojen käsittelyssä säädettiin 41 §;ssä. Myös syyttäjän tuli kuulla tietosuojavaltuutettua ennen henkilötietolain vastaisen menettelyä koskevan syytteen nostamista. tuomioistuimen tuli tällaisessa asiassa puolestaan varata tietosuojavaltuutetulle tilaisuus tulla kuulluksi.

---

[154] Paasonen & Luomala 2024, s. 46–47. HE 9/2018 vp, s. 96–99

[155] Tietosuojavaltuutetulla ja tietosuojalautakunnalla oli oikeus salassapitosäännösten estämättä saada tiedot käsiteltävistä henkilötiedoista sekä kaikki tiedot, jotka ovat tarpeen henkilötietojen käsittelyn lainmukaisuuden valvonnassa. Tietosuojavaltuutetulla oli oikeus tarkastaa henkilörekistereitä ja käyttää tarkastuksessa asiantuntijoita

Tietosuojavaltuutetun tehtäviin kuului myös tarkastaa rekisterinpitäjien ja niitä edustavien yhteisöjen laatimia toimialakohtaisia käytännesääntöjä, joiden tarkoituksena oli edistää henkilötietolain soveltamista ja hyvää tietojenkäsittelytapaa. Tietosuojavaltuutettu varmisti, että käytännesäännöt olivat henkilötietolain ja muiden henkilötietojen käsittelyä koskevien säännösten mukaisia (42§).

Tietosuojalautakunta oli toinen henkilötietolain mukaisista tietosuojaviranomaisista. Henkilötietolain 38 §:n 2 momentissa Tietosuojalautakunnan tehtävä oli käsitellä *henkilötietojen käsittelyyn liittyviä lain soveltamisalan kannalta periaatteellisesti tärkeitä kysymyksiä ja käyttää päätösvaltaa tietosuoja-asioissa* henkilötietolain mukaisesti (38 § 2 mom.). [156]

Tietosuojalautakunnalla oli myös lupatoimivalta (43 §). Se saattoi myöntää luvan henkilötietojen käsittelyyn, *jos käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi muussa kuin yksittäistapauksessa taikka yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai sivulliselle, jolle tiedot luovutetaan.* Tietosuojalautakunta saattoi myös myöntää luvan arkaluonteisten henkilötietojen käsittelyyn tärkeän yleisen edun vuoksi. Luvat voitiin myöntää määräajaksi tai toistaiseksi.

Tietosuojalautakunta saattoi 44 §:n mukaan tietosuojavaltuutetun hakemuksesta 1) kieltää henkilötietolain tai sen nojalla annettujen sääntöjen ja määräysten vastaisen henkilötietojen käsittelyn, 2) velvoittaa rekisterinpitäjän määräajassa oikaisemaan oikeudettoman teon tai laiminlyönnin, 3) määrätä rekisteritoiminnan lopetettavaksi, jos lainvastaiset toimet tai laiminlyönnit huomattavasti vaaransivat rekisteröidyn yksityisyyden suojaa, etuja tai oikeuksia, ellei rekisteristä ollut laissa toisin säädetty ja 4) peruuttaa antamansa luvan, jos edellytyksiä luvan myöntämiselle ei enää ollut tai rekisterinpitäjä oli toiminut luvan määräysten vastaisesti. Tietosuojavaltuutetun ja tietosuojalautakunnan päätöksiin sai hakea muutosta hallinto-oikeuteen valittamalla (45 §).[157]

---

[156] Henkilötietolain edeltäjän henkilörekisterilain ollessa voimassa rekisterinpitäjää velvoittava päätöksenteko kuului tietosuojalautakunnalle. Tietosuojavaltuutetulla oli mahdollisuus viedä tietosuojalautakunnan ratkaistavaksi asia, jossa rekisterinpitäjä ei tietosuojavaltuutetun omasta kehotuksesta muuttanut lainvastausta menettelyään. HE 96/1998 vp s. 9.

[157] Henkilötietolakia säädettäessä tietosuojavaltuutetun toimivaltuuksiin tehtiin muutoksia siten, että tietosuojavaltuutetun virheen oikaisua ja tarkastusoikeuden toteuttamista koskevat päätökset tulivat asianosaisia velvoittaviksi ja nämä tietosuojavaltuutetun tekemät päätökset olivat valituskelpoisia. Henkilötietolain voimaantulon myötä luovuttiin myös tietosuojalautakunnan yleisestä poikkeuslupatoimivallasta, mutta koska lainsäädännössä katsottiin olevan mahdotonta ennakoida kaikkia henkilötietojen käsittelytapauksia, joissa käsittely

3.2 Artiklan 58(2) mukaiset korjaavat toimivaltuudet

Ennen tietosuojalain voimaantuloa tietosuojavaltuutetulla ei ollut juurikaan toimivaltaa antaa oikeudellisesti velvoittavia päätöksiä. Tietosuojavaltuutetulla oli henkilötietolaissa säädetty toimivaltuus antaa rekisterinpitäjälle määräys rekisteröidyn 28 § mukaisen tarkastusoikeuden toteuttamisesta tai 29 §:n mukaisesta tiedon korjaamisesta, jos rekisteröity oli tuonut asian tietosuojavaltuutetun ratkaistavaksi. Tietosuojavaltuutettu saattoi myös tehostaa määräyksiään uhkasakolla (46 §) siten kuin uhkasakkolaissa (1113/1990) säädettiin. Tietosuoja valtuutetun ensisijainen tehtävä oli antaa ohjausta ja neuvontaa. Jos siitä ei ollut apua, tietosuojavaltuutetun tuli saattaa lainvastainen menettely tietosuojalautakunnan päätettäväksi tai ilmoittaa se syytteeseenpanoa varten (40 §). Varsinaista päätösvaltaa tietosuojaasioissa käytti tietosuojalautakunta (38 § 2 mom.). Se antoi tietosuojavaltuutetun hakemuksesta määräykset rekisterinpitäjille lainvastaisen käsittelyn kieltämisestä, oikaisemisesta tai rekisteritoiminnan lopettamisesta (44 §). Tietosuojalautakunnalla oli myös lupatoimivalta tietyissä tapauksissa (43 §).

Tietosuoja-asetuksen tullessa voimaan, tietosuojavaltuutetun toimivaltuudet laajenivat. Asetuksen 58 artiklassa säädetään valvontaviranomaisen tutkintavaltuuksista, korjaavista toimivaltuuksista ja hyväksymis- ja neuvontavaltuuksista (kohdat 1–3). Tietosuojalain 8 §:n mukaan Suomen tietosuojaviranomainen on tietosuojavaltuutettu. Tietosuoja-asetuksen 58(2) artiklan mukaan valvontaviranomaisen käytettävissä olevat korjaavat toimivaltuudet ovat: varoitus, huomautus, määräys, henkilötietojen käsittelyn rajoittaminen tai käsittelykiellon antaminen, sertifioinnin peruuttaminen tai määräyksen antaminen sertifiointielimelle sekä määräys tiedonsiirtojen keskeyttämisestä kolmanteen maahan tai kansainväliselle järjestölle[158]. Näiden lisäksi tietosuojavaltuutettu voi määrätä rekisterinpitäjälle hallinnollisen seuraamusmaksun.

Varoituksen antaminen, alakohta a) Tietosuojavaltuutettu voi ennakollisesti varoittaa rekisterinpitäjää tai muuta henkilötietojen käsittelijää, jos sen suunnittelemat henkilötietojen käsittelytoimet ovat todennäköisesti tietosuoja-asetuksen vastaisia.

---

voitaisiin sallia tyyppitilanteiden ulkopuolella, tietosuojalautakunnalle säädettiin mahdollisuus myöntää lupa henkilötietojen käsittelyyn. HE 96/1998 s. 27.

[158] Tiedonsiirron keskeyttämisestä säädetään tietosuoja-asetuksen 58 artiklan 2 kohdan j) alakohdassa. Tämä toimivaltuus jää tarkastelun ulkopuolelle sillä tutkielman aineisto koostuu vain kansallisista sosiaali- ja terveyspalveluista ja niiden tietosuojasta eikä aineistossa ollut kyseisen kohdan mukaisia tapauksia.

Huomautuksen antaminen, alakohta b. Jos rekisterinpitäjä tai henkilötietojen käsittelijä on jo ehtinyt tehdä käsittelytoimia, jotka ovat olleet tietosuoja-asetuksen vastaisia, tietosuojavaltuutettu voi antaa huomautuksen rekisterinpitäjälle tai henkilötietojen käsittelijälle.

Määräysten antaminen, alakohdat c, d, e, g ja j. Tietosuojavaltuutettu voi antaa useita erilaisia määräyksiä rekisterinpitäjälle tai henkilötietojen käsittelijälle.

Alakohdan c) mukaan valvontaviranomainen voi antaa määräyksen rekisterinpitäjälle tai henkilötietojen käsittelijälle noudattaa rekisteröidyn pyyntöjä, jotka koskevat tietosuoja-asetukseen perustuvien rekisteröidyn oikeuksien käyttöä.

Alakohta d) Määräys saattaa henkilötietojen käsittely asetuksen mukaiseksi**.** Jos rekisterinpitäjä tai henkilötietojen käsittelijä ei käsittele henkilötietoja tietosuoja-aseuksen mukaisesti, tietosuojavaltuutettu voi määrätä sen saattamaan henkilötietojen käsittelytoimet asetuksen mukaisiksi. Määräykseen voi tarvittaessa sisältyä määräaika ja toteuttamistavan määrittelyä.

Alakohta e) Määräys ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidylle. Määräyksen antamistoimivaltaa tietosuojavaltuutettu voi käyttää myös tilanteessa, jossa rekisterinpitäjä ei ole ilmoittanut tietoturvaloukkauksesta rekisteröidylle, vaikka siitä on aiheutunut tälle korkea riski. Tällöin tietosuojavaltuutettu voi määrätä rekisterinpitäjän ilmoittamaan henkilötietojen tietoturvaloukkauksesta sen kohteena olleelle rekisteröidylle.

Alakohdan g) mukaan tietosuojavaltuutettu voi määrätä rekisterinpitäjän tai henkilötietojen käsittelijän oikaisemaan tai poistamaan henkilötietoja tai rajoittamaan niiden käsittelyä asetuksen 16, 17 ja 18[159] artiklan perusteella sekä ilmoittamaan näistä toimenpiteistä tahoille, joille se on luovuttanut henkilötietoja tietosuoja-asetuksen artiklojen 17(9) ja 19[160] mukaisesti.

Alakohdan j) mukaan tietosuojavaltuutettu voi määrätä rekisterinpitäjän keskeyttämään tietojen siirron kolmannessa maassa olevalla vastaanottajalle tai kansainväliselle järjestölle.

[159] 16 artikla Oikeus tietojen oikaisemiseen, 17 artikla Oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”) ja 18 artikla Oikeus käsittelyn rajoittamiseen

[160] Henkilötietojen oikaisua tai poistoa tai käsittelyn rajoittamista koskeva ilmoitusvelvollisuus, jonka mukaan rekisterinpitäjän on ilmoitettava henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, ellei tämä ole mahdotonta tai vaadi kohtuutonta vaivaa

Henkilötietojen käsittelyn rajoittaminen tai käsittelykielto, alakohta f). Tietosuojavaltuutettu voi asettaa rekisterinpitäjälle tai henkilötietojen käsittelijälle väliaikaisen tai pysyvän rajoituksen henkilötietojen käsittelylle tai käsittelykiellon.

Sertifioinnin peruuttaminen tai määräyksen antaminen sertifiointielimelle, alakohta h). Tietosuojavaltuutettu voi peruuttaa tai määrätä sertifiointielimen peruuttamaan sertifiointi[161] tai kieltää sertifiointielintä antamasta sertifiointia, jos sertifiointia koskevat vaatimukset eivät alun perinkään täyty tai eivät muutosten vuoksi enää täyty.

Hallinnollinen sakko, alakohta i) Tietosuojavaltuutetulla on määräyksien, varoituksen ja huomautuksen lisäksi käytettävissä hallinnollinen sakko, josta Suomen lainsäädännössä käytetään hallinnollinen seuraamusmaksu -käsitettä.[162]. Tämä nimenomainen toimivaltuus oli yksi tietosuoja-asetuksen merkittävimmistä uudistuksista. Mahdollisuus määrätä seuraamusmaksuja tehosti henkilötietojen valvonnan seuraamusjärjestelmää. [163] Hallinnollinen maksu voidaan määrätä sekä muiden korjaavien toimenpiteiden lisäksi tai niiden sijasta. Tällaista seuraamusmaksuvaltuutta ei Suomessa ole aiemmin ollut. [164]

Kansallisessa lainsäädännössämme on poikettu hieman myös tietosuoja-asetuksen säännöksestä sen suhteen, kenellä on toimivaltuus määrätä hallinnollisia seuraamusmaksuja. Tietosuoja-asetuksen 58(2)(i) artiklan mukaan toimivaltaisen jäsenvaltion valvontaviranomainen on toimivaltainen määräämään hallinnollisia seuraamusmaksuja. Suomen oikeusjärjestelmässä yksittäiselle virkamiehelle, näin merkittävän toimivallan antaminen olisi perustuslakivaliokunnan mukaan erikoislaatuista.[165] Kansallisessa tietosuojalain 24 §:ssä päädyttiin siten säätämään, että seuraamusmaksun määrää seuraamuskollegio, johon kuuluvat tietosuo-

[161] Kyseessä sertifiointi, joka on annettu tietosuoja-asetuksen 42 ja 43 artiklan mukaisesti.
[162] Oikeudellisena käsitteenä *hallinnollista sakkoa* ei ole pidetty hyvin yhteensopivana suomalaisen oikeusjärjestelmän kanssa. Kansallisesti meillä sakkoa ja seuraamusmaksua on pidetty erillisinä käsitteinä: sakko on perinteisesti tarkoittanut rikosoikeudellista rangaistusta ja rahamääräinen hallinnollinen seuraamuksen nimitykseksi on suomen kielessä vakiintunut rikemaksu tai seuraamusmaksu. Ks. lisää Korpisaari, Pitkänen ja Warma-Lehtinen 2018, s. 535–536 ja PeVL 14/2018, s. 9.
[163] Saarenpää ja Riekkinen 2023, s. 234.
[164] Saarenpää ja Riekkinen 2023, s. 235.
[165] Perustuslakivaliokunta kiinnitti huomiota siihen, että kyseessä olevaan hallinnolliseen seuraamusmaksuun verrattavissa olevissa kilpailulain mukaisessa hallinnollisessa seuraamusmaksussa päättävä taho on markkinaoikeus (riippumaton tuomioistuin), jonka menettelyssä on vahvemmat menettelylliset oikeusturvatakeet. Ks. PeVL 14/2018, s. 18–19 ja Korpisaari, Pitkänen ja Warma-Lehtinen 2018, s. 536.

javaltuutettu ja apulaistietosuojavaltuutetut. Seuraamuskollegion puheenjohtajana toimii tietosuojavaltuutettu. Pykälän 4 momentin mukaan seuraamusmaksua ei voi määrätä julkishallinnon organisaatioille, kuten valtiolle, valtion liikelaitoksille, kunnille tai seurakunnille.

Määrätty seuraamusmaksu voi olla enintään 4 % rekisterinpitäjänä toimivan liikevaihdosta tai 20 miljoonaa euroa ja sen suuruus riippuu kunkin yksittäisen tapauksen olosuhteista. Tietosuoja-asetuksen 58(2) artiklan i alakohdan mukaan toimivaltaisen jäsenvaltion valvontaviranomainen on toimivaltainen määräämään hallinnollisia seuraamusmaksuja. Seuraamusmaksun suuruudesta annetut rajat aiheuttivat tietosuoja-asetusta kohtaan vastustusta, mutta koskevat kuitenkin lähinnä suuryrityksiä ja niiden perusteella voi muodostua harhaanjohtava kuva seuraamusjärjestelmästä. Toteutuneet seuraamusmaksut ovat olleet suhteellisen pieniä, ”*osin jopa kuvaannollisia”.*[166]

Uhkasakko, tietosuojalain 22 §. Tietosuojavaltuutettu voi myös käyttää tietosuoja-asetuksen 58 artiklan 2 kohdan c–g ja j alakohdissa kuvattujen määräysten, henkilötietojen käsittelyn rajoittamisen tai tietojen siirron keskeyttämisen tueksi ja kansallisen tietosuojalain 18 §:n 1 momenttiin perustuvan tietojen luovuttamista koskevan määräyksen tehosteeksi uhkasakkoa. Tarkemmin uhkasakon asettamisesta ja maksettavaksi tuomitsemisesta säädetään uhkasakkolaissa (1113/1990).

[166] Saarenpää ja Riekkinen 2023, s. 235.

4 Sosiaali- ja terveydenhuollon rekisterinpitäjille annettu ohjaus

Sosiaali- ja terveydenhuollon toimiala on tietosuojavaltuutetun toimiston suurin toimiala vireille tulleiden asioiden määrässä. Esimerkiksi vuonna 2022 vireille tulleita sosiaali- ja terveydenhuoltoon liittyviä asioita oli 2879, mikä oli noin 22 % kaikista vireille tulleista asioista.[167] Näistä noin 80 % oli henkilötietojen tietoturvaloukkausilmoituksia. Yleisesti terveydenhuollon tietoturvaloukkaukset ovat johtuneet inhimillisestä virheestä ja koskeneet pientä joukkoa ihmisiä, mutta laajavaikutteisempiakin tilanteita on ollut. Alla olevasta taulukosta ilmenee vuosien 2017–2024 välillä tietosuojavaltuutetun toimistossa sosiaali- ja terveydenhuoltoon liittyvien vireille tulleiden asioiden määrät.[168] Myös sosiaali- ja terveydenhuoltoon liittyvässä oikeudellisessa kirjallisuudessa on nostettu esille tietosuojavaltuutetun ratkaisujen määrä pitkällä aikavälillä.[169]

Vuosi	Vireille tulleet asiat
2017	553
2018	1878
2019	2195
2020	2700
2021	2852
2022	2879
2023	3183
2024	3372

Taulukko 1. Tietosuojavaltuutetun toimistossa sosiaali- ja terveydenhuoltoon liittyvät vireille tulleet asiat. (lähde: tietosuojavaltuutetun toimisto)

Koska kaikkien vireille tulleiden sote-asioiden määrät ovat tietosuoja-asetuksen voimaantulon jälkeen vuosittain näin suuria, tutkielman aineistoa oli rajattava. Sosiaali- ja terveydenhuoltoon liittyviä asioita oli vaikea rajata muulla tavoin maisteritutkielman kokoiseksi mie-

[167] Lähteet: tietosuojavaltuutetun toimisto (vuodet 2021–2024) ja tietosuojavaltuutetun toimintakertomukset vuosilta 2017–2020.
[168] Tietosuojavaltuutetun toimiston toimintakertomus 2022, s. 33–34.
[169] Ks. Voutilainen & Kurvinen 2024, s. 426.

lekkääksi ja helposti saatavilla olevaksi kokonaisuudeksi ilman tutkielman tekemiseen liittyviä tietosuojarajoituksia, tarkasteltavat tapaukset on tässä tutkielmassa rajattu Finlexissä julkaistuihin tapauksiin, joista tunnistettavat tiedot on jo poistettu.

