Referee-artikkeli

Tietosuojan viranomaisvalvonnan ja seuraamusjärjestelmän kehitys – tarkastelussa tietosuojavaltuutetun ja seuraamuskollegion päätöksiä vuosilta 2018–2022

Jyri Paasonen ja Mikko Luomala

TIIVISTELMÄ

Henkilötietojen suojaa koskeva lainsäädäntö on Suomessa kehittynyt ja muokkaantunut sekä teknologian kehityksen harppauksien että EU:n sääntelyn kehityksen myötä. Artikkelissa tarkastellaan tietosuojan viranomaisvalvontaa ja sitä koskevaa lainsäädännön kehitystä sekä seuraamusjärjestelmää. Lisäksi tarkastellaan tietosuojavaltuutetun ja seuraamuskollegion antamia yleisen tietosuoja-asetuksen mukaisia päätöksiä 2018–2022, jotka on julkaistu Finlexissä. Tietosuojavaltuutetun antamista päätöksistä merkittävä osa koski yrityksiä. Hallinnollisen seuraamusmaksun määräämisen ennustettavuus ei ole täysin selkeää. Euroopan tietosuojaneuvostossa on tunnistettu haaste, että seuraamusmaksujen määräämiskäytäntö ei ole yhdenmukaista. Tämän takia he ovat laatineet muun muassa ohjeen hallinnollisten seuraamusmaksujen laskemiseen. Ylipäätään Euroopassa tietosuojavalvontaviranomaiset ovat määränneet entistä enemmän seuraamusmaksuja, kun niiden kokonaismäärä on kasvanut 50 prosentin vuosivauhdilla. Tämä on herättänyt keskustelua useissa valtioissa siitä, että organisaatiot ovat yhä varovaisempia ilmoittamaan tietosuojarikkomuksista, koska pelkäävät sakkoja ja korvausvaatimuksia. Tietosuojan kannalta tietoturvallisuuden kontrollien tehokkuudella ja organisaatioiden riskienhallinnan sekä säätelyn toimivuudella on merkitystä, jotta henkilötietoja voidaan suojata tehokkaasti.

1 Johdanto

Tietosuojalainsäädännön valmistelu alkoi Suomessa 1970-luvun alkupuolella. Tietosuojakomitea jätti joulukuussa 1981 (1981:66) mietintönsä, johon sisältyi ehdotus henkilörekisterilaiksi, laiksi tietosuojalautakunnasta ja tietosuoja-asiamiehestä sekä laiksi yleisten asiakirjain julkisuudesta annetun lain muuttamisesta samoin kuin luonnokset annettaviksi asetuksiksi. Vuonna 1986 annettiin varsinaiseen lainsäädännön vahvistamiseen johtanut hallituksen esi-

tys, jonka eduskunta hyväksyi eräin muutoksin. Henkilörekisterilaki (471/1987) siihen liittyvine lainsäädäntöineen (472–477/1987) vahvistettiin tulemaan voimaan 1.1.1988.[1]

Yksilön oikeutta omiin tietoihinsa oli Suomessa suojattu perinteisesti ensisijaisesti rikosoikeudellisin keinoin, kuten jälkikäteisellä puuttumisella toimiin, joista oli aiheutunut yksilölle haittaa. Tästä esimerkkeinä olivat kotirauhaa, salakuuntelua ja -katselua sekä intimiteettisuojaa ja joukkotiedotusvälineitä koskevat säännökset. Henkilörekisterilainsäädännön voimaantulo vuonna 1988 muutti aikaisempaa tilannetta merkittävästi, koska uusi lainsäädäntö rakentui tavoitteelle ennakolta estää henkilötietojen käytöstä johtuvat yksityisyyden suojan loukkaukset. Tämän myötä yksilöllä oli lähtökohtaisesti päätösvalta siitä, miten häntä koskevia tietoja sai käyttää, jollei lainsäädännössä toisin osoitettu.[2]

Euroopan unioni hyväksyi direktiivin yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (95/46/EY, henkilötietodirektiivi). Direktiivi määritteli henkilötietojen suojaa koskevan sääntelyn perustason ja edellytti useissa kohdin henkilörekisterilakia yksityiskohtaisempaa ja rekisteröidyn oikeuksia laajentavaa sääntelyä.[3] Vuonna 1999 voimaan tuli henkilötietolaki (523/1999), jolla kumottiin henkilörekisterilaki.

Vuonna 2016 annettiin Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46 EY kumoamisesta (EU 2016/679, yleinen tietosuoja-asetus, General Data Protection Regulation), jonka tarkoituksena oli nykyaikaistaa ja yhdenmukaistaa EU:n tietosuojalainsäädäntöä. Yleinen tietosuoja-asetus on kansallisesti suoraan sovellettava säädös, mutta se jättää eräissä asioissa jäsenvaltioille direktiivinomaista kansallista liikkumavaraa. Yleisessä tietosuoja-asetuksessa on joitain velvoitteita jäsenvaltioille, esimerkiksi velvollisuus säätää eräistä kansallista valvontaviranomaista koskevista asioista. Yleistä tietosuoja-asetusta alettiin soveltaa kahden vuoden siirtymäajan jälkeen toukokuussa 2018.[4]

Yleisen tietosuoja-asetuksen edellyttämien muutosten seurauksena säädettiin henkilötietolain kumonnut henkilötietojen käsittelyyn sovellettava yleislaki, tietosuojalaki (1050/2018), joka tuli voimaan 1.1.2019. Tietosuojalakia sovelletaan rinnakkain yleisen tietosuoja-asetuksen kanssa. Tietosuojalaissa säädetään henkilötietojen käsittelyn oikeusperusteesta ja erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelystä eräissä tilanteissa, tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettavasta ikärajasta, valvontaviranomaisesta, seuraamuksista ja tietojenkäsittelyn erityistilanteista.[5]

Tämä artikkeli on jatkotutkimus kyberrikoksiin liittyviin tutkimuksiin, joissa olemme keskittyneet erityisesti kyberrikosten rangaistuskäytäntöön tuomioistuimissa vuosina 2015–2019. Olemme aiemmissa tutkimuksissamme tarkastelleet henkilörekisteri- ja tietosuojarikoksia, mutta emme tietosuojan valvontaviranomaisen päätöksiä ja tämän antamia seuraamuksia. Tämän artikkelin tavoitteena on paikata tätä tietovajetta tarkastelemalla lainopillisesti tietosuojan viranomaisvalvontaa ja seuraamuksia sekä sääntelyn kehitystä erityisesti

[1] Oikeusministeriö, EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Oikeusministeriön julkaisuja 35/2017, s. 15. Saatavissa osoitteessa http://urn.fi/URN:ISBN:978-952-259-612-3.

[2] HE 96/1998 vp: Hallituksen esitys eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi, s. 4.

[3] Oikeusministeriö 2017, s. 16.

[4] HE 9/2018 vp: Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, s. 4.

[5] HE 9/2018 vp, s. 1.

kansallisesta näkökulmasta. Empiirisesti tarkastellaan tietosuojavaltuutetun ja seuraamuskollegion antamia yleisen tietosuoja-asetuksen mukaisia päätöksiä 2018–2022, jotka on julkaistu Finlexissä.

Artikkelin alussa tarkastelemme tietosuojan viranomaisvalvontatoimintaa ja sitä koskevaa lainsäädännön kehitystä. Tämän jälkeen tarkastelemme tietosuojaa koskevaa seuraamusjärjestelmää, hallinnollisten seuraamusmaksujen määräämismenettelyä ja seuraamusjärjestelmän mahdollistamia muita sanktioita. Sitten analysoimme tietosuojavaltuutetun ja seuraamuskollegion antamia päätöksiä sekä kuvaamme yksittäisten tapausten piirteitä esimerkinomaisesti valottamaan tyypillisiä tietosuojaloukkauksia. Artikkelin lopussa esitämme kokoavia johtopäätöksiä.

2 Tietosuojan valvontaviranomaistoiminta ja lainsäädännön kehitys

Henkilörekisterilain säätämisen yhteydessä säädettiin ensimmäiset säännökset tietosuojan valvontaviranomaisista laissa tietosuojalautakunnasta ja tietosuojavaltuutetusta (474/1987). Automaattisen tietojenkäsittelyn kehittyminen ja tietojenkäsittelylaitteiston halpeneminen yhdessä yhteiskunnallisen päätöksenteon laajentumisen kanssa aiheuttivat tarpeen säätää tietosuojan valvontatehtäviä varten oma viranomaisorganisaatio oikeusministeriön yhteyteen. Lisäksi automaattisen tietojenkäsittelyn käyttöönotto ja toisaalta alan nopea laajeneminen lisäsivät myös merkittävästi yhä laajempien ja moninaisempien henkilötietoja sisältävien tiedostojen syntymistä. Valvontaviranomaisia koskeneilla säännöksillä pyrittiin paikkaamaan puutteellista lainsäädäntöä muun muassa säätämällä rekisteröityjen mahdollisuudesta valvoa heitä itseään koskevien tietojen rekisteröintiä.[6]

Tietosuojavaltuutetun tehtävät suuntautuivat henkilörekisterilain vastaisten menettelyjen ehkäisemiseen seuraamalla, valvomalla ja ohjaamalla henkilörekisterien perustamista, käyttöä ja niissä olevien tietojen luovutusta. Kansalaisilla oli oikeus tehdä ilmoitus tietosuojavaltuutetulle havaitsemistaan tai epäilemistään lainvastaisuuksista. Lisäksi rekisteröity pystyi tekemään tietosuojavaltuutetulle hakemuksen tarkastusoikeutta ja tietojen oikaisua koskevan määräyksen antamisesta. Varsinaisista kielloista, velvoitteista, uhkasakoista ja poikkeuslupien antamisesta päättäminen säädettiin tietosuojalautakunnan velvollisuudeksi.[7] Tietosuojalautakunnasta ja tietosuojavaltuutetusta annettuun lakiin tehtiin pieniä, lähinnä valtion virkamieslainsäädännöstä johtuneita muutoksia vuonna 1994, jolloin myös lain numero muuttui (389/1994).[8]

Tietosuojaviranomaisia koskeneita säännöksiä arvioitiin uudelleen henkilötietodirektiivin täytäntöönpanon ja henkilörekisterilain kumoamisen yhteydessä. Henkilötietolain esitöissä otettiin huomioon henkilötietodirektiivin asettamat velvoitteet jäsenvaltioille valvontaviranomaisesta säätämisestä. Direktiivin 28 artiklan mukaan jäsenvaltioiden oli säädettävä siitä, että jäsenvaltioiden henkilötietodirektiivin mukaisesti toteuttamien toimenpiteiden sovelta-

[6] HE 49/1986 vp: Hallituksen esitys eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi, s. 4, 8 ja 12–13.

[7] HE 49/1986 vp, s. 60.

[8] HE 311/1993 vp; Hallituksen esitys eduskunnalle laeiksi henkilörekisterilain ja yleisten asiakirjain julkisuudesta annetun lain 18 a §:n muuttamisesta sekä laiksi tietosuojalautakunnasta ja tietosuojavaltuutetusta, s. 1.

mista sen alueella valvoo yksi tai useampi julkinen viranomainen, jolla on riittävät toimivaltuudet. Henkilötietolakia edeltäneen lainsäädännön mukaan tietosuojavaltuutettu ei ollut voinut tehdä rekisterinpitäjää sitovia päätöksiä. Henkilötietolakiin uudistettiin tietosuojavaltuutetun päätösvalta rekisterinpitäjiin kohdistuvista sitovista määräyksistä rekisteröidyn tarkastusoikeutta ja tiedon korjaamista koskevissa asioissa, joista tuli myös valituskelpoisia. Muutoksen tarkoitus oli tehostaa tietosuojavaltuutetun toimivaltuuksia ja osaltaan taata rekisteröidylle henkilötietodirektiivin edellyttämät oikeussuojatakeet sekä selkeyttää tietosuojavaltuutetun ja tietosuojalautakunnan tehtävänjakoa. Henkilötietodirektiivin mukaisten riittävien oikeussuojakeinojen turvaamisen tarpeen takia henkilötietolakiin muutettiin myös tietosuojalautakunnan lupatoimivallan antamat päätökset ja määräykset muutoksenhakukelpoisiksi hallintolainkäyttölain periaatteiden mukaisesti. Yhtenä keskeisenä uudistuksena laajennettiin myös tietosuojavaltuutetun oikeutta määrätä itse asettamansa uhkasakko maksettavaksi. Tälläkin pyrittiin tehostamaan tietosuojavaltuutetun toimivaltuuksia henkilötietodirektiivin edellyttämällä tavalla.[9]

2.1 Yleinen tietosuoja-asetus velvoitti säätämään valvontaviranomaisesta

Nykyään yleinen tietosuoja-asetus sisältää varsin yksityiskohtaiset ja kattavat säännökset seuraamusjärjestelmästä ja valvontaviranomaisen toimivaltuuksista. Yleinen tietosuoja-asetus edellytti voimaan tullessaan valtioita säätämään valvontaviranomaisen perustamisesta, pätevyydestä ja kelpoisuusehdoista. Lisäksi jäsenvaltioiden tuli säätää valvontaviranomaisen jäsenten nimittämiseen sovellettavista säännöistä tai menettelyistä sekä kunkin valvontaviranomaisen jäsenen tai jäsenten toimikauden kestosta, jonka on oltava vähintään neljä vuotta. Yleinen tietosuoja-asetus ei sisällä säännöksiä valvontaviranomaisten lukumäärästä eikä valvontaviranomaisen organisaatiorakenteesta. Nämä jätettiin jäsenvaltioiden kansallisen liikkumavaran alueelle. Valvontaviranomaisen riippumatonta asemaa, toimivaltaa, tehtäviä, valtuuksia, yhteistyötä ja yhdenmukaisuutta koskevista säännöksistä on säädetty yleisen tietosuoja-asetuksen VI–VII luvuissa.[10] [11]

Huomionarvoista on, ettei Suomessa tietosuojaviranomaisella ole aiemmin ollut valtuuksia määrätä varsinaisia rangaistuksenomaisia hallinnollisia seuraamusmaksuja tai muita rangaistuksenomaisia hallinnollisia seuraamuksia, vaikkakin kansallisessa oikeusjärjestyksessä on kuitenkin sinänsä tavanomaista, että viranomaisella voi olla toimivalta määrätä kyseisiä seuraamusmaksuja. Tietosuoja-asetuksen voimaan tullessa Suomessa elettiinkin eräänlaista välivaihetta ennen tietosuojalain säätämistä, koska ei ollut sääntelyä viranomaisesta, jolla olisi ollut toimivalta määrätä tietosuoja-asetuksen mukaisia seuraamuksia.[12] [13]

---

[9] HE 96/1998 vp: Hallituksen esitys eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi, s. 27, 72 ja 75.

