Rekisteröidyn oikeudet ja rekisterinpitäjän toimintavelvollisuudet tietovuototilanteissa

Lapin yliopisto
Oikeustieteiden tiedekunta
Maisteritutkielma
Oikeusinformatiikka
Mari-Pauliina Kaarlela
Kevät 2020

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Rekisteröidyn oikeudet ja rekisterinpitäjän toimintavelvollisuudet tietovuototilanteissa
Tekijä: Mari-Pauliina Kaarlela
Opetuskokonaisuus ja oppiaine: Oikeusinformatiikka
Työn laji: Tutkielma X Lisensiaatintyö__
Sivumäärä: X+68
Vuosi: 2020
Tiivistelmä:

Tämä tutkimus käsittelee rekisteröidyn oikeuksia ja rekisterinpitäjän toimintavelvollisuuksia tietovuototilanteissa. Henkilötietojen suoja on perusoikeus, jolle on sisällytetty sääntelyvaraus perustuslain 10 §:n 1 momentissa. Yleisen tietosuoja-asetuksen toisena tavoitteena puolestaan on henkilötietojen suojan parantuminen asetuksen tultua voimaan. Tutkimukseni selvittää henkilötietojen toteutumista tietosuoja-asetuksen tasolla nimenomaan tietovuototilanteissa.

Tutkielman tavoite on selvittää, mitä henkilötiedoilla tarkoitetaan, miten niiden suoja nähdään osana perusoikeusjärjestelmää sekä miten tietosuoja-asetuksessa säädetään rekisterinpitäjän toimintavelvollisuuksista jälkikäteen, kun tietovuoto on tapahtunut. Mikäli rekisterinpitäjälle ei ole asetettu tarpeeksi toimintavelvollisuuksia, tutkin, mikä voisi olla sellainen jälkikäteinen keino, millä henkilötietojen suojan toteutuminen voitaisiin varmistaa. Toimintavelvollisuuksien kannalta tarkastelen myös sitä, mikä vaikutus rekisterinpitäjän asemalla on tietosuoja-asetuksen näkökulmasta. Tutkin myös sitä, miten rekisteröidyn oikeudet toteutuvat tietovuototilanteissa ja voisiko asetuksen nojalla rekisteröityä vastuuttaa enemmän henkilötietojen käsittelyperusteen perusteella.

Tutkimuksen metodi on oikeusdogmatiikka eli lainoppi, mutta tutkielma sisältää de lege ferenda -kannanottoja havaitessani puutteita tietosuoja-asetuksessa.

Tutkimuksen kannalta keskeinen johtopäätös on se, että tietosuoja-asetuksessa on jälkikäteisten toimintavelvoitteiden osalta aukko. Rekisteröity ei aina edes saa tietoa henkilötietojensa joutumisesta tietovuodon kohteeksi ja ei voi hakea tällä perusteella oikeutta suojan rikkoutumiselle. Tietosuoja-asetus ei myöskään ole tasavertainen sen suhteen, onko rekisterinpitäjä valtio vai yksityinen toimija. Rekisteröidyn oikeudet eivät tietovuototilanteissa aina nauti perusoikeustasoista suojaa.

Avainsanat: Henkilötietojen suoja, perusoikeudet, rekisterinpitäjä, rekisteröidyn oikeudet, rekisteröity, tietosuoja-asetus, tietovuoto.

Sisällys

Lähteet

Kirjallisuus ja artikkelit

Aarnio, Aulis. Oikeussäännösten systematisointi ja tulkinta: Ajatuksia teoreettisesta ja käytännöllisestä lainopista. Teoksessa: Häyhä, Juha (toim.). Minun metodini. Porvoo 1997.

Andreasson, Ari – Koivisto, Juha – Ylipartanen, Arto. Tietosuojavastaavan käsikirja. Helsinki 2013.

Andreasson, Ari – Koivisto, Juha – Ylipartanen, Arto. Tietosuojavastaavan käsikirja 2. Helsinki 2014.

Andreasson, Ari – Koivisto, Juha – Ylipartanen, Arto. Tietosuojakäsikirja johdolle. Tallinna 2015.

Andreasson, Ari – Riikonen, Jaana – Ylipartanen, Arto. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Tallinna 2019.

Guadamez, Andres. Habeas data: The Latin-American Response to Data Protection. The journal of information, Law and Technology. 2000.

Hallberg, Pekka – Karapuu, Heikki – Ojanen,Tuomas – Scheinin,Martin – Tuori,Kaarlo – Viljanen,Veli-Pekka. Perusoikeudet. Helsinki 2011.

Hakapää, Kari. Uusi kansainvälinen oikeus. Helsinki 2010.

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

Heiskanen, Jesse. Henkilötiedon käsite ja anonyymit tiedot eurooppalaisessa tietosuojalainsäädännössä. Edilex-julkaisu 2020.

Hildén, Jockum. Am I my IP address´s keeper? Revisiting the boundaries of information privacy. Helsinki 2017. Saatavissa Taylor & Francis online-palvelusta https://www-tandfonline-com..fi/doi/full/10.1080/01972243.2017.1294127 (maksullinen).

Huovila, Mika. Oikeuslähdeoppi ja oikeudellinen argumentaatio rikostuomion perusteluissa. Julkaisun pysyvä osoite https://oikeus.fi/hovioikeudet/helsinginhovioikeus/material/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/painetutjulkaisut/rikostuomionperusteleminen2005lisapainos2006./OS0uyDOHv/04_Oikeuslahdeoppi_ja_oikeudellinen_argumentaatio..._Mika_Huovila.pdf. Julkaistu 2020.

Husa, Jaakko – Mutanen, Anu – Pohjolainen, Teuvo. Kirjoitetaan juridiikkaa. Helsinki 2008.

Husa, Jaakko. Oikeusvertailu: teoria ja metodologia. Viro 2013.

Karhu, Juha. Perusoikeudet ja oikeuslähdeoppi. Lakimies 5/2003. Löytyy osoitteesta www.edilex.fi (maksullinen).

Kemppinen, Jukka. Informaatio-oikeuden alkeet. Tallinna 2013.

Kolehmainen, Antti. Tutkimusongelma ja metodi lainopillisessa työssä. Edilex 2015/29. Saatavissa https://www.edilex.fi/artikkelit/15461.pdf (maksullinen).

Konstari, Timo. Henkilörekisterilaki: Säännökset ja käytäntö. Lakimiesliiton kustannus 1992.

Korhonen, Rauno. Poliisin valvontakeinot ja kansalaisten yksityisyyden suoja. Helsinki 2005.

Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija. Uusi tietosuojalainsäädäntö. Helsinki 2018.

Korpisaari, Päivi. Tietovuodot kuuluvat demokratiaan. Lakimiesuutiset 6/2019. Saatavissa https://lakimiesuutiset.fi/tietovuodot-kuuluvat-demokratiaan/.

Laakso, Matti. Verkkopalvelun tarjoaja – Kunnioitatko käyttäjän yksityisyyttä? Teoksessa Näkökulmia tietoturvaan 2. Tampere 2014.

Lehtonen, Tuomas. Tietosuojalainsäädäntö ja julkisuusperiaate törmäävät vastakkain. Lakimiesuutiset 2/2020. Saatavissa https://lakimiesuutiset.fi/tietosuojalainsaadanto-ja-julkisuusperiaate-tormaavat-vastakkain/.

Mäenpää, Olli. Julkisuusperiaate. Helsinki 2016. E-kirja.

Määttä, Kalle. Oikeustaloustieteen perusteet. Helsinki 2006.

Neuvonen, Riku. Yksityisyyden suoja Suomessa. Helsinki 2014. E-kirja.

Niemi, Hanna-Leena. Teoksessa: Mitä oikeudet ovat? Filosofian ja oikeustieteen näkökulmia. Toimittaneet Maija Aalto-Heinilä & Kurki Vesa. Tallinna 2019.

Niemi, Marja-Leena (toim.). Oikeus tänään, osa 1. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 64. Rovaniemi 2016.

Niemi-Kiesiläinen, Johanna – Honkatukia, Päivi – Karma, Helena – Ruuskanen, Minna. Oikeuden tekstit diskursseina. Jyväskylä 2006.

Nieminen, Liisa (toim.). Perusoikeudet EU:ssa. Jyväskylä 2001.

Niinimäki-Rasta, Päivi. Tietosuojan vaikutustenarviointi -tehdäkö vai eikö tehdä, siinä pulma? Saatavissa: https://www-edilex.fi/uutiset/52706?allWords=identiteettivarkaus&offset=21&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=673667 (maksullinen).

Ojanen, Tuomas. EU-oikeuden perusteita. Helsinki 2003.

Ojanen, Tuomas. Johdatus perus- ja ihmisoikeusjuridiikkaan. Helsinki 2009.

Paavola, Jarkko toim. Näkökulmia tietoturvaan 2. Tampere 2014.

Pellonpää, Matti. Euroopan ihmisoikeussopimus. Helsinki 2005.

Pellonpää, Matti – Gullans, Monica – Pölönen, Pasi – Tapanila, Antti. Euroopan ihmisoikeussopimus. Helsinki 2018.

Pitkänen, Olli – Tiilikka, Päivi – Warma, Eija. Henkilötietojen suoja. Vantaa 2013.

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

Pulkkanen, Aleksi. 04/2018: Kooste ja tulkintaa tietosuojaviranomaisten ohjeista tietoturvaloukkausten informointiin liittyen. Saatavissa https://www.valmennus.eu/blogi/04-2018-kooste-ja-tulkintaa-tietosuojaviranomaisten-ohjeista-tietoturvaloukkausten-informointiin-liittyen. Kauppakamari 2018.

Päläs, Jenna. Johdatus jakamistalouteen ja jakamistalousjuridiikkaan. Teoksessa Päläs, Jenna – Määttä, Kalle. Jakamistalousjuridiikan käsikirja. Helsinki 2019.

Saarenpää, Ahti. Teoksessa Oikeusjärjestys, osa 1. 8. täydennetty painos. Toimittanut Tammilehto, Timo. Rovaniemi 2012.

Sajama, Seppo. Mikä tekee tutkimuksesta tieteellisen? s. 2 – 23 teoksessa Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edita Publishing Oy 2016.

Sankari, Valtteri – Wiberg, Matti. GDPR ei toimi: Tietosuojakäytännöt eivät noudata asetusta 2019. Saatavissa: http://www.julkari.fi/handle/10024/138277.

Saraviita, Ilkka. Perustuslaki. Helsinki 2011. E-kirja.

Savolainen, Jukka. Tietosuojavaltuutetun toimisto: Esimerkit avuksi tietoturvaloukkausten tunnistamiseen. Saatavissa https://www.edilex.fi/uutiset/57168?allWords=tietoturva&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=692136 (maksullinen).

Sitek, Magdalena – Terem, Peter – Wójcicka, Marta. Collective human rights in the first half of the 21st century. Józefów 2015.

Smouter, Kim 2018. The year of GDPR, How Europe's General Data Protection Regulation changes things for you. Saatavissa: https://onlinelibrary.wiley.com/doi/pdfdirect/10.1002/rwm3.20624 (maksullinen).

Soininen, Heidi 2017. KTM Heidi Soininen: Kyberidentiteettivarkauden prosessioikeudelliset haasteet. Edilex-julkaisu. Saatavissa https://www.edilex.fi/uutiset/51203 (maksullinen).

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

Vanto, Jarno. Henkilötietolaki käytännössä. Helsinki 2011.

Viljanen, Veli-Pekka. Teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka. Perusoikeudet. Helsinki 2011.

Viljanen, Vesa. Tietoturva. Saatavissa https://www.yksityisyydensuoja.fi/tietoturva.

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

Voigt, Paul – von dem Bussche, Axel. The EU General Data protection Regulation (GDPR) A Practical Guide. Springer International Publishing. Berlin 2017.

Virallislähteet

Kansalliset

HE 309/1993 vp. Hallituksen esitys eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

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

HE 284/2018 vp. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

Oikeusministeriö. Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita 4/2017. Löytyy osoitteesta https://tietosuoja.fi/documents/6927448/9666681/Miten+valmistautua+tietosuoja-asetukseen/8c5b9a96-a8ce-4c91-ad06-6e36130bd0e5/Miten+valmistautua+tietosuoja-asetukseen.pdf.

PeVL 14/2002 vp. Hallituksen esitys Kansaneläkelaitoksen toimeenpanemiin etuuksiin liittyviin tietojen saamista ja luovuttamista koskevien säännösten muuttamiseksi.

PeVL 27/2006 vp. Valtioneuvoston kirjelmä ehdotuksesta neuvoston puitepäätökseksi (III-pilarin tietosuoja).

PeVL 25/2010 vp. Hallituksen esitys laeiksi nuorisolain sekä opiskelijavalintarekisteristä ja ylioppilastutkintorekisteristä annetun lain 5 §:n muuttamisesta.

PeVL 14/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

Kansainväliset

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

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä helmikuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

Euroopan komissio 1990. Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security. COM (90) 314 final, 13.9.1990.

Euroopan komissio 1992. Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM (92) 422 final, 28.10.1993.

Euroopan komissio 2018. Euroopan komissio, annex to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Coordinated Plan on Artificial Intelligence. Saatavissa: https://ec.europa.eu/digital-single-market/en/news/coordinater-plan-artificial-intelligence.

Muut viranomaisjulkaisut

Artikle 29 Data protection working party. Saatavissa https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp239_en.pdf.

Eduskunta.fi Saatavissa https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_38+2010.pdf.

European Commission. Guidelines on Personal data breach. Saatavissa https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

European Commission. Saatavissa https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Saatavissa https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf?sequence=1&isAllowed=y.

Finlex. Saatavissa http://lainkirjoittaja.finlex.fi/4-perusoikeudet/4-2/#jakso-4-2-5.

HETU-työryhmän loppuraportti. Saatavissa https://api.hankeikkuna.fi/asiakirjat/beb585c4-f7b5-4f04-b15d-6f89c5ad72d1/3d8ba14b-0393-421d-a22e-6dae1c5efa29/RAPORTTI_20200409115946.pdf.

OECD. Saatavissa http://www.oecd.org/sti/ieconomy/privacylawenforcementco-operation.html.

Oikeusministeriö. Saatavissa https://oikeusministerio.fi/etusivu.

Perustuslakivaliokunta. Valiokunnan lausunto PeVL 14/2018vp – HE 9/2018 vp. Saatavissa https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_14+2018.pdf.