Sosiaali- ja terveydenhuoltoon liittyvien tapausten määrittelyssä rajauksena on tässä tutkielmassa käytetty rekisterinpitäjää, sillä sosiaali- ja terveydenhuollon asiakas- ja potilastietoja voidaan käsitellä myös muiden rekisterinpitäjien toimesta. Mikäli tietosuojavaltuutetun ratkaisun kohteena oleva rekisterinpitäjä on sosiaali- ja terveysalan toimija, tapaus kuuluu tämän tutkimuksen aineistoon. Tapaukset, jossa oli kyse tietojen luovuttamisesta sosiaali- ja terveysalan ulkopuolisille toimijoille (esimerkiksi vakuutusyhtiöt) on otettu aineistoon, jos tietosuojavaltuutettu on käsitellyt sosiaali- ja terveydenhuollon toimintayksikön tietojen luovuttamista, mutta tarkastelun ulkopuolelle on jätetty tapaukset, joissa kantaa on otettu potilastietojen pyytäjän toimintaan. Työterveyshuoltoon liittyen aineistoon kuuluvat tapaukset, joissa on kyse sosiaali- ja terveydenhuollon rekisterinpitäjän toimista luovutettaessa terveydentilaan liittyviä tietoja työnantajalle, mutta aineiston ulkopuolelle jäävät kysymykset työnantajien oikeudesta ylläpitää terveystietoihin liittyviä rekistereitä

Oppilas- ja opiskeluhuollon osalta rajaaminen oli vaikeaa, sillä niitä koskevia kysymyksiä rekisterinpitäjästä ja oikeudesta saada pääsy oppilasrekisteriin oli vaikea hahmottaa lainsäädäntömuutosten vuoksi. Vaikka sosiaali- ja terveydenhuollon palvelujen järjestämisvastuun siirtyessä kunnilta hyvinvointialueille, myös oppilas- ja opiskeluhuolto ja esimerkiksi kuraattoripalvelut siirtyivät hyvinvointialueiden vastuulle, henkilötietolain aikaiset oppilas ja opiskeluhuoltoon liittyvä tapaukset rajattiin aineiston ulkopuolelle. Ne muodostavat omanlaisensa kokonaisuuden lakimuutoksineen, joiden yksityiskohtiin tässä tutkielmassa ei ole mahdollisuutta syvällisemmin perehtyä. Lisäksi tietosuoja-asetuksen mukaisia ratkaisuja, jotka liittyisivät oppilas- tai opiskeluhuoltoon ei aineistossa ollut.

Kiinnostavan rajatapauksen kannanottojen rajaamisessa aiheuttivat tietosuojavaltuutetun ratkaisut, joissa yhteensä neljän eri kaupungin tai kuntayhtymän sosiaali- ja terveyspalvelut oli käsitellyt vapaaehtoisten tuki- ja sijaisperhetoimintaan tai lasten ja nuorten tukihenkilötoimintaan hakevien henkilöiden poliisin tietojärjestelmissä olevia rikos- ja rangaistusmerkintöjä tai muita poliisin rekistereissä olevia hakijaa koskevia tietoja (esimerkiksi kotihälytyksiä tai henkilön tekemiä rikosilmoituksia koskevia tietoja) tietosuojalain vastaisesti ilman

lain mukaista perustetta.[170] Nämä jäävät kuitenkin tutkielman aineiston ulkopuolelle, sillä vaikka rekisterinpitäjä oli sosiaalihuollon toimija, rekisteröidyt eivät olleet sosiaalihuollon asiakkaita, kuten tietosuojavaltuutettukin joutui rekisterinpitäjää muistuttamaan. [171]

Edellä kuvatuilla perusteilla rajattuna tietosuojavaltuutetun Finlexissä julkaisemia sosiaali- ja terveydenhuoltoon liittyviä tapauksia löytyi yhteensä 56. Tapauksista 36 oli jo kumotun henkilötietolain mukaisia tapauksia ja näistä 21 liittyi sosiaalihuoltoon ja 15 terveydenhuoltoon. Tietosuoja-asetuksen mukaisia päätöksiä aineistossa oli yhteensä 20, joista 4 liittyi sosiaalihuoltoon ja 16 terveydenhuoltoon. Pelkästään sosiaalialaan liittyviä tapauksia oli siten yhteensä 25 ja terveydenhuoltoon liittyviä tapauksia 31.

Millaisista aiheista TSV:n ratkaisuja on annettu. Aiheiltaan tietosuojavaltuutetun ratkaisut ovat hyvin moninaisia. Koska teknologian kehitys on ollut 2000-luvulla varsin nopeaa, näkyy aineistossa myös kehityksen tuomat tietosuojahaasteet. Tietosuojavaltuutettu on esimerkiksi ottanut vuosien varrella kantaa sähköpostin käyttöön sosiaali- ja terveydenhuollossa vuosina 2009, 2010 ja 2012. Tapauksissa muistutetaan, että rekisterinpitäjä on vastuussa tietoturvasta ja siitä, että se toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet, jotta henkilötiedot ovat turvassa. Ratkaisuissa muun muassa muistutetaan, että velvollisuudesta ei voi poiketa asiakkaan tai potilaan suostumuksella tai pyynnöstä. Sähköpostin käytössä sosiaali- ja terveysalalla on kuitenkin tullut muistaa myös se, että asiakas voi itse saada asiansa vireille myös suojaamatonta sähköpostia. [172] Tietosuojavaltuutettu kuitenkin ohjaa vastaamaan suojaamattomasta sähköpostista tuleviin arkaluonteisia henkilötietoja sisältäviin viesteihin puhelimitse tai kirjeitse. Kovin tuoreita ratkaisuja sähköpostin käytöstä ei tietosuojavaltuutetun julkaistussa ratkaisukäytännössä ole, joka johtunee siitä, että nykyään sosiaali- ja terveydenhuollossa on käytössä tietoturvallisia sähköisen asioinnin kanavia

[170] ATSV 8979/162/21; ATSV 8979/162/21; ATSV 7635/162/21 ja ATSV 6689/186/20. Osassa tapauksista sosiaali- ja terveystoimi oli pyytänyt tietoja poliisilta lain sosiaalihuollon asiakaan asemasta ja oikeuksista (812/2000) 20 §:n perusteella, vaikka vapaaehtoisiksi hakeutuvat eivät ole kyseisen lain 3§ 1 momentin 1) kohdan tarkoittamia sosiaalihuollon asiakkaita. Vapaaehtoisiin ei siten voitu soveltaa kyseistä lakia ja sosiaalipalvelujen tietojen käsittelylle ei ollut lain mukaista perustetta. Osassa tapauksista taas vapaaehtoiseksi hakevan oli edellytetty käyttävän itse rekisteröidyn tarkastusoikeuttaan poliisin henkilötietojen käsittelyyn ja toimittavan saamansa tiedot sosiaalitoimen nähtäväksi.
[171] ATSV 6689/186/20 kohdat 15–16.
[172] TSV 1475/41/2009 Sähköpostin ja tekstiviestien käyttäminen terveydenhuollossa; TSV 423/49/2009 Viranomainen ei saa asiakkaan suostumuksellakaan lähettää salassa pidettäviä asiakastietoja suojaamattomassa sähköpostissa; TSV 590/41/2012Asiakkaalle tarjottavista sähköisen asioinnin palveluista

ja uudemmat tapaukset liittyvätkin esimerkiksi sähköiseen ajanvaraukseen ja sähköiseen tunnistautumiseen.

Tietosuojavaltuutetun sosiaali- ja terveysalaa koskevat ratkaisut ovat jaoteltavissa *sisältönsä ja aihealueensa* mukaisesti karkeasti seuraaviin kokonaisuuksiin:

- Rekisterissä olevien henkilötietojen luovutus, siirto tai käyttöyhteyden antaminen tietoihin kolmannelle osapuolelle
- Kuka saa käsitellä tai kenellä voi olla pääsy sosiaali- ja terveydenhuollon arkaluonteisiin henkilötietoihin
- Mitä tietoja saa sosiaali- ja terveyshuollossa kerätä
- Tarkastusoikeuden käyttö omiin sosiaali- ja terveydenhuollon asiakas- ja potilastietoihin (kuka saa tarkastaa ja mihin tarkoitukseen tarkastusoikeutta käytetään)
- Tietojen poistaminen tai korjaaminen
- Tietoturvaloukkaus, jossa katosi, päätyi vääriin käsiin tai muuttui asiakkaiden tai potilaiden henkilötietoja
- Kysymyksiä siitä, kuka on, tai kuka saa olla, rekisterinpitäjä sosiaali- ja terveydenhuoltoon liittyville henkilötiedoille
- Uuden teknologian tai tekniikan käyttöönotto sosiaali- ja terveydenhuollon henkilötietojen käsittelyssä (Faksit, kameravalvonta, sähköposti, tekstiviestit, sähköinen ajanvaraus ja -tunnistautuminen, tietokoneavusteinen riskipotilaiden tunnistus)

Yllä olevassa jaottelussa korostuu henkilötietolain mukaisten tapausten jakautuminen, koska aineisto sisälsi niitä lukumäärällisesti enemmän. Tietosuoja-asetuksen mukaisten ratkaisujen aiheet ja sisältö tulevat sen sijaan esille jäljempänä tietosuojavaltuutetun korjaavien toimivaltuuksien käsittelyn yhteydessä.

4.1 Tietosuoja-asetuksen mukaiset tietosuojavaltuutetun ratkaisut

Ketä tietoturvaloukkaukset koskivat. Tietosuoja-asetuksen mukaisia tietosuojavaltuutetun ratkaisuja oli tarkastelussa yhteensä 20. Tapauksissa oli kyse joko yksittäisen rekisteröidyn oikeuksista tai useampaa rekisteröityä koskevasta tilanteesta. Yksittäisen rekisteröidyn tilanteesta, josta tämä oli kannellut tietosuojavaltuutetulle, oli kyse seitsemässä tapauksessa. Loput kolmetoista olivat tapauksia, joissa oli kyse joko useampaa rekisteröityä

koskevasta tietoturvaloukkauksesta, rekisterinpitäjän yleisestä toimintatavasta tai järjestelmästä, joka oli ollut tietosuoja-asetuksen vastainen ja jonka vaikutukset olivat kohdistuneet tai saattaneet kohdistua useampaan rekisteröityyn. Tapaukset jakaantuivat näissä kahdessa ryhmässä niin, että vain rekisteröidyn oikeus saada pääsy tietoihinsa maksutta, esiintyi molemmissa ryhmissä, eli se oli sekä yksittäisen rekisteröidyn kantelun aihe että tietosuojavaltuutetun laajempi valvonta asia, jossa se selvitti rekisterinpitäjän toimintatapaa

Miten vireille. Osa tapauksista oli tullut tietosuojavaltuutetun tietoon rekisterinpitäjän omasta ilmoituksesta, osa jonkin yksittäisen rekisteröidyn kantelun yhteydessä (esim. järjestelmällinen virheellinen toimintatapa tietojen luovuttamisessa vakuutusyhtiölle[173]). Myös rekisterinpitäjän ennakkokuulemispyynnön yhteydessä oli päädytty valvontaan.[174] Yhdessä tapauksessa oli tietosuojavaltuutetulle esitetty kysymys rekisterinpitäjästä ja käsittelijästä.[175] Kaikista tapauksista ei ilmennyt, mitä kautta tietosuojavaltuutettu oli saanut tiedon mahdollisesta tietosuojasäännösten vastaisesta toiminnasta.

4.1.1 Yksittäistä rekisteröityä koskevat tapaukset

Seitsemässä yksittäisen rekisteröidyn tapauksessa neljä koski rekisteröidyn 15 artiklan mukaista rekisteröidyn oikeutta tutustua tietoihinsa. Yksi koski tietojen luovutusta (terveystietojen luovutus kuljetuspalveluille, jossa rekisteröity pyysi tietosuojavaltuutettua antamaan määräyksen, jonka mukaan tietoja ei saa luovuttaa. Määräystä ei annettu, sillä tiedot olivat kuljetuspaleluja tarjoavalle välttämättömiä sen laissa säädetyn tehtävän toteuttamiseksi. Yksi koski tietojen minimointivelvollisuutta (optikkoliike). Ja yksi oikeutta tietojen poistoon.

Neljästä rekisteröidyn tarkastusoikeuteen liittyvästä tapauksesta yksi koski tilannetta, jossa kantelija pyysi saada tarkistaa itseään koskevia tietoja, toisen rekisteröidyn sosiaalihuollon asiakastiedoista. Tietosuojavaltuutettu ei antanut tapauksessa määräystä antaa pääsy tietoihin, koska se katsoi, että ”*sosiaalihuollon asiakkaan nimellä tallennetut tiedot koskevat*

[173] TSV 3096/161/21 Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi.
[174] ATSV 3895/83/22 Potilastietojen käsittely ennaltaehkäisyn ja ennakoinnin tarkoituksissa sekä automatisoidut yksittäispäätökset ja ATSV 6482/186/2020 Automatisoitujen yksittäispäätösten syntyminen ennakoivan terveydenhuollon työkalussa.
[175]TSV 5036/183/2019 Henkilötietojen rekisterinpitäjästä ja käsittelijästä. Tapauksessa kuntayhtymä, joka oli kehitysvammaisten erityishuoltoa koskevan lain (519/1977) 6 §:n 5 momentin mukainen erityishuollon kuntainliitto eli erityishuoltopiiri. Kuntayhtymä tuotti palveluja myös muille kuin jäsenkunnille ja se tiedusteli, milloin kuntayhtymä on rekisterinpitäjä ja milloin henkilötietojen käsittelijä.

kaikki sosiaalihuollon asiakasta, vaikka niissä kerrottaisiin muistakin henkilöistä". Kahdessa tapauksessa oli kyse siitä, että rekisteröity ei saanut pyytämiään itseään koskevia tietoja reksiterinpitäjältä ja yhdessä oli kyse siitä, että rekisteröidyltä oli peritty maksu röntgen- ja magneettikuvista, vaikka tietosuoja-asetuksen omien tietojen tarkastusoikeuden käytön tulisi olla rekisteröidylle 12(5) artiklan mukaan lähtökohtaisesti maksutonta.

Yksittäiseen rekisteröityyn kohdistuvista seitsemästä tapauksesta kolmessa ei ollut tietosuojavaltuutetun ratkaisun mukaan tapahtunut tietosuojasääntelyn rikkomusta (tarkastusoikeutta ei annettu toisen henkilön (lapsenlapsen) sosiaalihuollon tietoihin; tietoja sai luovuttaa kuljetuspalveluille kuljetusten järjestämisen mahdollistamiseksi; vanhemmalla, joka ei ollut lapsen laillinen edustaja, ei ollut oikeutta vaatia tietoja poistettavaksi).

4.1.2 Useampaa rekisteröityä koskevat tapaukset

Tietosuoja-asetuksen 4(12) artiklan mukaan henkilötietojen tietoturvaloukkauksena pidetään tietoturvaloukkausta, jossa tapahtuu siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen tuhoaminen, häviäminen, muuttuminen, luvaton luovuttaminen tai pääsy tietoihin, joko vahingossa tai lainvastaisesti.

Tällaisia henkilötietojen tietoturvaloukkauksia oli aineistossa yhteensä neljä ja ne kaikki liittyivät tapauksiin, jossa oli kyse useampaan rekisteröityyn kohdistuvasta tietoturvaloukkauksesta. Tunnetuin tietoturvaloukkauksista oli Psykoterapiakeskus Vastaamon tapaus, jossa yli 33 000 rekisteröidyn tiedot päätyivät kiristäjän haltuun. Kolme muuta tietoruvaloukkausta olivat Kelan asiakastietoja sisältävän postipaketin katoaminen (ei tietoa saiko joku ulkopuolinen paketin käsiinsä), rekisterinpitäjän käyttämän potilastietojärjestelmän ja Omakanta-palvelun välisessä tiedonsiirrossa tapahtunut ongelma, joka johti siihen, etteivät kaikki rekisteröidyt saaneet käyttöönsä koronarokotustodistusta (tietojen muuttuminen/eheys) sekä potilastietoja sisältäneen tietokoneen ja ulkoisen kiintolevyn päätyminen ulkopuoliselle.

Käsittelyn turvallisuuteen liittyi kolme tapausta, mihin sisältyy myös aiemmin mainitun läppärin ja kiintolevyn katoaminen, koska kyseisiä tietoja ei ollut salattu riittävällä tavalla ulkopuolisen pääsyltä. Kaksi muuta tapausta liittyivät asiakkaan tunnistamiseen sähköisessä ajanvarausjärjestelmässä (toisessa ajanvarausjärjestelmästä pystyi selvittämään henkilön henkilötunnuksen loppuosan, toisessa aikoja saattoi varata, vaikka henkilötunnus ja sukunimi eivät täsmänneet).

Kaksi tapausta liittyi tietojen automaattiseen käsittelyyn terveydenhuollon[176] ennakoivassa työkalussa ja rekisteröidyn oikeuteen olla joutumatta automaattisen päätöksenteon kohteeksi. Lisäksi näissä tapauksissa rekisterinpitäjä suunnitteli ennakoivaa työkalua, jolla se olisi käsitellyt pseudonymisoituja[177] tietoja ilman lakiin perustuvaa oikeutta käsitellä henkilötietoja. Molemmat tapaukset olivat tulleet tietosuojavaltuutetulle 36 artiklan mukaisina ennakkokuulemispyyntöinä, mutta olivat johtaneet myös kyseisiin valvontatoimiin. Työkalut eivät olleet vielä rekisterinpitäjillä käytössä.

Kahdessa tapauksessa oli kyse muun muassa tietojen minimointivelvollisuudesta. Näistä ensimmäisessä rekisterinpitäjällä oli menettelytapa, jossa se käytti rekisteröidyille lähetettäviä automatisoituja viestejä, joihin sisältyi tarpeettomasti henkilötunnus. Toisessa tapauksessa oli kyse rekisterinpitäjän yleisestä toimintatavasta antaa potilastietoja vakuutusyhtiölle seulomatta, jolloin myös se jätti noudattamatta tietojen minimointivaatimusta.