[10] HaVM 13/2018 vp: Hallintovaliokunnan mietintö hallituksen esityksestä eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, s. 11.

[11] HE 9/2018 vp, s. 43.

[12] HE 9/2018 vp, s. 8. 18.

[13] Jukka Lång – Tuomas Haavikko, Mitä muutoksia uusi kansallinen tietosuojalaki tuo käytännössä? Edilex 2019/2. Saatavissa osoitteessa www.edilex.fi/artikkelit/19271.

Yleisen tietosuoja-asetuksen 51 artiklan mukaan valvontaviranomainen on vastuussa asetuksen soveltamisen valvonnasta luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojaamiseksi henkilötietojen käsittelyssä ja henkilötietojen vapaan liikkuvuuden helpottamiseksi unionissa. Jäsenvaltioiden valvontaviranomaisten on myötävaikutettava asetuksen yhdenmukaiseen soveltamiseen kaikkialla unionissa, ja sitä varten valvontaviranomaisten on tehtävä yhteistyötä keskenään ja komission kanssa asetuksessa säädetyllä tavalla. Yleisen tietosuoja-asetuksen johdonmukaisen soveltamisen edistämiseksi asetuksessa säädetään Euroopan tietosuojaneuvoston perustamisesta, joka on riippumattomaton unionin elin. Keskeinen edellytys henkilötietojen suojaa valvoville viranomaisille on säädetty tietosuoja-asetuksen 52 artiklassa, jonka mukaan valvontaviranomaisen on toimittava täysin riippumattomasti hoitaessaan tehtäviään ja käyttäessään valtuuksiaan.[14]

Jäsenvaltioiden tulee yleisen tietosuoja-asetuksen 54 artiklan mukaan säätää myös siitä, voidaanko valvontaviranomaisen jäsenet nimittää uudelleen ja, jos voidaan, kuinka moneksi toimikaudeksi. Lisäksi jäsenvaltioiden kansallisen lainsäädännön tulee sisältää säännökset valvontaviranomaisen jäsenen tai jäsenten ja henkilöstön velvollisuuksia koskevista edellytyksistä, yhteensopimatonta toimintaa ja yhteensopimattomia ammatteja ja etuja koskevista kielloista toimikauden aikana ja sen jälkeen sekä tehtävien päättymistä koskevista säännöistä. Valvontaviranomaisen tehtävistä säädetään yksityiskohtaisesti yleisen tietosuoja-asetuksen 57 artiklassa. Tehtäviin kuuluu muun muassa asetuksen soveltamisen valvonta ja toimeenpano sekä henkilötietojen käsittelijöiden ja rekisterinpitäjien tietämyksen edistäminen niille asetuksen mukaan kuuluvista velvollisuuksista. Valvontaviranomaisen toimivalta perustuu tietosuoja-asetuksen 58 artiklaan.

2.2 Kansalliset valvontaviranomaista koskevat säännökset tietosuojalakiin

Säännökset valvontaviranomaisesta sisällytettiin tietosuojalain 3 luvun 8–20 §:ään. Yleisessä tietosuoja-asetuksessa tarkoitettuna kansallisena valvontaviranomaisena oikeusministeriön yhteydessä toimii tietosuojavaltuutettu, joka on toiminnassaan itsenäinen ja riippumaton (8 §). Tietosuojavaltuutettu säädettiin oikeusministeriön yhteydessä jatkamaan tietosuojavalvontaviranomaisena pienin rakenteellisin muutoksin. Valtuutetun itsenäisyys ja riippumattomuus tarkoittaa ratkaisu- ja muussa toiminnassa riippumattomuutta muiden tahojen, kuten viranomaisten tai eri intressiryhmien samoin kuin ratkaistavana olevan asian osapuolten, vaikutuksesta. Edellytykset on pitänyt säätää myös kansallisessa laissa, koska tietosuojavaltuutetun hoitaessa muita kuin yleisen tietosuoja-asetuksen mukaisia tehtäviä ei asetuksen riippumattomuutta koskeva 52 artikla tule suoraan sovellettavaksi.[15]

Tietosuojalain 9 §:n 1 momentin mukaan tietosuojavaltuutetulla on toimisto, jossa on vähintään kaksi apulaistietosuojavaltuutettua sekä tarpeellinen määrä tietosuojavaltuutetun tehtäväalaan perehtyneitä esittelijöitä ja muuta henkilöstöä. Valtuutetun lisääntyvän työmäärän ja käytännön kokemuksen näkökulmasta oli perusteltua säätää apulaistietosuojavaltuutetun virasta, jotta tietosuojavaltuutetun ratkaisu- ja puhevaltaa voitaisiin pysyvästi ja päätoimisesti hajauttaa tietosuojavaltuutetun toimiston sisällä useammalle taholle. Tietosuojavaltuutetun toimiston käsittelemien asioiden määrä olikin nelinkertaistunut vuoden 2000

[14] HE 9/2018 vp, s. 43.

[15] HE 9/2018 vp, s. 93.

jälkeen, ja myös yleisen tietosuoja-asetuksen myötä valtuutetun tehtävien määrän katsottiin kasvavan.[16]

Säännöksen myötä tietosuojavaltuutettu toimii toimistonsa päällikkönä, joten tämän tehtävänä on myös toimiston toiminnan yleinen johtaminen. Valtuutettu vastaa muun muassa toimiston sisäistä hallintoa koskevista asioista sekä siitä, että valvontaviranomaisen tehtävät hoidetaan tarkoituksenmukaisesti ja tehokkaasti. Tietosuojavaltuutetun tehtävänä on myös yhtenäisen tietosuojapolitiikan koordinointi ja kansallisen näkemyksen edustaminen eurooppalaisessa yhteistyössä. Apulaistietosuojavaltuutettu vastaa puolestaan tietosuojavaltuutetun sijaan tietyistä toimistolle kuuluvista henkilötietojen suojaa koskevista tehtävistä. Lisäksi apulaistietosuojavaltuutettu toimii tietosuojavaltuutetun sijaisena.[17]

Tietosuojalain 9 §:n 1 momenttiin on katsottu asianmukaiseksi säätää tietosuojavaltuutetun tehtävän tehokkaan hoitamisen resursoinnin näkökulmasta, että tietosuojavaltuutetun toimistossa on myös tarpeellinen määrä esittelijöitä ja muuta henkilöstöä.[18] Tähän on perustuslakivaliokunta kiinnittänyt lausunnossaan huomiota ja korostanut tietosuoja-asetuksen 52 artiklan 4 kohdan mukaista kunkin jäsenvaltion velvollisuutta varmistaa, että jokaiselle valvontaviranomaiselle osoitetaan tekniset, taloudelliset ja henkilöresurssit, tilat ja infrastruktuuri, jotka ovat tarpeen tehtävien suorittamiseksi ja valtuuksien käyttämiseksi tehokkaasti.[19]

Tietosuojalain 9 §:n 2 momentin mukaan tietosuojavaltuutettu nimittää toimiston virkamiehet ja ottaa palvelukseen toimiston muun henkilöstön. He toimivat tietosuojavaltuutetun yksinomaisessa ohjauksessa. Tällä turvataan valtuutetun itsenäistä ja riippumatonta asemaa. Sen sijaan apulaistietosuojavaltuutetun nimittää valtioneuvosto tietosuojalain 11 §:n mukaisesti. Molemmat, sekä tietosuojavaltuutettu että apulaistietosuojavaltuutettu, nimitetään valtioneuvoston toimesta viideksi vuodeksi kerrallaan. Tämä vastaa pitkälti aiempaa sääntelyä, sillä tietosuojalautakunnasta ja tietosuojavaltuutetusta annetun lain 6 §:n mukaan valtioneuvosto nimitti tietosuojavaltuutetun enintään viideksi vuodeksi.[20]

Myös valtuutettujen kelpoisuusvaatimukset tietosuojalaissa vastaavat pääosin aiempia tietosuojavaltuutetun viran kelpoisuusvaatimuksia. Tietosuojavaltuutetun ja apulaistietosuojavaltuutetun kelpoisuusvaatimuksena on tietosuojalain 10 §:n mukaan muu oikeustieteen ylempi korkeakoulututkinto kuin kansainvälisen ja vertailevan oikeustieteen maisterin tutkinto, hyvä perehtyneisyys henkilötietojen suojaa koskeviin asioihin sekä käytännössä osoitettu johtamistaito. Lisäksi edellytetään kykyä hoitaa kansainvälisiä tehtäviä. Tietosuojavaltuutetun ja apulaistietosuojavaltuutetun on annettava valtion virkamieslain (750/1994) 8 a §:ssä tarkoitettu selvitys sidonnaisuuksistaan (13 §).

Tietosuojalain 12 §:ssä säädetään tietosuojavaltuutetun toimiston asiantuntijalautakunnasta, joka on toimistoon kuuluva sisäinen asiantuntijaelin. Kyseessä on uudenlainen tietosuojalautakunnasta poikkeava toimielin, sillä lautakunta ei ole päätoiminen, vaan kokoontuu tarvittaessa puheenjohtajan koolle kutsumana. Sillä ei myöskään ole muodollista päätäntävaltaa. Ensimmäisen momentin mukaan asiantuntijalautakuntaan kuuluu puheenjohtaja, va-

16 HE 9/2018 vp, s. 93.

17 HE 9/2018 vp, s. 94.

18 HE 9/2018 vp, s. 94.

19 PeVL 3/2017 vp: Perustuslakivaliokunnan lausunto valtioneuvoston kirjelmän ehdotuksesta eduskunnalle Euroopan matkustajatieto- ja lupajärjestelmäksi (ETIAS), s. 6.

20 HE 9/2018 vp, s. 94–95.

rapuheenjohtaja ja kolme muuta jäsentä. Kullakin jäsenellä on henkilökohtainen varajäsen. Toisen momentin mukaan valtioneuvosto asettaa asiantuntijalautakunnan kolmen vuoden toimikaudeksi. Koska kyseessä on tietosuojavaltuutetun toimiston sisäinen asiantuntijaelin eikä muodollisia päätöksiä tekevä elin, ei kyse ole yleisen tietosuoja-asetuksen 54 artiklassa tarkoitetuista valvontaviranomaisen jäsenistä, joiden toimikauden pituuden on asetuksen mukaan oltava vähintään neljä vuotta.[21]

Tietosuojalain 12 §:n 3 momentin perusteella asiantuntijalautakunnan puheenjohtajaksi ja varapuheenjohtajaksi voidaan nimittää oikeustieteen muun ylemmän korkeakoulututkinnon kuin kansainvälisen ja vertailevan oikeustieteen maisterin tutkinnon suorittanut henkilö. Lisäksi puheenjohtajalta ja varapuheenjohtajalta edellytetään hyvää perehtyneisyyttä henkilötietojen suojaa koskeviin asioihin. Muilta jäseniltä ei edellytetä korkeakoulututkintoa, sillä heille riittää perehtyneisyys henkilötietojen suojaa koskeviin asioihin. Lisäksi edellytetään muuta tehtävän hoidon edellyttämää pätevyyttä. Lautakunnan jäsenten rikosoikeudellisesta virkavastuusta heidän suorittaessaan tietosuojalain mukaisia tehtäviä säädetään 4 momentissa. Jäsenten henkilökohtaisesta virkavastuusta säätäminen katsottiin tärkeäksi, sillä jäsenet eivät ole virkasuhteessa tietosuojavaltuutetun toimistoon. Asiantuntijalautakunnan jäsenellä on myös vahingonkorvauslain (412/1974) mukainen vahingonkorvausvastuu. Lisäksi 4 momentin mukaan lautakunnan jäsenille ja varajäsenille maksetaan tehtävästään palkkio.[22]