Valtioneuvosto 2017. Henkilötunnuksen uudistamista ja valtion takaaman identiteetin hallinnoimista koskeva työryhmä (HETU-työryhmä). Saatavissa https://valtioneuvosto.fi/hanke?tunnus=VM068:00/2017.

Valtiovarainministeriö 2009. VAHTI 8/2008 Valtionhallinnon tietoturvasanasto. Saatavissa https://www.vahtiohje.fi/web/guest/maaritelmat-t.

Valtiovarainministeriö 2020. Tiedonhallintalaki. Saatavissa https://vm.fi/tiedonhallintalaki.

Valtiovarainministeriö. Saatavissa https://vm.fi/artikkeli/-/asset_publisher/julkisen-hallinnon-digitaalista-turvallisuutta-kehitetaan.

WP 29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is"likely to result in a high risk" for the purposes of Regulation 2016/679. Saatavissa https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358.

WP 136, WP 29: Opinion 4/2007 on the concept of personal data. Annettu 20.6. 2007.

Oikeustapaukset

EIT 17.7.2008 I v. Suomi (viitattu 7.2.2020)

EUT C-201/14 Bara. (viitattu 1.2.2020).

Yhdistetyt asiat C–293/12 ja C–594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym. 2014, julkaistu sähköisessä oikeustapauskokoelmassa. (Digital Rights Ireland, viitattu 4.10.2019)

Muut lähteet

Datainspektionen. Saatavissa https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf. (Luettu 4.2.2020).

Digi- ja väestötietovirasto. Saatavissa https://dvv.fi/henkilotunnus. (Luettu 17.4.2020)

Elinkeinoelämän keskusliitto. Saatavissa https://ek.fi/ajankohtaista/uutiset/2016/05/12/hyotytietoa-yrityksille-eu-asetus-henkilotietojen-suojasta-julkaistu-lopullisessa-muodossaan/ (Luettu 9.2.2020)

ENISA. Saatavissa https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches ja https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. (Luettu 4.2.2020).

GDPR Enforcement Tracker. Saatavissa https://www.enforcementtracker.com/#. (Luettu 13.2.2020).

Kyberturvallisuuden sanasto. Saatavissa https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf (Luettu 14.3.2020).

KvaliMOTV. Saatavissa https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_3_6_1.html. (Luettu 7.2.2020).

Menetelmäopas. Saatavissa: https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_3_6_1.html (Luettu 6.2.2020)

Tietosuojauutiset. Saatavissa https://tietosuojauutiset.fi/2018/04/27/lapinakyvyyden-periaatteen-toteuttaminen-kaytannossa-wp29n-hiljattain-paivitetyn-ohjausasiakirjan-valossa/. (Luettu syksy 2019).

Tietosuojavaltuutetun toimisto. Saatavissa tietosuoja.fi. (Luettu syksy 2019/kevät 2020).

The White House 2008. Comprehensive National Cybersecurity Initiative. Saatavissa obamawhitehouse.archives.org. (Luettu 7.2.2020).

Valtiovarainministeriö 2009. VAHTI 8/2008 Valtionhallinnon tietoturvasanasto. Saatavissa https://www.vahtiohje.fi/web/guest/maaritelmat-t. (Luettu 6.2.2020).

Valtiovarainministeriö. Saatavissa https://vm.fi/artikkeli/-/asset_publisher/julkisen-hallinnon-digitaalista-turvallisuutta-kehitetaan. (Luettu 15.3.2020).

Teknologian tutkimuskeskus VTT Oy 2020. Saatavissa https://www.vtt.fi/sites/SHARE/mitä-on-jakamistalous. (Luettu 15.3.2020).

Lyhenteet

CSIRT	**Computer security incident response team**
EDPB	**European Data Protection Board**
EIT	**Euroopan ihmisoikeustuomioistuin**
EU	**Euroopan unioni**
OECD	**Taloudellisen yhteistyön ja kehityksen järjestö (Organization for Economic Co-Operation and Development).**
PL	**Perustuslaki**
RL	**Rikoslaki**
SEU	**Sopimus Euroopan unionista**
TSA	**Yleinen tietosuoja-asetus**
WP 29	**Article 29 Working Party, EU:n tietosuojatyöryhmä**

1 JOHDANTO

1.1 Taustaa

Tietosuoja ymmärretään yleensä yksityisten henkilöiden, rekisteröityjen, yksityisyyden suojan ja oikeusturvan varmistamiseksi säänneltyjen lakien ja erityislakien vaatimusten huomioon ottamisena. Tietosuojan tarkoituksena on neuvoa rekisterinpitäjiä henkilötietojen käsittelyssä sekä turvata tiedon kohdetta, sen yksityiselämää, etuja ja oikeuksia.[1] Tarkoituksena on osoittaa, milloin henkilötietoja voidaan käsitellä ja millä edellytyksillä.[2] Se on perustuslaissa turvattu oikeus, jonka tarkoitus on taata ihmisen oikeus elää elämäänsä niin kuin tahtoo ilman kenenkään perusteetonta puuttumista siihen. Henkilötietolainsäädäntö osoittaa rekisterinpitäjälle ne rajat, joiden puitteissa sen tulee käsitellä etenkin arkaluonteisia tietoja.[3]

Tiedon tarkoittamaton siirtyminen suojatun järjestelmän ulkopuolelle voi aiheuttaa tietoturvaloukkauksen. Tietosuoja-asetuksen[4] 3 artiklan 12 kohdan mukaisesti tämän tapahtuman seurauksena siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen siirtyminen suojatun järjestelmän ulkopuolelle voi johtaa vahingossa tai lainvastaisesti tapahtuvaan tuhoamiseen, häviämiseen, muuttamiseen tai jopa luvattomaan luovuttamiseen tai johtaa tietoihin pääsyyn. Tällainen tiedon tarkoittamaton siirtyminen voi aiheuttaa rekisteröidyn henkilötietojen suojan rikkoutumista tai saattaa rekisteröidyn rikollisuuden kohteeksi.[5]

Toukokuussa 2018 astui voimaan koko EU:n alueella suoraan sovellettava yleinen tietosuoja-asetus.[6] Tietosuoja-asetuksen yleisenä tavoitteena on yhdenmukaistaa EU:n jäsenvaltioiden tietosuojalakeja sekä helpottaa sen avulla palveluiden tarjontaa yli valtioiden

1 Andreasson – Koivisto – Ylipartanen 2013, s.14.
2 Tietosuojavaltuutetun toimisto ->Tietosuoja.
3 Andreasson – Koivisto – Ylipartanen 2013, s.14.
4 Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).
5 Henkilö voi joutua esimerkiksi petoksen kohteeksi, vahinko voi johtaa taloudelliseen menetykseen tai henkilö voi kärsiä sosiaalista vahinkoa kuten maineen menetys.
6 Suomessa tietosuoja-asetuksesta käytetään myös nimitystä GDPR, joka tulee englanninkielisistä sanoista General Data Protection Regulation.

rajojen. Asetuksen tavoitteena on suojata luonnollisten henkilöiden henkilötietoja, kun niitä käytetään asetuksen soveltamisalaan kuuluvissa tarkoituksissa.

Asetuksessa säädetyt tavoitteet henkilötietojen suojan parantamiseksi ovat lähtökohtaisesti *etukäteen* toteutettavia toimenpiteitä. Asetuksen perusteella tähän tähtääviä toimenpiteitä ovat esimerkiksi riittävät ennakolliset toimenpiteet, osoitusvelvollisuus ja vaikutustenarviointi.

Suomen perustuslain (PL, 731/1999) 10 §:ssä säädetään yksityiselämän suojasta. Pykälän 1 momentin mukaan *"jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla".* Henkilötietojen suoja on osa tätä perusoikeutta, ja sen suojelemiseksi on EU:n tasolla säädetty uusi yleinen tietosuoja-asetus.[7] Henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunta on EU:n tietosuojauudistuksen voimaantulon myötä tarkistanut henkilötietojen suojaa koskevan sääntelyn vaatimuksia. Valiokunta on todennut, että yleisen tietosuoja-asetuksen yksityiskohtainen sääntely muodostaa yleensä riittävän säännöspohjan perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta.[8]

Taustana tälle maisteritutkielmalle ovat lukuisat tietovuototilanteet, joita tapahtuu väistämättä, vaikka etukäteen tehtävät toimenpiteet olisi huolehdittu tietosuoja-asetuksen mukaisesti. Näistä tietovuototilanteista esimerkkinä voin mainita Verohallinnolta elokuussa 2019 lähteneet kirjeet, joissa teknisen virheen vuoksi ihmisten henkilötietoja sekoittui ja päätyi väärille henkilöille. Kyseisessä tietovuodossa vuoto tapahtui viranomaisen rekistereistä, ja mediassa tähän vuotoon suhtauduttiin kuin mihin tahansa inhimilliseen virheeseen. Verohallinnon tietosuojavastaava kommentoi mediassa, että todennäköisyys väärinkäytöksille vuodon kohteena olevien henkilötietojen osalta on pieni. Kirjeiden mukana vuoti kuitenkin esimerkiksi henkilötunnuksia väärille ihmisille. Apulaistietosuojavaltuutetun antaman ratkaisun perusteella sen ei tarvinnut antaa Verohallinnolle määräystä tietosuoja-asetuksen mukaisten velvoitteiden täyttämiseksi, koska Verohallinto pystyi selvittämään tietoturvaloukkauksen kulun sekä sitoutui ilmoittamaan loukkauksesta rekisteröidyille.[9]

[7] Tutkielmassa keskitytään vain tietosuoja-asetuksen toiseen tavoitteeseen, henkilötietojen suojaan.
[8] Valiokunnan lausunto PeVL 14/2018 vp -HE 9/2018 vp, s. 4.
[9] Tietosuojavaltuutetun toimisto -> ajankohtaista ->artikkeli -> Tietosuojavaltuutettu on päättänyt Verohallinnon tietoturvaloukkausten käsittelyn.

1.2 Tutkielman tavoitteet ja tutkimuskysymykset

Tietosuoja-asetus on ollut voimassa nyt kaksi vuotta, ja sen soveltamisen vaikutuksia voidaan jo nähdä. Asetus asettaa rekisterinpitäjille laajat velvollisuudet toimia etukäteen henkilötietojen suojan varmistamiseksi. Sen tarkoituksena on parantaa henkilötietojen suojan tasoa. Rekisterinpitäjiä sitoo velvollisuus pystyä todentamaan tietosuoja-asetuksen asianmukainen noudattaminen.[10]

Tässä maisteritutkielmassa tarkastelen tietosuoja-asetuksen mukaisia rekisteröidyn oikeuksia suhteessa tietovuototilanteisiin. Tarkastelun kohteena ovat rekisterinpitäjän toimintavelvollisuudet tietoturvaloukkausten tapahduttua, eli jälkikäteiset toimintatavat. Tarkastelen näitä oikeudellisia kysymyksiä voimassa olevan oikeuden kautta, *vallitsevan lainopin* mukaisesti.[11] Taustana tälle näkökulmalle on edellä kappaleessa 1.1. mainittu esimerkki.

Tarkastelun näkökulma on oikeusinformatiikan alaan liittyvä, koska tarkastelen tutkielmassa ihmisten, rekisteröityjen, oikeuksien suhdetta yhteiskuntaan muuttuvassa yhteiskunnassa. Tarkoituksenani on tutkia tätä tietosuoja-asetuksen mukanaan tuomaa oikeudellisesti merkityksellistä kehitystä. Lähestyn rikosoikeutta vain siitä näkökulmasta, että selvitän, mitä seurauksia rekisteröidylle voi aiheutua henkilötietojen väärinkäytöstä. Rajaan ulkopuolelle kuitenkin rikosoikeudelliset seuraukset ja tunnusmerkistöjen täyttymiset. Tutkielman lopussa otan kantaa rikoslain (39/1898) 38 luvun 9 §:ssä säädettyyn tietosuojarikokseen sen verran, että selvitän mitä haasteita kyseisessä pykälässä on rekisteröidyn oikeuksien toteutumisen näkökulmasta. Keskityn tutkielmassa lähinnä selvittämään rekisterinpitäjän velvollisuuksia ja rekisteröidyn oikeuksia tietoturvaloukkaustilanteissa. Sivuan rikosoikeutta vain muutamassa kappaleessa, kun selvitän, mitä mahdollisia seuraamuksia tietoturvaloukkauksista voi aiheutua rekisteröidylle. Jätän tutkielman ulkopuolelle myös tietosuoja-asetuksen toisen tavoitteen: vapaiden markkinoiden takaamisen ja sisämarkkinaulottuvuuden lujittamisen.

[10] Euroopan komissio 2018, s. 18.
[11] Kolehmainen 2015, s.2.

Koska tarkastelen oikeuksien ja velvollisuuksien toteutumista ja huomioon ottamista tietosuoja-asetuksessa, tutkimuskysymykseni ovat tiivistetysti: ” miten rekisterinpitäjän jälkikäteiset keinot tietoturvaloukkaustilanteissa on otettu huomioon tietosuoja-asetuksessa?” ja toisaalta myös ” miten rekisteröidyn oikeudet toteutuvat tietoturvaloukkaustilanteissa?”.

Tarkasteltavia kysymyksiä pyrin lähestymään selvittäen ensin henkilötietojen merkitystä perusoikeusjärjestelmässä, jatkan kohti asetuksessa määriteltyjä oikeuksia ja velvollisuuksia ja lopuksi tarkastelen näitä suhteessa tietoturvaloukkaustilanteisiin. Tutkielmani alussa käyn läpi henkilötietojen käsitettä ja perusoikeusluonnetta. Tarkoitus on, että lukija ymmärtää henkilötietojen suojan perusoikeusjärjestelmässä ja tietää, mitä henkilötiedoilla tarkoitetaan. Tämän lähtökohdan jälkeen käyn läpi tietosuoja-asetuksessa säädettyjä rekisteröidyn oikeuksia ja rekisterinpitäjän vastuita. Tarkoitus on, että lukija ymmärtää EU:n tasolla säädetyn asetuksen sisältöä suhteessa tarkasteltaviin tutkimuskysymyksiin. Tutkielmani lopussa käyn läpi näitä rekisterinpitäjän vastuita ja rekisteröidyn oikeuksia juuri tietoturvaloukkausten näkökulmasta. Tällä tavalla pyrin löytämään vastauksia tutkimuskysymyksiini.