Loput kolme tapausta olivat yksittäisiä omissa ryhmissään. Yksi oli puhdas kysymys tietosuojavaltuutetulle rekisterinpitäjästä ja käsittelijästä (aiemmin selitetty tapaus kehitysvammaisten erityishuoltopiirin rekisterinpitäjästä). Toinen tapaus liittyi rekisterinpitäjän virheelliseen yleiseen toimintatapaan pyytä maksu magneettikuvien toimittamisesta potilaalle, mikäli tämä ei osannut yksilöidä tietopyyntöä tarkastusoikeuden käytöksi, vaan pyysi kuvia suoraan yksiköstä (ei kirjaamon kautta). Kolmas tapaus liittyi rekisterinpitäjän tietoturvatestiin, jonka väittämän mukaan henkilökunnalla olisi oikeus katsella hoitamansa potilaan tietoja hoitosuhteen päätyttyä saadakseen palautetta työnsä tuloksista.

4.1.3 Henkilötietolain mukaiset tapaukset

Henkilötietolain mukaisia tapauksia aineistossa oli yhteensä 41.[178] Nämä tapaukset poikkeavat kuitenkin paljon tietosuoja-asetuksen mukaisista päätöksistä, joten niissä ei ole samalla tavalla selkeää onko jokin tietoturvaloukkaus tapahtunut vai onko reksiterinpitäjä vain tiedustellut asiaa etukäteen. Tietosuojavaltuutettu ei myöskään kovin selkeästi ilmaise, mikä on ollut henkilötietolain vastaista kyseisessä menettelyssä, vaan antaa tapauksissa pääsääntöisesti yleisempää ohjausta.

[176] Huom. Hallintolain 8b luku Asian ratkaiseminen automaattisesti, tullut voimaan tämän tapauksen julkaisemisen jälkeen. Ks. lisää myös HE 145/2022.
[177] Henkilötietojen käsittelyä siten, ettei niitä voida enää yhdistää tiettyyn henkilöön ilman lisätietoja.
[178] Kaikki aineistona tarkastellut tapaukset löytyvät lähteistä otsikon henkilötietolain mukaiset tapaukset alta.

Henkilötietolain mukaisista tapauksista viidessä voi nähdä **hyvän tiedonhallintatavan rikkomista tai vaarantumista**. Tapaukset olivat kaikki keskenään hyvin erilaisia. Yhdessä tapauksessa oli kyse yksityisvastaanoton potilaskortiston siirtymisestä kuolinpesälle ja tietosuojavaltuutetulta kysyttiin, kuinka kortiston kanssa tulisi menetellä, että se olisi henkilötietolain mukaista. Tietosuojavaltuutettu totesi lainsäädännössä olevan aukon kyseisenlaisten tapausten kohdalla eikä sillä ollut toimivaltaa asiassa, jossa ei ollut (enää) rekisterinpitäjää.

Toinen tapaus koski lääkärihelikopteritoimijan oikeutta tallentaa arkaluonteisia henkilötietoja (oikeus tallentaa tietoja, kun on suostumus, tiedot ovat toiminnassa saatuja tai muita välttämättömiä tietoja). Kolmannessa tapauksessa oli kyse vastaanottotoimintansa siirtävien vuokrahammaslääkärien oikeudesta ottaa potilasrekisterinsä mukaansa (yksityinen ammatinharjoittaja on vastuussa potilasrekisteristään ja sen tulee sopia kirjallisesti rekisterinpidosta, jos se ei vastaa siitä kokonaan itse).

Neljäs tapaus koski lääkereseptien kopioimista ja tallentamista tietokantaan toimeentulotukihakemuksen yhteydestä (voi tallentaa, jos se katsotaan tarpeelliseksi tiedoksi tukea myöntäessä, Sosiaali- ja terveysministeriö (STM) määrittää tarpeellisuuden, jos pyydetään vain nähtäväksi, ei ollut silloin henkilötietojen käsittelyä ja tietosuojavaltuutetulla ei silloin toimivaltaa). Viidennessä tapauksessa oli kyse sairaaloiden tekemistä ilmoituksista Kelalle, kun niillä oli potilaana henkilöitä, jotka saivat Kelan hoitotukea (pyydettiin yhtenäistä ohjeistusta, koska tiedon saaminen sairaalassa monesti vaikeaa ja jotkut sairaalat tekivät Kelalle turhia ilmoituksia (eli ilmeisesti ilmoittivat henkilöistä, jotka eivät olleet tuensaajia) tietosuojavaltuutettu muistutti, että tiedon luovuttajan tulee varmistua, että sen saajalla on laillinen oikeus käsitellä tietoja).

Tapauksissa tietosuojavaltuutettu totesi rekisteröidyn kantelun olleen **aiheeton** kolmessa tapauksessa. Ensimmäinen oli tarkastusoikeuden rajoitustapaus, josta valitettu hallinto-oikeuteen. Hallinto-oikeus piti tietosuojavaltuutetun päätöksen voimassa, eikä henkilöllä ollut oikeutta tarkistaa lapsensa tiedoista itseään koskevia kohtia. Toisessa tapauksessa oli kyse siitä, että perhehoitosopimusta tehtäessä oli lain mukaista tarkistaa samassa taloudessa asuvan täysi-ikäisen pojan tiedot, ilman tämän suostumustakin, sillä tiedot olivat tarpeellisia perhekodin sopivuutta arvioitaessa. Kolmas tapaus koski potilasrekisteritietojen luovuttamista vakuutusyhtiölle kokonaisuudessaan. Tietosuojavaltuutetun mukaan tapauksessa oli ollut tarpeellista antaa laajemmin tietoa.

Suurin osa (yhteensä 28) henkilötietolain mukaisista tapauksista oli yleisempiä kysymyksiä, joissa ei ollut selvästi kyse yksittäisen rekisteröidyn kantelusta tai tapahtuneesta rikkomuksesta. Niissä pyydettiin ohjausta, tiedusteltiin oikeaa menettelytapaa erilaisissa tilanteissa, mutta niistä ei voi päätellä oliko kysymyksessä olevia tilanteita jo tapahtunut, vai oliko kyse asian tiedustelusta ennakolta.

Seuraavaksi tarkastellaan tapauksia siitä, näkökulmasta, että mikä hyvän tiedonkäsittelytavan näkökulmasta on joko epäonnistunut tai ollut vaarassa epäonnistua tai vaarantua tapauksissa, jotka tietosuojavaltuutetun toimisto on nähnyt tarpeelliseksi julkaista

4.2 Sosiaali- ja terveydenhuollon tietosuojarikkomukset

Edellä kuvatuissa tietosuoja-asetuksen mukaisissa päätöksissä hyvä tietosuoja vaarantui seuraavien tietosuoja-asetuksen artikloiden rikkomuksina tai laiminlyönteinä.

- Tietoturvaloukkaus (4(12) artikla)
    - Tietojen eheys
    - Tietojen häviäminen
    - Tietojen päätyminen ulkopuoliselle
- Henkilötietojen käsittelyä koskevat periaatteet
    - Lainmukaisuus, kohtuullisuus ja läpinäkyvyys 5(1)(a) artikla)
    - Tietojen minimointivelvollisuus (5(1)(c) artikla)
    - Eheys ja luottamuksellisuus 5(1)(f) artikla)
    - Osoitusvelvollisuus (5(2) artikla)
- Henkilötietojen käsittelyn lainmukaisuus (6 artikla)
    - (artikla 6(1) käsittelyperusteen puuttuminen)
- Rekisteröidyn informointi henkilötietorekisteristä ja rekisterinpitäjästä (artikla 13)
- Rekisteröidyn pääsy omiin tietoihin ei toteutunut (15 artikla)
    - maksuton oikeuksien käyttö, (15(3) artikla)
    - rekisteröityjen oikeuksien käyttämisen helpottaminen (12(2) artikla)
    - perustelut, miksi tietoja ei ole annettu (12(4) artikla)
    - rekisteröidyn oikeuksien toteuttamisen määräajat (12(3) artikla)
- Oikeus tietojen poistamiseen (17 artikla) "oikeus tulla unohdetuksi"

- Oikeus olla joutumatta automatisoidun päätöksenteon kohteeksi (artikla 22)[179]
- Riittämättömät tekniset ja organisatoriset toimet tietojen suojaamiseksi (24(1) artikla)
- Sisäänrakennettu ja oletusarvoinen tietosuoja (25 artikla)
- Käsittelyn turvallisuus (32 artikla)
- Tietoturvaloukkauksen dokumentointi (33(5) artikla)
- Ilmoitusvelvollisuus tietoturvaloukkauksesta tai -poikkeamasta
    - tietoturvaloukkauksen uhreille (34(1) artikla)
    - tietosuojavaltuutetulle (33(1) artikla)
- tietosuojaa koskeva vaikutustenarviointi (35 artikla)

Hyvän tietosuojan tai tietojenkäsittelytavan vaarantumistilanteet voi jaotella myös sen mukaan, missä vaiheessa henkilötietojenkäsittelyprosessia ne ovat tapahtuneet: toimintojen *1) suunnitteluvaiheessa* (teknisen työkalun suunnitelmassa ei tunnistettu käsittelyperusteen puuttumista ja ryhmää, joka joutuisi automaattisen päätöksen teon kohteeksi tietämättään ja ilman suostumusta, Vastaamon riittämättömät tietoturvaratkaisut ja suojausmekanismit, ajanvarausjärjestelmän haavoittuvuus jäi tunnistamatta suunnitteluvaiheessa) *2) toiminta-vaiheessa* (tietoja katosi Kelan paketin mukana, rekisteröity ei saanut pyytämiään tietoja maksutta, potilastietoja luovutettiin vakuutusyhtiölle seulomatta, tekstiviesteissä tarpeettomasti henkilötunnus) vai *3) jälkiseuraamusten minimoinnissa* (ilmoittaminen tietoturvaloukkauksesta rekisteröidylle ja/tai tietosuojavaltuutetulle).

Oliko kyseessä *ihmisten tekemä virhe* (työntekijä jätti tietokoneen ja ulkoisen kiintolevyn paikkaan, josta se varastettiin, rekisterinpitäjän tietoturvatestissä virheellistä tietoa, päätettiin periä virheellisesti maksu röntgen kuvista tai rekisterinpitäjä ei luovuttanut pyydettyjä tietoja) vai *ohjelmiston virhe* (koronarokotetodistusten tekninen eheys) vai jokin *näiden yhdistelmä* (Vastaamossa tietoturva oli puutteellista, mutta se johtui siitä, ettei sitä ollut tehty huolella).

Huomioita tukee Saarenpään ja Riekkisen käsitys siitä, että henkilötietoja käsiteltäessä on useita erilaisia tilanteita, joissa tietosuoja voi vaarantua: laitteissa voi olla haavoittuvuuksia, ohjelmistoissa voi olla heikkoja ominaisuuksia, viestinnän muiden osapuolten toiminta voi vaarantaa tietosuojan, viranomaisilla voi olla puutteellinen asiantuntemus, näiden lisäksi

[179] Huom. Hallintolain 8b luku tullut voimaan tapauksen julkaisemisen jälkeen.

myös verkkoliikenteen valvonta ja oma osaamattomuus ovat keskeisimpiä riskejä.[180] Ei siis aina ole kyse siitä, että sosiaali- ja terveydenhuollon työtä tekevät ammattilaiset tekisivät virheitä, vaan niitä voi tapahtua jo suunnittelu vaiheessa.

4.3 Tietosuojavaltuutetun antama ohjaus

Tietosuojavaltuutetun antama ohjaus jakautui aineistossa selkeästi tietosuoja-asetuksen mukaisten ja henkilötietolain mukaisten tapausten välillä. Selkeimmin tietosuojavaltuutetun ohjaus näkyi vanhan henkilötietolain mukaisissa tapauksissa, jolloin suuri osa tapauksista oli tietosuojavaltuutetulle osoitettuja kysymyksiä ja tiedusteluja oikeasta toimintatavasta tai laintulkinnasta tietynlaisessa tilanteessa ja tietosuojavaltuutetun antamia vastauksia kysymyksiin. Tietosuojavaltuutetulta kysyttiin muun muassa siitä kuka missäkin tapauksessa on rekisterinpitäjä (kehitysvammaisten erityishuoltopiiriä koskeva tiedustelu) tai kenelle voi antaa pääsy- tai lukuoikeuden rekisterinpitäjän rekisteriin (esim. sosiaalityössä). Vaikka ohjausta oli määrällisesti enemmän henkilötietolain mukaisissa tapauksissa, seuraavaksi keskitytään pääasiassa tietosuoja-asetuksen mukaisiin tapauksiin.

Henkilötietolain mukaisissa tapauksissa tietosuojavaltuutetun antama ohjaus oli kantaaottavampaa ja vastasi yleensä esitettyyn kysymykseen tietynlaisesta tilanteesta. Tapaukset olivat myös useammin tulleet vireille rekisterinpitäjän aloitteesta ja yleensä nimenomaan kysymyksestä. Tietosuoja-asetuksen mukaisissa ratkaisuissa oli pääosin kyse joko rekisteröidyn kantelusta tietosuojavaltuutetulle omassa tapauksessaan tai tapauksen tutkiminen tietosuojavaltuutetun omasta aloitteesta (esim. koronarokotustodistuksien käytettävyys). Vain yksi tietosuoja-asetuksen mukainen tapaus koski rekisterinpitäjän esittämää kysymystä (kysymys kehitysvammahuollon erityishuoltopiiristä ja rekisterinpitäjästä. Kyseinen ratkaisu on annettu 2.9.2019, joten on mahdollista, että kysymys on esitetty henkilötietolain voimassaolon aikana, vireilletulo aika ei kuitenkaan näy julkaistuista ratkaisuista. Tapaus sopii kuitenkin profiililtaan hyvin henkilötietolain mukaisiin tapauksiin).

Mitä tietosuoja-asetuksen artiklaa on rikottu. Tietosuojavaltuutetun päätöksissä selkein ohjaus sosiaali- ja terveydenhuollon rekisterinpitäjille on ollut valvontapäätöksen perusteena oleva tietosuojavaltuutetun ilmoitus siitä, minkä tietosuoja-asetuksen artiklan rikkomisesta

[180] Saarenpää ja Riekkinen 2023, s. 208.

tai laiminlyönnistä rekisterinpitäjän toiminnassa on ollut kyse. Koska tapaukset ovat yksittäiseen reksiterinpitäjään kohdistuvia hallinnollisia päätöksiä, niiden tulee perustua lakiin ja sen vuoksi rikotun artiklan tai pykälän ilmoittaminen ei ole pelkkää ohjausta kyseiselle rekisterinpitäjälle, mutta niille rekisterinpitäjille tai rekisteröidyille, jotka voivat kohdata samankaltaisia tilanteita, rikotun säännöksen nimeäminen toimii myös ohjauksena. Esimerkiksi tapauksessa TSV 3096/161/21 Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi, tietosuojavaltuutettu ilmoittaa, että rekisterinpitäjä ei ole huomioinut tietosuoja-asetuksen ”*tietojen rajausvaatimuksia, eikä rekisterinpitäjän toimintatapa ole yleisen tietosuoja-asetuksen 5(1)(c) artiklan ja 25(2) artiklan mukainen*”. Sen artiklan nimeäminen, jota rekisterinpitäjän toiminta ei ole noudattanut, on siis lähtökohtaisesti tapauksissa toimivaltuuksien käytön peruste, mutta julkaistussa tapauksessa sillä voidaan nähdä myös ohjauksellista merkitystä. Tapauksissa oli eroavaisuuksia siinä, miten tietosuojavaltuutetun 58(2)(d) artiklan mukainen määräys saattaa *käsittelytoimet tietosuoja-asetuksen mukaisiksi* oli muotoiltu. Osassa tapauksista oli kerrottu nimenomaiset artiklat, joiden mukaiseksi toimet pitäisi saattaa, osassa vain yleisesti muotoiltu ”tietosuoja-asetuksen mukaisiksi”.

Ohjaukseksi kutsuttu ohjaus. Tarkastelun kohteena olleissa tietosuoja-asetuksen mukaisissa tapauksissa vain kolmessa oli selvästi eroteltuna oman väliotsikon alle tietosuojavaltuutetun antama ohjaus.[181] Näissä tapauksissa tietosuojavaltuutettu antoi ohjausta, joka sisälsi suosituksia tai esimerkkejä teknisistä tai organisatorisista toimista (mm. ottaa käyttöön vahva tunnistautuminen ajanvarausjärjestelmässä; rajata henkilötunnuksen käyttöä tekstiviesteissä; käytäntö, jonka mukaan potilastiedot saisi vain kerran vuodessa maksutta oli perustunut henkilötietolain aikaiseen käytäntöön). Yhdessä tapauksessa oli kyseessä tiedustelu ja tietosuojavaltuutetun vastaus siihen[182], mikä käytännössä oli kokonaisuutenaan rekisterinpitäjälle annettua neuvontaa. Lisäksi valvonta-asiaksi muuttuneesta ennakkokuulemisasian yhteydessä[183] apulaistietosuojavaltuutettu antoi samalla kirjallisia neuvoja ennakkokuulemispyynnön perusteella (mm. rekisterinpitäjän mahdollisuudesta saada peruste henkilötie-

[181] ATSV/29/2020 Henkilötunnuksen sisältävien automatisoitujen tekstiviestien lähetys terveydenhuollossa, ATSV 6629/163/21 Oikeus tutustua magneettikuviin maksutta ja ATSV 5546/163/2019 Henkilötietojen käsittelyn turvallisuus ajanvarausjärjestelmässä.
[182] TSV 5036/183/2019 Henkilötietojen rekisterinpitäjästä ja käsittelijästä
[183] ATSV 3895/83/22 Potilastietojen käsittely ennaltaehkäisyn ja ennakoinnin tarkoituksissa sekä automatisoidut yksittäispäätökset.

tojen käsittelylle pyytämällä rekisteröidyiltä suostumusta prosessin aikaisemmassa vaiheessa tai arvioimalla käsittelyn perustumista muuhun lainsäädäntöön kuten sosiaali- ja terveystietojen toissijaisesta käsittelystä annetun lain (552/2019) 37 §:n).