2.3 Tehtävistä ja toimivaltuuksista

Tietosuojavaltuutetun tehtävistä ja toimivallasta säädetään tietosuojalain 14 §:ssä, jonka 1 momenttiin sisältyy informatiivinen viittaus valvontaviranomaisen tehtäviä ja toimivaltuuksia koskevaan yleisen tietosuoja-asetuksen 55–59 artiklaan. Tietosuojavaltuutetun tehtävät ja toimivaltuudet seuraavat suoraan tietosuoja-asetuksesta. Lisäksi yleisen tietosuoja-asetuksen 58 artiklan 6 kohdan mukaan jäsenvaltio voi säätää laissa, että sen valvontaviranomaisella on muita kuin asetuksessa säädettyjä valtuuksia. Tämän vuoksi momentissa todetaan tietosuojavaltuutetulla olevan myös muita tehtäviä, jolla otetaan huomioon valtuutetun laaja yleistoimivalta ja muusta lainsäädännöstä tulevat tehtävät ja toimivaltuudet. Tietosuojavaltuutettu myös edustaa 3 momentin mukaan Suomea Euroopan tietosuojaneuvostossa. Lisäksi 4 ja 5 momentissa tietosuojavaltuutetun tehtäviksi on säädetty yleisen tietosuoja-asetuksen 43 artiklassa tarkoitetun sertifiointielimen akkreditointi sekä tietosuoja-asetuksen 59 artiklassa tarkoitetun vuosittaisen toimintakertomuksen laatiminen. Toimintakertomus toimitetaan eduskunnalle ja valtioneuvostolle, minkä lisäksi se on pidettävä yleisesti saatavilla.[23]

Tietosuojalain 15 §:n perusteella tietosuojavaltuutettu ratkaisee asiat esittelystä, mutta voi yksittäisessä tapauksessa myös itse ratkaista asioita. Valtuutettu ei kuitenkaan voi esimerkiksi työjärjestyksellä määrätä asiasta. Asiat tulevat vireille tietosuojavaltuutetun toimistossa joko rekisteröidyn, rekisterinpitäjän, henkilötietojen käsittelijän tai muun henkilön toimesta taikka tietosuojavaltuutetun omasta aloitteesta.[24] Apulaistietosuojavaltuutetun tehtävistä ja toimivaltuuksista säädetään puolestaan tietosuojalain 16 §:ssä, jonka mukaan tietosuojaval-

[21] HE 9/2018 vp, s. 96.
[22] HE 9/2018 vp, s. 96–97.
[23] HE 9/2018 vp, s. 96–97.
[24] HE 9/2018 vp, s. 99.

tuutetun ja apulaistietosuojavaltuutetun välisestä tehtävien jaosta määrätään tietosuojavaltuutetun toimiston työjärjestyksessä. Apulaistietosuojavaltuutetulla on tehtäviensä hoidossa samat toimivaltuudet kuin tietosuojavaltuutetulla. Lain esitöiden mukaan apulaistietosuojavaltuutetulla voi olla erilaisia tietosuojavaltuutetun toimiston tehtäväkenttään kuuluvia tehtäviä ja myös 14 §:ssä säädettäväksi ehdotettuja tehtäviä, jos siitä on työjärjestyksessä määrätty. Apulaistietosuojavaltuutettu hoitaa itsenäisesti sille työjärjestyksen mukaan kuuluvat tehtävät.[25]

Asiantuntijalautakunnan tehtävistä ja asioiden käsittelystä asiantuntijalautakunnassa säädetään tietosuojalain 17 §:ssä, jonka 1 momentin mukaan lautakunnan tehtävänä on tietosuojavaltuutetun pyynnöstä antaa lausuntoja henkilötietojen käsittelyä koskevan lainsäädännön soveltamiseen liittyvistä merkittävistä kysymyksistä. Asiantuntijalautakunnalla katsotaan olevan erityisen korostunut merkitys tilanteissa, joissa on kyse kansallisesta, yleistä tietosuoja-asetusta täydentävän lainsäädännön tulkinnasta.[26] Asiantuntijalautakunta voi myös 2 momentin mukaan kuulla ulkopuolisia asiantuntijoita. Kolmannessa momentissa säädetään lisäksi asiantuntijalautakunnan sihteeristä, jona toimii tietosuojavaltuutetun toimiston esittelijä. Tietosuojalain valvontaviranomaista koskeva 3 luku sisältää myös säännökset tietosuojavaltuutetun tiedonsaanti- ja tarkastusoikeudesta (18 §), yhteistyöstä kolmansien maiden valvontaviranomaisten kanssa (18 a §), asiantuntijoiden käytöstä (19 §) ja virka-avusta (20 §).

3 Tietosuojan seuraamusjärjestelmän kehitys

Henkilörekisterilakiin sisällytettiin rangaistussäännös, jolla kriminalisoitiin muun muassa automaattisen tietojenkäsittelyn avulla ylläpidettävään henkilörekisteriin tunkeutuminen (45 §). Kriminalisointi liittyi henkilörekisterien käyttöön liittyvien turvallisuusriskien pienentämiseen. Rekisterinpitäjälle asetettiin velvollisuus suojata rekisterit luvattomalta käytöltä, ja henkilötietoja sai luovuttaa ulkomaille vain erityisluvalla. Sen sijaan tiedostossa olevan tiedon lainvastaista muuttamista tai hävittämistä ei kriminalisoitu, koska ne päätettiin jättää rikoslain (39/1889) kokonaisuudistuksen yhteydessä säädettäväksi. Rikoslain kokonaisuudistuksen ensimmäisessä vaiheessa, jonka säännökset tulivat voimaan vuonna 1991, toteutettiin luvattoman käytön, petoksen, vahingonteon ja väärennyksen tunnusmerkistön nykyaikaistaminen. Säännökset soveltuivat siten automaattisten tietojen käsittelyn mahdollistamien tekojen arvostelemiseen[27]. Rikoslain kokonaisuudistuksen oli tarkoitus täydentää rikoslakia muun muassa tietojärjestelmiin kohdistuvia vahingontekoja sekä tietorikoksia koskevin säännöksin. Kokonaisuudessaan rangaistusseuraamukset liitettiin henkilörekisterilain 8 luvun 43–46 §:iin, joita vastaavat säännökset oli tarkoitus siirtää myöhemmin rikoslakiin.[28]

Henkilörekisterilaissa säädettynä henkilörekisteririkoksena pidettiin tahallista lainvastaista tekoa, joka loukkasi rekisteröidyn yksityisyyden suojaa tai aiheutti hänelle muuta vahinkoa tai olennaista haittaa, kuten esimerkiksi tallensi henkilörekisteriin arkaluonteisia tietoja.

[25] HE 9/2018 vp, s. 99.

[26] HE 9/2018 vp, s. 99.

[27] HE 94/1993 vp: Hallituksen esitys eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi, s. 133.

[28] HE 49/1986 vp: Hallituksen esitys eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi, s. 4, 20 ja 55.

Rangaistusasteikoksi henkilörekisteririkokselle oli säädetty sakkoa tai vankeutta enintään vuosi (43 §). Lievemmille lainvastaisille teoille, kuten tietolähteen tai tietojen luovuttamista koskevan kirjaamisvelvollisuuden laiminlyönnille, säädettiin rikosnimikkeeksi henkilörekisteririkkomus. Lisäksi henkilörekisteririkkomuksesta tuomittiin myös se, joka syyllistyi henkilörekisteririkoksena tarkoitettuun tekoon törkeästä huolimattomuudesta. Rangaistuksena henkilörekisteririkkomuksesta oli sakko (44 §). Henkilörekisteriin tunkeutumisena tuomittiin se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta tai muulla petollisella toiminnalla läpäisi tunnistuskontrollin tai vastaavan turvajärjestelyn ja siten oikeudettomasti tunkeutui automaattisen tietojenkäsittelyn avulla ylläpidettyyn henkilörekisteriin. Henkilörekisteriin tunkeutumisesta tuomittiin sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi (45 §). Lisäksi vielä henkilörekisteriä koskevan salassapitovelvollisuuden rikkonut tuomittiin sakkoon tai vankeuteen vähintään kuudeksi kuukaudeksi (46 §).

Henkilörekisterilailla saatettiin silloin ajan tasalle henkilötietojen rekisteröintiä ja yksityisyyden suojaa koskenut lainsäädäntö rangaistussäännöksineen. Rangaistussääntely havaittiin kuitenkin henkilörekisterejä valvovien viranomaisten toimesta puutteelliseksi siltä osin, etteivät säännökset koskeneet yhteysvaatimuksen vastaista tietojen rekisteröintiä, vaikka tämä vaatimus oli henkilörekistereiden asianmukaisuuden kannalta lain keskeisimpiä.[29] Yhteysvaatimuksesta säädettiin henkilörekisterilain 5 §:n 1 momentissa, jonka mukaan henkilörekisteriin merkittäväksi sai kerätä tai tallettaa ilman rekisteröidyn suostumusta tai tietosuojalautakunnan lupaa tietoja vain sellaisista henkilöistä, joilla oli asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan, jollei rekisterin pitäminen johtunut rekisterinpitäjälle säädetystä taikka lain tai asetuksen nojalla määrätystä tehtävästä.

3.1 Rikoslain lukuisat uudistukset

Rikoslaki on peräisin vuodelta 1889, ja sitä on uudistettu useita kertoja, mutta vielä ennen vuotta 1995 siitä puuttuivat tarkat tieto- ja viestintärikoksiin liittyvät säännökset. Rikoslain kokonaisuudistuksen toisessa vaiheessa, vuonna 1995 voimaan tulleella rikoslain muuttamisesta annetulla lailla (578/1995) säädettiin paheksuttavimmat henkilörekisterilain säännösten loukkaamistapaukset rangaistaviksi rikoslain tieto- ja viestintärikoksia koskevassa 38 luvussa. Lain esitöissä tunnistettiin uuden tietotekniikan kehityksestä ja käyttöönotosta johtuneet haasteet ja haavoittuvuudet erityisesti tiedon tallennuksessa sekä käsittelyn ja siirron uusien muotojen luotettavuudessa, tietoon liittyvien uusien taloudellisten arvojen suojaamisessa sekä kansalaisten yksityisyyden turvaamisessa uuden tekniikan aiheuttamia vaaroja vastaan. Muutoksella pyrittiin korostamaan uuden säännöstön yleistä painoarvoa ja yhteiskunnallista merkitystä, jota edellytti myös se, että tärkeimpiin säännöksiin liittyi vankeusrangaistusuhka. Näin ollen henkilörekisteririkoksesta säädettiin jatkossa rikoslain 38 luvun 9 §:ssä. Säännös vastasi henkilörekisterilain säännöstä, minkä lisäksi rangaistavaksi säädettiin sellaisten henkilöiden tietojen tallettaminen henkilörekisteriin, joilla ei ollut asiallista yhteyttä rekisterinpitäjän toimintaan.[30] Tämän lisäksi rikoslain 38 lukuun lisättiin rangaistussäännökset viestintäsalaisuuden loukkauksesta (3 §), törkeästä viestintäsalaisuuden loukkauksesta (4 §),

[29] HE 94/1993 vp, s. 141.

[30] HE 94/1993 vp, s. 132, 141 ja 145.

tietoliikenteen häirinnästä (5 §), törkeästä tietoliikenteen häirinnästä (6 §), lievästä tietoliikenteen häirinnästä (7 §) ja tietomurrosta (8 §).

Henkilörekisterilain korvanneeseen henkilötietolakiin rangaistussäännökset koottiin sen 48 §:n 1 momenttiin, johon lisättiin viittaussäännökset rikoslain säännöksiin henkilörekisteririkoksesta, henkilörekisteriin kohdistuvasta tietomurrosta ja henkilötietolain 33 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta. Henkilötietolain 48 §:n 2 momentissa säädettiin henkilötietorikkomuksesta. Momentti vastasi henkilörekisterilain 44 §:ää, minkä lisäksi siihen lisättiin tietosuojalautakunnan lupaan liitetyn lainvoimaisen määräyksen rikkominen tahallaan tai törkeästä huolimattomuudesta rangaistavaksi henkilötietorikkomuksena. Säännös poikkesi henkilörekisterilaista myös siten, että henkilörekisteririkkomuksesta ei enää tuomittu sitä, joka laiminlöi tietolähteen tai tietojen luovuttamista koskevan kirjaamisvelvollisuuden. Henkilötietorikkomusta koskeneilla säännöksillä pantiin toimeen henkilötietodirektiivin 24 artiklan jäsenmaille asetettu velvollisuus määritellä sanktiot, joita sovellettiin direktiivin mukaisesti säädettyjen säännösten rikkomistapauksissa.[31] Henkilötietolain säätämisen yhteydessä myös rikoslain henkilörekisteririkosta koskenutta rangaistussäännöstä muutettiin. Muutoksella selkeytettiin henkilörekisteririkoksen ja -rikkomuksen rajaa tekomuotojen erojen selkeyttämisellä sekä henkilörekisteririkoksen syyksiluettavuuden laajentamisella törkeän tuottamuksen kattavaksi.[32]

Henkilötietolain soveltamisen aikana EU:n henkilötietodirektiivin mukaisen jäsenvaltion henkilötietojen suojaa määrittävän lainsäädännön noudattamisen sanktiointia ei ollut kokonaan harmonisoitu. Näin ollen vuonna 2016 voimaan tulleen yleisen tietosuoja-asetuksen keskeinen tavoite, joka selittää myös asetuksen valintaa sääntelyinstrumentiksi, on sen johdanto-osan kappaleen 10 mukaan varmistaa yhdenmukainen ja korkeatasoinen luonnollisten henkilöiden suojelu ja poistaa henkilötietojen liikkuvuuden esteet unionissa harmonisoimalla luonnollisten henkilöiden oikeuksien ja vapauksien suojelun taso näiden tietojen käsittelyssä.[33]

3.2 EU:n neuvoston puitepäätösten ja yleissopimuksen vaatimuksien kansallinen implementointi

Ennen yleisen tietosuoja-asetuksen voimaantuloa rikoslain tieto- ja viestintärikoksia koskeva luku on saatettu vastaamaan muun muassa eräiden EU:n neuvoston puitepäätösten ja yleissopimuksen vaatimuksia. Vuonna 2007 voimaan tulleella rikoslain muuttamisesta annetulla lailla (540/2007) saatettiin rikoslaki vastaamaan vuonna 2001 Budapestissä tehdyn Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen sekä tietojärjestelmiin kohdistuvista hyökkäyksistä tehdyn neuvoston puitepäätöksen (2005/222/YOS) vaatimuksia. Edellä mainitulla rikoslain muuttamisesta annetulla lailla ankaroitettiin 38 luvun tietoliikenteen häirintää (5 §), törkeää tietoliikenteen häirintää (6 §) ja lievää tietoliikenteen häirintää (7 §) koskeneita säännöksiä, jolloin myös näiden rikosten yritys tuli rangaistavaksi. Lisäksi lisättiin

[31] HE 96/1998 vp, s. 75–76.