Asetuksen perusteella on määritelty hyvin ennakoivia toimenpiteitä henkilötietojen keräämiseen ja käyttämiseen, mutta jälkikäteiset keinot vahinkojen korjaamiseksi eivät ole tarpeeksi yksityiskohtaisesti säänneltyjä. Tarkoitukseni on pohtia näitä jälkikäteisiä keinoja ja sitä, ovatko tämän hetkisen asetuksen mukaiset keinot riittäviä vai onko niissä aukkoja suhteessa rekisteröidyn oikeuksien toteutumiseen. Pyrin myös tuomaan näkökulmia esille sen suhteen, onko tietosuoja-asetuksessa nähtävillä mahdollisia aukkoja sen mukaan, kuka on rekisterinpitäjä ja miten rekisteröidyn oikeudet todella toteutuvat.

1.3 Tutkimusmetodi ja lähdeaineisto

Metodilla tarkoitetaan sitä keinoa tai menetelmää, jolla tutkielman kannalta tarvittava tieto voidaan saavuttaa. Tutkimusmetodini on lähtökohtaisesti oikeusdogmaattinen, eli voimassa olevan lain sisältöä tutkiva. Tutkimuskohteena oikeusdogmatiikassa on voimassa oleva ja velvoittava oikeus. Voimassa oleva oikeus sitoo lainopin harjoittajaa.[12] Lainopin

[12] Hirvonen 2011, s. 21 – 22, 26.

tarkoituksena on tutkia sääntöjen tulkintaa ja oikeussäännösten systematisointia.[13] Systematisoinnissa jäsennetään oikeudenalojen käsitteitä ja oikeusperiaatteita sekä teoreettisia rakennelmia.[14] Systematisoinnin avulla selvitetään oikeusjärjestyksen muodostamaa kokonaisuutta ja jäsennellään voimassa olevaa oikeutta luomalla ja kehittämällä oikeudellista käsitejärjestelmää.[15] Sen on nähty olevan lainsäätäjän tehtävän jatkoa.[16] Tutkielmassa tutkin voimassa olevaa tietosuoja-asetusta ja sitä, miten tietosuoja-asetus velvoittaa rekisterinpitäjiä toimimaan tietoturvaloukkausten jo tapahduttua. Tutkielmassa pyrin jäsentelemään tietosuoja-asetuksesta peräisin olevaa oikeudellista informaatiota rekisteröidyn perusoikeuksien toteutumisen kannalta. Pyrin myös ottamaan huomioon tarkasteltavien kysymysteni kannalta sellaiset olennaiset seikat, joita lainsäätäjä olisi voinut säädellä yksityiskohtaisemmin kuin nyt tämän hetkisen lainsäädännön mukaan.

Vaikka oikeustieteellisessä kirjallisessa työssä voisi olla myös muita tieteenaloja koskevia elementtejä ydinongelman ollessa kuitenkin juridinen[17], tutkielmani on lähinnä oikeudellinen. Tutkielma keskittyy perusoikeuden suojan toteutumiseen voimassa olevan lainsäädännön näkökulmasta. Tutkielmassa esitetään kuitenkin de lege ferenda -näkökulmaan liittyviä ratkaisumalleja siitä näkökulmasta, mitä perusoikeuden, henkilötietojen suojan toteuttamisen kannalta voitaisiin lainsäädännössä tehdä muutoksia. De lege ferenda -tutkimus kohdistuu lainsäädännöllisten ratkaisumallien arviointiin juuri sen suhteen, mihin tuleva lainsäädäntö voisi perustua. Tällöin tutkimuksessa ehdotetaan uutta ratkaisuehdotusta, joka koskee tulevaa lainsäädäntöä.[18] Tutkielmassa olen de lege ferenda -otteeseen perustuen esittänyt ratkaisuehdotuksia sen suhteen, miten lainsäädäntöä voitaisiin muuttaa yhdenvertaisemmaksi rekisterinpitäjien välillä.

Tutkielmani lähteet koostuvat EU-tason lähteistä, kansallisista oikeuslähteistä, aiheeseen liittyvistä uutisista ja julkaisuista. Julkaisut, joita käytän lähteinä, ovat oikeustieteellisiä julkaisuja sekä ammatillista oikeuskirjallisuutta. Lähteinä käytetään myös eräitä Euroopan ihmisoikeustuomioistuimen (EIT) tasolta tulleita oikeustapauksia. Koska tutkielma on oikeustieteiden tiedekunnan tutkielma, tulee tutkielmassa näkymään myös eri oikeuslähteiden velvoittavuus. Tutkielmassa nojataan paljon EU:n tasolta tulleisiin

[13] Aarnio 1997, s. 36 – 37.
[14] Hirvonen 2011, s. 25.
[15] Husa – Mutanen – Pohjolainen 2008, s. 20.
[16] Kolehmainen 2016, s.128.
[17] Ks. Husa – Mutanen – Pohjolainen 2008, s. 19.
[18] Kolehmainen 2016, s. 108.

suosituksiin ja ammattilaisten laatimiin artikkeleihin aiheista. Suositukset ovat lähinnä *sallittuja oikeuslähteitä*, eli ne eivät velvoita sellaisenaan. Niillä on kuitenkin tarkoitus auttaa asetuksen luettavuutta ja yhtenäistää sen soveltamista riippumatta niiden oikeuslähdeluonteesta.[19] Sallittujen oikeuslähteiden avulla voidaan lainopillista tulkintaa selventää, ja samalla päädytään systematisoinnin prosessiin. Systematisoinnin prosessissa hajanainen informaatio pakataan selviin yhdistelmiin.[20]

1.4 Tutkimusalasta

Tutkielman aihe kuuluu oikeusinformatiikkaan. Oikeusinformatiikan puitteissa tutkitaan ja opetetaan oikeuden ja informaation sekä oikeuden ja tietotekniikan välisiä suhteita eri muodoissaan. Tutkimuksen kohteena oikeusinformatiikassa on myös oikeudelliset sääntely- ja tulkintakysymykset, joita näiden suhteiden välillä ilmenee.[21]

Oikeusinformatiikkaa on luonnehdittu muutosten oikeustieteeksi, koska se on uusi tiede ja siihen liittyy vakiintuneesti yhteiskunnan muutos varhemmasta palveluyhteiskunnasta informaatioyhteiskunnaksi. Myös vaikutus muuttuvaan oikeuskulttuuriin, tieteellinen yleissivistys ja kansainvälisyys ovat tälle ominaisia tunnusmerkkejä.[22]

Henkilötietojen suoja on osa persoonallisuusoikeutta, joka on osa siviilioikeutta. Henkilötietojen suojaa järjestävä tietosuojalainsäädäntö on samalla ollut ja on vakiintuneimpia oikeusinformatiikan alaan kuuluvia tutkimusaiheita. Samassa rajapinnassa henkilötietojen suojan kanssa on myös julkisuusperiaate. Julkisuusperiaatteen mukaisesti jokaisen julkisen hallinnon tietojärjestelmien päätekäyttäjän tulee jo viranomaisten toiminnan julkisuudesta annetun lain (JulkL, 621/1999) perusteella tuntea yksityisyyden, henkilötietojen suojan ja julkisuuden merkitys hallinnon tietojärjestelmiä käytettäessä.[23]

Tietosuoja-asetus tutkielman kohteena on varsin uusi, kun se on tätä kirjoitettaessa ollut voimassa vasta pari vuotta. Siitä on kuitenkin ehditty tehdä jo lukuisia tutkielmia. Oikeusinformatiikan puitteissa tämän asetuksen tutkiminen on ajankohtaista, koska siinä yhdistyvät oikeudelliset sääntely- ja tulkintakysymykset. Näihin kysymyksiin ei varsinaisesti ole vielä voitu asetuksen voimassaolon aikana puuttua ja ottaa kantaa

19 Oikeuslähteiden velvoittavuudesta ks. lisää esim. Huovila 2020, kohta 2.2.
20 Sajama 2016, s. 40.
21 Saarenpää 2012, s. 410.
22 Saarenpää 2012, s. 415.
23 Saarenpää 2012, s. 416.

ratkaisevasti. Tietosuoja-asetuksessa ovat vastakkain myös informointi ja oikeudet, joten oikeusinformatiikan alaan kuuluvana tutkimuskohteena asetus on ajankohtainen.

2 HENKILÖTIETOJEN SUOJA

2.1 Mitä henkilötiedot ovat?

Tietosuojalainsäädännön näkökulmasta henkilötiedon määritelmä eurooppalaisessa tietosuojalainsäädännössä on erittäin laaja.[24] Tietosuoja-asetuksen 4 artiklan 1 kohdan mukaan kaikki tunnistettu tai tunnistettavissa olevat luonnolliseen henkilöön[25] liittyvät tiedot ovat henkilötietoja. Tällaisia tietoja ovat luonnollista henkilöä koskevat tiedot, joista tiedon kohde voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen perusteella. Tunnistetietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitiedot, verkkotunnistetiedot[26] taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella tunnistettavissa oleva tieto. Henkilötietoja ovat siten esimerkiksi terveystiedot, tiedot työpaikasta, tiedot asuinpaikasta tai jopa perheestä. Kaikki tiedot, millä ihminen voidaan tunnistaa joko suoraan tai epäsuorasti koskemaan juuri häneksi, muodostavat kyseisen henkilön henkilötiedot. Henkilötiedon määritelmä on tietosuoja-asetuksen soveltamisen kannalta tärkeä. Kaikki tiedot, mitä ei voida todentaa henkilötiedoiksi, jäävät asetuksen soveltamisalan ulkopuolelle.

Henkilötietojen käsite tulisi ymmärtää mahdollisimman laajasti. Yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä annettu yleissopimus (36/1992) määrittelee henkilötiedot lyhyesti luonnollisen henkilön *tiedoiksi, mitkä tarkoittavat mitä tahansa tietoja, jotka koskevat tunnistettua tai tunnistettavissa olevaa yksilöä* (2 artiklan a-kohta). Yksinkertaisimmillaan se voidaan tunnistaa yhtä luonnollista henkilöä koskevaksi, kuten sormenjälki tai henkilötunnus. Sormenjälki ja henkilötunnus ovat yksilökohtaisia, joten ne ovat suoraan tunnistettavissa tiettyä ihmistä koskeviksi. Määritelmän perusteella henkilötieto voi olla myös auton rekisterikilpi, internetin selailuhistoria, valokuva tai jopa kaupan bonusostohistoria. Kun arvioidaan, onko jokin tieto henkilötieto, on tarpeen selvittää henkilön tunnistettavuus tiedon perusteella.[27] Kun henkilötiedoksi käsitetään myös

[24] Ks. esim. Euroopan komissio 1990, s. 19 tai Euroopan komissio 1992, s. 10.
[25] Luonnollisella henkilöllä tarkoitetaan ihmistä.
[26] Voidaanko IP-osoitetta pitää henkilötietona vai ei, on kiistanalainen kysymys tietojen yksityisyyden suhteen. IP-osoitteen teknisistä ominaisuuksista, sekä EU:n ja Yhdysvaltojen oikeuskäytännön, EU:n tietosuojaelimen ja WP 29 työryhmän käytäntöjen valossa suhtautumisesta osoitteen henkilötieto-ominaisuuteen voit katsoa lisää esim. tandonline-com.ezproxy.ulapland.fi.
[27] Ks. lisää Vanto 2011, s. 22-26.

esimerkiksi internetin selailuhistoria, voidaan tähän kohdistaa hieman kritiikkiä. Jos selailuhistoria ei koostu erikseen mistään kirjautumista vaativista sivustoista, niin voidaanko tällöin selailuhistoriaa kuitenkaan yhdistää johonkin tiettyyn henkilöön? Määritelmä tulee ymmärtää laajasti, mutta onko kaikkien tunnistamiseen yhteydessä olevien tietojen suojeleminen tärkeää? Onko kaikki nämä tunnistamiseen yhteydessä olevat tiedot kuitenkaan tarpeen määritellä *henkilötiedoiksi*?

> Esimerkiksi auton rekisterikilpi, jolla tarkoitetaan ajoneuvojen rekisteröinnistä annetun valtioneuvoston asetuksen (893/2007) 2 §:n 1momentin 14 kohdan mukaan ajoneuvoon kiinnitettävää kilpeä, jossa on ajoneuvon rekisterinumero. Saman asetuksen 22 §:n perusteella rekisterikilvet on kiinnitettävä tiettyyn ajoneuvoon tarkoin määritellyllä tavalla ja 23 §:n perusteella sen on oltava liikenteessä vaikeudetta luettavissa. Henkilötiedon laajan määritelmän perusteella rekisterikilpi tulee ymmärtää henkilötiedoksi. Ajoneuvon omistaja on selvitettävissä rekisterikilven perusteella. Rekisterikilpeä voidaan pitää omistajan henkilötietona. Silti kilpi on määrätty pidettäväksi nähtävillä, kun ajoneuvo on liikenteessä.

Tietosuoja-asetusta edeltävää henkilötietodirektiiviä varten laadittu Euroopan tietosuojatyöryhmä WP 29:n lausunto 4/2007 auttaa edelleen henkilötiedon käsitteen pilkkomisessa.[28] Lausunto jakaa henkilötiedon käsitteen neljään toisiinsa liittyvään osatekijään. Näitä osatekijöitä ovat 1. kaikenlaiset tiedot, 2. koskeva, 3. tunnistettu tai tunnistettavissa oleva ja 4. luonnollinen henkilö. Lausunnon perusteella *kaikenlaiset tiedot* tulee ymmärtää laajasti, ja sitä arvioitaessa on huomio kiinnitettävä tiedon luonteeseen, sisältöön ja esitystapaan. Osatekijä kaksi on *koskeva* osatekijä. Tämän osatekijän perusteella tietyn tarkasteltavana olevan tiedon tulee olla tiettyä henkilöä koskeva tieto, jotta se voidaan ymmärtää henkilötiedoksi. Henkilö on myös lausunnon mukaisesti *tunnistettavissa* tuon tiedon perusteella, ja tiedon on nimenomaisesti liityttävä *luonnolliseen henkilöön*, eli ihmiseen.[29] Lähtökohtaisesti, kun tiedot kertovat jotain henkilöstä, niiden voidaan katsoa koskevan häntä.[30]

Reunaehdot henkilötiedon käsitteen määritelmälle tulevat tietosuoja-asetuksesta, eli Euroopan unionin tasolta. Määritelmä on tarkoituksellisesti säädetty laajaksi unionin tasolla. Laajan määritelmän avulla pyritään ehkäisemään henkilötietojen suojaa koskevan lainsäädännön kiertämistä.[31] Kansallisella tasolla Suomessa ei voida kyseistä asetusta

[28] Ks. lisää Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 52.
[29] WP 136, s. 6 – 7.
[30] WP 136, s. 8.
[31] WP 136, s. 4. Tästä henkilötiedon käsitteestä voit katsoa lisää Heiskanen 2019.

rikkomatta säätää omaa kansallista henkilötiedon käsitettä, joka olisi suppeampi kuin Euroopan unionin lainsäädännössä määritelty henkilötiedon käsite.[32] Suomessa tietosuoja-asetuksen myötä säädettiin myös kansallinen tietosuojalaki (1050/2018), jossa säädetään henkilötietojen käsittelystä siltä osin kuin tietosuoja-asetus mahdollistaa kansallisen liikkumavaran.