Konkreettisia toimintatapaehdotuksia. Tietosuojavaltuutettu antoi myös muutamissa tapauksissa rekisterinpitäjälle esimerkkejä toimintavaihtoehdoista, jotka olisivat tapauksessa lainmukaisia. Tapauksessa ATSV 29/2020 oli kyse hyvinvointialueen toimintatavasta lähettää potilaille tekstiviestejä, jotka sisälsivät potilaan henkilötunnuksen sekä tietoja laboratoriotutkimuksista. Apulaistietotuojavaltuutettu antoi päätöksen lopussa ohjausta, jossa se ohjeisti hyvinvointialuetta esimerkiksi rajaamaan tekstiviesteihin sisältyviä henkilötietoja ja antoi esimerkin mahdollisesta tavasta ilmoittaa rekisteröidylle epäonnistuneesta laboratoriotutkimuksesta (asia muotoillaan yleisellä tasolla ja siihen lisätään kehotus ottaa yhteyttä laboratorioon). Lisäksi tietosuojavaltuutettu ohjeisti hyvinvointialuetta arvioimaan muita vaihtoehtoisia tapoja rekisteröidyille tiedottamisessa. Myös tapauksessa, jossa rekisterinpitäjä oli luovuttanut vakuutusyhtiölle potilastietoja seulomatta, tietosuojavaltuutettu ohjasi rekisterinpitäjää jatkossa toimittamaan potilastiedot lausunnon muodossa, toissijaisesti peittämällä tarpeettomat tiedot potilasasiakirjoista ja vain poikkeustapauksissa luovuttamaan potilastiedot kokonaisuudessaan tietyltä aikaväliltä.

Tietosuojavaltuutettu antoi ohjausta myös tapauksissa, joissa rekisterinpitäjä oli soveltanut **virheellistä tai vanhentunutta ohjetta** tai sillä oli virheellinen säännönmukainen käytäntö. Tapauksessa TSV 3096/161/21 (Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi), rekisterinpitäjä vetosi liikennevakuutuslain (279/1959) 21 a §:ään, joka oli voimassa tapahtuma-ajankohtana, mutta kumottu 1.1.2017 alkaen. Tapauksessa se oli huomioitava koska kyse oli rekisteripitäjän edelleen jatkuvasta järjestelmällisestä toimintatavasta. Virheellisestä ja vanhentuneesta ohjeistuksesta oli kyse tapauksissa ATSV 6745/163/18 Potilastietojen käsittely ammatillista kehittymistä varten hoitosuhteen päätyttyä, jossa rekisterinpitäjän toiminta oli perustunut tietosuojavaltuutetun lausuntoon vuodelta 2011 (tapauksen diaarinumero ei ole tiedossa), mutta joka ei enää ollut ajan tasalla tietosuojalainsäädännön muutosten jälkeen. Myös tapauksessa ATSV 6132/151/19 Potilaan tarkastusoikeuden toteuttaminen terveydenhuollossa röntgen- ja magneettikuvien osalta, reksiterinpitäjä oli perustanut toimintansa tietotuojavaltuutetun aiempaan lausuntoon (Dnro 2546/41/2008), joka sekin perustui kyseisenä ajankohtana jo kumotun henkilötietolain tulkintaan.

Viittaaminen suosituksiin ja ohjeisiin. Tietosuojavaltuutettu antoi tapauksissa myös käytännönläheisempiä ohjeita rekisterinpitäjille viittaamalla erilaisiin suosituksiin tai toisten viranomaisten antamiin ohjeisiin. Aiemmin kuvatussa potilastietojen luovuttamisessa vakuutusyhtiölle, ohjeistus antaa tiedot lausuntomuodossa, oli viittaus Lääkäriliiton suositukseen, jossa potilastietojen luovuttamisesta vakuutusyhtiölle ohjeistetaan luovuttamaan potilaan terveydentilaa koskevat tiedot lausunnon muodossa, *ellei erityislainsäädännössä erikseen ole menettelystä toisin säädetty*. Myös sähköisen tunnistautumisen yhteydessä erikseen antamassaan ohjauksessa tietosuojavaltuutettu oli viitannut Sosiaali- ja terveysalan lupa- ja valvontaviraston ja Asiakas- ja potilasturvallisuuskeskuksen ohjeisiin vahvasta tunnistamisesta etäpalveluissa luotettavana pidettävänä tunnistamisena sekä Digi- ja väestöviraston suositukseen (annettu 2.11.2020).

Tietoteknistä ohjausta. Tietosuojavaltuutettu oli aineiston mukaan antanut myös teknisempää ohjausta kuvaamalla sähköpostiviestien ja tekstiviestien salausta tai liikkumista tietoverkoissa salaamattomina. [184] Toisessa tapauksessa, jossa potilastietoja sisältävä tietokonesalkku oli varastettu, tietosuojavaltuutettu kuvasi millaisia keinoja ulkopuolisella voi olla päästä käsiksi salaamattomiin tietoihin, jos tietokone tai ulkoinen kiintolevy joutuu ulkopuolisen käsiin.[185] Samassa tapauksessa tietosuojavaltuutettu ohjeisti, että paperisia potilasasiakirjoja ei tulisi viedä ulkotiloihin ilman asianmukaista suojausta ja valvontaa.

Ohjausta valvontaprosessin aikana. Muutamassa tapauksessa tietosuojavaltuutettu mainitsi päätöksessään antaneensa rekisterinpitäjälle ohjausta jo valvontaprosessin aikana. Esimerkiksi tapauksessa ATSV 3/2019 (Henkilön tunnistaminen terveydenhuollon sähköisessä ajanvarausjärjestelmässä) tietosuojavaltuutettu oli selvityspyynnön yhteydessä antanut ohjausta tietosuoja-asetuksen 32 artiklasta sekä antanut rekisterinpitäjälle tiedoksi apulaistietosuojavaltuutetun päätöksen toisesta vastaavasta tapauksesta, joka liittyi verkkoajanvarausjärjestelmään. Kahdessa muussa tapauksessa ohjausta oli annettu kesken prosessin ja siihen

---

[184] ATSV/29/2020 Henkilötunnuksen sisältävien automatisoitujen tekstiviestien lähetys. Päätöksessä olevaa yleistä ohjausta: "*SMS-viestien sisältöä ei suojata välityksen aikana esimerkiksi salakirjoituksella muutoin kuin mobiililaitteen ja matkapuhelinverkon tukiaseman välisen radioliikenteen osalta. SMS-viestijärjestelmä (SS7) ei tarjoa edellytyksiä viestisisällön tai viestin välitystietojen salaamiselle*." ja 1475/41/2009 ja 590/41/2012.

[185] 4022/171/22 Arkaluonteisten henkilötietojen asianmukainen suojaaminen ja henkilötietojen turvallinen käsittely. Päätöksestä: "*Erillisen käynnistysmedian ja yleisesti saatavilla olevien ohjelmistojen avulla on myös mahdollista nollata Windows-käyttäjän salasana ja kirjautua tämän jälkeen Windowsiin normaalisti. Vaihtoehtoisesti massamuisti voidaan siirtää toiseen laitteeseen ja lukea tiedot tällä toisella laitteella. Näin ollen rekisterinpitäjän käyttämä pelkkä salasanasuojaus on ollut selkeästi puutteellinen keino suojata tietokoneelle tallennettuja rekisteröityjen henkilötietoja*."

viitattiin päätöksessä lähinnä raskauttavana tekijänä hallinnollisen seuraamusmaksun perusteluissa, koska rekisterinpitäjä ei ollut ohjauksesta huolimatta korjannut toimintaansa riittävästi.[186]

Hyvät ja huonot esimerkit: Tietosuojavaltuutetun päätöksien ohjausvaikutusta voi tarkastella myös kiinnittämällä huomiota päätökseen kokonaisuutena. Tapauksista nousi muutama esimerkki sekä hyvin hoidetusta tilanteesta tietoturvaloukkauksen tapahtumisen jälkeen että suhtautumisesta, joka vaikutti piittaamattomalta. Vaikka näissä osittain hyvin hoidetuissakin tapauksissa oli siis tapahtunut tietosuojaloukkaus ja niissäkin oli myös parantamisen varaa, tapauksissa TSV 2691/171/19 (Kelan kadonnut postipaketti) ja ATSV 6602/161/2021 (virhe koronarokotustodistusten käytettävyydessä), tuli ilmi useita rekisterinpitäjien oikeita toimia vaikutusten minimoimiseksi kuten tiedottaminen rekisteröidyille, joita loukkaus koski, vaihtoehtoisten tapojen valmistelua ja oma-aloitteista ilmoittamista tietosuojavaltuutetulle. Varoittavina esimerkkeinä puolestaan voi aineistosta nostaa kaksi tapausta, joissa voi nähdä kuvauksen siitä, miten ei pitäisi toimia. Tällaisia tapauksia ovat Vastaamon tietoturvan laiminlyöntiin liittyvä tapaus ATSV 1150/161/2021 sekä lääkäriklinikan (kauneuskirurgia) ATSV 8493/161/21 toiminta tietojen tarkastuspyynnön yhteydessä. Vastaamon tapauksessa henkilötietojen tietoturvallisuus oli laiminlyöty ja sen seurauksena tapahtui vakava tietomurto, josta Vastaamo ei ilmoittanut rekisteröidyille eikä tietosuojavaltuutetulle määräaikojen puitteissa. Toisessa tapauksessa oli kyse tilanteesta, jossa rekisteröity ei saanut lääkäriklinikalta tarkistettavaksi itseään koskevia tietojaan useista yrityksistä huolimatta, rekisterinpitäjä ei vastannut tietosuojavaltuutetun selvityspyyntöihin toistuvista puheluista ja sähköposteista huolimatta ja rekisterinpitäjä ei ollut informoinut asiakkaitaan rekisterinpitämisestään. Kyseiset tapaukset ovat monivaiheisia ja niiden ohjausvaikutus kohdistuu sekä muihin rekisteripitäjiin että rekisteröityihin.

Ei tietosuojavaltuutetun toimialaan kuuluva. Vanhemmissa henkilötietolain mukaisissa tapauksissa tietosuojavaltuutettu joutui toisinaan ilmoittamaan asian vireille saattajalle, että tietosuojavaltuutettu ei ole tapauksessa toimivaltainen ja ohjasi tiedustelun toimivaltaiselle viranomaiselle. Esimerkiksi kuolinpesään kuuluvan henkilötietorekisterin säilyttämiseen liittyvässä tapauksessa tietosuojavaltuutettu myös ilmoitti tiedottaneensa Sosiaali- ja terveysministeriötä kyseessä olevasta asiasta, jonka oikeustilassa vaikutti olevan aukkoja.

[186] ATSV 9707/152/19 Rekisteröidyn oikeus tutustua tietoihinsa ja oikeuden puutteellinen toteutus ja ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä.

Myös henkilötietolain mukaisissa kameravalvontaan liittyvissä tapauksissa tietosuojavaltuutettu ei ollut toimivaltainen ottamaan kantaa kaikkiin kysyttyihin asioihin.[187]

4.4 Artiklan 58(2) mukaisten toimivaltuuksien käyttö

Tietosuojavaltuutettu on edellä kuvatun ohjauksen ja neuvonnan lisäksi kohdistanut vuosien 2018–2024 aikana sosiaali- ja terveydenhuollon rekisterinpitäjiin myös sille tietosuoja-asetuksen 58 artiklan 2 kohdassa säädettyjä korjaavia toimivaltuuksia. Kuten jo edellä on kerrottu korjaavia toimivaltuuksia ovat varoitus, huomautus, erilaiset määräykset, henkilötietojen käsittelyn rajoittaminen tai käsittelykiellon antaminen, sertifioinnin peruuttaminen tai määräyksen antaminen sertifiointielimelle sekä määräys tiedonsiirtojen keskeyttämisestä kolmanteen maahan tai kansainväliselle järjestölle. Näiden lisäksi tietosuojavaltuutettu voi määrätä myös hallinnollisen seuraamusmaksun muiden korjaavien toimenpiteiden lisäksi tai niiden sijasta.

Tietosuojavaltuutettu on julkaissut tietosuoja-asetuksen soveltamisen aloittamisen jälkeen (2018) Finlexissä yhteensä **20** sosiaali- ja terveysalaan[188] liittyvää tapausta, jotka kuuluvat tämän tutkielman aineistoon. Tietosuoja-asetuksen 58 artiklan 2 kohdan mukaisia toimivaltuuksia tietosuojavaltuutettu on käyttänyt näistä yhteensä **16** tapauksessa. Neljässä tapauksessa tietosuojavaltuutettu ei käyttänyt mitään korjaavaa toimivaltuutta.

Ei käytetty korjaavia toimivaltuuksia. Niistä neljästä tapauksesta, joissa toimivaltuuksia ei käytetty, kahdessa rekisteröity pyysi tietosuojavaltuutettua antamaan reksisterinpitäjälle määräyksen noudattaa rekisteröidyn pyyntöä päästä käsiksi tietoihinsa (alakohta c). Kummassakaan tapauksessa hakijalla ei ollut lainmukaista oikeutta saada pyytämiään tietoja (tapauksissa toisessa kyseessä rekisteröidyn isoäiti ja toisessa henkilö, joka ei ollut lapsen laillinen edustaja, edunvalvoja tai huoltaja)[189]. Kolmannessa tapauksessa oli kyse yleisestä tiedustelusta rekisterinpitäjästä ja henkilötietojen käsittelijästä[190] ja neljännessä tapauksessa

[187] TSV 702/49/2004 Kameravalvonta nuorisokodissa; TSV 1357/41/2010 Kotihoidon kameravalvonta; TSV 539/451/2011 Kameravalvonta perhekodissa.
[188] Tapauksista neljä kohdistuu sosiaalialan ja loput 16 terveysalan rekisterinpitäjiin.
[189] ATSV 9492/153/22 Rekisteröidyn oikeuksien käyttäminen alaikäisen lapsen puolesta ja TSV 28/523/2018 Jäljennösten saaminen sosiaalihuollon asiakastiedoista
[190] TSV 5036/183/2019 Kysyjän oli kehitysvammaisten erityishuoltoa järjestävä kuntayhtymä, joka toimi erityishuoltopiirinä ja se tiedusteli tietosuojavaltuutetulta, milloin kyseinen kuntayhtymä on rekisterinpitäjä ja milloin henkilötietojen käsittelijä, kun se tuottaa palveluja muille jäsenkunnille sekä sosiaalihuoltolain (1301/2014) että kehitysvammaisten erityishuollosta annetun lain (519/1977) mukaan. Tietosuojavaltuutetun vastauksen mukaan kuntayhtymä oli rekisterinpitäjä silloin kun se oli lain mukaan järjestämisvastuussa palve-

hakija pyysi tietosuojavaltuutettua antamaan määräyksen, jolla kiellettäisiin rekisterinpitäjää luovuttamasta tietoja terveydenhuollon kuljetusyritykselle ja käyttämästä automaattista profilointia. Tietosuojavaltuutetun ratkaisun mukaan kyseisessä kuljetuspalvelun toteuttamisessa asiakastietojen käsittely ei ollut automaattista päätöksentekoa ja lisäksi tietojen käsittely oli tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi, joten hakijalla ei ollut tapauksessa tietojen käsittelyn vastustamis- tai rajoittamisoikeutta.[191]

4.4.1 Mitä korjaavia toimivaltuuksia on käytetty

Tapauksissa, joissa tietosuojavaltuutettu oli käyttänyt tietosuoja-asetuksen 58 artiklan 2 kohdan mukaisia korjaavia toimivaltuuksiaan kahdestatoista tapauksesta **yhdeksässä** oli käytetty vain yhtä korjaavaa toimivaltuutta ja **seitsemässä** tapauksessa oli käytetty useampaa kuin yhtä. Useimmiten tietosuojavaltuutettu oli käyttänyt yhtä aikaa kahta korjaavaa toimivaltuutta (kuudessa tapauksessa) ja yhdessä tapauksessa yhteensä neljää eri toimivaltuutta samanaikaisesti[192]. Korjaavien toimivaltuuksien määrät aineistoon kuuluvissa tapauksissa on esitetty taulukossa 2.

4.4.2 Millaisissa tapauksissa toimivaltuuksia on käytetty

Kaikki aineistoon kuuluvat tietosuojavaltuutetun tietosuoja-asetuksen mukaiset päätökset ja niissä käytetyt toimivaltuudet löytyvät Liitteessä 1 olevassa taulukossa. Tapaukset ovat taulukossa julkaisuajan kohdan mukaisessa järjestyksessä. Seuraavalla sivulla olevassa Taulukossa 2. on esitetty korjaavat toimivaltuudet ja niiden esiintyvyys aineistossa yksin käytettynä toimivaltuutena, jonkin toisen toimivaltuuden kanssa käytettyinä sekä lukumäärät yhteensä.

Seuraavan sivun taulukon (Taulukko 2) jälkeen tarkastellaan lyhyesti tapauksia, joissa tietosuojavaltuutettu oli käyttänyt 58(2) artiklan mukaisia korjaavia toimivaltuuksia. Toimivaltuudet käydään läpi siinä järjestyksessä, miten usein niitä aineiston tapauksissa käytettiin.

---

luista ja käsittelijä, silloin kun sen tuottamien palvelujen järjestämisvastuu oli palvelun ostaneen kunnan sosiaaliviranomaisella. Huomaa lisäksi, että asia oli todennäköisesti tullut vireille henkilötietolain voimassaolon aikana ja siksi tapaus muistuttaa enemmän vanhempia tapauksia kuin muut tietosuoja-asetuksen mukaiset ratkaisut.

[191] TSV 5242/157/2018 Tietojen luovuttaminen sosiaali- ja terveydenhuollosta kuljetuspalveluille kuljetusten järjestämistä varten.

[192] ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä.

TSA 58(2) artiklan mukainen korjaava toimivaltuus	Annettu yksistään	Annettu yhteydessä jonkin toisen kanssa	Yhteensä
a) varoitus, että aiotut käsittelytoimet ovat todennäköisesti tietosuoja-asetuksen vastaisia	2	0	2
b) huomautus, että käsittelytoimet ovat olleet tietosuoja-asetuksen vastaisia	3	6	9
c) määräys noudattaa rekisteröidyn pyyntöä	0	3	3
d) määräys saattaa käsittelytoimet tietosuoja-asetuksen mukaisiksi	3	4	7
e) määräys ilmoittaa rekisteröidylle tietoturvaloukkauksesta	1	0	1
f) väliaikainen tai pysyvä rajoitus henkilötietojen käsittelylle	0	0	0
g) määräys tietojen oikaisuun tai poistamiseen	0	0	0
h) sertifioinnin peruuttaminen	0	0	0
i) hallinnollinen sakko	0	3	3
j) määräys keskeyttää tietojen siirto	0	0	0
Toimivaltuuksia ei käytetty lainkaan	4	-	4

Taulukko 2. Tietosuojavaltuutetun tietosuoja-asetuksen 58 artiklan 2 kohdan mukaisten korjaavien toimivaltuuksien käyttö sosiaali- ja terveydenhuollon rekisterinpitäjiin.