[32] HE 96/1998 vp, s. 77–78.

[33] Mikael Koillinen, Hallinnolliset seuraamukset tietosuojan sanktiomekanismina. Defensor Legis 4/2016, s. 570–571. Saatavissa osoitteessa https://www.edilex.fi/defensor_legis/168990005.

uudet rangaistussäännökset tietojärjestelmän häirinnästä (7 a §) ja törkeästä tietojärjestelmän häirinnästä (7 b §).

Tietojärjestelmiin kohdistuvista hyökkäyksistä tehdyn neuvoston puitepäätöksen 7 artiklan enimmäisrangaistuksen vähimmäistasoa koskevat vaatimukset saatettiin vastaamaan Suomen lainsäädäntöä säätämällä rikoslain tieto- ja viestintärikoksia koskevaan lukuun tietomurron törkeää tekomuotoa koskeva säännös (8 a §). Lisäksi uudella 12 §:n säännöksellä oikeushenkilön rangaistusvastuu laajennettiin kattamaan viestintäsalaisuuden loukkauksen, törkeän viestintäsalaisuuden loukkauksen, tietoliikenteen häirinnän, törkeän tietoliikenteen häirinnän, tietomurron, törkeän tietomurron, tietojärjestelmän häirinnän ja törkeän tietojärjestelmän häirinnän rikokset.[34] Rikoslain 38 luku saatettiin vastaamaan puitepäätöksen (2005/222/YOS) korvaamisesta annetun Euroopan parlamentin ja neuvoston tietoverkkorikosdirektiivin 2013/40/EU vaatimuksia vuonna 2015 voimaan tulleella rikoslain muuttamisesta annetulla lailla (368/2015). Keskeisimpiä uudistuksia olivat uudet säännökset identiteettivarkaudesta (9 b §) ja määritelmät (11 §) -säännös, joka sisälsi tietojärjestelmän ja datan määritelmät.

Suomessa seuraamusjärjestelmä on aiemmin painottunut vahvasti rikosoikeudelliseen järjestelmään, sillä kansallisella tietosuojaviranomaisella ei ole ollut henkilötietolain nojalla mahdollisuutta määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle hallinnollisia seuraamusmaksuja.[35] Yleisen tietosuoja-asetuksen johdanto-osan 11 kappaleen mukaan henkilötietojen suojaaminen tehokkaasti koko EU:n alueella edellyttää samantasoisia valtuuksia valvoa henkilötietojen suojaa koskevien sääntöjen noudattamista ja samantasoisia seuraamuksia sääntöjen rikkomisesta jäsenvaltioissa.[36] Ongelmaksi nähtiin, että seuraamusten taso ja ala vaihtelivat EU:n jäsenvaltioiden välillä, ja myös yleisen tietosuoja-asetuksen johdanto-osan kappaleessa 150 hallinnollisia seuraamuksia perustellaan erityisesti sillä, että hallinnolliset sakot ovat tarpeen asetuksen rikkomisen vuoksi määrättävien hallinnollisten seuraamusten lujittamiseksi ja yhdenmukaistamiseksi.[37]

3.3 Yleisen tietosuoja-asetuksen myötä seuraamusmaksut

Yleisen tietosuoja-asetuksen 83 artikla sisältää yleiset edellytykset hallinnollisten seuraamusmaksujen määräämiselle. Seuraamusmaksu määrätään tietosuoja-asetuksen 83 artiklan 2 kohdan mukaisesti kunkin yksittäisen tapauksen olosuhteiden perusteella asetuksen 58 artiklan 2 kohdan a–h ja j alakohdissa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta. Artiklan 84 kohdan 3 mukaan asetuksen eräiden säännösten rikkomisesta määrätään hallinnollinen seuraamusmaksu, joka on suuruudeltaan enintään 10 000 000 euroa, tai jos kyseessä on yritys, kaksi prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta

[34] HE 153/2006 vp: Hallituksen esitys eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta., s. 1 ja 67–68.

[35] Jyri Paasonen – Mikko Aaltonen – Mikko Luomala, Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset. Defensor Legis 4/2021, s. 971 ja 979. Saatavissa osoitteessa https://www.edilex.fi/defensor_legis/250670013.

[36] HE 153/2006 vp, s. 1 ja 67–68.

[37] Mikael Koillinen 2016, s. 570.

kokonaisliikevaihdosta sen mukaan, kumpi näistä on suurempi. Tällainen seuraamusmaksu määrätään rekisterinpitäjän ja henkilötietojen käsittelijän 8, 11, 25–39, 42 ja 43 artiklan mukaisten velvollisuuksien rikkomisesta, sertifiointielimen 42 ja 43 artiklan mukaisten velvollisuuksien rikkomisesta sekä 41 artiklan 4 kohdassa tarkoitetun valvontaelimen velvollisuuksien rikkomisesta.[38]

Yleisen tietosuoja-asetuksen 83 artiklan 5 kohdan mukaan asetuksen eräiden muiden säännösten rikkomisesta voidaan määrätä seuraamusmaksu, joka on enintään 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Tällainen korkeampi seuraamusmaksu voidaan määrätä esimerkiksi yleisen tietosuoja-asetuksen 5, 6, 7 ja 9 artiklassa tarkoitettujen käsittelyn perusperiaatteiden rikkomisesta, suostumuksen edellytykset mukaan luettuna, sekä rekisteröityjen 12–22 artiklojen mukaisten oikeuksien rikkomisesta. Lisäksi korkeampi seuraamusmaksu voidaan määrätä asetuksen 44–49 artiklojen sekä asetuksen IX luvun mukaisesti hyväksytystä jäsenvaltion lainsäädännöstä johtuvien velvollisuuksien rikkomisesta, valvontaviranomaisen 58 artiklan 2 kohdan nojalla antaman määräyksen, väliaikaisen tai lopullisen rajoituksen tai tietovirtojen keskeyttämismääräyksen noudattamatta jättämisestä tai 58 artiklan 1 kohdan mukaista pääsyn antamista koskevan velvollisuuden rikkomisesta.[39]

Hallintovaliokunta kiinnitti mietinnössään muun ohella huomiota hallinnollisen sakon määräämiseen liittyviin näkökohtiin. Yleisen tietosuoja-asetuksen 83 artiklan 2 kohdan mukaan hallinnollisen sakon määräämisessä ja sen suuruutta arvioitaessa on otettava huomioon useita seikkoja, kuten rikkomisen luonne, vakavuus, kesto, vahingollisuus, toistuvuus, tahallisuus ja tuottamuksellisuus. Näin ollen sääntely ei perustu ankaraan vastuuseen eikä käännettyyn todistustaakkaan, mikä on perusteltua Euroopan ihmisoikeussopimuksessa ja perustuslain (731/1999) 21 §:ssä tarkoitetun oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon kannalta.[40]

Lisäksi perustuslakivaliokunta on todennut, että kohdassa mainittujen seikkojen keskinäisen suhteen arvioimiseen jää merkittävästi harkinnanvaraa erityisesti hallinnollisen sakon suuruuden arvioimisessa, sillä asetuksessa asetetaan vain sakon enimmäistaso. Näin ollen hallintovaliokunta on katsonut hyvän hallinnon takeiden noudattamisen tärkeäksi hallinnollisen sanktion määräämisessä, koska hallinnollisessa sakossa on asiallisesti kyse rangaistusluonteisesta taloudellisesta seuraamuksesta, jonka Euroopan ihmisoikeustuomioistuin ja perustuslakivaliokunta ovat katsoneet rinnastuvan rikosoikeudelliseen seuraamukseen.[41]

3.4 Toimivalta seuraamusmaksujen määräämisessä

Toimivalta hallinnollisen sakon määräämiseen kuuluu yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan i alakohdan mukaan jäsenvaltion valvontaviranomaiselle. Suomessa kyseinen toimivalta kuuluu tietosuojavaltuutetulle. Näin ollen edellä esitettyjen hallinnollista seuraa-

[38] HE 9/2018 vp, s. 45.

[39] HE 9/2018 vp, s. 45–46.

[40] HaVM 13/2018 vp, s. 11–12.

[41] PeVL 14/2018 vp: Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, s. 18.

musmaksua koskevien tietosuoja-asetuksen artiklojen nojalla voidaan katsoa kansallisen valvontaviranomaisen toimivaltuuksien laajentuneen merkittävästi suoraan asetuksen nojalla.[42]

Yleisessä tietosuoja-asetuksessa on jätetty kansallista liikkumavaraa muun muassa tietosuoja-asetuksen 83 artiklan 7 kohdassa, jonka mukaan jäsenvaltiot voivat asettaa sääntöjä siitä, voidaanko viranomaisille tai julkishallinnon elimille määrätä kansallisesti hallinnollisia seuraamusmaksuja ja missä määrin. Erityisesti edellä mainittuun kohtaan jätetty laaja kansallinen liikkumavara herätti paljon keskustelua tietosuojalain valmisteluvaiheessa. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmäkään ei päässyt liikkumavaran käytöstä yksimielisyyteen. Mietinnössään työryhmä totesi muun muassa poikkeamisen tietosuoja-asetuksessa säädetystä seuraamusjärjestelmästä edellyttävän väistämättä vaihtoehtoista, tehokasta seuraamusjärjestelmää, joka voisi olla esimerkiksi rikosoikeudellinen, mutta sen arviointiin työryhmällä ei ollut kompetenssia tai tosiasiallista mahdollisuutta.[43] [44]

Tietosuojalain esitöissä ehdotettiin säädettäväksi sen 24 §:n 4 momenttiin, ettei hallinnollista seuraamusmaksua voida määrätä valtion viranomaisille, valtion liikelaitokselle, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille eikä tasavallan presidentin kanslialle. Tätä perusteltiin muun muassa sillä, että viranomaiselle määrättävän hallinnollisen seuraamusmaksun katsottiin olevan Suomen yleisen oikeusjärjestyksen kannalta vieras menettely, minkä vuoksi oli perusteltua sulkea seuraamus julkishallinnon osalta pois. Lisäksi oikeusjärjestys kohdistaa julkishallintoon muita erityisvaatimuksia, jotka osaltaan perustelevat tätä sääntelyratkaisua. Viranomaisia sitoo hallinnon lainmukaisuusperiaate, ja viranomaisten on myös noudatettava hallinnon yleislakeja. Viranomaisissa tapahtuva lainmukainen henkilötietojen käsittely kuuluu viranomaisissa työskentelevien virkavelvollisuuksiin. Virkamiehen asemaan kuuluu myös muita laajempi vastuu työssä tehdyistä virheistä, johon liittyy virkavastuun toteutuminen ensinnäkin rikosoikeudellisena virkavastuuna, kurinpidollisena virkavastuuna ja vahingonkorvausvastuuna.[45]

Hallintovaliokunta totesi lakiesitykseen liittyen, että yleinen tietosuoja-asetus ja ehdotettu tietosuojalaki koskevat myös Suomen evankelisluterilaista kirkkoa ja Suomen ortodoksista kirkkoa, jotka ovat julkisyhteisöjä. Kummankin kirkon seurakunnissa, keskushallinnossa ja hiippakunnissa käsitellään henkilötietoja ja ylläpidetään henkilörekistereitä. Tämän vuoksi katsottiin perustelluksi lisätä 24 §:n 4 momenttiin myös kirkot sellaisiksi julkisyhteisöiksi, joille hallinnollista seuraamusmaksua ei voida määrätä.[46]

Tietosuojalain 24 §:n 4 momentti ei välittömästi vaikuta haitallisesti yksityisten toimijoiden asemaan, mutta asettaa julkisen ja yksityisen sektorin toimijat eriarvoiseen asemaan suhteessa huomattavaan sanktioriskiin. Kysymys on merkityksellinen erityisesti terveyden- ja sosiaalihuollon palveluiden tarjoamisessa, joiden osalta yksityiset ja julkiset palveluntarjoajat kilpailevat samoilla markkinoilla. Eriarvoisuus voi näyttäytyä myös alihankintaketjuissa ja ulkoistuksissa, joissa voi muodostua yllättäviä ja perusteettomia erisuhtaisia vastuita. Lisäksi linjauksella on merkitystä myös virkamiehen vastuuaseman näkökulmasta. Siinä, missä rikosoikeudellisen vastuun soveltumisala yksityisen sektorin puolella korvautuu organisaa-

[42] HaVM 13/2018 vp, s. 11–12.

[43] HE 9/2018 vp, s. 46.

[44] Oikeusministeriö 2017, s. 24.

[45] HE 9/2018 vp, s. 105–106.