Kaikki tiedot, jotka voidaan yhdistää henkilöön, tulee ymmärtää hänen henkilötiedoikseen. Kun jokin tieto ymmärretään henkilötiedoksi, on tarpeen selvittää kohteen tunnistettavuus tiedon perusteella. Henkilötiedon määritelmässä tiedolla voidaan tarkoittaa säilytystietoja, merkkejä ja merkintöjä, jotka koskevat tunnistettavuutta. Näiden tietojen tulee olla henkilökohtaisia, jotta ne voivat ylipäänsä kuulua asetuksen soveltamisalaan. Tietoja pidetään henkilökohtaisina, jos tiedot koskevat tunnistettua tai tunnistettavissa olevaa henkilöä.[33]

Tunnistettavuus, eli mahdollisuus selvittää, kuka on kyseessä, on yksi tietosuoja-asetuksen kriteereitä henkilötiedolle. Kuitenkaan, jos tunnistamistestin myötä ei selviä, kuka on kyseessä, tieto ei läpäise testiä. Tällöin tieto ei ole henkilötieto asetuksen tarkoittamalla tavalla. Pelkkä tunnistettavuuden mahdollisuus tekee tiedosta kuitenkin henkilötiedon, jos tietoja yhdistelemällä henkilö voidaan tunnistaa.[34] Jos tunnistettavuus tiedon perusteella on raja sille, milloin kyse on henkilötiedosta ja milloin ei, on henkilötiedon käsite jossain määrin liian vaikea hahmottaa järkeväksi lainsäädännölliseksi käsitteeksi. Jos kuitenkin tutkitaan tuota mahdollisuutta, että henkilö on ylipäänsä tunnistettavissa tiedon välityksellä yhdistelemällä tietoja toisiinsa, päästään lähemmäksi lainsäädännön tarkoittamaa henkilötiedon käsitettä. Toisiinsa yhdisteltävien tietojen tulee olla henkilökohtaisia, jotta ne voivat täyttää määritelmän. Ja täyttäessään määritelmän ne tulevat asetuksen suojan piiriin.[35]

Henkilötiedoista *henkilötunnus*[36] on tarkin henkilön yksilöimiskeino. Henkilötunnus on jokaisen henkilökohtainen, ja ei ole olemassa kahta ihmistä, joilla olisi sama henkilötunnus.

[32] Ympäristöministeriö 2018 s. 36.
[33] Voigt – von dem Bussche 2017, s. 11.
[34] Voigt – von dem Bussche 2017, s. 13.
[35] Henkilötiedon käsitteen määritelmä on tärkeä henkilötietojen suojan näkökulmasta. Tämän suojan tehokkaan toteutumisen näkökulmasta on tärkeää, että lainsäädäntö pystyy tunnistamaan tilanteet, joissa ihmisiä tulee suojata heitä koskevien tietojen käsittelyssä. Suojan toteutumisen kannalta tulee pohtia jokaista tilannetta arvioitaessa sitä, mitä lainsäädännön soveltamatta jättämisestä voi seurata. Ks. lisää WP 136, s. 4.
[36] Suomessa on ollut kaksivuotinen työryhmä HETU, joka on pyrkinyt selvittämään henkilötunnuksen uudistamista, tarkoituksena esittää uusi kansallinen ratkaisu henkilöiden yksilöimiseksi. HETUsta lisää

Tunnistamisen keinona se on tarkoitettu pysyväksi, koska sitä käytetään henkilöiden yksilöintiin eri viranomaisten rekistereissä ja tietojärjestelmissä sekä näiden välisessä tietoliikenteessä. Koska se on tarkoitettu pysyväksi, sitä voidaan muuttaa vain, jos syntymäaika tai sukupuoli on ollut virheellinen tai jos henkilö vahvistetaan kuuluvaksi vastakkaiseen sukupuoleen.[37] Hyvin poikkeuksellisissa tilanteissa se voidaan muuttaa henkilön suojelemiseksi. Tällöin perusteena tulee olla henkilön terveyden tai turvallisuuden uhka tai toistuva henkilötunnuksen väärinkäyttäminen.[38] Digi- ja väestötietotietoviraston varmennepalveluista annetussa laissa (661/2009) säädetään henkilötunnuksen antamisesta (11 §) sekä sen korjaamisesta ja muuttamisesta (12 §).[39]

Koska henkilötunnus henkilötietona on sen verran arka henkilön yksilöimisen väline, on sen käsittelylle asetettu erityisiä edellytyksiä. Henkilötunnuksen avulla henkilö voidaan erottaa muista samannimisistä ja mahdollisesti samana päivänä syntyneistä ihmisistä.[40] Tietosuojalain 29 §:ssä säädetään kansallisella tasolla henkilötunnuksen käsittelystä täsmentäen asetusta kansallisen liikkumavaran puitteissa. Pykälän perusteella henkilötunnusta saa käsitellä lähtökohtaisesti rekisteröidyn suostumuksella tai, jos laki säätää käsittelystä. Pykälän perusteella, jos rekisteröidyn yksilöiminen on tärkeää laissa säädetyn tehtävän suorittamiseksi (29:1 §:n 1 kohta), rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi (29:1 §:n 2 kohta) tai jos yksilöintiä tarvitaan historiallista tai tieteellistä tutkimusta taikka tilastointia varten (29:1 §:n 3 kohta), on henkilötunnusta lain perusteella lupa käyttää. Kyseisen lain 29 §:n 4 momentti säätää vielä, että henkilötunnusta ei tule merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Tietosuojalaissa säädetyt henkilötunnuksen hyväksyttävät käyttötarkoitukset täydentävät tietosuoja-asetuksen sääntelyä. Henkilötunnus henkilötietona on arka ja yksilöivä tieto, joten

osoitteessa valtioneuvosto.fi/ -> hankkeet-> hanke henkilötunnuksen uudistamista ja valtion takaaman identiteetin hallinnoimista koskeva työryhmä (HETU-työryhmä).

37 HETU-työryhmä on antanut 6.4.2020 loppuraportin henkilötunnuksen uudistamisesta. Kyseisessä loppuraportissa esitetään sukupuolineutraalia henkilötunnusta, jonka numeroyhdistelmä muodostettaisiin satunnaisesta numeroavaruudesta. Työryhmän loppuraportti on löydettävissä osoitteesta valtioneuvo.fi -> hankkeet -> hanke henkilötunnuksen uudistamista ja valtion takaaman identiteetin hallinnoimista koskeva työryhmä (Hetu-työryhmä) ->lausuntoaika 8.4.2020-31.5.2020 ->asiakirjat -> 1. HETU-uudistuksen loppuraportti. Julkaisun pysyvä osoite on http://urn.fi/URN:ISBN:978-952-367-296-3.

38 Digi ja väestötietovirasto -> Henkilöasiakkaat -> Henkilötiedot väestötietojärjestelmässä -> Henkilötunnus -> Henkilötunnuksen muuttaminen.

39 Huomaa, että nykyisin henkilötunnusta ei saisi käyttää tunnistamisen välineenä. Sitä kuitenkin kysytään usein, kun tarvitsee päästä esimerkiksi asiakkaan tietoihin hänen asioidessaan esim. viranomaisessa.

40 Hanninen – Laine – Rantala – Rusi – Varhela 2017, s. 44.

sen väärinkäyttämiseen tulee suhtautua vakavasti. Henkilötunnuksen joutuessa väärinkäytetyksi saattaa rekisteröity joutua vaihtamaan tunnusta kokonaan.

2.2 Henkilötiedot osana itsemääräämisoikeutta

Henkilöllä on oikeus tietoon. Oikeus tietoon käsittää sekä itseään koskevan että yhteiskuntaa koskevan tiedon. Tämä oikeus on osa tiedollista itsemääräämisoikeuttamme[41], joka tulee turvata yksilön tiedon tarpeena erilaisin oikeuksin, kuten perusoikeuksin.[42] Persoonallisuus on hyvin vahva osa henkilötietojen suojaa, johon on myös liitetty tiedollinen itsemääräämisoikeus. Näiden vuoksi henkilöllä tulisi olla suuri mahdollisuus vaikuttaa siihen, kuka, miten ja missä käsittelee hänen henkilötietojaan.[43]

Itsemääräämisoikeuden puitteissa henkilö voi päättää itseään koskevista asioista, valvoa niiden toteutumista sekä saada oikeusturvaa yhteiskunnassa. Se on yksilön oikeus, joka voidaan jakaa viiteen elementtiin: oikeus sisäiseen vapauteen, oikeus ulkoiseen vapauteen, oikeus kompetenssiin, oikeus valtaan ja oikeus tietoon. Näistä oikeus sisäiseen vapauteen tarkoittaa oikeutta henkiseen loukkaamattomuuteen ja oikeus ulkoiseen vapauteen oikeutta olla fyysisesti yksin ja liikkua sekä valita asuinpaikkansa vapaasti. Tähän ulkoiseen vapauteen sisältyy myös esimerkiksi kotirauhaa koskeva säännös, jonka suhdetta henkilötietojen suojaan käsittelen myöhemmin. Myös oikeus kompetenssiin, eli kelpoisuus itse toimia omassa asiassaan, on tärkeä. Oikeudella valtaan tarkoitetaan tässä yhteydessä esimerkiksi sitä, että henkilöllä on oikeus määrätä itseään koskevasta informaatiosta. Oikeus tietoon sisältää myös läpinäkyvyyden yhteiskunnan ja yksilöiden välillä, jotta yksilön vapaudet voisivat olla turvatummat.[44] Oikeus kompetenssiin, eli kyky toimia itse omassa asiassaan, voidaan nähdä tietosuoja-asetuksen myötä esimerkiksi suostumuksen antamisessa. Suostumusta käsittelen tarkemmin kappaleessa 3.2.2. Oikeus valtaan, eli itseään koskevaan informaatioon, on myös tietosuoja-asetuksen näkökulmasta tärkeä. Tämän itsemääräämisoikeuden puitteissa henkilö voi käyttää oikeuttaan saada häntä koskevat tiedot poistetuiksi sekä käyttää muuten tarkistusoikeuttaan ja muita asetuksen

41 Tiedollinen itsemääräämisoikeus, *habeas data*. Sen kansainvälisestä kehityksestä voit katsoa lähemmin esimerkiksi Guadamuz 2000.
42 Saarenpää 2016, s. 213-214.
43 Neuvonen 2014. s. 59.
44 Saarenpää 2012, s. 228-233.

mukaisia oikeuksia. Näitä rekisteröidyn oikeuksia käsittelen tarkemmin jäljempänä kappaleessa 3.1.

Henkilötietoja tarvitaan moniin eri tarkoituksiin, kuten hyvinvointivaltiollisten palvelujen tarjoamiseen, väestön hallinnointiin sekä myös kaupallisiin tarkoituksiin ja kaupankäynnin mahdollistamiseen. Toimivan yhteiskunnan ja markkinoiden kannalta on tärkeää, että henkilö luopuu osasta yksityisyyttään. Tämän vuoksi henkilötietojen suojassa keskeistä on määritellä ne ehdot, joiden perusteella henkilötietoja saa käsitellä.[45] Vaikka yhteiskunnan ja markkinoiden toiminnan kannalta on tärkeää, että ihmiset luopuvat osasta yksityisyyttään, on tämä yksityisyydestä luopuminen tehtävä ihmistä palvellen. Henkilötietojen käsittely yhteiskunnan toimivuuden kannalta ei saa kuitenkaan olla liian vaikeaa ihmisen itsemääräämisoikeuden kannalta. Henkilötietojen käsittely on kokonaisuutena toteutettava siten, että ihmiset voivat suhteellisen vaivattomasti pitää huolta omista tiedoistaan ja päättää, missä määrin luopuvat yksityisyydestään.

2.3 Henkilötietojen suoja perusoikeutena

Henkilötietojen suoja on perusoikeus[46], josta säädetään Euroopan unionin (EU) tasolla Euroopan unionin perusoikeuskirjan (perusoikeuskirja, 2012/C 322/02) 8 artiklan 1 kohdassa ja Euroopan toiminnasta tehdyn sopimuksen (SEUT, 2016/C 202/01) 16 artiklan 1 kohdassa.[47] Näiden molempien kohtien mukaan henkilötietojen suoja on jokaisen oikeus, ja henkilötietoja on käsiteltävä asianmukaisesti ja tiettyä tarkoitusta varten. Tämän perusoikeuden toteutumista varten on säädetty tietosuoja-asetus, jonka tavoitteena on tukea vapauden, turvallisuuden oikeuden alueen ja talousunionin kehittämistä, taloudellista ja sosiaalista edistystä, talouksien lujittamista ja lähentämistä sisämarkkinoilla sekä luonnollisten henkilöiden hyvinvointia.[48] Henkilötietojen suojan suhteen perusoikeusluonne ilmenee siten, että tämä suoja voi toteutua vertikaalisesti. Yksilö saa tällöin suojaa valtion

[45] Neuvonen 2014. s. 60.
[46] Perusoikeudet kuuluvat jokaiselle Suomen oikeudenkäyttöpiirissä olevalle ihmiselle. Tällä perusperiaatteella on läheinen liityntä perustuslain syrjintäkieltoon (PL 6.2 §), jonka perusteella ketään ei saa ilman hyväksyttävää perustetta asettaa eri asemaan esimerkiksi alkuperän perusteella, ks. lisää esim. Ojanen 2009, s. 21 – 22.
[47] Ks. myös SEUT 16(2) artikla, jossa Euroopan parlamentille ja neuvostolle asetetaan velvollisuus antaa tarkempaa sääntelyä henkilötietojen käsittelystä unionin toimintaelimissä ja jäsenvaltioissa silloin, kun heidän toimintansa kuuluu unionin oikeuden soveltamisalaan.
[48] TSA, johdanto-osa kohta (2).

puuttumiselta yksityisyyteen. Jo aiemmin voimassa ollut henkilötietodirektiivi[49] asetti vaatimuksia myös horisontaalisuhteissa, kun yksityiselle rekisterinpitäjälle asetettiin velvollisuuksia, jotka koskivat yksityisten henkilöiden henkilötietojen suojaa.[50] Sama pätee nyt voimassa olevaan tietosuoja-asetukseen, kun rekisterinpitäjä voi olla sekä yksityinen että julkinen.