B) huomautus. Tietosuojavaltuutettu oli useimmin käyttänyt tietosuoja-asetuksen 58(2)(b) artiklan mukaista toimivaltuutta antaa rekisterinpitäjälle (tai henkilötietojen käsittelijälle)

huomautus siitä, että henkilötietojen käsittely on ollut tietosuoja-asetuksen vastaista. Artiklan mukainen huomautus oli annettu yhteensä yhdeksässä päätöksessä, joista kolmessa huomautus oli ainut käytetty toimivaltuus. Huomautuksia tietosuojavaltuutettu oli antanut sekä ainoana seuraamuksena että yhdessä muiden artiklan mukaisten toimivaltuuksien kanssa.

Huomautus tietosuoja-asetuksen vastaisesta henkilötietojen käsittelystä seuraavissa tapauksissa:

- ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä
- ATSV 1150/161/2021 Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen (Vastaamo)
- ATSV 9707/152/19 Rekisteröidyn oikeus tutustua tietoihinsa ja oikeuden puutteellinen toteutus
- ATSV 6629/163/21 Oikeus tutustua magneettikuviin maksutta
- TSV 3096/161/21 Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi
- TSV 8235/154/18 Asiakkaan pyyntö henkilötietojen poistosta ja henkilötietojen käsittelyperuste
- ATSV 4022/171/22 Arkaluonteisten henkilötietojen asianmukainen suojaaminen ja henkilötietojen turvallinen käsittely
- ATSV 6602/161/2021 Koronarokotustietojen käytettävyys ja tietoturvaloukkauksesta ilmoittaminen
- ATSV 5546/163/2019 Henkilötietojen käsittelyn turvallisuus ajanvarausjärjestelmässä

Huomautukseen johtivat vakavuusasteeltaan hyvin erilaiset tilanteet kuten tilanne, jossa rekisteröidyille ei tiedotettu siitä, että heidän koronarokotustodistuksensa olivat hetken aikaa teknisesti toimimattomia ja toisena ääripäänä Psykoterapiakeskus Vastaamon erittäin vakava tietoturvan laiminlyönti ja tietomurto, johon myös liittyi rekisteröidyille tiedottaminen tapahtuneesta tietosuojaloukkauksesta. Alla kuvatussa tapauksessa tietosuojavaltuutettu taas antoi rekisterinpitäjälle b kohdan mukaisen huomautuksen, mutta ei käyttänyt muita toimivaltuuksia.

ATSV 4022/171/22 Arkaluonteisten henkilötietojen asianmukainen suojaaminen ja henkilötietojen turvallinen käsittely

Tapauksessa rekisterinpitäjä oli jättänyt tietokonelaukun ulkotilassa ilman valvontaa, jolloin laukku ja sen sisältö: kannettava tietokone, kaksi ulkoista kiintolevyä sekä henkilötietojasisältäviä paperiasiakirjoja, oli varastettu. Apulaistietosuojavaltuutettu huomautti, että paperiasiakirjoja ei tulisi viedä ulkotiloihin ilman asianmukaista suojaamista ja valvontaa. Tapauksen henkilötiedot olivat terveystietoja, jotka kuuluvat erityisiin henkilötietoryhmiin ja joita rekisterinpitäjän olisi tullut suojata erityisen hyvin. Varastettu tietokone oli suljettu ja sen sai auki salasanalla. Tietokoneen massamuisti tai sen sisältämät henkilötiedot eivät olleet salattuja. Apulaistietosuojavaltuu-

tetun mukaan sisäänkirjautumisen vahvakaan salasana ei yksin estä pääsyä salaamattomiin tietoihin, jos sivullisella on fyysinen pääsy laitteelle. Tietokoneen fyysinen hallinta mahdollistaa pääsyn salaamattomiin tietoihin usein eri tavoin. Tietokoneelle tallennettujen rekisteröityjen henkilötietojen salaamiseksi pelkkä salasanasuojaus oli ollut selkeästi puutteellinen keino. Koska myöskään ulkoisten kiintolevyjen tiedot eivät olleet salattuja, henkilötietojen suojaus oli niidenkin osalta *selkeästi* puutteellinen. Apulaistietosuojavaltuutetun mukaan rekisterinpitäjän menettely oli ollut tietosuoja-asetuksen 32 artiklan 1 ja 2 kohtien vastaista.[193] Apulaistietosuojavaltuutettu antoi rekisterinpitäjälle 58 artiklan 2 kohdan b-alakohdan mukainen huomautuksen tietosuoja-asetuksen säännösten vastaisista henkilötietojen käsittelytoimista.

D) määräys. Seuraavaksi eniten (yhteensä **7** tapausta) tietosuojavaltuutettu oli antanut rekisterinpitäjälle d-alakohdan mukaisen määräyksen saattaa henkilötietojen käsittely tietosuoja-asetuksen mukaiseksi. Kyseinen määräys annettiin seuraavissa tapauksissa:

- ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä
- ATSV 6629/163/21 Oikeus tutustua magneettikuviin maksutta
- ATSV 6132/151/19 Potilaan tarkastusoikeuden toteuttaminen terveydenhuollossa röntgen- ja magneettikuvien osalta
- TSV 3096/161/21 Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi
- ATSV /29/2020 Henkilötunnuksen sisältävien automatisoitujen tekstiviestien lähetys terveydenhuollossa
- ATSV /3/2019 Henkilön tunnistaminen terveydenhuollon sähköisessä ajanvarausjärjestelmässä
- ATSV 6745/163/18 Potilastietojen käsittely ammatillista kehittymistä varten hoitosuhteen päätyttyä

Tapauksissa oli rikottu tai laiminlyöty rekisteröidyn tarkastusoikeuden käyttämiseen liittyviä oikeutta saada jäljennös itseä koskevista tiedoista, oikeutta saada jäljennös lähtökohtaisesti maksutta (röntgen ja magneettikuvat) sekä rekisterinpitäjän velvollisuutta helpottaa rekisteröidyn oikeuksien käyttöä (informointi tarkastusoikeuden lähtökohtaisesta maksuttomuudesta). Lisäksi tapauksissa oli laiminlyöty tietojen minimointivelvollisuutta käyttämällä automaattisesti lähetetyissä tekstiviesteissä tarpeettomasti henkilötunnuksia. Määräys oli annettu myös rekisterinpitäjälle tarkistaa potilastietojen käsittely vastaamaan tietosuoja-asetuksen artiklan 5(1)(b) mukaista käyttö-tarkoitussidonnaisuuden periaatetta tapauksessa, jossa rekisterinpitäjä piti lainmukaisena oikeutta katsoa ammatillisen kehittymisen tarkoi-

[193] Tietosuoja-asetuksen 32 artiklassa säädetään henkilötietojen käsittelyn tuvallisuudesta ja sen mukaan rekisterinpitäjän tulee toteuttaa riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, esimerkiksi henkilötietojen salaus, estääkseen ulkopuolisten pääsyn henkilötietoihin.

tuksessa potilastietoja 3 kk hoitosuhteen päättymisen jälkeen. Henkilötietojen käsittelyn turvallisuus oli myös vaarassa tapauksessa, jossa sähköisen ajanvarausjärjestelmän tunnistautumismenetelmä ei ollut riittävä, eikä täyttänyt tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdissa asetettua turvallisuuden tasoa. Myöskään seuraavassa tapauksessa rekisterinpitäjä ei ollut käsitellyt henkilötietoja tietosuoja-asetuksen määräysten mukaisesti.

> **TSV 3096/161/21** *Potilastietojen luovuttaminen vakuutusyhtiölle ja tietojen minimointi*
>
> Tapauksessa oli kyse terveydenhuollon rekisterinpitäjän järjestelmällisestä toimintatavasta luovuttaa potilastietoja kokonaisuudessaan ja seulomattomina vakuutusyhtiölle. Velvollisuus luovuttaa tiedot on perustunut liikennevakuutuslakiin (460/2016), mutta tietojen antaminen kokonaisuudessaan rikkoi tietosuoja-asetuksen 5(1)(c) artiklan tietojen minimoinnin periaatetta ja oli myös 25(2) artiklan vastainen (vaatimus sisäänrakennettuun ja oletusarvoiseen tietosuojaan teknisten ja organisatoristen toimien osalta). Myös liikennevakuutuslain mukaan tiedot rajattava tarpeellisiin (kumottu laki 279/1959 21 a§) ja välttämättömiin (uusi laki 460/2016 82 §). Tietosuojavaltuutetun mukaan rekisterinpitäjän tulee seuloa potilastiedoista tarpeelliset tiedot ja antaa ne vakuutusyhtiölle lausunnon muodossa tai toissijaisesti asiakirjajäljennöksinä tarpeettomat tiedot peittäen, jos jäljennösten luovuttamiselle on selkeitä perusteita. Vain poikkeustapauksessa rekisterinpitäjä voi luovuttaa kaikki potilasasiakirjat tietyltä ajanjaksolta. Tietosuojavaltuutettu antoi rekisterinpitäjälle 58(2)(d) artiklan mukaisen määräyksen saattaa henkilötietojen käsittelytoimet tietosuojasääntelyn mukaisiksi sekä 58(2)(b) artiklan mukaisen huomautuksen.

I) hallinnollinen seuraamusmaksu oli määrätty yhteensä kolmessa tapauksessa. Seuraamusmaksun yhteydessä mainitaan, että kyseistä toimivaltuutta voi käyttää sekä yhdessä toisten toimivaltuuksien rinnalla tai niiden sijasta. Tätä hyvin painavaa toimivaltuutta olikin aineiston tapauksissa käytetty aina yhdessä jonkin toisen korjaavan toimivaltuuden kanssa. Tietosuoja-asetuksen mukaan 58(2)(i) artiklan mukaisen hallinnollisen seuraamusmaksun määrää tietosuojavaltuutettu, mutta kuten jo aiemmin on käynyt ilmi, kansallisessa lainsäädännössä (tietosuojalaissa) on säädetty hallinnollisen seuraamusmaksun määrääminen tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen muodostaman seuraamuskollegion ratkaistavaksi.

Hallinnollisen seuraamusmaksun edellytyksistä säädetään tietosuoja-asetuksen 83 artiklassa. Seuraamusmaksun (sakon) tulee olla yksittäisessä tapauksessa tehokas, oikeasuhtainen ja varoittava ja lisäksi ne määrätään jokaisen tapauksen olosuhteiden mukaisesti joko muiden toimivaltuuksien lisäksi tai niiden sijasta. Artiklan 2 kohdan a alakohdassa säädetään lisäksi, että hallinnollisen sakon suuruudesta päätettäessä on otettava huomioon tapahtuneen tietosuoja-asetuksen säännöksen rikkomisen luonne, vakavuus ja kesto, sekä kyseisen hen-

kilötietojenkäsittelyn luonne, laajuus tai tarkoitus. Lisäksi on huomioitava niiden rekisteröityjen määrä, joihin rikkominen on vaikuttanut tai vaikuttaa ja heille aiheutuneen vahingon[194] suuruus.

Seuraamuskollegio oli määrännyt hallinnollisen seuraamusmaksun seuraavissa tapauksissa:

- ATSV 9707/152/19 Rekisteröidyn oikeus tutustua tietoihinsa ja oikeuden puutteellinen toteutus
- ATSV 1150/161/2021 Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen (Vastaamo)
- ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä

Tutkielman havainnot sosiaali- ja terveysalalla annetuista hallinnollisista seuraamusmaksuista poikkeaa laajemmasta aineistosta tehdystä tutkimuksesta, jossa havaittiin, että seuraamismaksujen määräämiskäytännöt eivät ole yhteneviä eivätkä ne ole aina ennustettavissa, koska seuraamusmaksu on voitu määrätä myös tapauksissa, joissa rekisterinpitäjä on yrittänyt tietosuojaloukkauksen tapahduttua tehdä korjaavia toimenpiteitä rekisteröityjen suojaksi.[195] Tämän tutkielman otanta oli hyvin pieni ja siihen sisältyi vain kolme tapausta, jossa seuraamusmaksu määrättiin, mutta niille kaikille oli yhteistä tietosuojatoimien tai rekisteröidyn oikeuksien räikeä rikkominen. Kahdessa tapauksessa rekisterinpitäjä ei ollut yrittänyt tehdä korjaavia toimenpiteitä rekisteröidyn hyväksi ja kolmannessa (Vastaamo) tapauksessa toimenpiteitä kyllä tehtiin, mutta itse rikkomus oli niin suuri ja perustui huolimattomuuteen, joten seuraamusmaksulle oli painavat perusteet toimenpiteistä huolimatta. Seuraavassa tapauksessa seuraamuskollegio määrisi rekisterinpitäjälle 5000 € seuraamusmaksun:

> **ATSV 8493/161/21** Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä
>
> Tapauksessa oli kyse rekisteröidyn henkilötietojensa tarkastusoikeutta[196] koskevasta kantelusta. Rekisteröity ollut pyynnöistään huolimatta saanut potilastietojaan lääkäriklinikalta, jonka asiakkaana hän oli ollut. Tietosuojavaltuutettu lähetti rekisterinpitäjälle useita selvityspyyntöjä, mutta rekisterinpitäjä ei vastannut kaikkiin asianmukaisesti tai ne olivat ristiriidassa kantelijalta saatujen tietojen kanssa. Lääkäriklinikka esimerkiksi kertoi toimittaneensa rekisteröidylle kaikki tämän pyytäneet asiakirjat (minkä rekisteröity kiistänyt) sekä kertonut, että rekisteröity

[194] Tietosuoja-asetuksen johdanto-osan 85 kohdassa fyysisinä, aineellisina tai aineettomina vahinkoina mainitaan henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintä, identiteettivarkaus tai petos, taloudelliset menetykset, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen, salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys tai muuta merkittävä taloudellinen tai sosiaalinen vahinko.
[195] Paasonen & Luomala 2022 s. 65.
[196] Tietosuoja-aseuksen 15 artiklan 1 kohta, jonka mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin sekä kohdissa a-h luetellut tiedot.

saa tiedot saapumalla yksikköön paikan päälle. Lisäksi lääkäriklinikka kertoi, että osa rekisteröidyn potilastiedoista ei ollut sen hallussa, vaan rekisteröityä hoitaneen kirurgin. Tietotuojavaltuutettu ei saanut lääkäriklinikalta selvitystä siitä, minkä tahon se katsoi olevan rekisterinpitäjä lääkäriklinikan omistajan omien vastaanottojen osalta, joilla rekisteröity myös käynyt.

Tietosuojavaltuutettu antoi tapauksessa rekisterinpitäjälle 58(2)(c) artiklan mukaisen määräyksen noudattaa vireille saattajan pyyntöä saada pääsy tietoihin siltä osin kuin se koskee tietoja, joiden rekisterinpitäjä se oli; 58(2)(b) artiklan mukaisen huomautuksen tietosuoja-asetuksen säännösten vastaisista käsittelytoimista rekisteröidyn oikeuksien toteuttamisessa ja rekisteröityjen informoinnissa sekä 58(2)(d) artiklan mukainen määräys saattaa käsittelytoimet tietosuoja-asetuksen säännösten mukaisiksi. Lisäksi tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen muodostama tietosuojakollegio katsoi, etteivät yllä mainitut tietosuoja-asetuksen mukaiset huomautukset ja määräykset olleet riittäviä seuraamuksia tietosuoja-asetuksen rikkomisen luonne ja vakavuus huomioiden. Seuraamuskollegio määräsi rekisterinpitäjälle näiden lisäksi tietosuoja-asetuksen 58(2)(i) artiklan mukaisen hallinnollisen seuraamusmaksun, joka oli suuruudeltaan 5000 euroa. Tietosuojakollegio piti tapauksessa raskauttavana rekisterinpitäjän passiivisuutta asian käsittelyssä, korjaavien toimenpiteiden tekemisessä, asianmukaisten teknisten ja organisatoristen toimenpiteiden käyttöönotossa, rekisteröidylle aiheutuneiden vahinkojen lievittämisessä sekä rekisterinpitäjän piittaamattomuutta tietosuojasääntelyä kohtaan, rikkomisen järjestelmällisyyttä ja rikkomisen kohdistumista terveystietoihin.

Tarkastelun kohteena olevissa tapauksissa seuraamusmaksujen suuruudet olivat tapauksissa 1600 €, 5000 € ja 608 000 €. Euromäärältään suurin hallinnollinen sakko liittyi paljon julkisuudessa esillä olleeseen Psykoterapiakeskus Vastaamon[197] tapaukseen.

Vastaamon kohdalla kiinnostava yksityiskohta on se, että seuraamuskollegio määräsi sille huomattavan hallinnollisen seuraamusmaksun (608 00 €), vaikka yritys oli haettu konkurssiin ja sen taloudellinen toiminta oli lakannut seuraamusmaksusta päätettäessä. Seuraamuskollegio perusteli päätöstään sillä, että vaikka Vastaamon taloudellisen toiminnan harjoittaminen oli päättynyt, se ei tarkoittanut henkilötietojen käsittelyn lakkaamista. Seuraamuskollegio katsoi, että Vastaamolle määrättävät seuraamusmaksu voi konkurssista huolimatta olla Euroopan unionin tuomioistuin käytännön tarkoittamalla tavalla varoittava[198].

Edellä mainittujen tapausten lisäksi tapauksessa *TSV 3096/161/21 Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi* oli arvioitu hallinnollisen seuraamusmaksun määräämistä huomautuksen ja määräyksen lisäksi, mutta sitä ei pidetty tapauksessa aiheellisena. Tietosuojavaltuutetun mukaan rekisterinpitäjän toimintapa (potilastietojen seulomaton luovuttaminen) oli moitittava, mutta kyseessä oli kuitenkin lakiin perustuva velvollisuus

[197] ATSV 1150/161/2021 Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen.
[198] Lisäksi varoittavuudesta mainitaan ratkaisussa. että seuraamusta voidaan julkisasiamies Kokottin mukaan pitää varoittavana, jos se saa pidättäytymään rikkomasta päämääriä ja säännöksiä. Merkitystä on seuraamuksen laadun ja suuruuden mukaan myös sillä, miten todennäköisesti seuraamus määrätään, jolloin säännösten rikkoja tulee joutua pelkäämään, että rikkomuksesta todellisuudessa tulee seuraamuksia.

luovuttaa tietoja eikä tietosuojavaltuutetun tiedossa ollut muita tapauksia, jossa potilastietoja olisi annettu vastaavalla tavalla seulomatta ja kokonaisuudessaan vakuutusyhtiölle. Lisäksi tietosuojavaltuutettu katsoi, ettei kyseisessä tapauksessa tietojen luovuttaminen ollut ollut laajamittaista, joten se katsoi määräyksen muuttaa toimintatapaa ja huomautuksen olevan oikeasuhtaisempi seuraamus kuin hallinnollinen seuraamusmaksu.