[46] HaVM 13/2018 vp, s. 40–41.

tioon kohdistuvalla sakkovastuulla, jää julkisella sektorilla vastuuta viime kädessä kantamaan yksittäinen virkavelvollisuutensa laiminlyönyt virkamies, jonka sanktio on taloudellisen sanktion sijaan rikosoikeudellinen. Todetuista epäsuhtaisista asetelmista mahdollisesti syntyvät ongelmat on tiedostettu tietosuojalain valmistelussa. Hallituksen esityksessä todetaankin julkisen sektorin jättämisestä seuraamusuhan ulkopuolelle, että tietosuoja-asetuksen rikkomisesta viranomaiselle aiheutuvien seuraamuksien tehokkuutta on seurattava ja kilpailullisten vaikutusten arviointia pystytään arvioimaan vasta, kun seuraamusmaksuista kertyy ratkaisukäytäntöä niin unionissa kuin jäsenvaltioissa.[47] [48]

4 Hallinnollisten seuraamusmaksujen määräämismenettely

Tietosuojalain lakiehdotuksessa olisi alun perin säädetty hallinnollisesta seuraamusmaksusta päättäminen tietosuojavaltuutetulle tietosuojavaltuutetun päätöksentekoa koskevan 15 §:n mukaisesti. Perustuslakivaliokunta piti kuitenkin perustuslain kannalta ongelmallisena sitä, että hallinnollinen seuraamusmaksu voitaisiin määrätä ilman esittelyä, jos tietosuojavaltuutettu päättäisi harkintansa mukaan luopua esittelystä. Tällainen lakiehdotukseen valittu vaihtoehto merkitsisi sitä, että hallinnollisen seuraamusmaksun määräämiseen sovellettaisiin hallintolakia (434/2003). Lisäksi valiokunta kiinnitti huomiota siihen, että oikeusturvaintressi on ehdotetussa hallinnollisessa seuraamusmaksussa voimakkaasti korostunut ottaen huomioon seuraamusmaksun sanktioluonteen ja ankaruuden. Yleisen tietosuoja-asetuksen mahdollistamat hyvin suuret hallinnolliset seuraamusmaksut eivät rinnastu viranomaisten Suomessa määräämiin hallinnollisiin seuraamuksiin.[49]

Tämän vuoksi valiokunta piti ehdotusta perustuslain 21 §:n vastaisena ja vertasi sitä lausunnossaan rahoitusmarkkinoiden valvonnassa määrättävien hallinnollisten seuraamusmaksujen päätöksentekomenettelyyn, joka on osoitettu tietyissä tilanteissa monijäseniselle toimielimelle, Finanssivalvonnan johtokunnalle. Lisäksi on hallinnollisia seuraamusmaksuja, joista päättää tuomioistuin, kuten markkinaoikeuden kilpailulain (948/2011) nojalla määräämät seuraamusmaksut. Valiokunta katsoi, että myös yleisen tietosuoja-asetuksen osalta hallinnollisesta seuraamusmaksusta päättäminen tuli säätää monijäsenisen toimielimen tehtäväksi. Tietosuojavaltuutetulle voitiin sen sijaan osoittaa seuraamusmaksun määräämistä edeltävä asian selvittäminen ja muu valmistelu sekä esittely. Näin määräämismenettelyn riippumattomuus, puolueettomuus ja asianmukaisuus voitaisiin turvata perustuslain 21 §:n edellyttämällä tavalla.[50]

Perustuslakivaliokunnan lausuntojen vuoksi hallintovaliokunta ehdotti, että yleisen tietosuoja-asetuksen 83 artiklassa säädetyn hallinnollisen sakon (hallinnollinen seuraamusmaksu) määrää tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen yhdessä muodostama seuraamuskollegio, jonka puheenjohtajana toimii tietosuojavaltuutettu. Päätös tehdään esittelystä. Seuraamuskollegio käyttää merkittävää julkista valtaa, minkä vuoksi kokoonpanon tulee käydä perustuslain 2 §:n 3 momentin ja 119 §:n 2 momentin takia ilmi suoraan laista.[51]

[47] HE 9/2018 vp, s. 57.

[48] Jukka Lång – Tuomas Haavikko 2019, s. 5.

[49] PeVL 14/2018 vp, s. 19–20.

[50] PeVL 14/2018 vp, s. 19–20.

[51] HaVM 13/2018 vp, s. 14.

Hallinnollista seuraamusmaksua koskevan tietosuojalain 24 §:n mukaan seuraamuskollegio on päätösvaltainen kolmijäsenisenä ja kollegion päätökseksi tulee kanta, jota enemmistö on kannattanut. Äänten mennessä tasan päätökseksi tulee kanta, joka on lievempi sille, johon seuraamus kohdistuu. Seuraamusmaksu voidaan määrätä myös yleisen tietosuoja-asetuksen 10 artiklan rikkomisesta noudattaen, mitä tietosuoja-asetuksen 83 artiklan 5 kohdassa ja tietosuojalaissa säädetään. Sääntelyn tarkoituksena on, että hallinnollista seuraamusmaksua koskevan asian valmistelee ja esittelee tietosuojavaltuutetun toimiston esittelijä, ja näin ollen tietosuojalain 9 §:n mukaisesti tietosuojavaltuutetun toimistossa tulee olla tarpeellinen määrä tietosuojavaltuutetun tehtäväalaan perehtyneitä esittelijöitä.[52]

Lakivaliokunta piti tärkeänä, että jatkossa selvitetään, onko hallinnollisen seuraamusmaksun määräämismenettelyä ja päätöksenteon kokoonpanoa mahdollista vielä edellä esitetystä kehittää ja vahventaa. Lisäksi se katsoi aiheelliseksi selvittää esimerkiksi esityksen valmistelussakin esillä ollutta vaihtoehtoa, jossa valvontaviranomainen organisoitaisiin tietosuojavirastoksi, jossa toimisi sekä tietosuojavaltuutettu että seuraamuslautakunta.[53] Hallintovaliokunnan mielestä virastomuotoa voitaisiin pitää henkilöviranomaisorganisaatiota luontevampana ratkaisuna kansalliselle valvontaviranomaiselle ottaen myös huomioon tietosuojavaltuutetun toimiston henkilöresurssien lisäys.[54]

Tietosuoja-asetus loi jäsenvaltioiden valvontaviranomaisille oikeuden määrätä hallinnollinen seuraamusmaksu asetuksen säännöksiä rikkoneelle rekisterinpitäjälle tai henkilötietojen käsittelijälle. Tätä voidaan pitää yhtenä merkittävimpänä tietosuoja-asetuksen tuomana muutoksena, sillä henkilötietodirektiivissä ei säädetty seuraamusmaksuista. Hallinnolliset seuraamusmaksut ovat olleetkin viime vuosien aikana vilkkaan akateemisen tarkastelun kohteena. Eräs keskeinen impulssi tähän keskusteluun on ollut muun muassa Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytäntö koskien *ne bis in idem* -kieltoa tilanteessa, jossa sopimusvaltiossa on määrätty rikosoikeudellisen seuraamuksen ohella jokin muu seuraamus, jota valtionsisäisessä oikeudessa on pidetty muuna kuin rikosoikeudellisena seuraamuksena. *Ne bis in idem* -kiellon soveltamisala ei rajoitu vain rikosoikeudellista rangaistusta koskeviin tuomioihin, vaan se ulottuu myös rangaistusluonteisiin hallinnollisiin seuraamuksiin. Niin ikään yleisen tietosuoja-asetuksen 83 artiklassa tarkoitettuja hallinnollisia seuraamusmaksuja olisi pidettävä tällaisina rangaistusluonteisina hallinnollisina seuraamuksina.[55] Perustuslakivaliokunta on vakiintuneesti katsonut, että lainvastaisesta teosta määrättävä maksu ei ole perustuslain 81 §:n mukainen vero tai maksu, vaan rangaistusluonteinen taloudellinen seuraamus, jonka takia valiokunta on rinnastanut tällaiset seuraamukset rikosoikeudellisiin seuraamuksiin.[56]

Yleisen tietosuoja-asetuksen mukaisten hallinnollisten seuraamusmaksujen luonne on omaksuttu kilpailuoikeudesta, jossa kilpailuoikeudellisten seuraamusmaksujen tarkoituksena on rangaista kilpailulainsäädännön rikkojaa, mutta samalla estää väärinkäytöksiä ja

[52] HaVM 13/2018 vp, s. 40.

[53] LaVL 5/2018 vp: Lakivaliokunnan lausunto hallituksen esityksestä eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, s. 10.

[54] HaVM 13/2018 vp, s. 15.

[55] HE 9/2018 vp, s. 44–45; Mikael Koillinen 2016, s. 572.

[56] Ks. esim. PeVL 28/2014 vp: Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laiksi yhteisen kalastuspolitiikan seuraamusjärjestelmästä ja valvonnasta sekä eräiksi siihen liittyviksi laeiksi.

antaa taloudellinen kannustin lainsäädännön noudattamiselle. Kilpailun ja kuluttajien suojeleminen, esimerkiksi pitämällä tuotteiden hinnat kohtuullisina, on kilpailulainsäädännön pyrkimyksenä. Sen sijaan tietosuojasääntelyn tarkoituksena on suojella yksilöiden henkilötietoja ja yksityisyyttä. Toisaalta yleisen tietosuoja-asetuksen rikkomisella ei välttämättä ole suoria yksilöön vaikuttavia negatiivisia taloudellisia vaikutuksia, mutta seuraamusmaksuilla on merkitystä nimenomaan rikkomusten vähentämisen ja vastuuvelvollisuuden lisäämisen näkökulmista.[57]

Seuraamusmaksujen hallinnollinen luonne näkyy siinä, että ne määrää hallinnollinen valvontaviranomainen, joka määrää seuraamusmaksun maksettavaksi valtiolle sakon täytäntöönpanosta annetun lain (672/2002) mukaan. Yleisen tietosuoja-asetuksen alkuperäisessä suomenkielisessä kieliversiossa hallinnollisista seuraamusmaksuista käytettiin termiä hallinnollinen sakko, jonka katsottiin terminä olleen ongelmallinen, sillä sakolla tarkoitetaan rikosoikeudellista rangaistusta. Tämän takia asetuksen suomenkielistä kieliversiota oikaistiin vuonna 2021 ja termi muutettiin hallinnolliseksi seuraamusmaksuksi.[58] Perustuslakivaliokunnan vakiintuneen käytännön mukaan hallinnollisten seuraamusmaksujen maksuvelvollisuuden ja maksun suuruuden perusteista sekä maksuvelvollisen oikeusturvasta samoin kuin lain täytäntöönpanon perusteista on säädettävä täsmällisesti ja selkeästi laissa.[59]

Euroopan tietosuojaneuvosto hyväksyi täysistunnossaan 24.5.2023 julkisen kuulemiskierroksen jälkeen ohjeen hallinnollisten seuraamusmaksujen laskemisesta. Ohjeen tarkoituksena on yhdenmukaistaa kansallisten tietosuojaviranomaisten tapoja yleisen tietosuoja-asetuksen perusteella määrättyjen seuraamusmaksujen suuruuden laskennassa. Ohjeessa on seuraamusmaksun laskemiseen viisivaiheinen menetelmä, jossa huomioidaan muun muassa rikkomusten määrä, raskauttavat tai lieventävät tekijät, seuraamusmaksujen lakisääteinen enimmäismäärä ja tehokkuutta, varoittavuutta sekä oikeasuhteisuutta koskevat vaatimukset.[60]

Tietosuojalain 24 §:ssä säädetään muutoksenhausta, jonka 1 momentin mukaan muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019). Seuraamusmaksuihin liittyen on kaksi korkeimman hallinto-oikeuden ratkaisua. Korkein hallinto-oikeus on ensimmäisessä päätöksessään (KHO 2023:81) saattanut voimaan tietosuojavaltuutetun toimiston seuraamuskollegion päätöksen määrätystä seuraamusmaksusta. Tätä tapausta käsitellään tarkemmin myöhemmin.

Toisessa päätöksessään (KHO:2023:82) korkein hallinto-oikeus puolestaan arvioi, oliko seuraamuskollegio voinut määrätä yhtiölle seuraamusmaksun saamansa selvityksen perusteella. Seuraamuskollegion päätöksessä oli katsottu, että yhtiö olisi kerännyt henkilötietoja tarpeettomasti työhönottoprosessin yhteydessä. Määrätty seuraamusmaksu oli suuruudeltaan 12 000 euroa. Hallinto-oikeus kumosi seuraamuskollegion päätöksen seuraamusmaksun määräämisestä sekä tietosuojavaltuutetun päätöksen tietyiltä osin. Korkein hallinto-oikeus totesi, että tietosuojavaltuutetun toimiston saaman selvityksen perusteella ei voitu osoittaa,

[57] Roope Liuha, Tietosuoja-asetuksen mukaisten hallinnollisten seuraamusmaksujen määrääminen yritykselle. Edilex 2022, s. 47–48. Saatavissa osoitteessa https://www.edilex.fi/opinnaytetyot/26988.

[58] Liuha 2022, s. 48.

[59] PeVL 28/2014 vp, s. 2.

[60] Euroopan tietosuojaneuvosto 2023: Guidelines 04/2022 on the calculation of administrative fines under the GDPR. European Data Protection Board 2023. Saatavilla osoitteessa https://edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-calculation-administrative-fines-following_en.

että yhtiö olisi kyseisellä ajanjaksolla kerännyt tarpeettomia henkilötietoja ilman lainmukaista käsittelyperustetta. Näin ollen hallinto-oikeuden päätöstä ei muutettu.