Kritiikkiä voidaan kuitenkin esittää sille, saako yksilö enää suojaa suhteessa valtion puuttumiseen tietosuoja-asetuksen myötä. Tietosuoja-asetuksen voimaantulon myötä voidaan ajatella myös niin, että valtio otti enemmän ohjat omiin käsiinsä, kun EU:n tasolta säädettiin, miten henkilötietojen käyttöä tulee kontrolloida. Samalla asetus mahdollisti valtioille keinot valvoa asetuksen toteutumista ja sitä, kuinka yksilöiden tietoja kerätään, tallennetaan ja käytetään. Vertikaalisuhde vahvistui, mutta samalla se toisesta näkökulmasta heikentyi. Valtiolla on asetuksen voimaantulon myötä suuremmat intressit pitää huolta ihmisten yksityisyydestä, mutta myös paremmat keinot vahtia tätä yksityisyyttä. Ja keinot, joilla sitä vahditaan, myös osaltaan puuttuvat tai kontrolloivat kansalaistensa yksityisyyttä.

Koska henkilötietojen suoja on perusoikeus, tulee se ottaa huomioon kaikissa periaatteissa ja säännöissä, jotka koskevat henkilöiden suojelua henkilötietojen käsittelyssä. Euroopan ihmisoikeussopimuksen (EIS, 63/1999) 8 artiklan perusteella henkilötietojen suoja on myös osa yksityiselämän suojaa.[51] Kaikki henkilötiedot eivät välttämättä kuulu yksityiselämän suojan alaan, vaikka ne olisivat henkilötietoja. Henkilötiedot kuuluvat yksityiselämän piiriin silloin, kun henkilötiedot voidaan yhdistää jotain tiettyä henkilöä koskeviksi. Henkilötietoja käsiteltäessä tulee ottaa huomioon myös muut perusoikeudet, jotka yhdessä muodostavat henkilön yksityisyyden suojan.

Tietosuoja-asetuksen johdanto-osan perusteella henkilötietojen käsittely on suunniteltava siten, että se palvelee ihmistä. Perusoikeutena henkilötietojen suoja ei ole absoluuttinen, vaan sitä on tarkasteltava suhteessa muihin perusoikeuksiin suhteellisuusperiaate huomioiden sekä tarkasteltava sen tehtävää yhteiskunnassa. Saman kohdan perusteella tulee huomioida myös muut henkilöiden perusoikeudet, joita henkilötietojen käsittelyyn

[49] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
[50] Neuvonen 2014, s. 60. Tämä vertikaalisuhteessa toteutuva suoja vallitsee esimerkiksi Yhdysvalloissa ja on ollut myös Saksassa.
[51] Kansallisella tasolla yksityiselämän suojasta säädetään perustuslain (731/1999) 10 §:ssä.

kohdistuu.[52] Henkilötietojen suoja pätee myös kuolleisiin tietyn määrittelemättömän ajan[53], vaikka tietosuoja-asetuksen perusteella asetus ei käsittele kuolleiden henkilötietojen suojaa.

Henkilötietojen suoja omana perusoikeutena on suhteellisen uusi tunnustettu perusoikeus. Muuttuva yhteiskunta ja maailman digitalisoituminen ovat edesauttaneet tämän perusoikeuden omaa sääntelytarvetta. Henkilötietojen suojajärjestelmä rakentuu kolmen eri säännöstön varaan. Nämä suojajärjestelmän säännökset kattavat henkilötietojen käsittelyn edellytykset ja siinä toteutettavat menettelytavat, rekisteröidyn oikeuksia sääntelevät sekä tietosuojan valvontajärjestelmiin perustuvat tavat. Jo Euroopan perusoikeuskirjassa henkilötietojen suoja on jaettu viiteen eri tekijään: henkilötietojen käsittelyn asianmukaisuuteen, käsittelyn perustuminen suostumukseen tai lakiin, käyttötarkoituksen määrittelyvelvoitteeseen, rekisteröidyn tarkastusoikeuteen ja oikeuteen virheen oikaisuun sekä riippumattoman valvontaviranomaisen perustamiseen.[54]

Koska henkilötietojen suojasta perusoikeutena on säädetty EU:n tasolla, se on saavuttanut perusoikeusluonteen. Perusoikeusluonne vahvistaa henkilötietoja koskevan lain tulkintaa. Tämä taas johtaa siihen, että jo lainsäätämisvaiheessa kansallisen lainsäädännön tulee olla sopusoinnussa ihmis- ja perusoikeuksien kanssa. Jos kyse ei ole tällöin perusoikeuskollisiosta lainsäätämistilanteessa, niin perusoikeuskirjassa vahvistetut periaatteet vaikuttavat kaikkeen henkilötietojen käsittelyyn. Sama vaikutus on myös lainsoveltamistilanteessa. Tällöin perusoikeusjärjestelmän yhtenäisyyden kannalta on olennaista, että konkurrenssitilanteissa annetaan painoarvoa henkilötietojen suojan erityispiirteille osana yksityisyyden suojaa. [55]

Henkilötietojen suoja on tunnustettu perusoikeudeksi, mutta silti siitä ei samaan tapaan keskustella ääneen kuin esimerkiksi tasa-arvosta tai yhdenvertaisuudesta. Henkilötietojen toistuvat tietovuodot ikään kuin ohitetaan vain yhdellä uutisoinnilla, ja mahdollisille vuodosta kärsineille henkilöille ei välttämättä edes informoida siinä laajuudessa, kuin olisi tarpeen. Uutiset eivät myöskään kerro, että tapahtuneet tietovuodot loukkaavat henkilöiden perusoikeuksia sanomattakaan siitä, että kyseisistä tietovuodoista sen kummemmin informoitaisiin rekisteröityjä. Henkilötietojen suoja on jo EU:n tasolla määritelty

[52] TSA, johdanto-osa kohta (4).
[53] Tietosuojalautakunta 2/2008.
[54] Nieminen 2001, s. 373 – 374.
[55] Neuvonen 2014, s. 61.

perusoikeus, jonka turvaamiseen tietosuoja-asetuksella pyritään. Kuitenkaan tämä perusoikeus ei saa riittävästi huomiota tavallisten kansalaisten, rekisteröityjen, keskuudessa. Tähän on myös osaltaan medialla vaikutusta. Toisaalta taas henkilötietojen käyttämiseen liittyvä uutisointi on selvästi lisääntynyt, kun tietosuoja-asetus on astunut voimaan ja digitalisoitumisesta on tullut osa arkipäivää. Ja, koska uutisointi on myös lisääntynyt, on sen pakko ollut myös nostattaa kansalaisten keskuudessa mielenkiintoa henkilötietojen käsittelyä kohtaan. Kyseinen perusoikeus tulee ottaa huomioon kaikessa, missä säädetään henkilötiedoista tai niiden suojasta, mutta on kyseenalaista, huomioidaanko sitä tarpeeksi kuitenkaan. Ja jos kyseinen perusoikeus huomioidaan, tehdäänkö se tarpeeksi laajasti, kuten perusoikeudet tulisi huomioida.

Yksityis- ja perhe-elämän kunnioittamisesta[56] säädetään Suomen perustuslain 10 §:ssä. Perustuslain 10 §:n 1 momentti sisältää henkilötietojen suojaa koskevan sääntelyvarauksen. Perusoikeusuudistuksen esitöissä tätä sääntelyvarausta on luonnehdittu toteamalla, että säännös viittaa tarpeeseen lainsäädännöllisesti turvata yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä.[57] Käsitteenä yksityiselämä voidaan ymmärtää perusoikeusuudistuksen esitöiden mukaan henkilön yksityistä piiriä koskevaksi yleiskäsitteeksi.[58] Koska se on ymmärrettävissä yleiskäsitteeksi, se sisältää monesti myös henkilökohtaisen koskemattomuuden, kunnian ja kotirauhan suojan. Tämän takia yksityiselämän suojasäännös yleissäännöksenä usein täyttää muiden henkilön yksityistä piiriä turvaavien perusoikeuksien jättämää suoja-aukkoa.[59]

Koska henkilötietojen suoja sisältyy yksityiselämän suojan piiriin, on lainsäätäjän turvattava henkilötietojen suoja tavalla, jota voidaan koko perusoikeusjärjestelmän kokonaisuus huomioon ottaen pitää hyväksyttävänä. Sekä yksityiselämän että henkilötietojen suojan kannalta lähtökohtana perustuslain 10 §:n 1 momentissa on, että säännöksen soveltamisala ei koske oikeushenkilöitä.[60] Tietosuoja-asetuksessa puolestaan säädetään siitä, miten yksityiset henkilöt, yritykset ja organisaatiot käsittelevät henkilötietoja Euroopan unionissa.

[56] Yksityis- ja perhe-elämän kunnioittamisen suoja on kehittynyt hallitusmuodon muuttuessa. Sääntelytarve on muotoutunut sähköisten viestintämuotojen nopean kehityksen myötä ja kyseinen suoja on saanut nykyaikaisia muotojaan, laajentumalla uusiin medioihin ja teknisiin valvontamenetelmiin. Ks. tästä lisää esimerkiksi Saraviita 2011, s. 178-179.
[57] HE 309/1993 vp, s. 52-53.
[58] HE 309/1993vp, s. 53.
[59] Viljanen 2011, s.329 -391.
[60] Lainkirjoittajan opas -> Kansallisten säädösten valmistelua koskevat ohjeet -> 4 Perusoikeudet.

Tietosuoja-asetusta ei sovelleta vainajien tai oikeushenkilöiden henkilötietojen käsittelyyn.[61] Asetus ei koske asetuksen 2 artiklan 1 kohdan c-alakohdan perusteella myöskään yksityishenkilöiden välillä tapahtuvia toimia, joissa henkilötietoja käytetään yksinomaan henkilökohtaisessa tai kotitaloutta koskevassa toiminnassa.

Henkilötietojen suojasta tulee säätää lailla. Suojan toteutumisen kannalta perustuslakivaliokunta on vakiintuneesti pitänyt tärkeinä suojelukohteina ainakin rekisteröinnin tavoitetta, rekisteröitävien henkilötietojen sisältöä, niiden sallittuja käyttötarkoituksia mukaan luettuna tietojen luovutettavuus sekä tietojen säilytysaikaa henkilörekisterissä ja rekisteröidyn oikeusturvaa.[62] Sinänsä perustuslakivaliokunnan suojelukohteista puuttuu yksilön itsemääräämisoikeus, jonka puitteissa henkilö voi valvoa henkilötietojensa käyttöä ja vaikuttaa niiden käytettävyyteen.

Perusoikeuskirjassa on erilliset artiklat yksityis- ja perhe-elämän kunnioittamiseen (7 artikla) sekä henkilötietojen suojaan (8 artikla). Näiden artiklojen suhde on kiinteä, koska niiden kummankin soveltaminen voi olla tarpeen samassa tilanteessa. [63] EIS 8(1) artikla on suhteellisen saman sisältöinen kuin perusoikeusoikeuskirjan 7 artikla. Näiden molempien artikloiden perusteella yksityiselämä tulee ymmärtää laajassa merkityksessä, unohtamatta ammattitoimintaa yksityiselämän käsitteen ulkopuolelle.

Ihmis[64]- ja perusoikeutena henkilötietojen suojan kytkeytyessä osaksi yksityisyyden suojaa, tämä suoja rakentuu kahdelle osa-alueelle, henkilötietojen suojalle ja tietoturvalle. Henkilötietojen suojalla määritellään henkilötiedot ja niiden käsittelyn edellytykset, ja tietoturvalla puolestaan asetetaan näiden tietojen käsittelylle konkreettinen viitekehys. Suojan ulottuvuuksia tulkittaessa tulee tukea hakea aineellisesta lainsäädännöstä, kuten tietosuoja-asetuksesta ja tietosuojalaista.[65]

Yksityisyyden suoja ihmis- ja perusoikeutena on laaja-alainen, jos tarkastellaan oikeuslähdeopillista näkökulmaa. Oikeuslähdeopin[66] näkökulmasta katsottuna voidaan

[61] TSA, artiklat 1,2; johdanto-osan kappaleet 1, 2, 14, 18, 27.
[62] Ks. esim. PeVL 25/2010 vp, s. 2/11, PeVL 27/2006 vp, s. 2/1 ja PeVL 14/2002, s. 2.
[63] C – 293/12ja C – 594/12 Digital Rights Ireland 2014, kohta 29.
[64] Ihmisoikeuksien tarkastelu pohjautuu ihmisarvon käsitteelle. Ihmisarvon käsitteestä ja sen kriittisestä tarkastelusta ks. Niemi 2019, s. 129 – 145.
[65] Neuvonen 2014, s. 60 – 61.
[66] Oikeuslähdeopin kautta esim. tuomioita on helpompi perustella, kun otetaan vahvojen oikeuslähteiden tueksi sallittuja ja heikkoja oikeuslähteitä. Oikeuslähdeopista ks. lisää esim. Aarnio 1989. Perusoikeuksista ja oikeuslähdeopista ks. esim. Karhu 2003, s. 789 – 807. Myös Huovila 2020 kirjoittaa oikeuslähteistä.

yläkäsitteenä puhua joko yksityiselämän suojasta tai yksityisyyden suojasta. Rauno Korhosen näkemyksen mukaan yksityisyys on yläkäsite, joka voidaan ryhmitellä neljään eri ulottuvuuteen: 1. informaatioyksityisyys, 2. fyysinen yksityisyys, 3. viestintäyksityisyys sekä 4. alueellinen yksityisyys. Nämä ulottuvuudet eivät ole toisensa poissulkevia tai tyhjentäviä, mutta ne antavat kuvan käsitteen moniulotteisuudesta.[67] Tarkasteltaessa yksityisyyden suojaa ja henkilötietojen käsittelyä tulee aina huomioida myös julkisuusperiaate, varsinkin, jos rekisterinpitäjänä on valtio.