C) määräys. Tietosuojavaltuutettu oli käyttänyt seuraavissa kolmessa tapauksessa 58(2)(c) artiklan mukaista korjaavaa toimivaltuutta määrätä reksiterinpitäjä noudattamaan rekisteröidyn pyyntöä oikeutensa toteuttamisesta:

- ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä
- ATSV 6132/151/19 Potilaan tarkastusoikeuden toteuttaminen terveydenhuollossa röntgen- ja magneettikuvien osalta
- TSV 8235/154/18 Asiakkaan pyyntö henkilötietojen poistosta ja henkilötietojen käsittelyperuste

Määräystä oli käytetty aina yhdessä jonkin toisen toimivaltuuden kanssa. Kahdessa tapauksessa oli kyse määräyksestä, joka velvoitti rekisterinpitäjää toteuttamaan rekisteröidyn oikeutta saada tieto itseä koskevista tiedoista ja oikeutta saada niistä jäljennös. Kolmannessa tapauksessa rekisteröity pyysi tietojensa poistoa optikkoliikkeen rekisteristä ja tietosuojavaltuutettu antoi rekisterinpitäjälle määräyksen poistaa rekisteristä tiedot, jotka eivät olleet potilaslain mukaisia potilastietoja.

> **ATSV 6132/151/19** Potilaan tarkastusoikeuden toteuttaminen terveydenhuollossa röntgen- ja magneettikuvien osalta
>
> Tapauksessa sairaanhoitopiiri oli säännönmukaisesti perinyt maksun röntgen- ja magneettikuvien lähettämisestä potilaalle. Perusteina maksulle pidettiin sairaanhoitopiirissä sitä, että kuvia ei ollut mahdollista tulostaa paperille, joten kuluja tuli levykkeistä, sihteerin työstä, laskutuksesta ja postikuluista ja niistä perittiin potilaalta 25 euron maksu. Tietosuoja-asetuksen 15(3) mukaan rekisterinpitäjän on toimitettava rekisteröidylle jäljennös käsiteltävistä henkilötiedoista ja kohtuullisen maksun voi pyytää vain, jos rekisteröity pyytää useampia jäljennöksiä. Artiklan 12(5) mukaan kaikki 15 artiklaan perustuvat tiedot ja toimenpiteet ovat rekisteröidylle maksuttomia. Apulaistietosuojavaltuutettu antoi rekisterinpitäjälle 58(2)(c) artiklan mukaisen määräyksen noudattaa rekisteröidyn pyyntöä, joka koskee tietosuoja-asetukseen perustuvien rekisteröidyn oikeuksien käyttöä, eli oikeutta saada tämän pyytämät röntgen- ja magneettikuvat maksutta CD tai DVD-levykkeellä.[199]

Lisäksi 58(2)(c) artiklan mukaista määräystä pyydettiin tapauksissa, joissa tietosuojavaltuutettu ei sitä määrännyt. Näissä tapauksissa pyydettiin oikeutta tarkistaa itseä koskeva tiedot

[199] Rekisterinpitäjän katsottiin jättäneen noudattamatta tietosuoja-asetuksen 12(5), 15(1) ja 15(3) artikloja eikä maksun periminen röntgen- ja magneettikuvista ollut siis tietosuoja-asetuksen mukainen.

lapsenlapsen asiakastiedoista sekä oikeutta oikaista ja poistaa alaikäisen lapsen tietoja, mutta määräystä ei annettu koska pyytäjä ei ollut lapsen huoltaja eikä laillinen edustaja. Tietosuojavaltuutetun antamaa määräystä ei myöskään annettu tapauksessa, joka koski kuljetuspalvelujen järjestämistä ja siinä annettavien tietojen käyttökieltoa, koska tiedot katsottiin välttämättömiksi palvelun järjestämisen kannalta

A) varoitus. Tietosuojavaltuutettu voi 58(2)(a) artiklan mukaan varoittaa ennakollisesti rekisterinpitäjää tai muuta henkilötietojen käsittelijää, jos sen suunnittelemat henkilötietojen käsittelytoimet ovat todennäköisesti tietosuoja-asetuksen vastaisia Tarkastelussa olevista tapauksessa oli käytetty varoitusta seuraavissa kahdessa tapauksessa:

- ATSV 3895/83/22 Potilastietojen käsittely ennaltaehkäisyn ja ennakoinnin tarkoituksissa sekä automatisoidut yksittäispäätökset
- ATSV 6482/186/2020 Automatisoitujen yksittäispäätösten syntyminen ennakoivan terveydenhuollon työkalussa

Tapauksissa rekisterinpitäjä oli saattanut vireille tietosuoja-asetuksen 36 artiklan mukaisen ennakkokuulemispyynnön, joka oli molemmissa tapauksissa päätynyt myös valvonta-asiaksi, johon liittyen varoitukset oli annettu. Tapauksen liittyivät automatisoitujen yksittäispäätösten syntymiseen (22 artikla). Toisessa tapauksessa asiaa ei käsitelty ennakkokuulemispyyntönä vaan pelkkänä valvonta-asiana[200] ja toisessa asia käsiteltiin valvonta asiana ja sen lisäksi päätöksessä annettiin kirjallisia neuvoja ennakkokuulemispyynnön perusteella

Molemmissa päätöksissä tietosuojavaltuutettu katsoi, että automatisoituja yksittäispäätöksiä todennäköisesti muodostuisi niiden potilaiden kohdalla, joita automaattinen riskimallityökalu ei poimisi tarkempaan ammattihenkilön suorittamaan arviointiin. Kummassakaan tapauksessa rekisterinpitäjä ei ollut suunnittelemassaan työkalussa tunnistanut 22 artiklan mukaisten automatisoitujen yksittäispäätösten todennäköistä muodostumista, mikä oli varoituksen perusteena:

ATSV 6482/186/2020 Automatisoitujen yksittäispäätösten syntyminen ennakoivan terveydenhuollon työkalussa[201]

> Tapauksessa rekisterinpitäjä suoritti työkalun avulla yleistä profilointia käsitellessään asiakkaiden tietoja automaattisesti ja tehdessään päätelmiä asiakkaan terveydentilasta ja hoidon tehostamistarpeesta. Asiakkaan hoidosta ei kuitenkaan päätetty pelkästään profiloinnin tuloksen perusteella, vaan terveydenhuollon ammattilainen kävi potilastiedot vielä läpi järjestelmästä ennen

[200] ATSV 6482/186/2020.
[201] Hallintolain 8b luku voimaan päätöksen jälkeen. Ks. myös HE 145/2022 s. 95.

päätöstä toimenpiteistä. Potilaalla oli mahdollisuus kieltää työkalun käyttö hänen hoitoonsa ensimmäisen yhteydenoton yhteydessä. Apulaistietosuojavaltuutetun mukaan tapauksessa ei syntynyt automatisoituja yksittäispäätöksiä niiden potilaiden kohdalla, jotka työkalun avulla poimitaan terveydenhuollon ammattihenkilön tarkempaan arviointiin, joka perusteella päätös toimenpiteestä lopulta tehdään. Sen sijaan niiden potilaiden kohdalla, joita työkalun tuottaman tiedon vuoksi ei poimittu terveydenhuollon ammattilaisen tarkempaan tarkasteluun, työkalun avulla automatisoituja yksittäispäätöksiä todennäköisesti syntyi, koska työkalun tekemää päätöstä ei ammattihenkilö erikseen arvioinut kuten poimittujen potilaiden kohdalla tapahtuisi. Apulaistietosuojavaltuutettu antoi rekisterinpitäjälle tietosuoja-asetuksen 58 artiklan 2 kohdan a alakohdan mukaisen varoituksen, koska henkilötietojen käsittelytoimet, joita rekisterinpitäjä oli suunnitellut, olivat todennäköisesti tietosuoja-asetuksen vastaisia. Rekisterinpitäjä ei ollut tunnistanut tilannetta, jossa automatisoituja yksittäispäätöksiä todennäköisesti muodostuisi eikä siten ollut varmistanut, että tietosuoja-asetuksen 22 artiklassa säädetyt perusteet automatisoidulle tietojenkäsittelylle olivat olemassa.

E) määräys. Tietosuojavaltuutettu oli myös antanut yhdelle rekisterinpitäjälle tietosuoja-asetuksen 58(2)(e) artiklan mukaisen määräyksen ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidylle. Tätä määräystä tietosuojavaltuutettu voi yleensä käyttää tilanteessa, jossa rekisterinpitäjä ei ole ilmoittanut jo tapahtuneesta tietoturvaloukkauksesta rekisteröidylle, vaikka siitä on aiheutunut tälle korkea riski.

TSV 2691/171/19 Henkilötietoasiakirjoja sisältävän postipaketin katoaminen

Tapauksessa Kelan vakuutuspiiriin skannaukseen matkalla ollut postipaketti katosi. Paketti sisälsi Kelan etuuksia hakeneiden asiakkaiden toimittamia asiakirjoja, joissa oli salassa pidettäviä asiakastietoja kuten terveydentilaa ja taloudellista asemaa koskevia tietoja. Kyseessä oli tietojen lainvastainen tai vahingossa tapahtunut tuhoutuminen tai häviäminen, joka loukkasi tietojen luottamuksellisuutta ja esti tietojen saatavuuden ja käytön. Kelan tiedossa ei ollut, keiden asiakkaiden asiakirjoja lähetyksessä oli, joten tietoturvaloukkauksesta ei voitu tiedottaa kaikille sen kohteena oleville asiakkaille. Osa asiakkaista sai tiedon tietoturvaloukkauksesta otettuaan itse yhteyttä Kelaan huomatessaan, ettei heidän hakemusasiansa ollut edennyt. Muutama tietoturvaloukkauksen kohteeksi joutunut henkilö tunnistettiin, koska he olivat asioineet kelan palvelutiskillä ja heille Kela tiedotti tietoturvaloukkauksesta puhelimitse. Kaikki tietoturvaloukkauksen kohteet eivät olleet Kelan tiedossa, joten heille tiedottaminen henkilökohtaisesi oli mahdotonta, joten tietotuoja-asetuksen 58(2)(e) [202]artiklan nojalla tietosuojavaltuutettu määräsi rekisterinpitäjän tiedottamaan tietosuojaloukkauksesta käyttämällä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille voitiin tiedottaa tietoturvaloukkauksesta yhtä tehokkaalla tavalla. Tietosuojavaltuutettu ei määrännyt rekisterinpitäjää enää tiedottamaan tietoturvaloukkauksesta niille henkilöille, jotka olivat jo saaneet tiedon asiakirjojensa katoamisesta, mutta rekisterinpitäjän oli varmistettava, että annettu informaatio sisälsi tietosuoja-asetuksen 34(1) artiklan kohdassa mainitut asiat.

[202] Tietosuojavaltuutetun ratkaisussa ei mainita artiklan alakohtaa, mutta e) alakohdan mukaan voi määrätä tiedottamaan tietoturvaloukkauksesta.

Lisäksi myös Psykoterapiakeskus Vastaamon tietomurtotapauksen yhteydessä tietosuojavaltuutettu oli antanut 58(2)(e) artiklan mukaisen määräyksen tiedottaa rekisteröidyille henkilökohtaisesti tietomurrosta. Tämä käy ilmi apulaistietosuojavaltuutetun ratkaisusta 1150/161/2021. Kyseessä on kuitenkin ratkaisu, joka annettu eri diaarinumerolla kuin tämä.

G) määräys oikaista tai poistaa henkilötietoja. Artiklan 58(2)(g) mukaan tietosuojavaltuutettu voi määrätä rekisterinpitäjän tai henkilötietojen käsittelijän oikaisemaan tai poistamaan henkilötietoja tai rajoittamaan niiden käsittelyä asetuksen 16, 17 ja 18[203] artiklan perusteella sekä ilmoittamaan näistä toimenpiteistä tahoille, joille se on luovuttanut henkilötietoja tietosuoja-asetuksen 17 artiklan 2 kohta ja 19 artiklan[204] mukaisesti. Aineistossa oli yksi tapaus, jossa rekisteröity oli pyytänyt tällaista määräystä tietosuojavaltuutetulta, mutta tietosuojavaltuutettu katsoi, ettei määräystä ollut aiheellista antaa.

- TSV 5242/157/2018 Tietojen luovuttaminen sosiaali- ja terveydenhuollosta kuljetuspalveluille kuljetusten järjestämistä varten

Tapauksessa rekisteröity pyysi tietosuojavaltuutettua antamaan rekisterinpitäjälle määräyksen, joka koski tietojen luovuttamisen kieltämistä terveydenhuollosta kuljetuspalveluyritykselle. Tietosuojavaltuutettu ei kuitenkaan määrännyt g) kohdan mukaista kieltoa tai rajoitusta, koska se katsoi, että tietojen käsittely oli tarpeellista rekisterinpitäjän lakisääteisen velvollisuuden noudattamiseksi ja siten 6(1)(c) artiklan mukainen.

[203] 16 artikla: oikeus tietojen oikaisemiseen, 17 artikla: oikeus tietojen poistamiseen ja 18 artikla: oikeus käsittelyn rajoittamiseen.
[204] Ilmoitusvelvollisuus, jonka mukaan rekisterinpitäjän on ilmoitettava henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, ellei tämä ole mahdotonta tai vaadi kohtuutonta vaivaa.

5 Hyvinvointialueet uusina reksiterinpitäjinä

Sote-uudistuksen tausta ja tavoitteet. Sosiaali- ja terveydenhuollon kokonaisuudistusta on suunniteltu ja valmisteltu jo pitkään, mutta oikeudellisesti kestävän mallin löytämistä edelsi muun muassa kaksi kariutunutta uudistusyritystä.[205] Uudistuksen tavoitteena oli hyvinvointi- ja terveyserojen kaventaminen, yhdenvertaisten ja laadukkaiden sosiaali-, terveys- ja pelastustoimen palveluiden turvaaminen; turvallisuuden, palveluiden saavutettavuuden ja saatavuuden parantaminen; ammattitaitoisen työnvoiman saannin turvaaminen; yhteiskunnallisten muutosten tuomiin haasteisin vastaaminen ja kustannusten kasvun hillitseminen.[206]

Toteutunut sosiaali- ja terveyshuollon kokonaisuudistus, josta käytetään myös lyhennystä sote-uudistus[207] on yksi Suomessa tehdyistä merkittävimmistä hallinnollisista uudistuksista[208]. Uudistuksen jälkeen vuoden 2023 alussa sosiaali- ja terveydenhuollon ja pelastustoimen järjestämisvastuu siirtyi kunnilta ja kuntayhtymiltä 21 hyvinvointialueelle. [209] Aluejaon pohjana on maakuntajako, mutta Uudenmaan maakunnassa toteutettiin erillisratkaisu. Uudella maalla toimii neljä hyvinvointialuetta, joiden lisäksi Helsingin kaupunki vastaa edelleen sosiaali- ja terveyshuollon ja pelastustoimen tehtävissä Helsingissä ja erikoissairaanhoidon osalta vastuu siirtyi HUS-yhtymälle.[210] Tässä tutkielmassa hyvinvointialuenimitystä käytettäessä tarkoitetaan sisällyttää siihen myös Uudenmaan erillisratkaisu.

Lainsäädäntö. Hyvinvointialueet ovat perustuslain 121§ 4 mom. tarkoittamia *kuntaa suurempia itsehallintoalueita*. Kansanvaltaisuus hyvinvointialueilla toteutuu vaaleilla valitun aluevaltuuston kautta, joka käyttää alueilla ylintä toimivaltaa. Hyvinvointialueen hallintosäännössä määritellään sen talouden ja toiminnan organisointi ja toimivallan siirto. Hyvinvointialuilla on alue- ja palvelustrategiat, jotka koskevat toiminnan tavoitetta ja sosiaali- ja terveyspalvelujen (myös pelastuspalvelujen) järjestämistä.[211]

---

[205] Pääministeri Jyrki Kataisen hallituksen (2011–2015) kaksitasoinen kuntayhtymämalli sosiaali- ja terveyspalvelujen tuottamiseen kaatui perustuslakiongelmiin mm. kansanvaltaisuuden vähäisyyteen ja kuntien rahoitusvastuun ongelmallisuuteen. Pääministeri Juha Sipilän hallituksen (2015–2019) maakunta- ja sote-uudistus taas törmäsi myös perustuslakiin. Uudistuksen ongelmia aiheuttivat mm. yhtiöittämispakko, valinnanvapaus, maakuntien määrä, rahoitus, aikatauluongelmat ja uudistuksen laajuus. Ks. lisää Niemivuo 2022, s. 103–141. ja Leppänen, Sorvettula & Valli-Lintu 2024, s. 11–26.
[206] HE 241/2020, s.1.
[207] Ilmaisu sote-uudistus on vakiintunut puhekieleen ja sitä käytetään esimerkiksi Leppänen, Sorvettula & Valli-Lintu: Hyvinvointialue järjestäminen, hallinto ja talous -kirjassa, 2024.
[208] Niemivuo 2022, s. 223 Niemivuo mainitsee, että uudistus on merkittävä rakenteellinen uudistus Suomessa.
[209] Leppänen, Sorvettula & Valli-Lintu 2024, s. 26–28.
[210] Ks. Uudenmaan erillisratkaisusta Leppänen, Sorvettula & Valli-Lintu 2024, s. 661–696.
[211] Leppänen, Sorvettula & Valli-Lintu 2024, s. 26–28.