5 Seuraamusjärjestelmän mahdollistamat muut sanktiot

Tietosuojalain säätämisen yhteydessä rikoslain 38 luvun henkilörekisteririkosta koskenut 9 § korvattiin tietosuojarikoksella. Muutoksella otettiin huomioon tietosuojalainsäädännön seuraamusjärjestelmän perustavanlaatuinen muutos hallinnollisten seuraamusmaksujen myötä, jolloin rikosoikeudellinen vastuu tulee kyseeseen vain tilanteissa, joissa lainvastainen henkilötietojen käsittely ei ole yleisen tietosuoja-asetuksen nojalla hallinnollisten seuraamusmaksujen piirissä.

Rikoslain 38 luvun 9 §:n 1 momentin mukaan, joka muutoin kuin yleisessä tietosuoja-asetuksessa tarkoitettuna rekisterinpitäjänä tai henkilötietojen käsittelijänä tahallaan tai törkeästä huolimattomuudesta hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla, luovuttaa henkilötietoja tai siirtää henkilötietoja vastoin yleisessä tietosuoja-asetuksen, tietosuojalain, henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) tai henkilötietojen käsittelyä koskevan muun lain henkilötietojen käyttötarkoitussidonnaisuutta, luovuttamista tai siirtämistä koskevaa säännöstä ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava tietosuojarikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Rangaistussäännös tulee siten sovellettavaksi ainoastaan tilanteessa, jossa henkilön ei voida katsoa toimineen rekisterinpitäjän tai henkilötietojen käsittelijän ominaisuudessa. Esimerkkinä tällaisesta toiminnasta voidaan mainita uteliaisuudesta tapahtuva henkilötietojen käsittely ilman käsittelyyn oikeuttavaa perustetta.[61]

Tietosuojarikoksesta voidaan tuomita myös 9 §:n 2 momentin mukaan se, joka tahallaan tai törkeästä huolimattomuudesta toimii vastoin sitä, mitä 1 momentin 1–4 kohdissa säädetään henkilötietojen käsittelyn turvallisuudesta. Tällainen tilanne voi tulla kyseeseen, jos esimerkiksi rekisterinpitäjän palveluksessa hävittää henkilötietoja vastoin tietoturvallisuudesta säädettyä.[62] Tietosuojalain 26 § sisältää lisäksi viittaussäännöksen muihin rikoslain rangaistussäännöksiin, jotka voivat tulla kyseeseen lain rikkomisten vuoksi määrättävinä rikosoikeudellisina seuraamuksina.

Ensimmäisen momentin mukaan rangaistus viestintäsalaisuuden loukkauksesta ja törkeästä viestintäsalaisuuden loukkauksesta säädetään rikoslain 38 luvun 3 ja 4 §:ssä sekä rangaistus tietomurrosta ja törkeästä tietomurrosta 38 luvun 8 ja 8 a §:ssä. Rangaistus tietosuojalain 35 §:ssä säädetyn vaitiolovelvollisuuden ja 36 §:ssä säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla laissa säädetä ankarampaa rangaistusta. Toisen momentin mukaan rikoslain 38 luvun 10 §:n 3 momentissa säädetään syyttäjän velvollisuudesta kuulla tietosuojavaltuutettua ennen 1 momentissa mainittuja rikoksia koskevan syytteen nostamista samoin kuin tuomioistuimen velvollisuudesta varata tällaista asiaa käsitellessään tietosuojavaltuutetulle tilaisuus tulla kuulluksi.

[61] HE 9/2018 vp, s. 124.

[62] HE 9/2018 vp, s. 124–125.

Tietosuojavaltuutetun toimivaltuuksiin kuuluu yleisen tietosuoja-asetuksen mahdollistama uhkasakko. Tietosuojalain 22 §:n 1 momentin mukaan tietosuojavaltuutettu voi asettaa tietosuoja-asetuksen 58 artiklan 2 kohdan c–g ja j alakohdissa tarkoitetun päätöksen ja tietosuojalain 18 §:n 1 momenttiin perustuvan tietojen luovuttamista koskevan määräyksen tehosteeksi uhkasakon. Uhkasakon asettamisesta ja tuomitsemisesta maksettavaksi säädetään uhkasakkolaissa (1113/1990). Uhkasakkoa ei saa 2 momentin mukaan asettaa luonnolliselle henkilölle 1 momentissa tarkoitetun tietojen luovuttamista koskevan määräyksen tehosteeksi silloin, kun henkilöä on aihetta epäillä rikoksesta ja tiedot koskevat rikosepäilyn kohteena olevaa asiaa.

Uhkasakon määräämättä jättämisen kynnys on 22 §:n 2 momentissa liitetty ilmaisuun *on aihetta epäillä*. Lakivaliokunta on todennut uhkasakon määräämättä jättämisen kynnyksestä, ettei siitä ole muodostunut vakiintunutta linjaa, vaan lainsäädäntöratkaisut vaihtelevat. Valiokunnan näkemyksen mukaan *on aihetta epäillä* -ilmaisua puoltaa se, että se antaa tietojenantovelvolliselle luonnolliselle henkilölle suojaa laaja-alaisemmin, joten se on paremmin sopusoinnussa itsekriminointisuojan kanssa.[63]

Vaikkakin tietosuojalainsäädäntö muuttui perustavanlaatuisesti yleisen tietosuoja-asetuksen antamisen yhteydessä, on hallintovaliokunta huomauttanut lausunnossaan myös tietosuoja-asetuksen mahdollistamista muista valvontaviranomaisen keinoista ja toimivaltuuksista. Valvontaviranomaisen niin sanotuista korjaavista toimivaltuuksista säädetään tietosuoja-asetuksen 58 artiklan 2 kohdassa. Näitä ovat muun muassa rekisterinpitäjälle tai henkilötietojen käsittelijälle annettava huomautus tai varoitus siitä, että aiotut käsittelytoimet ovat asetuksen vastaisia (a ja b alakohta), sekä käsittelyn väliaikainen tai pysyvä rajoittaminen, mukaan lukien käsittelykielto (f alakohta).[64]

6 Tietosuojavaltuutetun ja seuraamuskollegion päätöksiä sekä tietosuojatapausten piirteitä

Tietosuojavaltuutetun toimistossa käsiteltävänä olevien asioiden määrä on kasvanut yleisen tietosuoja-asetuksen voimaantulon jälkeen. Viime vuosina vireille tulleiden asioiden määrä on ollut noin 11 000 asiaa. Tietosuojavaltuutetun toimistoon tuli vuonna 2022 vireille yhteensä 11 095 asiaa, joista suurimman osan muodostivat tietoturvaloukkausilmoitukset (5 445 ilmoitusta). Niiden määrä onkin kasvanut vuosittain.[65]

Finlexissä on julkaistu tietosuojavaltuutetun päätöksiä EU:n yleisen tietosuoja-asetuksen, rikosasioiden tietosuojalain ja henkilötietolain tulkinnasta[66]. Tarkastelemme näitä päätöksiä vuosilta 2018–2022. Kaiken kaikkiaan päätöksiä oli julkaistu yhteensä 119 (taulukko 1), joista 48 oli tietosuojavaltuutetun ratkaisemia ja 55 apulaistietosuojavaltuutetun ratkaisemia.

---

63 LaVL 5/2018 vp, s. 22–23.

64 HaVM 13/2018 vp, s. 11.

65 Tietosuojavaltuutettu, Tietotosuojavaltuutetun toimiston toimintakertomus 2022. K 14/2023 vp. Tietosuojavaltuutetun toimisto 2023. Saatavissa osoitteessa https://tietosuoja.fi/documents/6927448/169954657/TSV+Toimintakertomus+2022.pdf/74eca5fa-bc1d-77ef-1a0e-b81df6bb0c5e/TSV+Toimintakertomus+2022.pdf?t=1690784877980

66 Ei ole tietoa, millä perusteella tietosuojavaltuutetun toimisto julkaisee yhdessä Finlexin kanssa päätöksiä, koska kaikkia päätöksiä ei julkaista, kun vertaa julkaistujen päätöksien lukumääriä muun muassa toimintakertomuksessa ilmoitettuihin päätöksiin. Rajasimme tutkimuksen koskemaan Finlexissä julkaistuja päätöksiä.

Tietosuojavaltuutetun seuraamuskollegio oli puolestaan ratkaissut kymmenen tapausta. Yksi päätös oli korkeimman hallinto-oikeuden, ja se koski Jehovan todistajien ovelta ovelle -saarnaamistyön yhteydessä keräämiä henkilötietoja.

Taulukko 1. Tietosuojatapausten päätöksentekijät vuosina 2018–2022.

Päätöksentekijä	**Lukumäärä**
KHO	1
Apulaistietosuojavaltuutettu	55
Apulaistietosuojavaltuutettu ja seuraamuskollegio	5
Tietosuojavaltuutettu	48
Tietosuojavaltuutetun seuraamuskollegio	10
Yhteensä	**119**

Tapauksista suurin osa (109 tapausta) oli päätöksiä. Joukossa oli myös esimerkiksi muutamia kannanottoja, lausuntoja ja määräyksiä tai päätös ja ohjaus yhdistelmä tapauksia (taulukko 2).

Taulukko 2. Tietosuojatapausten ratkaisut vuosina 2018–2022.

	Lukumäärä
Kannanotto	2
Lausunto	2
Määräys	2
Päätös	109
Päätös ja ohjaus	3
Muu	1
Yhteensä	**119**

Suurin osa päätöksistä kohdistui yrityksiin (86 tapausta). Neljätoista tapausta koski kunnan viranomaista ja kahdeksan valtion viranomaista. Tapaukset liittyivät myös usean eri toimialan toimintaan, ja niistä 14 kohdistui yksityisen pysäköinninvalvonnan yrityksiin, 14 suoramarkkinointiyrityksiin, kahdeksan julkiseen terveydenhuoltoon ja viisi hakukoneyhtiöihin sekä viisi Liikennevakuutuskeskukseen. Loput tapaukset jakaantuivat tasaisesti eri toimialojen kesken ja osan tapauksien osalta ei voitu luotettavasti selvittää tietosuojavaltuutetun asiakirjoista, että mitä organisaatiota tai yritystä päätös koski. Alla olevassa taulukossa (taulukko 3) on kuvattu tarkemmin päätöksien kohteena olevat organisaatiot.

Taulukko 3. Tietosuojatapausten päätöksien kohteet vuosina 2018–2022.

Kohde	**Lukumäärä**
Uskonnollinen yhdyskunta	1
Julkinen terveydenhuolto	8
Sosiaalipalvelut	3
Posti	2
Elokuvayhtiö	2
Taksiyhtiö	2
Pankki	4
Arvopaperien välitysyritys	1
Kiinteistönvälitysyritys	1
Hakukoneyhtiö	5
Teleoperaattori	1
Suoramarkkinointiyritys	14
Yksityinen pysäköinninvalvontayritys	14
Matkailualan yritys	2
Asunto-osakeyhtiö	2
Liikennevakuutuskeskus	5
Kiinteistösijoittajayhtiö	1
Ammattikorkeakoulu	1
Terveyspalveluyritys	4
Valokuvaamoyritys	1
Terveydenhuollon ammattihenkilö	1
Potilasvakuutuskeskus	1
Yliopisto	1
Oikeusrekisterikeskus	2
Luottotietoyhtiö	4
Kuntayhtymä	1
Optikkoyritys	2
Lämpö-, vesijohto- ja ilmastointiasennusyritys	1
Rakennusalan yritys	1
Yksityinen elinkeinonharjoittaja	1
Lehden kustantaja	1
Autoliike	3
Uutistoimisto	1
Siivousalan yritys	1
Korkein oikeus	2
Ulkoministeriö	1
Poliisiammattikorkeakoulu	1
Vakuutusyhtiö	1
Lehdet ja uutispalvelut	1
Laivayhtiö	1
Verohallinto	1
Kirjasto	1
Valtion tieto- ja viestintätekniikkakeskus	1
IT-alan yritys	1
Sairaanhoitopiiri	1
Yksityinen perintätoimisto	1
Yritys (toimiala tuntematon)	4
ei tietoa (n/a)	7
Yhteensä	**119**

Hallinnollisia seuraamusmaksuja määrättiin yhteensä 2 182 800 euron edestä vuosina 2020–2022 (taulukko 4). Vuosina 2018 ja 2019 ei määrätty yhtään hallinnollista seuraamusmaksua. Suurin hallinnollinen seuraamusmaksu oli 750 000 euroa, joka kohdistui yksityiseen perintätoimistoon. Seuraamusmaksuja määrättiin yhteensä 18 tapauksessa. Maksujen keskiarvo oli 128 400 euroa.

Taulukko 4. Määrätyt hallinnolliset seuraamusmaksut vuosina 2018–2022.