Viranomaisen toimiessa tietosuojalainsäädännön puitteissa rekisterinpitäjänä, ei tule unohtaa perustuslain 21 §:ssä säädettyä oikeusturvaa. Kyseinen pykälä sisältää hyvän hallinnon takeet ja lisäksi 22 §:ssä säädetään, että viranomaisen on turvattava perus- ja ihmisoikeuksien toteutuminen. Hyvän hallinnon periaatteista säädetään tarkemmin hallintolaissa (434/2003) ja perustuslain 124 §:n mukaisesti sen vaatimuksia tulee noudattaa julkisten hallintotehtävien hoitamisessa. Perustuslain 21 § ja 22 § koskevat nimenomaisesti vain viranomaisia. Viranomaisen on turvattava perusoikeuksien toteutuminen, eli henkilötietojen suoja tässä tapauksessa, mutta vastaavasti viranomaiselle ei aseteta kuitenkaan velvoitteita tämän suojan rikkoutumisesta.

Henkilötietojen suojasta perusoikeutena säädetään useissa kansainvälisissä sopimuksissa. Lisäksi myös Suomen kansallinen lainsäädäntö pyrkii ottamaan huomioon henkilötietojen suojan, kun sille on sisällytetty sääntelyvaraus yksityis- ja perhe-elämän suojaa koskevassa pykälässä (PL 10.1 §). Muuten sen suhde muihin perusoikeuksiin on tasavertainen, vaikka se on suhteellisen uusi tunnustettu perusoikeus. Tässä kohden ei ole tarpeen eritellä sen tarkemmin henkilötietojen suojan suhdetta kaikkiin perusoikeuksiin.

2.4 Henkilötietojen väärinkäytöksistä

2.4.1 Väärinkäytöksistä aiheutuvat seuraukset

Tietosuoja-asetuksen tavoitteena oli luoda suojausjärjestelmä, joka huomioi yhä enemmän kansalaisten henkilötietojen suojaa ja varmistaa suojausjärjestelmän toimimisen muuttuvassa yhteiskunnassa jättäen kuitenkin tarpeeksi liikkumavaraa markkinoiden

[67] Korhonen 2005, s. 22.

näkökulmasta. Liikkumavaran jättämisellä tavoitellaan sitä, että merkittävät tietopohjaiset innovaatiot voivat tapahtua Euroopan maaperällä. Lähtökohtaisesti Brysselin lainsäätäjät eivät olettaneet kaikilta tietosuojaviranomaisilta täysin tehokasta tietoturvan toteuttamista. Heidän pyrkimyksensä oli, että vuosi vuodelta tuo kuilu eri jäsenmaiden välillä kuroutuisi ja tietosuojasta tulisi yhtenäisempää.[68] Tietosuoja-asetuksen myötä tuo kuilu on ainakin yhtenäistynyt, kun asetus koskee sellaisenaan kaikkia EU:n jäsenmaita ja jäsenmaiden alueella toimivia rekisterinpitäjiä. Liikkumavaran jättämiseen voidaan myös kohdistaa kritiikkiä, jos mietitään pieniä rekisterinpitäjiä, joita koskee myös samalla tavalla asetuksen asettamat tavoitteet kuin suurempia rekisterinpitäjiä. Rekisterinpitäjän asemalla ei ole merkitystä sen suhteen, mitä asetuksen velvoitteet ovat. Asetus ei kohdista varsinaisesti eroavaisuuksia toimenpiteisiin, joita rekisterinpitäjille asetetaan.[69]

Rikoslain (RL, 368/2015) 38 luvussa säädetään tieto- ja viestintärikoksista. Henkilötietojen[70], etenkin henkilötunnuksen, väärinkäyttö voi johtaa rikoslain 38 luvun 9 a §:n mukaiseen identiteettivarkauteen[71]. Tällöin rikokseen syyllistyy henkilö, joka erehdyttääkseen kolmatta osapuolta käyttää oikeudettomasti toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jonka tietoja käytetään oikeudettomasti. Tämä rikos on kriminalisoitu Suomessa vuonna 2015. Jo seuraavana vuonna, 2016, poliisin tietoon tuli yli 2000 identiteettivarkaustapausta.

Kyberrikollisuuden muotoja, jotka kohdistuvat osaltaan henkilötietojen käyttämiseen, ovat myös petos (RL 36 luku), vainoaminen ja laiton uhkaus (RL 25:7 a ja RL 25:7) sekä mahdollisesti yksityisyyden, rauhan ja kunnian loukkaaminen (RL 24 luku). Tietoturvaloukkaukset voivat johtaa rekisteröidyn kannalta myös muihin ongelmiin.

68 Smouter 2018.

69 Tietosuoja-asetuksen lähestymistapa on riskiperusteinen. Tämän lähestymistavan tarkoituksena on ohjata rekisterinpitäjiä kokonaisvaltaiseen tietosuojariskien huomiointiin ja tukea osoitusvelvollisuuden toteuttamista. Lähestymistapa ei erottele rekisterinpitäjiä pieniin ja suuriin yrityksiin, vaan se asettaa rekisterinpitäjälle toteuttamisvastuun lähestymistavan suhteen.

70 Henkilötietojen suoja on osa yksityisyyden suojaa, joka on osa yksityisyyttä. Yksityisyyden loukkaamista voidaan lähestyä ainakin neljässä eri suhteessa: 1. yksityisyyttä ei haluta määritellä diskrinktiivisesti, 2. equilibrium on tapana ohittaa, 3. huomio kohdistetaan loukkauksen kohteen sijaan siihen, miten yksityisyyttä voidaan teknisesti ottaen loukata, ja 4. koskemattomuus. Tätä koskemattomuutta, luokse pääsyä, lähestytään aktiivisten tekojen kautta. Tästä yksityisyyden loukkaamisesta katso lisää esim. Mahkonen Sami1997, s. 82 eteenpäin.

71 Identiteettivarkaudessa identiteettiä ei varsinaisesti varasteta, vaan se säilyy tosiasiallisen omistajan hallussa jonkun toisen käyttäessä sitä samaan aikaan oikeudettomasti hyväkseen. Ks. lisää Soininen 2017.

Seurauksena voi olla esimerkiksi henkilötietojen leviäminen, taloudellinen vahinko ja salassapitovelvollisuuden suojaamien tietojen paljastuminen. Näitä vaikutuksia tietosuojavaltuutettu on arvioinut rekisteröidylle todennäköisiksi asiassa, jossa Kelan toimistoon jättämiä asiakirjoja sisältänyt postipaketti katosi matkalla vakuutuspiirin skannauskeskukseen.[72] Henkilötietojen rikkomukset voivat johtaa myös rekisteröityjen kannalta vakaviin vaikutuksiin kohdistuessaan yksityiselämään. Näistä esimerkkeinä voidaan mainita nöyryyttäminen, taloudelliset menetykset, fyysiset ja psykologiset vahingot sekä jopa hengenuhka.[73] Lisäksi median epäkohtelias uutisointi voi pilata maineen tai olla raskasta henkisesti.

2.4.2 Kyberturvallisuus ja henkilötiedot

Kyberturvallisuus[74] on keino tarkastella tietoliikenne- ja viestintäjärjestelmien toimivuutta ja toiminnan turvaamista yhteiskunnallisella tasolla. Suomen kyberturvallisuusstrategiassa se määriteltiin ”tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.”[75] Samaan aikaan Suomen kansallisen strategian kanssa valmisteltiin EU:n tasolla kyberturvallisuusstrategiaa, joka julkaistiin helmikuussa 2013. Tässä strategiassa on nostettu viisi korkean tason päätavoitetta: kyberkestävyyden saavuttaminen, kyberrikollisuuden vähentäminen, kyberpuolustusvalmiuksien kehittäminen, kyberturvallisuusteollisuuden ja teknologian kehittyminen sekä tietoturvan huolehtiminen osaksi EU:n päätöksentekoa.[76]

Jakamistalouden[77] näkökulmasta tietovuodot aiheuttavat suuria riskejä kyberturvallisuudelle. Jaettaessa tietoja yhdellä sivustolla ottaa tämä sivusto yhteyttä johonkin toiseen sivustoon ja jakaa nämä tiedot sinne käytettäviksi. Kun henkilö käy tällaisella sivustolla, jossa kerätään tietoja, muodostuu tästä aina myös seurantakoodi.[78] Verkkoinfrastruktuurissa on kyettävä havaitsemaan ja reagoimaan tietoturvallisuuteen

[72] EU:n yleisen tietosuoja-asetuksen mukainen päätös 2691/171/19.
[73] Enisa.europa.eu. Enisa on Euroopan unionin cyberturvallisuusvirasto.
[74] Kybertoimintaympäristön määritelmästä, jossa ihminen on osana, katso esim. The White House 2008. Comprehensive National Cybersecurity Initiative, myös kyberturvallisuuden määritelmästä täydennyksineen ks. Kyberturvallisuuden sanasto 2018, s. 22.
[75] Puolustusministeriö 2013, s. 3. katso myös Paavola 2014, s. 10 kybertoimintaympäristön määritelmästä.
[76] Paavola 2014, s. 8-12.
[77] Jakamistalouden määritelmästä katso esim. vtt.fi. tai vastaavasti Päläs – Määttä 2019, s. 4-11.
[78] Laakso 2014, s. 30.

liittyviin tapahtumiin. Tämän varmistamiseksi tietoturvallisuusonnettomuuksien reagointiryhmällä, CSIRT[79], tulisi olla riittävästi tarpeellista tietoa tietoturvatapahtumista ja tietoturvaan kohdistuvista uhkista. Tämän varmistamiseksi CSIRT jakaa eri jakamisalustoilla tietoja tietoturvahälytyksistä ja -tapahtumista. CSIRT-ryhmän käyttö näillä alustoilla voi johtaa henkilötietojen lisäkäsittelyyn, jolloin kysymykseen tulee tietosuoja-asetuksen soveltaminen heidän osaltaan. CSIRT-ryhmän ensisijainen tarkoitus on suojella eri sivustojen käyttäjien yksityisyyttä.

Digitaalinen turvallisuus kattaa riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen, kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Digitaalisella turvallisuudella tavoitellaan kansalaisten suojaa suhteessa yhteisöihin ja yhteiskuntaan niiltä riskeiltä ja uhilta, jotka voivat kohdistua etenkin henkilötietoihin.[80] Tietovuodot on lueteltu keskeisiin tietoturvauhkiin, joita kyberturvallisuuteen liittyy.[81]

Kyberturvallisuuden ja jakamistalouden yhteydessä puhutaan yksilön vastuuttamisesta. Media uutisoi siitä, miten yksilöiden toimintaa verkkopalveluissa seurataan, mutta jättää aina vastuun suojautumisesta yksilöille. Median perusteella ihmisiä kehotetaan vähentämään digitaalista jalanjälkeä, mutta ei tuoda esille sitä, miten paljon verkkopalvelut keräävät käyttäjän toiminnasta automaattisesti tietoja ja siirtävät ne hyödynnettäviksi ulkomailla, esimerkiksi ulkomaisissa pörssiyhtiöissä. Näistä tietojen keräämisistä ei ole haittaa, jos käyttäjä voi etukäteen selvittää hänestä kerättävien tietojen laadun ja käyttötarkoituksen.[82] Tietosuoja-asetuksella on pyritty juuri siihen, että käyttäjällä olisi yhä enemmän oikeuksia valvoa omien tietojensa käyttöä. Myös rekisterinpitäjälle on asetettu enemmän velvollisuuksia toimia rekisteröidyn oikeuksien takaamiseksi.

Tietosuoja-asetuksen myötä kyberturvallisuuden toteuttaminen on kasvanut siinä mielessä, että yksilön vastuuttamisesta on päästy kohti sitä, että rekisterinpitäjällä on enemmän vastuuta toiminnastaan. Asetuksen voimaantulon myötä, on yksi kyberturvallisuuden viidestä päätavoitteesta toteutunut: tietosuoja on osa EU:n päätöksentekoa. Yksilöllä on asetuksen voimaan tultua konkreettisia oikeuksia henkilötietojensa keräämisen ja

[79] Computer security incident response team. Ks. lisää osoitteesta enisa.europa.eu.
[80] Valtiovarainministeriö -> Ajankohtaista -> Artikkeli -> Julkisen hallinnon digitaalista turvallisuutta kehitetään.
[81] Enisa.europa.eu 2020.
[82] Laakso 2014, s.28-29.

käyttämisen suhteen. Jossain määrin kyberturvallisuus on kasvanut ainakin yksilön näkökulmasta.

3 OIKEUDET JA VASTUUT TIETOSUOJA-ASETUKSESSA

3.1 Rekisteröidyn oikeudet

3.1.1 Tietosuoja-asetuksen mukainen rekisteröity

Tietosuoja-asetusta sovelletaan asetuksen 2 artiklan 1 kohdan mukaan henkilötietojen käsittelyyn, kun tällainen käsittely on osittain tai kokonaan automaattista, sekä ei-automaattiseen henkilötietojen käsittelyyn silloin, kun tiedot muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa. Saman artiklan 2 kohdan perusteella asetus ei tule sovellettavaksi esimerkiksi henkilötietojen käsittelyyn, kun käsittelyä suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan tai jota suorittavat jäsenvaltiot toteuttaessaan SEU[83] V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa tai jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa.