Hyvinvointialueita ja sosiaali- ja terveyshuoltoa koskeva sääntely on laaja kokonaisuus, johon kuuluu sekä uusia lakeja, että lakimuutoksia. Lisäksi hyvinvointialueisiin liittyvää sääntelyä on julkisoikeuden yleislaeissa, kuten vaalilaissa ja hallinnon yleislaeissa.[212] Keskeisimpiä hyvinvointialueita koskevista laeista ovat:

- laki hyvinvointialueesta (611/2021),
- laki sosiaali- ja terveydenhuollon järjestämisestä (612/2021)[213]
- laki pelastustoimen järjestämisestä (613/2021)
- hyvinvointialue- ja maakuntajakolaki (614/2021),
- laki sosiaali- ja terveydenhuollon sekä pelastustoimen järjestämisestä Uudellamaalla (615/2921).
- laki sosiaali- ja terveydenhuoltoa ja pelastustoimea koskevan uudistuksen toimeenpanosta ja sitä koskevan lainsäädännön voimaanpanosta (616/2021),
- laki hyvinvointialueiden rahoituksesta (617/2021),
- laki sosiaali- ja terveydenhuollon asiakasmaksuista (1201/2020).[214]

Hyvinvointialueiden tehtävät. Kuten jo aiemmin mainittiin, hyvinvointialueet ovat itsehallinnollisia alueita, jonka vuoksi niille kuuluvista tehtävistä säädetään aina lailla.[215] Hyvinvointialuelain 6 §:ssä säädetään hyvinvointialueen erityistoimialasta, elin sen tehtävät säädetään lailla, eikä hyvinvointialueilla siten ole itsehallinnollisista piirteistään huolimatta yleistä toimivaltaa kuten kunnilla. Hyvinvointialueen lakisääteisiä tehtäviä ovat sotejärjestämislain 8 §:n mukaan[216] sosiaali- ja terveyshuollon tehtävät sekä pelastustoimen järjestämistä koskevan lain 4 §:n mukaan pelastustoimen tehtävien järjestäminen alueellaan. Hyvinvointialue voi kuitenkin ottaa hoitaakseen tehtäviä oman päätöksen mukaan, mikäli ne tukevat sen lakisääteisiä tehtäviä.[217]

Hyvinvointialuelain 7 §:n mukaan hyvinvointialueen on vastattava sille lailla säädettyjen tehtävien hoitamisesta, hyvinvointialueen asukkaan laissa säädettyjen oikeuksien toteutumisesta ja palvelukokonaisuuksien yhteensovittamisesta. Lisäksi hyvinvointialueen tulee järjestää palvelujen ja muiden toimenpiteiden 1) yhdenvertainen saatavuus, 2) tarpeen, määrän ja laadun määritteleminen, 3) tuottamistavan valinta, 4) tuottamisen ohjaus ja valvota ja 5)

---

[212] Niemivuo 2022, s.272–274.
[213] Ns. sosiaali- ja terveydenhuollon järjestämislaki tai sote järjestämislaki. Jatkossa käytetään sosiaali- ja terveydenhuollon järjestämislaki nimitystä.
[214] Listaus: Niemivuo 2022, s. 272–274.
[215] PL 121 § 4 mom ”*Itsehallinnosta kuntia suuremmilla hallintoalueilla säädetään lailla*.”
[216] Hyvinvointialue vastaa sosiaali- ja terveydenhuollon järjestämisestä alueellaan
[217] Hyvinvointialuelain 6 §:n toinen virke: ”Hyvinvointialue voi lisäksi alueellaan ottaa hoitaakseen sen lakisääteisiä tehtäviä tukevia tehtäviä. Hyvinvointialueen itselleen ottama tehtävä hoitaminen ei saa laajuudeltaan olla sellainen, että se vaarantaa hyvinvointialueen lakisääteisten tehtävien hoitamisen”.

viranomaiselle kuuluvan toimivallan käyttäminen. Näiden tehtävien siirtäminen yksityiselle tuottajalle ei ole mahdollista, mutta järjestämisvastuun siirtämisestä toiselle hyvinvointialueelle on asia, josta hyvinvointialueet voivat sopia.[218]

Hyvinvointialueet rahoittavat toimintansa pääosin valtion rahoituksen avulla, mutta lisäksi hyvinvointialueet saavat tuloja asiakasmaksuista ja mahdollisista muista tuloista. Valtion rahoituksesta säädetään laissa hyvinvointialueiden rahoituksesta (rahoituslaki). Valtion rahoitus ei kata hyvinvointialueen mahdollisesti itselleen ottamia tehtäviä.[219]

Laissa sosiaali- ja terveydenhuollon järjestämisestä (sotejärjestämislaki) säädetään asiakas- ja potilastietojen rekisterinpidosta (58§). Sen mukaan hyvinvointialue on sote-palveluiden järjestämisestä vastaavana toimivaltaisena viranomaisena tietosuoja-asetuksen mukainen rekisterinpitäjä sen toiminnassa syntyneille ja sille (kunnilta) siirtyneille asiakas- ja potilastiedoille.

Matti Niemivuo huomauttaa kirjassaan *Uusi aluehallinto*, että hyvinvointialue- ja sosiaali- ja terveydenhuollon uudistuksen yhteydessä perustuslakivaliokunta on ottanut useasti kantaa henkilötietojen käsittelyyn. Sääntely voi silti näiden täsmennysten jälkeenkin olla vaikeaa ja abstraktia hyvinvointialueen asukkaille. Niemivuo korostaakin hyvinvointialueiden vastuuta rekisterinpitäjinä toimia tietosuoja-asioissa tarkasti ja asiallisesti. Hän luottaa kuitenkin tietosuojavaltuutetun valvonnan toimivuuteen.[220] Tämä tutkielma antaakin perustaa tälle luottamukselle, sillä tutkielma on osoittanut, miten monenlaisiin tietosuojakysymyksiin tietosuojavaltuutettu on sosiaali- ja terveydenhuoltoon liittyen ottanut kantaa ja miten monipuolista tapausten ohjauksellisuus on ollut. Lisäksi vakavien tietosuojarikkomusten suhteellisen vähäinen määrä aineistossa, kertoo hyvää sosiaali- ja terveydenhuollon tietosuojan tämänhetkisestä tasosta. Hyvinvointialueiden ei tarvitse aloittaa tietosuojatyötään alusta.

Hyvinvointialuemallia on kritisoitu siitä, että hyvinvointialueet ovat liian pieniä ja niitä on liikaa Suomen väkilukuun nähden. On noussut epäilys siitä, että kaikki hyvinvointialueet eivät todellisuudessa pysty tarjoamaan perustuslain edellyttämiä riittävän laadukkaita sosi-

[218] Leppänen, Sorvettula & Valli-Lintu 2024, s. 114–117.
[219] Leppänen, Sorvettula & Valli-Lintu 2024, s. 521–525.
[220] Niemivuo 2022, s. 436, missä viitataan myös PeVL 26/2017 vp, 15 ja 65/2018 vp ja PeVL 17/2021 vp kappaleet 176–190.

aali- ja terveyspalveluja. Hyvinvointialueet voivat siten joutua tekemään yhteystyötä toistensa kanssa.[221] Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen tietosuojan kanssa, tällaisissa tilanteissa voi tulla samanlaisia ongelmia tietoihin pääsyn ja järjestelmien yhteensopivuuden kanssa kuin aiemmin kuntayhtymien tai kuntaliitosten kanssa.[222] Tosin sosiaali- ja terveydenhuollon asiakas- ja potilastiedot siirtyivät uudistuksen myötä kunnilta hyvinvointialueille ja siirrot suunniteltiin osana uudistusta joten hyvinvointialueiden yhdistyminen ei todennäköisesti ole yhtä sääntelemätön tilanne kuin kuntayhtymien aikaan.

Hyvinvointialueiden perustamista ja sote-uudistuksen valmistelua kritisoitiin siitä, että vaikka se oli huomattava rakenteellinen ja yhteiskuntapoliittisesti merkittävä uudistus, sitä ei tehty ja valmisteltu parlamentaarisesti ja mahdollisimman suuren yhteisymmärryksen turvin. Uudistuksen myötä kansanvalta lisääntyi sosiaali- ja terveydenhuollosta alueilla päätettäessä, mutta samaan aikaan valtion keskushallinnon asema vahvistui rahoituksen kautta tapahtuvan ohjauksen vuoksi. Lisäksi itsehallintomuotoisen hyvinvointialueen todellista itsehallintoa kaventaa merkittävästi siltä puuttuva verotusoikeus. [223]

5.1 Mitä hyvinvointialueiden tulee ottaa huomioon jatkossa

5.1.1 Tietosuojan vaaranpaikat

Vaikka aineisto on pieni empiiriseen tutkimukseen, siinä toistuu tiettyjä teemoja, joihin hyvinvointialueiden sosiaali- ja terveyspalvelujen järjestäjinä olisi hyvä kiinnittää huomiota tietosuojatoimissa ja henkilöstön koulutuksessa. Aineistosta käy ilmi, että sosiaali- ja terveydenhuollon (etenkin terveydenhuollon) asiakkailla on ollut hankaluuksia käyttää tietosuoja-asetuksen 15 artiklan mukaista oikeuttaan tutustua omiin tietoihinsa ja saada niistä maksutta jäljennös. Myös vahva tunnistautuminen on myös aiheuttanut sosiaali- ja terveysalan asiakkaille ja potilaille ongelmia tietosuojan näkökulmasta.

Sosiaali- ja terveysalan toimijoilla voi myös aineiston mukaan nähdä jonkinasteista haluttomuutta tai tietämättömyyttä siitä, milloin tietoturvaloukkauksesta on tehtävä ilmoitus sen kohteille ja/tai tietosuojavaltuutetulle. Kyseinen toimi on tarpeellinen, vaikka se ei enää estä

[221] Ks. Niemivuo 2022, s. 462.
[222] Esim. tietosuojavaltuutetun kaksi kannanottoa kuntaliitoksiin ja isäntäkuntamalliin liittyen: TSV 150/49/2007 Isäntäkuntamalli ja rekisterinpitäjä sekä asiakastietojen siirtäminen palvelujen järjestämisvastuun siirtyessä ja TSV 617/41/2008 Henkilötietojen siirtäminen palvelujen järjestämisvastuun siirtyessä esimerkiksi uudelle kunnalle.
[223] Niemivuo 2022, s. 223–224, 456–457 ja 460–463.

tietoturvaloukkausta tapahtumasta, koska se on jo tapahtunut, mutta asiakkaan näkökulmasta sillä voi olla huomattavia vaikutuksia riippuen siitä, millaisia tietoja hänestä on mahdollisesti päätynyt ulkopuoliselle. Myös tietosuojavaltuutetun näkökulmasta tietoturvaloukkauksesta ilmoittamatta jättäminen on ongelmallista, sillä tämä ei voi antaa muitakaan toimintaohjeita rekisterin pitäjälle, jollei viranomainen tiedä loukkauksen tapahtuneen. Syy ilmoittamatta jättämiseen voi olla tietämättömyys tai haluttomuus kertoa virheestä ja joutua mahdollisten sanktioiden kohteeksi. Kuitenkin rekisterinpitäjän oma ilmoitus on valittu valvonnan lähtökohdaksi, koska muu valvonta olisi kohtuuttoman raskasta ja kallista ja vaikeaa toteuttaa.

Uudet teknologiat ovat aina aluksi tuoneet ongelmia ja haasteita. Sähköpostin tietoturva, faksin ja tekstiviestin käyttö. Kameravalvonta. Sähköiset asiointikanavat ja ajanvarausjärjestelmien tietoturva ja väärinkäyttäminen. Automaattinen päätöksenteko ja tekoälyn käyttö. Tarkoitettu helpottamaan, mutta ei ole nähty aukkoja. Uuden teknologian käytön alussa tulisi huolellisemmin varmistaa, ettei se mahdollista väärinkäyttöä tai siinä ole tietoturva-aukkoja.

Tekoälyn käyttö sosiaali- ja terveydenhuollon asiakas- ja potilasrekistereissä ei vielä näkynyt tietosuojavaltuutetun ratkaisukäytännössä, joka oli tämän tutkielman aiheena, mutta se voi tuoda uusia tietosuojakysymyksiä. Automaattinen päätöksenteko on lähellä tekoälyn käyttöä ja sen yhteydessä tietosuojavaltuutettu joutui huomauttamaan rekisterinpitäjää siitä, että päätös olla tarjoamatta palvelua pelkän automaattisen tietojen käsittelyn ehdotuksen pohjalta, on myös automaattinen päätös, jonka kohteeksi joutumisesta on oltava mahdollisuus kieltäytyä ja joka tulisi ammattilaisen myös tarkistaa.

Tietojen minimointi vaikuttaa myös olevan hankala kysymys sosiaali- ja terveydenhuollon toimijoille. Alan luonteen vuoksi voi rekisterinpitäjästä tai yksittäisestä työntekijästä tuntua, että enemmän tietoa on parempi kuin liian vähän tietoa. Tietosuoja-asetus rajoittaa kuitenkin tallennettavan tiedon niihin, mitkä ovat tarpeellisia riittävien ja turvallisten sosiaali- ja terveyspalveluiden tarjoamiselle. Verrattuna tietosuojavaltuutetun aiempaan ratkaisukäytäntöön kumotun henkilötietolain osalta, uudemmat ratkaisut eivät enää yhtä selkeästi osoita epätietoisuutta siitä, kenelle voi antaa pääsyn sosiaali- ja terveyspalvelujen asiakas ja potilastietoihin. Tiedon tarve ei kuitenkaan voi mennä lain edelle, vaikka se voisi helpottaakin käytännön työtä.

Tämän vuoksi myös jatkossa on tärkeää huomioida, mitä Lasse Lehtosen vuonna 2015 ilmestyneessä Terveysoikeuskirjassa kirjoittaa tehokkuuden ja digitaalisten työkalujen sekä

tietovarastojen hyödyntämisen ansoista terveydenhuollossa. Tehokkuuden tavoittelu voi johtaa siihen, että yhä useammalla viranomaisella olisi halukkuutta ja omasta mielestään myös tarve päästä sosiaali- ja terveystietoihin. Tämä kuitenkin uhkaa luottamuksellisuutta, joka on hoitosuhteessa olennainen perusta. Potilas- ja asiakastiedot ovat salassa pidettäviä syystä, sillä jos potilas joutuu salaamaan tietoja lääkäriltä tai jopa valehtelemaan, tiedot eivät ole luotettavia, mikä heikentää niiden käytettävyyttä. Tietojen oikeellisuus on ratkaisevan tärkeää niiden hyödyntämismahdollisuuksille.[224] Sosiaali- ja terveydenhuollon asiakas- ja potilastietojen suhteen tasapainoillaan varmasti jatkossakin tiedon olemassaolon ja hyödynnettävyyden kanssa. Kaikkea olemassa olevaa tietoa ei saa hyödyntää, vaikka se helpottaisi asioiden hoitamista, jos tiedon hyödyntämiseen ei ole lainmukaista perustetta.

Tutkielman sivulöydöksenä nousi myös esiin muutama tapaus, joissa sosiaali- ja terveydenhuollon toimija oli kehittänyt uuden lakiin perustumattoman käytännön. Tapauksissa neljän eri kaupungin tai kuntayhtymän sosiaali- ja terveyspalvelut olivat käsitelleet vapaaehtoisten tuki- ja sijaisperhetoimintaan tai lasten ja nuorten tukihenkilötoimintaan hakevien henkilöiden poliisin tietojärjestelmissä olevia rikos- ja rangaistusmerkintöjä tai muita poliisin rekistereissä olevia hakijaa koskevia tietoja (esimerkiksi kotihälytyksiä tai henkilön tekemiä rikosilmoituksia koskevia tietoja) ilman lain mukaista perustetta.[225] Tämä kertoo sosiaali- ja terveydenhuollon (tapauksessa sosiaalihuollon) toimijoiden tarpeesta saada tietoa ja halusta ja velvollisuudesta järjestää tuki- ja vapaaehtoistoimintaa turvallisesti. Nämä ovat joskus ristiriidassa yksilön oikeuksien kanssa. Tämä on yksi vaaranpaikka, jossa sote-toimijoiden tulisi olla hereillä.

5.1.2 Onnistumisia

Tietosuojavaltuutetun julkaistuista ratkaisuista sosiaali- ja terveysalan tietosuojakysymyksissä on myös näkyvissä positiivista kehitystä alan tietosuojakäytännöissä. Aineisto ei suppeudessaan anna mahdollisuutta tehdä kovin pitkälle meneviä johtopäätöksiä siitä, mitkä aiheet ja asiat ovat määrällisesti suurimpia ongelmakohtia, mutta ratkaisuista on nähtävissä muutamia kehityslinjoja.

[224] Lehtonen, Lohiniva-Kerkelä ja Pahlman 2015, s. 382–383.

[225] ATSV 8979/162/21; ATSV 8979/162/21; ATSV 7635/162/21 ja ATSV 6689/186/20.

Ensinnäkin asiointikanavat sosiaali- ja terveyspalveluissa ovat myös kehittyneet turvallisemmiksi, vaikka uusien teknologioiden käyttö onkin aiheuttanut myös tietoturvaloukkauksia. Sosiaali- ja terveyshuollossa on eletty muun yhteiskunnan mukana teknologian kehitystä telefakseista ja tekstiviesteistä kohti sähköpostin käyttöä ja sähköisten asiointikanavien ja ajanvarausjärjestelmien kehitystä ja vahvan sähköisen tunnistautumisen käyttöä. Asiakkaiden ja potilaiden on helpompi käyttää 15 artiklan mukaista tarkastusoikeuttaan OmaKanta palvelun avulla, kun pääsyä tietoihin ei aina tarvitse pyytää suoraan rekisterinpitäjältä, vaan tietoihin on pääsy sähköisen tunnistautumisen avulla.[226] Toisaalta helppo pääsy omiin tietoihin voi vähentää esimerkiksi potilaalle annettavaa ammattilaisen ohjausta ja neuvontaa, mikä taas voi johtaa väärinkäsityksiin.[227] Lääketieteellinen termistö ei ole aina kovin helppolukuista alaa tuntemattomille. Tämä tulisi ottaa huomioon digitaalisia palveluja suunniteltaessa, jottei terveydenhuoltojärjestelmä tällaisten tapausten vuoksi turhaa kuormitu.[228]

Suostumuksen pyytämisen tietojen keräämistä ja tallentamista varten voi myös olettaa parantuneen, koska tietosuojavaltuutetun julkaistuissa ratkaisuissa ei enää ole sitä koskevia tapauksia, toisin kuin henkilötietolain mukaisissa tapauksissa oli. Lisäksi tarkastusoikeus toisen henkilön tietoihin tai toisin sanoen itsestä toisen henkilön tietoihin kirjattuihin tietoihin, ei myöskään esiinny enää uusissa ratkaisuissa samalla tavalla kuin henkilötietolain mukaisissa ratkaisuissa. Tässä yhteydessä rekisterinpitäjän eli hyvinvointialueiden tulee jatkossakin kiinnittää siihen huomiota, kuka on rekisteröity ja mitä asioista toisista henkilöistä on välttämätöntä kirjata rekisteröidyn tietoihin. Eli tietojen kirjaamisvaiheessa tulee noudattaa tietojen minimointivelvoitetta ja sen lisäksi tietoja luovutettaessa rekisterinpitäjän tulee tunnistaa, kenen tiedoista asiassa on kyse, eli kuka on asiassa rekisteröity, jonka palveluja varten tiedot on kirjattu. Tällä periaatteella löytyy henkilötietolain aikana paljon askarruttaneeseen kysymykseen vastaus, eli kenellä tietoihin on ja ei ole tarkastusoikeutta.