Kohde	**Seuraamusmaksu (€)**	**Vuosi**
Posti	100 000	2020
Yritys (toimiala tuntematon)	16 000	2020
Yritys (toimiala tuntematon)	12 500	2020
Suoramarkkinointiyritys	7 000	2020
Taksiyhtiö	72 000	2020
Ammattikorkeakoulu	25 000	2021
Terveyspalveluyritys	608 000	2021
Liikennevakuutuskeskus	52 000	2021
Matkailualan yritys	6 500	2021
Terveyspalveluyritys	5 000	2021
Yksityinen pysäköinninvalvontayritys	75 000	2021
Lehden kustantaja	8 500	2021
Suoramarkkinointiyritys	8 300	2022
Lehdet ja uutispalvelut	85 000	2022
Laivayhtiö	230 000	2022
Terveyspalveluyritys	122 000	2022
Yksityinen perintätoimisto	750 000	2022
Yhteensä	**2 182 800**	

Taulukossa 5 on eroteltuna päätöksien kohteena olevien eri yhteisön oikeudelliset muodot. Taulukossa on myös määrällisesti eroteltu eri toimenpiteiden määrät, joita on kumuloitunut eri yhteisöille. Yritykset saivat 52 huomautusta, 49 määräystä ja 17 hallinnollista seuraamusmaksua. Yhdelle kunnalliselle toimijalle ei voitu yleisen tietosuoja-asetuksen perusteella määrätä hallinnollista seuraamusmaksua, mutta heille annettiin toimenpideohjeistus tietosuoja-asioiden kuntoon laittamiseksi. Tietojen keräämiskielto asetettiin yhdelle uskonnolliselle yhteisölle. Lisäksi tietosuojavaltuutettu antoi muutamat lausunnot ja kannanotot yrityksille ja valtion viranomaiselle sekä kunnalliselle toimijalle.

Taulukko 5. Määrätyt seuraamusmaksut eri organisaatiotyypeille vuosina 2018–2022.

Kohde	Lausunto tai kannan-otto	Ohjaus	Toimen-pideohjeet asioiden kuntoon laittami-seksi	Huomautus	Varoitus	Määräys	Hallin-nollinen seuraamus-maksu	Hallinnollista seuraamus-maksua ei voida määrätä	Tietojen keräämisen kielto asetettiin
Yritys	3	3	0	52	0	49	16	0	0
Kunnallinen toimija	1	1	1	8	1	5	0	1	0
Valtion viranomainen	1	0	0	4	0	4	0	0	0
Uskonnollinen yhdyskunta	0	0	0	0	0	0	0	0	1
Valtionyhtiö	0	0	0	0	0	1	1	0	0
Säätiö	0	0	0	0	0	0	0	0	0
Ei tietoa	1	0	0	3	1	2	0	0	0

Lopuksi tarkastellaan vielä yksittäisiä tietosuojatapauksia, joissa on määrätty hallinnollinen seuraamusmaksu. Näiden esimerkkitapausten tarkoituksena on havainnoida, millaisia tietosuojatapauksia päätyy valvontaviranomaiselle. Lisäksi osaa tapauksia on käsitelty myös muissa oikeusprosesseissa, joten myös niitä on käsitelty samassa yhteydessä.

Ensimmäisessä tapauksessa (18.5.2020) käsiteltiin yrityksen ajotietojärjestelmästä saatavien sijaintitietojen käyttöä työntekijöiden työajanseurantaa varten. Asia tuli vireille vuonna 2020. Tietosuojavaltuutettu selvitti, oliko tietojärjestelmän käyttöönotossa noudatettu tietosuojaa koskevaa lainsäädäntöä, erityisesti tietosuojaa koskevaa vaikutusten arviointia. Rekisterinpitäjä antoi tietosuojavaltuutetulle selvityksen, jossa se totesi, että seurantatietoja käytetään työntekijöiden työajan valvontaan. Rekisterinpitäjä ei ollut tehnyt vaikutusten arviointia seurantatietojen keräämiselle. Rekisterinpitäjä vetosi myös siihen, että tietojärjestelmä, joka keräsi henkilöiden seurantatietoja, oli ISO 27001 -standardisertifioitu. Tietosuojavaltuutetun mukaan työntekijöitä on pidettävä heikommassa asemassa olevina suhteessa työnantajaan, ja tietosuoja-asetuksen 35 artiklan 4 kohdan mukaan heitä koskevien tietojen keräämisen vaikutusten arvioinnit pitää tehdä. Tietosuojavaltuutettu katsoi, että työntekijöiden sijaintitietojen käsittely ei ole ollut sellaista, että se vastaisi tietosuoja-asetuksen vaatimuksia koskien riskiperusteista lähestymistapaa ja vaikutusten arviointia. Pelkkä sertifiointi ei ollut riittävä tietosuoja-asetuksen vaatimusten täyttämiseksi. Tietosuojavaltuutettu ja seuraamuskollegio määräsivät yritykselle 16 000 euron hallinnollisen seuraamusmaksun. Yrityksen liikevaihto oli vuonna 2019 noin 20 miljoonaa euroa.

Toisessa tapauksessa (26.5.2020) käsiteltiin taksialan yrityksen kameravalvonnan lainmukaisuutta ja tietojen minimoinnin näkökulmaa. Asia tuli vireille vuonna 2019. Päätöksessä arvioitiin sijaintitietojen, äänitietojen ja kameravalvontavideon tietojen keräämisen perusteita ja tietojen keräämisen minimoinnin tarvetta sekä tietosuojaa koskevaa vaikutusten arviointia ja profilointia. Osa autoista keräsi sekä ääntä että kuvaa. Tietojen keräämistä yritettiin oikeuttaa turvallisuussyiden perusteella. Rekisteripitäjällä oli ollut noin neljä miljoonaa asiakasta ja yli 2 000 taksiautoa. Apulaistietosuojavaltuutettu ja seuraamuskollegio määräsivät taksialan yritykselle 72 000 euron hallinnollisen seuraamusmaksun kameravalvonnan tasapainotestin tekemisen puutteista, äänen keräämisen osalta tehtävän minimointiperiaatteen laiminlyömisestä, tietojenkäsittelyn avoimuuden laiminlyömisestä, kaikkien tietojenkäsittelijöiden

määrittelyn laiminlyömisestä, tietojenkäsittelyn vaikutusten arvioinnin puutteellisuudesta ja siitä, että tietoselosteet eivät vastanneet tietojenkäsittelyn kokonaiskuvaa. Yrityksen liikevaihto oli vuonna 2019 noin 10 miljoonaa euroa.

Kolmannessa tapauksessa (16.12.2021) käsiteltiin vakuutusyhtiön oikeutta saada tietoja. Asia tuli vireille vuonna 2017. Rekisteröidyn mukaan Liikennevakuutuskeskus oli hankkinut hänestä enemmän tietoja kuin oli tarpeen kerätä ja käsitellä korvausasian käsittelemiseksi. Liikennevakuutuskeskus voi pyytää lausuntoa rekisteröidystä koskien korvausasiaa, mutta Liikennevakuutuskeskus oli tulkinnut asian niin, että korvauksenhakijan potilasasiakirjamerkintöjä voitiin vaatia täydessä laajuudessaan potilastietojärjestelmistä. Tämä tulkinta oli tietosuojavaltuutetun mukaan tietosuoja-asetuksen 5(1)(c) artiklan tietojen minimoinnin periaatteen vastaista. Siten Liikennevakuutuskeskus oli käsitellyt tarpeettomia potilastietoja korvausasioihin liittyen. Tietosuojavaltuutettu ja seuraamuskollegio määräsivät 52 000 euron hallinnollisen seuraamusmaksun Liikennevakuutuskeskukselle. Liikennevakuutuskeskuksen liikevaihto oli vuonna 2020 noin 8 miljoonaa euroa.

Neljännessä tapauksessa (16.12.2021) käsiteltiin oikeutta tulla unohdetuksi. Tapauksessa rekisteröity epäili, ettei matkatoimisto käsitellyt viisumilomakkeeseen syötettäviä henkilötietoja tietosuoja-asetuksen mukaisesti. Tapaus tuli vireille vuonna 2019. Viisumilomake oli salaamattoman http-protokollayhteyden takana ja loi tiedoston avoimeen Internet-verkkoon, jossa se oli kaikkien luettavissa. Rekisteröity oli pyytänyt tietojensa poistamista, mutta matkatoimisto ei reagoinut pyyntöön. Rekisterinpitäjän mukaan verkkopolun arvaaminen oli melko mahdotonta. Tietosuojavaltuutettu katsoi, että henkilötiedot pitää suojata riskiperusteisesti, ja totesi että tietoturva-asetuksen 32 artiklaa on rikottu. Tietosuojavaltuutettu ja seuraamuskollegio määräsivät 6 500 euron hallinnollisen seuraamusmaksun matkatoimistolle. Matkatoimiston tilikausien 1.7.2019–30.6.2020, 1.7.2020–30.6.2021, ja 1.7.2020– 30.6.2021 liikevaihto oli yhteensä noin 900 000 euroa.

Viidennessä tapauksessa (21.4.2021) käsiteltiin rekisteröidyn oikeutta saada tarkastaa tietonsa ja saada ne poistetuksi pysäköinninvalvontayrityksen tietojärjestelmistä. Tietosuojavaltuutetulle tuli 11 samaa pysäköinninvalvontayritystä koskenutta kantelua. Suurimmassa osassa tapauksista rekisteröidyt olivat itse pyytäneet pääsyä omiin tietoihinsa ja/tai pyytäneet, että heidän henkilötietonsa poistetaan pysäköinninvalvontayrityksen tietojärjestelmistä. Tapaukset tulivat vireille vuosina 2017–2020. Rekisteröidyt eivät ole halunneet antaa pysäköinninvalvontayrityksen tarkastuksen toteuttamiseksi omaa kotiosoitetta ja sosiaaliturvatunnusta, mikä haluttiin arvioida tietosuojavaltuutetun toimistossa sekä pitääkö tietojen poistaminen hoitaa tietyllä lomakkeella. Osa rekisteröidyistä halusi myös tietää, miten pysäköinninvalvontayritys on saanut heidän henkilötietonsa, kun he eivät niitä ole yritykselle antaneet. Tietosuojavaltuutetun mukaan pysäköinninvalvontayritys ei noudattanut tietojen minimoinnin periaatetta reklamaatiolomaketietojen keräämisessä eikä yritys ole noudattanut tietosuoja-asetusta. Tietosuojavaltuutetun seuraamuskollegio langetti pysäköinninvalvontayritykselle 75 000 euron hallinnollisen seuraamusmaksun. Yrityksen liikevaihto oli vuonna 2019 reilut 12 miljoonaa euroa.

Kuudennessa tapauksessa (7.12.2021) käsiteltiin Psykoterapiakeskus Vastaamo Oy:n (jäljempänä Vastaamo) TOR-verkkoon vuotaneen potilastietokannan tietomurtoa, jossa varastettiin 33 000 ihmisen potilas- ja henkilötiedot. Asia tuli vireille vuonna 2020. Potilastietokannassa oli erittäin arkaluontoisia terveystietoja rekisteröidyistä potilaista, ja yrityksen potilastietokanta oli Valviran luokittelun mukaan B-luokan järjestelmä, jota ei ollut kytketty

kansalliseen Kanta-potilasjärjestelmään. Tutkinnan mukaan tietomurrossa olisi päästy kirjautumaan luvatta palvelimen potilastietokantaan ainakin 20.12.2018 ja 15.3.2019. Apulaistietosuojavaltuutettu arvioi, että jää epäselväksi, milloin Vastaamolle on tullut tiedoksi, että tietoja oli kadonnut palvelimelta tietomurron myötä. Vastaamo oli toteuttanut tietoturvallisuuden parannuksia maaliskuussa 2019 ja syyskuussa 2020. Vastaamo konsultoi myös ulkopuolista IT-asiantuntijaa. Se totesi vuonna 2019 tehdyssä selvityksessään, että Vastaamon tietoturvallisuudessa oli edelleen puutteita, vaikka se korjasi tietoturvallisuuttaan vuoden 2019 tietomurron jälkeen.

Apulaistietosuojavaltuutetun mukaan Vastaamo ei ollut myöskään dokumentoinut vuonna 2018 tapahtunutta tietoturvallisuusloukkausta niin kuin tietosuoja-asetuksen 33 artiklan 5 kohdassa vaaditaan. Vastaamo ei noudattanut dokumentoitua ilmoitusmenettelyä tietosuojaloukkaustilanteessa eikä se ollut myöskään noudattanut ilmoitusvelvollisuuden 72 tunnin aikarajaa tietosuojaloukkauksien ilmitulosta. Vastaamon olisi pitänyt tehdä ilmoitus myös vuoden 2019 luvattomasta tietomurrosta tietokantaan. Apulaistietosuojavaltuutettu arvioi, että Vastaamon tapa hoitaa tietoturvallisuutta ja tietosuoja-asetuksen velvoitteita on ollut törkeän huolimatonta, mistä yrityksen on täytynyt olla tietoinen. Potilastietokanta oli kaksi ja puoli vuotta puutteellisesti suojattu. Apulaistietosuojavaltuutettu ja seuraamuskollegio määräsivät Psykoterapiakeskus Vastaamo Oy:lle 608 000 euron hallinnollisen seuraamusmaksun. Vastaamon liikevaihto oli vuonna 2020 yli 14 miljoonaa euroa.

Vastaamon tapausta on käsitelty ja tullaan vielä käsittelemään eri rikosprosesseissa. Helsingin käräjäoikeus tuomitsi huhtikuussa 2023 Vastaamon entisen toimitusjohtajan *Ville Tapion* tietosuojarikoksesta kolmen kuukauden ehdolliseen vankeusrangaistukseen. Helsingin käräjäoikeus katsoi, että Tapio syyllistyi tietosuojarikokseen, koska hän ei ollut toteuttanut Vastaamossa yleisen tietosuoja-asetuksen vaatimusta käsiteltävien henkilötietojen pseudonymisoinnista ja salauksesta. Käräjäoikeuden mukaan potilastietokantaan oli tallennettu asiakkaiden henkilötietoja ja käyntimerkintöjä selkokielisinä ilman riittävää salausta. Tuomio ei ole vielä lainvoimainen. Vastaamon tietomurrosta epäilty on puolestaan vangittu helmikuussa 2023. Häntä epäillään muun muassa törkeästä tietomurrosta ja törkeästä yksityiselämää loukkaavan tiedon levittämisestä. Keskusrikospoliisin mukaan tähän mennessä noin 24 000 uhria on tehnyt asiassa rikosilmoituksen ja heistä noin 8 600 on täyttänyt sähköisen lausumalomakkeen. Vastaamon tietomurrolla on ollut laajaa yhteiskunnallista merkitystä.