Asetuksessa rekisteröity on määritelty henkilötiedon määritelmän kanssa samassa kohdassa. Asetuksen 4 artiklan 1 kohdan perusteella rekisteröity on luonnollinen henkilö, johon liittyviä henkilötietoja rekisterissä pidetään yllä. Rekisterillä tarkoitetaan asetuksen 4 artiklan 6 kohdan perusteella mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Tietojoukko voi olla keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Rekisterin määritelmästä voidaan rekisteröidyn määritelmä johtaa siten, että *rekisteröity on luonnollinen henkilö, jonka tietoja rekisterissä esiintyy. Näitä henkilötietoja käytetään asetuksen soveltamisalan piiriin kuuluvissa rekistereissä.*

3.1.2 Informointivelvollisuus lähtökohtana

Rekisterinpitäjällä on velvollisuus informoida rekisteröityä avoimesti henkilötietojen käsittelystä jo ennen varsinaisten käsittelytoimien aloittamista.[84] Informointivelvollisuus oli määritelty jo aiemmin voimassa olevassa henkilötietolaissa rekisterinpitäjän yhdeksi tärkeimmäksi velvollisuudeksi. Sen tarkoituksena on varmistaa, että rekisteröidyllä on

[83] Euroopan unionista tehty sopimus, SEU.
[84] Hanninen – Laine – Rantala – Rusi – Varhela 2017, s. 73.

mahdollisuus saada tieto häntä itseään koskevien henkilötietojen käsittelystä jo niiden keräämisvaiheessa. Rekisterinpitäjän informointivelvollisuudella pyritään siihen, että rekisteröidyllä on mahdollisuus käyttää omia oikeuksiaan kattavammin aiempaan lainsäädäntöön verrattuna. Informointivelvollisuudella tarkoitetaan sitä, että rekisterinpitäjän tulee antaa vähimmäistiedot rekisteröidylle. Tietoja, jotka rekisteröidylle tulee antaa, ovat tiedot rekisterinpitäjästä ja sen edustajasta, henkilötietojen käsittelyn tarkoituksesta ja siitä, mihin tietoja säännönmukaisesti luovutetaan sekä miten henkilö voi käyttää etenkin tarkastus-, virheenkorjaus- ja kielto-oikeuttaan.[85] Tietojenkäsittely tulisi olla asetuksen perusteella läpinäkyvää. Tämä tarkoittaa, että tietojen pitäisi olla helposti saatavilla, ne olisi toimitettava tiiviisti esitetyssä ja helposti ymmärrettävässä muodossa. Tietojen ilmaisun pitäisi olla selkeää ja yksinkertaista kielellisesti.[86]

Tietosuojatyöryhmä WP 29[87] on todennut ennen tietosuoja-asetuksen voimaantuloa, että informointivelvollisuuden toteuttaminen asetuksen mukaisesti on rekisterinpitäjän oman harkinnan varassa. Rekisterinpitäjän on kuitenkin tarvittaessa pystyttävä osoittamaan osoitusvelvollisuusperiaatteen mukaisesti, miksi valittu tapa toteuttaa tietosuoja-asetuksen mukaista informointivelvollisuutta. Informointivelvollisuudella toteutetaan myös läpinäkyvää tietosuojaa, joka on asetuksen yksi tärkeimmistä tavoitteista.[88]

Informointivelvollisuudessa yhdistyvät sekä rekisterinpitäjän oikeus päättää, kuinka sitä toteuttaa, että velvollisuus pystyä osoittamaan, miten sitä on toteutettu. Sillä pyritään takaamaan rekisteröidyn mahdollisuus toteuttaa oikeuksiaan, kun rekisteröityä on tiedotettu henkilötietojen käsittelystä. Rekisteröidyn oikeuksien toteuttamisen kannalta se on hyvin keskeinen periaate, jolla myös pyritään luomaan koko tietosuoja-asetuksen mukaista tarkoitusta: henkilötietojen suojan toteutumista yksilö huomioiden.

Tietosuoja-asetuksen 30 artiklassa säädetään käsittelytoimia koskevasta selosteesta. Artiklan perusteella informointivelvollisuuteen sisältyvät tiedot on määriteltävä käsittelytoimia koskevassa selosteessa. Seloste laaditaan valvontaviranomaista varten, ja se on osa rekisterinpitäjän dokumentointivelvollisuutta. Koska artiklan mukaisesti

[85] Pitkänen – Tiilikka – Warma 2013, s. 196.
[86] Hanninen – Laine – Rantala – Rusi – Varhela 2017, s. 73.
[87] Riippumaton EU:n työryhmä, joka käsitteli yksilöiden suojelua henkilötietojen käsittelyssä koskevia kysymyksiä 25. toukokuuta 2018 asti. TSA 29 artiklan mukainen työryhmä.
[88] Tietosuojauutiset.fi, läpinäkyvyyden periaatteen toteuttaminen käytännössä WP 29:n hiljattain päivitetyn ohjausasiakirjan valossa, 2018.

informointivelvollisuuden on oltava osa kyseistä selostetta, on informointivelvollisuus tällöin osa dokumentointivelvollisuutta. Informaation tulee olla saatavissa joko kirjallisessa tai sähköisessä muodossa.[89]

> *Informointivelvollisuudesta voidaan kuitenkin poiketa, jos tietojen siirrosta on esimerkiksi säädetty laissa.* ***EUT:n Bara-ratkaisussa (C-201/14)*** *oli kysymys siitä, voitiinko verotustietoja siirtää ja millä edellytyksillä Verohallinnolta vakuutuskassalle. Euroopan unioni tuomioistuin totesi, että viranomaisella on velvollisuus ilmoittaa rekisteröidylle henkilötietojen siirtämisestä toiselle viranomaiselle, koska henkilötietojen asianmukaisen käsittelyn vaatimus velvoittaa viranomaista ilmoittamisesta. Tapauksessa tietojen siirtämisestä ei ollut säädetty laissa, vaan Verohallinnon ja vakuutuskassan välillä tehdyllä pöytäkirjalla, jota ei ollut julkaistu julkisesti. Tämän perusteella rekisteröityä olisi tullut informoida.*

Informointivelvoitteen on koettu lisäävän rekisteröidyn mahdollisuuksia vaikuttaa henkilötietojensa käsittelyyn. Siitä huolimatta rekisteröidyn informointivelvollisuus on koettu haasteellisena.

3.1.3 Rekisteröidyn oikeudet tietosuoja-asetuksessa

Rekisteröidyn oikeudet tulee ottaa huomioon suunniteltaessa henkilötietojen käsittelyä. Tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet ovat osaltaan samat kuin henkilötietolaissa, mutta niitä on asetuksessa myös säännelty yksityiskohtaisemmin aiempaan verrattuna. Lisäksi on säädetty uusia oikeuksia. Henkilötietojen käsittelyn oikeusperuste vaikuttaa siihen, mitä oikeuksia rekisteröidyllä on.[90]

Tietosuoja-asetuksen 3 luku säätää näistä rekisteröidyn oikeuksista ja oikeuksien toteuttamistavoista. Tietosuoja-asetuksen 12 – 14 artiklojen mukaan rekisteröidyn oikeuksiin kuuluu oikeus saada tieto henkilötietojen käsittelystä helposti ymmärrettävässä ja saatavilla olevassa muodossa. Asetuksen 15 artiklan mukaisesti rekisteröidyllä on oikeus saada vahvistus rekisterinpitäjältä siitä, käsitelläänkö häntä koskevia henkilötietoja, ja jos käsitellään, oikeus saada pääsy hänestä kerättyihin henkilötietoihin. Virheelliseksi havaitsemansa tiedot rekisteröidyllä on oikeus saada oikaistuksi (TSA 16 artikla) tai vastaavasti oikeus tietyin edellytyksin saada tiedot poistetuiksi (TSA 17 artikla). Rekisteröidyllä on oikeus rajoittaa tietojen käsittelyä tietosuoja-asetuksen 18 artiklan mukaisesti sekä siirtää tiedot järjestelmästä toiseen (TSA 20 artikla) ja vastustaa

89 Voutilainen 2019, s. 96.
90 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 171, 174.

henkilötietojen käsittelyä 21 artiklan perusteella. Näihin oikeuksiin vaikuttaa se, mistä tiedot on kerätty ja millä perusteella henkilötietoja käsitellään.

Rekisteröidyllä on oikeus saada tieto henkilötietojensa käsittelystä selkeästi ymmärrettävässä muodossa. Rekisterinpitäjällä on velvollisuus toimittaa henkilötietojen käsittelyä koskevat tiedot rekisteröidylle muodossa, joka on esitetty tiiviisti, täyttää läpinäkyvyyden periaatteen, on helposti ymmärrettävissä sekä helposti saatavilla. Rekisteröidyn esitettyä pyynnön saada nähdä nämä tiedot tulee rekisterinpitäjän antaa näitä koskeva informaatio asetuksen mukaisessa määräajassa. Rekisterinpitäjän täytyy antaa tieto pyynnön perusteella ryhdyttyihin toimenpiteisiin viivytyksettä, kuitenkin viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Rekisterinpitäjän kieltäytyessä rekisteröidyn pyynnöstä on rekisterinpitäjällä myös kuukausi aikaa perustella rekisteröidylle, miksi hän ei ryhdy rekisteröidyn vaatimiin toimenpiteisiin. Myös kieltäytyessään on rekisterinpitäjän kerrottava rekisteröidylle tämän käytettävissä olevista oikeussuojakeinoista, kuten oikeudesta tehdä valitus valvontaviranomaiselle. Asetuksessa säädetään kattavasti rekisteröidylle informoimisesta, kun henkilötietoja kerätään suoraan rekisteröidyltä tai muualta kuin rekisteröidyltä itseltään. [91]

Vaikka informointivelvollisuudesta säädetään kattavasti asetuksen 15 artiklassa, ei asetus kuitenkaan säädä muodosta tai keinosta, jolla informointivelvollisuuden piiriin kuuluvat tiedot on rekisteröidylle annettava. Muoto, jolla informointivelvollisuus voidaan täyttää, riippuu yksittäistapauksesta, ja informaatio voidaan tapaus huomioon ottaen antaa joko sähköisesti, internetsivustolla tai postitse kirjeenä.[92] Tässä suhteessa asetus on jättänyt rekisterinpitäjälle mahdollisuuden toteuttaa informointivelvollisuus monin eri tavoin. Rekisterinpitäjälle jää toisaalta vastuu pystyä osoittamaan, että informointivelvollisuus on täytetty.

Rekisteröidyn oikeudesta saada pääsy tietoihin säädetään artiklassa yksityiskohtaisemmin kuin aiemmin henkilötietolaissa. Tämän oikeuden nojalla rekisteröity on oikeutettu saamaan jäljennöksen häntä koskevista henkilötiedoista. Tietosuoja-asetus ei määrittele määrämuotoa kyseiselle pyynnölle. Tarvittaessa rekisterinpitäjä voi vahvistaa rekisteröidyn henkilöllisyyden pyytämällä lisätietoja itsestään, jos rekisterinpitäjällä on perusteltu syy

[91] Oikeusministeriö 2017, s. 19.
[92] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 175.

epäillä pyynnön tehneen luonnollisen henkilön henkilöllisyyttä. Rekisterinpitäjän tulee reagoida rekisteröidyn pyyntöön tässäkin tapauksessa kuukauden kuluessa. Jos rekisterinpitäjä pitää tällaista pyyntöä kohtuuttomana tai perusteettomana, on rekisterinpitäjän perusteltava rekisteröidylle nämä pyynnön hylkäämisen perusteet. [93]

Oikeus tulla unohdetuksi on rekisteröidylle säädetty oikeus, jonka perusteella rekisteröity voi esittää rekisterinpitäjälle pyynnön henkilötietojensa poistamiseksi.[94] Tästä säädetään tietosuoja-asetuksen 17 artiklassa, joka sisältää useita alakohtia, joiden perusteella rekisteröity voi pyytää rekisterinpitäjää viivytyksettä poistamaan[95] häntä koskevat tiedot. Tämän artiklan rinnalla sovelletaan lisäksi tietosuoja-asetuksen 12 artiklan mukaisesti yleisiä säännöksiä viestinnästä ja läpinäkyvästä informoinnista. Kyseiseen rekisteröidyn oikeuteen vaikuttaa kuitenkin se, millä perusteella henkilötietoja on kerätty ja minkälaisesta rekisteristä on kyse. Esimerkiksi viranomaisten henkilörekistereistä poistaminen ei ole mahdollista vain pyynnön avulla.

Oikeus tietojen rajoittamiseen on yksi rekisteröidyn oikeuksista. Rekisteröidyllä on tämän oikeuden nojalla neljässä eri tilanteessa oikeus saada aktiivinen käsittely rajoitetuksi. Rajoittamista koskevia menetelmiä voivat olla esimerkiksi valittujen tietojen siirtäminen toiseen käsittelyjärjestelmään tai käyttäjien pääsyn estäminen henkilötietoihin. Henkilötietojen käsittelyn osalta järjestelmässä on tuotava riittävän selkeästi esille käsittelyn rajoittaminen. Käsittelyn rajoittaminen on myös varmistettava teknisesti. Rekisteröidyn pyyntö rajoittaa henkilötietojensa käyttämistä ei estä rekisterinpitäjän säilyttämismahdollisuuksia. Rekisterinpitäjä saa pyynnöstä huolimatta säilyttää kyseisen henkilön henkilötietoja, mutta niiden käyttöä vain rajoitetaan pyynnön avulla. [96]

Rekisteröity saa halutessaan siirtää rekisterinpitäjälle toimittamansa häntä koskevat henkilötiedot rekisterinpitäjältä toiselle. Rekisterinpitäjä, jolle tiedot on alun perin toimitettu, ei voi estää rekisteröidyn siirto-oikeutta. Tiedot on oikeus saada siirtää suoraan rekisterinpitäjältä toiselle, mikäli tämä siirto on teknisesti mahdollista. Tiedot on voitava siirtää myös systemaattisesti, yleisesti luettavassa muodossa. [97] Viranomaisten toiminta

[93] Oikeusministeriö 2017, s. 26-27.
[94] Oikeusministeriö 2017, s. 25.
[95] Tietosuoja-asetuksessa ei ole määritelty, mitä poistaminen tarkoittaa. Riittävänä ei kuitenkaan pidetä tietojen siirtämistä vain ”roskakoriin”, vaan ne tulee poistaa siten, ettei rekisterinpitäjä, käsittelijä tai kolmas osapuoli voi saada niitä enää käsiinsä. Ks. lisää Voight- von dem Busshe 2017, luku 5.5.2.4.
[96] Oikeusministeriö 2017, s. 26.
[97] Oikeusministeriö 2017, s.25.

kuitenkin perustuu lakiin, ja heidän henkilötietojensa kerääminen rekisterinpitäjänä on lakiperusteista, joten tässä suhteessa tämä rekisteröidyn oikeus ei aina voi toteutua. Oikeuden toteutumista estää jo se, että Suomessa on vain yksi Verohallinto tai yksi Kansaneläkelaitos. Näiden toimijoiden rekistereistä toiseen siirto ei onnistu, koska tarjolla ei ole toista veroviranomaista tai vastaavasti kansalaisten etuuslaitosta.

Osaan käsittelyperusteista liittyy rekisteröidyn oikeus vastustaa henkilötietojensa käsittelyä. Vastustamisoikeudesta säädetään tietosuoja-asetuksen 21 artiklassa. Tällaisia vastustamisoikeuden käyttöön liittyviä käsittelyperusteita ovat käsittelyt, jotka liittyvät yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttöön tai kolmannen oikeutetun edun toteuttamiseen. Vastustamisoikeus on myös silloin mahdollista, kun henkilötietojen käsittely koskee suoramarkkinointia sekä tietyin edellytyksin myös käsittelyä tieteellistä, historiallista tai tilastollista tutkimusta varten. Tällöin tästä oikeudesta voidaan säätää poikkeuksia kansallisella lailla. Kun rekisteröity käyttää vastustamisoikeuttaan, rekisterinpitäjällä ei lähtökohtaisesti ole enää oikeutta käsitellä kieltäytyneen henkilötietoja. Käsittelykiellolle on kuitenkin määritelty asetuksessa tiettyjä poikkeuksia.[98]

Poikkeuksista esimerkkinä voidaan mainita luotonanto. Kun rekisteröity on käyttänyt vastustusoikeuttaan, tulee rekisterinpitäjän osoittaa tärkeä ja perusteltu syy sille, miksi rekisteröidyn henkilötietojen käsittely on tärkeää. Luotonanto voidaan esimerkiksi evätä sillä perusteella, että luotonmyöntäjä ei ole tarpeeksi päässyt tarkistamaan rekisteröidyn eli luotonsaajan maksukykyä. Maksukyky voidaan tutkia vain tarkastelemalla eri rekistereitä, joista selviää henkilön mahdolliset ulosottovelat tai omistuksessa olevat kiinteistöt, joita käytetään mahdollisesti luoton vakuutena.