---

[226] Tarkastusoikeuden kehittymistä ja käytettävyyttä kuvaa hyvin Etelä-Suomen lääninhallituksen päätös (ESLH-2004-09473/So-38), jossa tarkastusoikeuden tosiasialliseksi epäämiseksi katsottiin tapaus, jossa psykiatri ei vastaanottanut kirjattuna kirjeenä lähetettyä tarkastuspyyntöä. Vastaavan kaltaisia tarkastusoikeuden epäämisiä tuskin tapahtuu suuressa määrin nykyään. Referoitu päätös: Myllynpää 2010, s. 188.
[227] Lehtonen, Lohiniva-Kerkelä ja Pahlman 2015, s. 382–383.

[228] Lehtonen, Lohiniva-Kerkelä ja Pahlman 2015, s. 382–383.

6 Johtopäätökset

Tietosuojavaltuutettu ohjaa julkaistujen ratkaisujen lisäksi sekä sosiaali- ja terveydenalan toimijoita että asiakkaita omilla verkkosivuillaan.[229] Tutkimustulokset eivät siten anna kokonaiskuvaa sosiaali- ja terveysalaan kohdistamista tietosuojavaltuutetun päätöksistä, vaan tarkasteli julkaistuja ratkaisuja yhtenä ohjauksen muotona.

Mikä tietosuojassa oli pettänyt. Selvien tietomurtojen ja tietoturvaloukkausten vähäinen määrä aineistossa on sekä yllättävää että huojentavaa. Uudet teknologiat ja viestintävälineet nousevat tapauksissa esille uudestaan ja uudestaan. Asiakkaiden ja potilaiden tietoturva vaikuttaa olevan vaarassa erityisesti uusien toimintojen käyttöönotossa, vaikka käsiteltävä ja siirrettävä tieto on pysynyt yhtä arkaluonteisena kaiken aikaa. Tietojen päätyminen ulkopuolisille on ollut vaarassa mm. faksin käytössä, salaamattomien sähköpostien yleistyessä ja sähköisissä ajanvarausjärjestelmissä. Täsmälleen samoihin riskeihin ei sentään aina ole kompastuttu uudestaan vaan uhkatilanteet ovat myös muuttuneet fyysisistä teknisemmäksi, eivätkä tulokset siis osoita, että mitään ei olisi opittu, vaan että uudistuva teknologia luonnollisesti tuo myös uusia tapoja saattaa tietosuoja vaaraan.

Tietosuoja on pettänyt useimmiten yksittäisten rekisteröityjen, mutta välillä myös laajempien joukkojen kohdalla. Tulokset osoittivat myös sen, että tietosuoja voi pettää useassa eri prosessin vaiheessa suunnitteluvaiheesta, toteuttamiseen ja tietosuojarikkomuksen jälkitoimien minimoimiseen saakka. Syy tietosuojan pettämiseen voi olla tekniikassa, tiedonpuutteessa, inhimillisissä virheissä tai tietämättömyydessä. Valitettavasti myös välinpitämättömyys saattoi olla ainakin yhden tapauksen taustalla, mikä on anteeksiantamatonta. Nopeasti muuttuva lainsäädäntö on voinut olla osaltaan aiheuttamassa sitä, että myös vanhentuneita ohjeita on saatettu soveltaa lainsäädännön muuttumisesta huolimatta. Sosiaali- ja terveydenhuollossa usein turvaudutaankin sisäisiin ohjeisiin, joiden ajantasaisuudesta tulisi huolehtia.

Ohjaus ja toimivaltuudet Tietosuojavaltuutetun rooli on muuttunut yleisestä neuvojen ja ohjauksen ja epäselvien tilanteiden selvittäjästä enemmän tuomioistuinmaiseen ennakkoratkaisutoiminnan suuntaan, jossa ratkotaan yksittäinen tapaus ja julkaistaan merkittävimmät ohjaustarkoituksessa. Tietosuojavaltuutetun antama ohjaus ei seiso päätöksissä kissankokoisin kirjaimin, eikä aina edes kovin selkeänä. Ohjausta on kuitenkin annettu monenlaisissa

[229] Ks. esimerkiksi https://tietosuoja.fi/usein-kysyttya-terveydenhuolto ja https://tietosuoja.fi/usein-kysyttya-sosiaalihuolto.

asioissa ja monella eri tavalla. Rekisterinpitäjät ja henkilötietojen käsittelijä voivat löytää päätöksistä konkreettisia toimintavaihtoehtoja, joilla käsittelytoimet voi tehdä lainmukaisesti. Tietosuojavaltuutettu on myös antanut ohjausta salaukseen, sen puuttumiseen liittyen sähköpostiviestejä ja tekstiviestejä koskien. Tietosuojavaltuutetun ratkaisuista voi löytää myös hieman nurinkurisesti myös vaihtoehtoja, kuinka voi päästä käsiksi salasanalla suojattuun kannettavan tietokoneen tai kiintolevyn sisältöön, vaikka ohjaus lienee annettu siksi, että reksiterinpitäjät osaisivat salata tiedot riittävän vahvasti.

Tietosuojavaltuutettu on käyttänyt 58(2) artiklan mukaisia korjaavia toimivaltuuksiaan verraten säästeliäästi. Eniten toimivaltuuksista on käytetty b) alakohdan mukaista huomautusta siitä, että reksiterinpitäjän toiminta ei ole täyttänyt tietosuoja-asetuksen vaatimuksia. Huomautus on toimivaltuus valikoiman hellävaraisimmasta päästä. Toinen usein käytetty toimivaltuus oli d) alakohdan mukainen määräys reksiterinpitäjälle saattaa henkilötietojen käsittelytoimet tietosuoja-asetuksen mukaisiksi. Myös tämä toimivaltuus on usein helposti perusteltavissa ja silti tehokas tapa osoittaa rekisterinpitäjälle tietosuojan korjaustarpeet. Toimivaltuuksista ankarinta, kiinnostavinta ja ehkä pelätyintäkin hallinnollista seuraamusmaksua tietosuojavaltuutettu on käyttänyt sosiaali- ja terveydenhuollon reksiterinpitäjiin ja henkilötietojen käsittelijöihin tarkasti harkiten. Määrätyt seuraamusmaksut ovat olleet varsin maltillisia lukuun ottamatta massiivista Psykoterapiakeskus Vastaamon tapausta. Korjaavat toimivaltuudet vaikuttavat tukevan hyvin tietosuojavaltuutetun valvontatoimia.

Tutkielman toteuttaminen. Tutkielman aihe oli ajankohtainen ja tuore tutkielmaa aloitettaessa, mutta sen valmistumisen viivästyessä tietosuojaa ja myös sote-alan tietosuojaa koskevaa kirjallisuutta alkoi ilmestyä enemmän[230]. Uudet teokset helpottivat tutkielman tekoa, mutta osaltaan myös alentavat sen arvoa ”ensimmäisen aallon” tutkimuksena. Esimerkiksi Voutilainen ja Kurvinen ovat kirjoittaneet teoksen: Asiakas- ja potilastietojen käsittelyn sääntely (2024), jossa tarkastellaan osittain samoja tietosuojavaltuutetun ratkaisuja läpi, kuin tässä tutkielmassa. Samoin Defensor legisissä julkaistu artikkeli[231] Tietosuojan viranomaisvalvonnan ja seuraamusjärjestelmän kehitys, käsittelee samaa aihepiiriä. Näkökulma tässä tutkielmassa on kuitenkin eri ja aineistossa mennään syvemmälle kuin edellä mainituissa

[230] Esim. Korpisaaren tietosuoja, Asiakas- ja potilastietojen käsittelyn sääntely. Ei vielä julkaistu: Lindström, Amanda, Liisa Murto, ja Assi Uuskallio. Asiakastietojen Käsittely Sosiaali- Ja Terveydenhuollossa.
[231] Paasonen & Luomala 2024, s. 40–66.

julkaisuissa, joten tutkielma lunastaa paikkansa oikeustieteellisen tiedon kartuttamisessa. Tutkielmalla on arvoa myös tietosuojavaltuutetun ohjaukseen kohdistuvana tutkimuksena.

Tutkielman aineiston rajaamisessa tuli valita laaja, julkaisematon aineisto ja sen saatavuus ja tietosuojakysymykset tai pienempi julkaistu aineisto. Julkaistut päätökset ovat ohjauksellisesti merkityksellisempiä, joten aineistona se palveli tutkimuskysymyksiin vastaamista. Aineiston selvä jakautuminen kahden eri lainsäädännön kesken toi haasteita, mutta myös perspektiiviä. Oikeus on kuitenkin dynaamista ja sitä on vaikea kuvata pysäytyskuvana, joten tutkielmassa kuvataan osaltaan myös muutosta. Lisäksi muuttuvien osien määrää lisäsi sekä tietosuojalainsäädännön pirstaleisuus, sosiaali- ja terveydenhuollon lainsäädännön monitahoisuus ja molempien sääntelyn muuttuminen tarkastelujakson aikana.[232] Lisäksi myös sosiaali- ja terveydenhuollon järjestämisvastuun siirtyminen hyvinvointialueille ja siihen liittyvä uusi lainsäädäntö toi vielä yhden muuttujan haasteelliseen säädösviidakkoon. Kaikkia sääntelyn nyansseja ja muutoksia oli mahdotonta sisällyttää tutkielmaan.

Jatkotutkimusta. Tutkielman pohjalta nousi muutamia ajatuksia jatkotutkimuksen aiheiksi, joita oikeustieteellisessä tutkimuksessa voisi tarkastella. Tämä tutkielma keskittyi sosiaali- ja terveydenhuollon rekisterinpitäjiin, jotka käsittelevät terveystietoja. On kuitenkin myös muita toimijoita, joilla on lain mukaan oikeus käsitellä vastaavia arkaluonteisia tietoja, kuten työnantajat ja vakuutusyhtiöt. Olisi myös kiinnostavaa tehdä vertaileva tutkimus jonkin toisen alan saamasta tietosuojavaltuutetun ohjauksesta. Tällaisia aloja voisi olla poliisi (turvallisuus ja oikeushallinto), työelämän toimijat, opetusala, finanssisektori tai jollain muulla tavalla koottu tietosuojavaltuutetun yhtenäinen valvontakohde.

Tietosuojavaltuutetusta löytyy vähän kirjallisuutta. Tietosuojavaltuutettu ja sen valvonta nostetaan kyllä yleensä tietosuojaa koskevien kirjojen yhdeksi alaluvuksi, mutta luvuissa on lähinnä toistettu tietosuojavaltuutettua koskevaa sääntelyä (kuten tässäkin tutkielmassa). Mielestäni olisi paikallaan kirjoittaa tietosuojavaltuutetusta, sen toiminnasta, historiasta, tehtävien muuttumisesta ja toimivallan lisääntymisestä. Tietosuojavaltuutetun tehtävästä ja merkityksestä yhteiskunnassa voisi kirjoittaa tutkimuksen, historiikin, oppikirjan tai tietokirjamaisen teoksen. Myös tietosuojavaltuutetun ennakkokuulemispyynnöistä löytyy myös hyvin vähän tietoa, vaikka ne vastaavat jollain tavalla vanhoja tapauksia, joissa kysyttiin

[232] Myös Voutilainen ja Kurvinen 2024, s. 5–6, ovat kuvanneet sosiaali- ja terveydenhuoltoon liittyvää lainsäädäntökenttää sekavaksi ja vaikeaselkoiseksi ja tämänkin tutkielman tekoaikaa sosiaali- ja terveydenhuollon lainsäädännön osalta turbulenttiseksi ajaksi.

tietystä asiasta tietosuojavaltuutetun kantaa. Niistä saisi hyvin tuoretta tietoa siitä, millaiset asiat tietosuojassa rekisterinpitäjiä askarruttaa.

Tietosuojavaltuutetun ratkaisut osoittautuivat yllättävän monimuotoisiksi. Niissä oli karkea yhtenäinen rakenne, mutta sitä voisi luettavuuden vuoksi yksinkertaistaa. Ratkaisuissa oli jonkin verran eroja alaotsikoiden ja käsittelyn etenemisen selostusten kesken ja ne olivat usein sääntelyn ja yksityiskohtaisten kuvausten kudelma, jonka seuraamista järjestelmällinen rakenne voisi helpottaa. Tapaukset on kuitenkin tarkoitettu ohjeeksi sekä rekisterinpitäjille että rekisteröidyille, joiden tietämys tietosuoja-alasta ja sen käsitteistä vaihtelee. Joissain päätöksissä oli kuitenkin ilahduttavasti rakenne, joka muistutti korkeimpien oikeuksien ennakkopäätösten rakennetta kappalenumerointeineen ja alussa olevalla oikeuskysymyksen ja lopputuloksen tiivistämisenä.[233] Tähän suuntaan julkaistavien päätösten soisi jatkossa kehittyvän lisää.

Aivan lopuksi voidaan todeta, että tietosuojavaltuutettu on tämän tutkielman perusteella auttanut sosiaali- ja terveydenhuollon toimijoita toteuttamaan hyvää tiedonhallintatapaa ja hyvää tietosuojaa osoittaen rikkomukset ja laiminlyönnit sekä antamalla yleisempääkin ohjausta. Tietosuojassa on aina kehittämisen varaa ja arkaluonteisimpia tietojamme tulee suojata jatkossa vieläkin paremmin, mutta tutkielman tekijää huojensi se, että selvää huolimattomuutta tai välinpitämättömyyttä tietosuojaa kohtaan esiintyi sosiaali- ja terveydenhuollossa loppujen lopuksi hyvin vähän.

[233]Esimerkiksi: ATSV 5546/163/2019 Henkilötietojen käsittelyn turvallisuus ajanvarausjärjestelmässä.

7 LIITTEET

LIITE 1 Korjaavat toimivaltuudet tietosuoja-asetuksen mukaisissa tapauksissa

Dnro ja otsikko	Käytetyt toimivaltuudet
ATSV/29/2020 Henkilötunnuksen sisältävien automatisoitujen tekstiviestien lähetys terveydenhuollossa	d) määräys saattaa käsittelytoimet tietosuoja-asetuksen mukaisiksi
ATSV 6629/163/21 Oikeus tutustua magneettikuviin maksutta	b) huomautus, että käsittelytoimet ovat olleet tietosuoja-asetuksen vastaisia d) määräys saattaa käsittelytoimet tietosuoja-asetuksen mukaisiksi
ATSV 9707/152/19 Rekisteröidyn oikeus tutustua tietoihinsa ja oikeuden puutteellinen toteutus	b) huomautus, että käsittelytoimet ovat olleet tietosuoja-asetuksen vastaisia i) hallinnollinen sakko
ATSV TSV/3/2019 Henkilön tunnistaminen terveydenhuollon sähköisessä ajanvarausjärjestelmässä	d) määräys saattaa käsittelytoimet tietosuoja-asetuksen mukaisiksi
ATSV 4022/171/22 Arkaluonteisten henkilötietojen asianmukainen suojaaminen ja henkilötietojen turvallinen käsittely	b) huomautus, että käsittelytoimet ovat olleet tietosuoja-asetuksen vastaisia
ATSV 9492/153/22 Rekisteröidyn oikeuksien käyttäminen alaikäisen lapsen puolesta	-
ATSV 6482/186/2020 Automatisoitujen yksittäispäätösten syntyminen ennakoivan terveydenhuollon työkalussa	a) varoitus, että aiotut käsittelytoimet ovat todennäköisesti tietosuoja-asetuksen vastaisia
ATSV 5546/163/2019 Henkilötietojen käsittelyn turvallisuus ajanvarausjärjestelmässä	b) huomautus, että käsittelytoimet ovat olleet tietosuoja-asetuksen vastaisia
ATSV 3895/83/22 Potilastietojen käsittely ennaltaehkäisyn ja ennakoinnin tarkoituksissa sekä automatisoidut yksittäispäätökset	a) varoitus, että aiotut käsittelytoimet ovat todennäköisesti tietosuoja-asetuksen vastaisia
ATSV 8493/161/21 Rekisteröidyn tarkastusoikeuden toteuttaminen ja informointi potilastietojen käsittelystä	b) huomautus, että käsittelytoimet ovat olleet tietosuoja-asetuksen vastaisia c) määräys noudattaa rekisteröidyn pyyntöä

	d) määräys saattaa käsittely-toimet tietosuoja-asetuksen mukaisiksi i) hallinnollinen sakko
ATSV 6602/161/2021 Koronarokotustietojen käytettävyys ja tietoturvaloukkauksesta ilmoittaminen	b) huomautus, että käsittely-toimet ovat olleet tietosuoja-asetuksen vastaisia
ATSV 1150/161/2021 Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen	b) huomautus, että käsittely-toimet ovat olleet tietosuoja-asetuksen vastaisia i) hallinnollinen sakko
ATSV 6132/151/19 Potilaan tarkastusoikeuden toteuttaminen terveydenhuollossa röntgen- ja magneettikuvien osalta	c) määräys noudattaa rekisteröidyn pyyntöä d) määräys saattaa käsittely-toimet tietosuoja-asetuksen mukaisiksi
ATSV 6745/163/18 Potilastietojen käsittely ammatillista kehittymistä varten hoitosuhteen päätyttyä	d) määräys saattaa käsittely-toimet tietosuoja-asetuksen mukaisiksi
TSV 3096/161/21 Potilastietojen luovuttaminen vakuutusyhtiöille ja tietojen minimointi	b) huomautus, että käsittely-toimet ovat olleet tietosuoja-asetuksen vastaisia d) määräys saattaa käsittely-toimet tietosuoja-asetuksen mukaisiksi
TSV 8235/154/18 Asiakkaan pyyntö henkilötietojen poistosta ja henkilötietojen käsittelyperuste	b) huomautus, että käsittely-toimet ovat olleet tietosuoja-asetuksen vastaisia c) määräys noudattaa rekisteröidyn pyyntöä
TSV 5242/157/2018 Tietojen luovuttaminen sosiaali- ja terveydenhuollosta kuljetuspalveluille kuljetusten järjestämistä varten	-
TSV 5036/183/2019 Henkilötietojen rekisterinpitäjästä ja käsittelijästä	-
TSV 28/523/2018 Jäljennösten saaminen sosiaalihuollon asiakastiedoista	-
TSV 2691/171/19 Henkilötietoasiakirjoja sisältävän postipaketin katoaminen	e) määräys ilmoittaa rekisteröidylle tietoturvaloukkauksesta