Seitsemännessä tapauksessa (18.5.2020) tietosuojavaltuutetun toimistoon tehtiin kahdeksan kantelua koskien Posti Group Oyj:n (jäljempänä Posti) muuttoilmoitustietoja aikavälillä 24.2.2017–15.1.2020. Näistä asioista kuusi on saatettu vireille henkilötietolain voimassaoloaikana ja kaksi yleisen tietosuoja-asetuksen soveltamisen aloittamisen jälkeen. Kussakin asiassa on ollut kysymys siitä, että tehdyn osoitteenmuutosilmoituksen jälkeen rekisteröity on saanut yhteydenottoja ja suoramarkkinointia eri yrityksiltä. Tietosuojarikkomukseksi katsottiin vuosina 2017–2019 tehdyt osoitteenmuutosilmoitukset, joiden aikana rekisteröidyille ei ollut informoitu tuote-ehtoja ja ne eivät tulleet aidosti rekisteröidyn hyväksyttäväksi, koska rekisteröidyt eivät tienneet oikeudesta kieltää tietojensa luovuttaminen. Apulaistietosuojavaltuutettu ja seuraamuskollegio määräsivät Postille 100 000 euron hallinnollisen seuraamusmaksun osoitetietojen automaattisesta luovuttamista ostopalveluna suoramarkkinointiyrityksille. Postin liikevaihto oli vuonna 2019 noin 1,56 miljardia euroa.

Posti valitti päätöksestä hallinto-oikeuteen. Helsingin hallinto-oikeus on antamallaan päätöksellä 2.11.2021 (nro H5413/2021) hylännyt Postin valituksen apulaistietosuojavaltuutetun

päätöksestä, mutta kumonnut yhtiön valituksesta seuraamuskollegion päätöksen hallinnollisen seuraamusmaksun määräämisestä. Hallinto-oikeuden päätöksen perusteluissa on seuraamusmaksua koskevan ratkaisun osalta todettu, että kyseessä oleva rikkominen on koskenut suurta määrää rekisteröityjä ja jatkunut varsin pitkään. Hallinto-oikeus on kuitenkin päätöksessä kuvatulla tavalla todennut kyseessä olevan rikkomisen olleen osin tulkinnanvarainen. Hallinto-oikeuden mukaan seuraamusmaksun määrääminen Postille annetun huomautuksen lisäksi oli tehokasta ja varoittavaa. Siten hallinto-oikeus on päätöksessä kuvattujen seikkojen punninnan perusteella katsonut, että seuraamusmaksun määräämistä ei kuitenkaan rikkomisen laatu ja sen rekisteröityihin kohdistuvat vaikutukset kokonaisuutenakaan arvioiden voida pitää oikeasuhteisena seuraamuksena. Tähän nähden hallinto-oikeus on katsonut yleisen tietosuoja-asetuksen 83 artiklan 1 ja 2 kohtien perusteella, että seuraamuskollegiolla ei ole tässä tapauksessa ollut perusteita määrätä Postille seuraamusmaksua.

Tietosuojavaltuutettu pyysi korkeimmalta hallinto-oikeudelta lupaa valittaa Helsingin hallinto-oikeuden päätöksestä. Tietosuojavaltuutettu vaati valituksessaan, että hallinto-oikeuden päätös kumotaan siltä osin kuin seuraamuskollegion päätös seuraamusmaksun määräämisestä on kumottu ja seuraamuskollegion päätös saatetaan voimaan. Korkein hallinto-oikeus myönsi valitusluvan ja antoi päätöksensä 12.9.2023 (KHO:2023:81). Korkein hallinto-oikeus katsoi, että yleisen tietosuoja-asetuksen 12 artiklan 1 kohdassa ja 13 artiklan 1 ja 2 kohdassa, joissa käytetään ilmaisua ”tietojen toimittaminen”, edellytettiin rekisterinpitäjältä aktiivisia toimenpiteitä sanotuissa kohdissa tarkoitettujen tietojen saattamiseksi rekisteröityjen tietoon. Postin ei ole voitu katsoa saattaneen tietoja edellä tarkoitetusta tietojen luovuttamisesta tietyille organisaatioille ja oikeudesta kieltää mainittu yhteystietojen luovuttaminen aktiivisin toimenpitein sekä selkeästi niille sähköisen muuttoilmoituksen tehneille henkilöille, jotka eivät olleet saaneet postinohjauspalveluiden tuote-ehtoja hyväksyttäväkseen. Korkein hallinto-oikeus katsoi lisäksi, että seuraamuskollegio oli yleisen tietosuoja-asetuksen rikkomisen takia voinut määrätä Postille 100 000 euron suuruisen hallinnollisen seuraamusmaksun. Korkein hallinto-oikeus korosti seuraamusmaksun edellytysten arvioinnissaan, että Postin sähköisellä osoitteenmuutospalvelulla oli erittäin paljon käyttäjiä, joiden tietotekniset valmiudet vaihtelivat.

7 Johtopäätökset

Henkilötietojen suojaa koskeva lainsäädäntö on Suomessa kehittynyt ja muokkaantunut sekä teknologian kehityksen harppauksien että EU:n sääntelyn kehityksen myötä. Merkittävimmät askelmerkit kehitykselle ovat olleet ennen kaikkea ylipäänsä tiedon ja sen myötä henkilötietojen irrottautuminen fyysisestä alustastaan digitaaliseen muotoon siirryttäessä. Lainsäädännöllisiä kehityskohtia on jouduttu puntaroimaan eri vuosikymmenten aikana hyvin dynaamisessa toimintaympäristössä. Erityisen paljon henkilötietojen suojaamisessa lainsäädännöllisesti on jouduttu kiinnittämään huomiota muuttuvien sekä kokonaan uusien rikossäännösten tarpeellisuuteen teknologian kehityksen, uusien uhkien ja henkilötietojen käsittelyä koskevien toimintamallien muuttumisen myötä.

Tähän mennessä käänteentekevin sääntelyn muutos erityisesti tietosuojan seuraamusjärjestelmän ja valvontaviranomaisen velvollisuuksien näkökulmasta on EU:n yleinen tietosuoja-asetus. Asetuksen tarkoituksena on ollut luoda ajanmukainen, vahva, yhtenäinen ja kattava tietosuojakehys. Uudistus katsottiin tarpeelliseksi erityisesti informaatioteknologian

nopean kehityksen ja jäsenvaltioiden hajanaisten henkilötietojen suojaa koskevien säädösten ja niiden epäyhtenäisen soveltamisen vuoksi. Yleisen tietosuoja-asetuksen pohjautuessa pitkälti suoraan sovellettavaan sääntelyyn jäsenvaltioissa jättäen kuitenkin osittaista kansallista liikkumavaraa kansalliselle sääntelylle, on Suomessa jouduttu pohtimaan toden teolla rajanvetoja esimerkiksi liikkumavaran käyttämiselle ottaen huomioon kansallinen jo olemassa oleva sääntely sekä käytettävissä olevat resurssit.

Esimerkiksi tietosuojalain lainvalmisteluaineistojen valiokuntien lausunnoissa on useassa kohdassa tunnistettu kehittämistarpeet tietosuojaviranomaisen toiminnalle ja organisoitumiselle. Erityisen paljon valiokunnat ottivat kantaa tietosuoja-asetuksella uudistettuun hallinnollisten seuraamusten määräämiseen, jota määräysvallan toteuttamisen näkökulmasta jouduttiin pohtimaan perustuslain julkisen vallan käytön ja hyvän hallinnon takeiden periaatteiden pohjalta.[67] Perustuslakivaliokunta onkin todennut lausunnossaan hallinnollisen seuraamusmaksun määräämiseen säädetyn toimielimen, seuraamuskollegion, täyttävän pääosin julkista valtaa käyttävän valtionhallinnon toimielimen vähimmäisvaatimukset, mutta katsoi, ettei ratkaisua voida pitää perustuslain 21 §:n kannalta optimaalisena. Vaikkakin kolmen virkamiehen muodostamaa seuraamuskollegiota voidaan sinänsä pitää monijäsenisenä toimielimenä, hallintovaliokunta totesi kollegionimikkeen olleen epäonnistunut, vaikka perustuslaista ei ilmennyt estettä sen käyttämiselle.[68]

Hallinnolliset seuraamusmaksut ovat olleetkin viime vuosien aikana vilkkaan akateemisen tarkastelun kohteena. Eräs keskeinen impulssi tähän keskusteluun on ollut muun muassa Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytäntö koskien *ne bis in idem* -kieltoa tilanteessa, jossa sopimusvaltiossa on määrätty rikosoikeudellisen seuraamuksen ohella jokin muu seuraamus, jota valtionsisäisessä oikeudessa on pidetty muuna kuin rikosoikeudellisena seuraamuksena. *Ne bis in idem* -kiellon soveltamisala ei rajoitu vain rikosoikeudellista rangaistusta koskeviin tuomioihin, vaan se ulottuu myös rangaistusluonteisiin hallinnollisiin seuraamuksiin.

Tietosuojavaltuutetun antamista päätöksistä merkittävä osa koski yrityksiä. Yksittäisiä julkista sektoria koskevia päätöksiä oli myös eri organisaatioihin liittyen. Esimerkiksi julkisen terveydenhuollon tietosuojassa oli puutteita, ja yhdessä päätöksessä tehtiin hallinnollista seuraamusmaksun määräämisharkintaa, mutta tietosuojalaki ei mahdollista hallinnollisen seuraamuksen määräämistä julkiselle toimijalle. Hallinnollisten seuraamusmaksujen määräämiskäytännöt eivät ole aineiston perusteella yhtenevät ja välillä perusteeksi olla määräämättä seuraamusmaksua riitti, että yrityksen toimiala ei ole ensisijaisesti tietojenkäsittely ja kyseessä on pienyritys. Hallinnollisen seuraamusmaksun määräämisen ennustettavuus ei ole selkeää, koska sen voi saada, vaikka olisi yrittänyt tehdä korjaavia toimenpiteitä tietosuojaloukkaustilanteessa.

Täytyy korostaa, että yleisen tietosuoja-asetuksen 83 artiklan 1 kohdan mukaan tietosuoja-asetuksen rikkomisesta määrättävien hallinnollisten sakkojen määräämisen on kussakin yksittäisessä tapauksessa oltava tehokasta, oikeasuhteista ja varoittavaa. Tietosuoja-asetuksen 83 artiklan 2 kohdan mukaan hallinnolliset sakot määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti. Tämän takia on tärkeää, että päätöksistä valitetaan ja saadaan en-

[67] Ks. esim. HaVM 13/2018 vp, s. 39.

[68] PeVL 24/2018 vp: Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, s. 3.

nakkopäätöksiä[69]. Euroopan tietosuojaneuvostossa on tunnistettu haasteet, että seuraamusmaksujen määräämiskäytäntö ei ole yhdenmukaista. Tämän takia he ovat muun muassa laatineet hallinnollisten seuraamusmaksujen laskemiseen ohjeen, jonka tarkoituksena on yhdenmukaistaa kansallisten tietosuojaviranomaisten tapoja yleisen tietosuoja-asetuksen perusteella määrättyjen seuraamusmaksujen suuruuden laskennassa.[70]

Ylipäätään Euroopassa tietosuojavalvontaviranomaiset ovat määränneet entistä enemmän seuraamusmaksuja, kun niiden kokonaismäärä on kasvanut 50 prosentin vuosivauhdilla. Tämä on herättänyt useissa valtioissa keskustelua siitä, että organisaatiot ovat yhä varovaisempia ilmoittamaan tietosuojarikkomuksista, koska pelkäävät sakkoja ja korvausvaatimuksia.[71] Tietosuojan kannalta tietoturvallisuuden kontrollien tehokkuudella ja organisaatioiden riskienhallinnan sekä sääntelyn toimivuudella on merkitystä, jotta voidaan tehokkaasti suojata henkilötietoja. Tietorikoksilla voidaankin vahingoittaa laajasti yhteiskuntaa[72], kuten Vastaamon tapaus osoittaa. Tämän takia olisi tärkeää tehdä vertailevaa tutkimusta tietosuojavalvontaviranomaisten välillä ja tutkia myös hallinnollisen seuraamusjärjestelmän hyötyjä tietosuojan sekä tietoturvallisuuden kehittämisen näkökulmasta. Tietorikollisuus onkin merkittävä haaste koko rikosoikeusjärjestelmälle.[73]

[69] Ks. esim. KHO:2023:81 ja KHO:2023:82.

[70] Euroopan tietosuojaneuvosto 2023.

[71] Ks. esim. Ross McKean – Ewa Kurowska-Tober – Heidi Waem – Rachel de Souza, DLA Piper GDPR Fines and Data Breach Survey: January 2023. DLA Piper 2023. Saatavissa osoitteessa https://www.dlapiper.com/en-ae/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023.

[72] Ks. esim. Aldona Kipane, Meaning of profiling of cybercriminals in the security context. SHS Web Conf. 01009/2019, s. 1–15. Saatavissa osoitteessa https://doi.org/10.1051/shsconf/20196801009.

[73] Jyri Paasonen – Mikko Aaltonen – Mikko Luomala 2021, s. 987.