Säätämällä yksityiskohtaisemmin rekisteröidyn oikeuksista tietosuoja-asetuksen tasolla tavoitteena on parantaa rekisteröidyn tietosuojaa. Tarkemmalla sääntelyllä rekisteröidyn oikeuksista saadaan rekisterinpitäjä ohjattua läpinäkyvämpään tietojen käsittelyyn, kun rekisteröidyn oikeudet vaativat tietojen vastuullista käsittelyä.[99]

98 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 250-255.
99 Ks. esim. Korpisaari – Pitkänen – Warma-Lehtinen 2018 lisää hallinnollisesta sakosta, joka voidaan määrätä näistä rekisteröidyn oikeuksien loukkaamisista. s.174.

Rekisteröidyn oikeudet ovat selkeitä, ja niistä on pyritty säätämään yksityiskohtaisemmin jo EU:n tasolla. Ne tulee huomioida kaikissa henkilötietojen käsittelyn vaiheissa, mutta silti ne ovat vaikeasti löydettävissä rekisteröidyn näkökulmasta esimerkiksi sosiaalisessa mediassa. Selailemalla esimerkiksi Instagramia ei kovin helposti löydy rekisteröidyn oikeuksista tietoa.[100] Tämän suhteen voisi vielä tietynlaista kehitystä tapahtua, jotta rekisteröidyn oikeudet olisivat yhtä helposti painalluksen takana toteutettavissa kuin esimerkiksi kuvan julkaisemisessa. Kun tällaista asetuksen tasoista kehitystä vielä työstettäisiin esimerkiksi sosiaalisen median kannalta, tämä olisi askel kohti tietoturvallisempaa yhteiskuntaa. Ajatus rekisteröidyn oikeuksista ja niiden yksityiskohtaisemmasta sääntelystä on hyvä, mutta vielä konkreettisemmin se loisi yhteiskunnasta turvallisemman, kun säädettäisiin myös siitä, kuinka helposti näiden oikeuksien toteuttamisen tulisi olla rekisteröityjen käytettävissä. Tähän päästäisiin esimerkiksi säätämällä niistä konkreettisista toimenpiteistä, joita tulisi olla eri rekisteritilanteissa rekisteröidyn käytettävissä. Sivustolle kirjauduttuaan yksilöllä olisi esimerkiksi mahdollisuus valita välilehti, jossa nämä hänen oikeutensa olisivat käytettävissä, ja tuon välilehden kautta rekisteröity voisi myös tarvittaessa käyttää näitä oikeuksiaan

3.1.4 Vertailua Ruotsiin ja EIT:n oikeuskäytäntöön

Ruotsissa henkilötietojen suojelun taso on nostettu korkealle, ja heidän tavoitteenaan on olla digitalisoinnissa edelläkävijänä. Ruotsin tietosuojaviranomaisen, Datainspektionen, julkaisema raportti tietosuoja-asetuksen vaikutuksista osoittaa, että Ruotsilla on kova pyrkimys varmistaa kansalaistensa luottamusta digitaalisiin palveluihin. Datainspektionen raportin perusteella ruotsalaiset näkevät, että tietosuoja-asetuksen soveltamisen punaisena lankana on yksilöiden perusoikeuksien suojan vahvistuminen osana henkilötietojen käsittelyä. Ruotsin raportti tietosuoja-asetuksen täytäntöönpanosta keskittyy siihen, kuinka paljon asetuksen tavoitteita on saavutettu vuodessa asetuksen voimaan astumisesta.[101]

Ruotsissa Datainspektionen nähdään kansalaisten perusoikeuksien valvojana. Sen päätehtävänä on ihmisoikeuksien suojeleminen henkilötietojen käsittelyssä. Viranomaisena se tarkistaa lakien ja sääntöjen noudattamista sekä määrää tarvittaessa hallinnollisia sakkoja

[100] Esim. Instagramin sovelluksessa on rekisteröidyn ensin mentävä asetuksiin ja asetuksissa kohtaa ”tietoja” , jonka jälkeen vielä kohtaan ”tietokäytäntö” ja tässä tietokäytännössä vasta kohta IV käsittelee sitä, kuinka rekisteröity voi käyttää oikeuksiaan.
[101] Datainspektionen.se -> globalassets->document->rapporter->nationell integritetsrapport 2019.

toimista. Datainspektionen vastaa myös ennakolta kansalaisten kysymyksiin tietosuojaa koskien.

Datainspektion on toteuttanut tutkimuksen vuosi tietosuoja-asetuksen voimaantulosta. Tuloksen perusteella kansalaiset tuntevat tietosuoja-asetuksen, jonka nähdään vahvistavan yksilöiden oikeuksia. Kansalaisille suunnatun tutkimuksen perusteella he hahmottivat erityisesti oikeutensa tietoon sekä henkilötietojen siirrettävyyden. Ruotsin kansalaiset ovat tutkimuksen perusteella tietoisia tietosuoja-asetuksesta sekä sen myötä yksilöille vahvistetuista oikeuksista. He ovat myös tietoisia riskeistä. Tutkimuksen perusteella ruotsalaiset kantavat huolta siitä, että erityisesti rikolliset pääsisivät käsiksi heidän henkilötietoihinsa. Eniten ruotsalaiset luottavat henkilötietojen käsittelyssä terveydenhuoltoon, viranomaisiin ja pankkeihin rekisterinpitäjinä.[102]

Euroopan ihmisoikeustuomioistuimen ratkaisussa *EIT 17.7.2008, I v. Suomi*, on kysymys siitä, että sairaalan katsottiin laiminlyöneen riittävän potilastietojen käytönvalvonnan järjestämisen.[103] Jälkikäteen ei ollut selvitettävissä, mitä väärinkäyttöä laiminlyönnin vuoksi aiheutui. Ratkaisun perusteella jälkikäteinen vahingonkorvauksen mahdollisuus ei ole yksityisyyden suojan toteuttamiseksi riittävää.[104] Tapauksessa EIT katsoi, että pääsyä potilastietojärjestelmään ei ollut kontrolloitu tarpeeksi. Jälkikäteen oli mahdotonta osoittaa aukottomasti mahdollisia väärinkäytöksiä, koska käytöstä ei ollut tallennettu lokitietoja. [105] Tapauksen ratkaisussa todetaan, että Euroopan ihmisoikeussopimuksen vaikutukset kohdistuvat myös valtion turvaamisvelvollisuuteen yksityisten henkilöiden välillä eivätkä ainoastaan yksityisten henkilöiden ja viranomaisten välisiin suhteisiin.[106] Suomelle langetettiin tuomio, jossa todettiin Suomen laiminlyöneen positiiviset velvoitteensa Euroopan ihmisoikeussopimuksen 8 artiklan toteuttamisessa.[107] Tapauksen perusteluiden osalta voidaan todeta, että jälkikäteinen vahingonkorvauksen mahdollisuus ei toteuta yksityisyyden suojan toteutumista riittävästi.

[102] Datainspektionen.se -> globalassets->document->rapporter->nationell integritetsrapport 2019.
[103] Ratkaisun kohta 29.
[104] Ratkaisun kohta 47.
[105] Ratkaisun kohta 44.
[106] Ratkaisun kohta 36.
[107] Ratkaisun kohta 48.

3.1.5 Rekisteröidyn oikeussuojakeinot

Tietosuoja-asetuksen VIII luvussa säädetään oikeussuojakeinoista, vastuusta ja seuraamuksista. Artiklassa 77 säädetään oikeudesta tehdä valitus valvontaviranomaiselle. Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan tietosuoja-asetusta. Rekisteröity voi tehdä valituksen erityisesti siinä jäsenvaltiossa, jossa hänen vakinainen asuinpaikkansa tai työpaikkansa on taikka jossa väitetty rikkominen on tapahtunut. Valituksen tekijällä on oikeus saada tieto valituksen etenemisestä ja ratkaisusta. Valvontaviranomaisella on ilmoitusvelvollisuus näistä tiedoista valituksen tekijälle. Myös 78 artiklan mukaiset oikeussuojakeinot tulee huomioida valituksen yhteydessä.

Asetuksen 78 artiklan perustella rekisteröidyillä on oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaista vastaan. Artiklan ensimmäisen kohdan perusteella jokaisella on oikeus tehokkaisiin oikeussuojakeinoihin itseään koskevaa valvontaviranomaisen oikeudellisesti sitovaa päätöstä vastaan. Tehokkaisiin oikeussuojakeinoihin tukeutuminen ei kuitenkaan rajoita muita hallinnollisia muutoksenhakukeinoja tai muita oikeudellisia oikeussuojakeinoja. Oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaista vastaan on silloin, jos valvontaviranomainen ei ole käsitellyt valitusta tai ilmoittanut rekisteröidylle kolmen kuukauden kuluessa 77 artiklan nojalla tehdyn valituksen etenemisestä tai ratkaisuista. Valvontaviranomaista vastaan nostettu kanne on nostettava sen jäsenvaltion tuomioistuimessa, johon valvontaviranomainen on sijoittautunut.

Asetuksen 79 artiklan perusteella rekisteröidyllä on oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan. Artiklan ensimmäisen kohdan perusteella jokaisella on oikeus tehokkaisiin oikeussuojakeinoihin, jos rekisteröity katsoo asetuksen mukaisia oikeuksiaan loukatun sillä perusteella, ettei hänen henkilötietojensa käsittelyssä ole noudatettu tätä asetusta. Artiklan toisen kohdan perusteella kanne rekisterinpitäjää tai henkilötietojen käsittelijää vastaan on nostettava sen jäsenvaltion tuomioistuimessa, jossa rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikka. Kanne voidaan myös nostaa sen jäsenvaltion tuomioistuimessa, jossa rekisteröidyn vakinainen asuinpaikka on. Tätä mahdollisuutta ei kuitenkaan ole, jos rekisterinpitäjä tai henkilötietojen käsittelijä on jäsenvaltion viranomainen, jonka toiminta liittyy sen julkisen vallan käyttöön.

Kanteen nostaminen Suomen ulkopuolella ei siten ole mahdollista 79 artiklan 2 kohdan perusteella esimerkiksi Suomen Verohallintoa vastaan, jos rekisteröidyn asuinpaikka on vaikka Ruotsissa tai muualla Suomen ulkopuolella. Rekisteröidyn tulisi tällöin nostaa kanne Suomessa, koska verohallinto on viranomainen, jonka toiminta perustuu julkisen vallan käyttöön. Tällöin tulee miettiä, asettaako asetus rekisteröidyt väistämättä eri asemaan sen perusteella, missä rekisteröity asuu. Verohallinnolla Suomessa on erittäin paljon rekisteröityjä Suomen ulkopuolella, koska henkilöt voivat olla Suomessa yleisesti tai rajoitetusti verovelvollisia tai heillä voi muuten olla Suomeen verokytköksiä. Tällaisten henkilöiden henkilötietojen vuotaessa esimerkiksi tavallisen postin mukana ovat rekisteröityjen oikeusturvakeinot vaikeasti toteutettavissa. Tietosuoja-asetus ei tällöin kata kaikkea turvaa ja ei pääse tavoitteeseen suojata luonnollisten henkilöiden henkilötietojen käyttöä ja suojaa.

Tietosuoja-asetuksen 82 artiklan perusteella rekisteröidyllä on oikeus vahingonkorvaukseen tietosuoja-asetuksen rikkomisesta, mukaan lukien tietosuoja-asetukseen liittyvien muiden säännösten rikkominen. Vahingonkorvausasiaa ajetaan kansallisesti toimivaltaisessa yleisessä tuomioistuimessa. Jos tietoturvaloukkaus täyttää rikoksen tunnusmerkistön, käsitellään rikosasiat rikosprosessissa.[108] Kuten Voutilainen on myös todennut teoksessaan, ovat tietosuoja-asetukseen liittyvät oikeusturvamenettelyt sekavia.[109] Samaa asiaa voidaan joutua käsittelemään valvonta-asiana, hallintoprosessissa, siviiliprosessissa sekä rikosprosessissa.

Valtion ylimpinä laillisuusvalvojina toimii lisäksi eduskunnan oikeusasiamies, josta säädetään perustuslain 109 §:ssä, sekä valtioneuvoston oikeuskansleri, josta säädetään perustuslain 108 §:ssä. Heidän tehtävänään on varmistaa henkilötietojen suojan toteutuminen perusoikeustasolla valvomalla suojan toteutumista. Kumpikaan näistä laillisuusvalvojista ei kuitenkaan ole muutoksenhakuviranomainen. Tämän vuoksi tietosuoja-asetuksen mukaisesti valittaminen rekisterinpitäjää vastaan tietoturvaloukkaustilanteissa ei ole mahdollista näille viranomaisille.

[108] Henkilötietojen käsittelyyn liittyviä rikosnimikkeitä on mm. tietosuojarikos, virkavelvollisuuden rikkominen sekä yksityiselämää loukkaava tiedon leviäminen.
[109] Ks. Voutilainen 2019, s. 630. Vuotilainen toteaa, että sekavat oikeusturvamenettelyt ovat jo omiaan vaarantamaan rekisteröidyn, rekisterinpitäjien ja henkilötietojen käsittelijöiden oikeusturvan.

3.2 Rekisterinpitäjän vastuut

3.2.1 Mitä vastuu pitää sisällään?

Rekisteröidyn oikeuksiin liittyy käänteisesti rekisterinpitäjän vastuut. Tietosuoja-asetus määrittelee joukon velvollisuuksia rekisterinpitäjille. Näiden velvollisuuksien tarkoituksena on toteuttaa rekisteröidyn oikeuksia. Rekisterinpitäjän vastuista säädetään tietosuoja-asetuksen 24 artiklassa. Artiklan perusteella rekisterinpitäjän on toteutettava tarvittavat toimenpiteet, joilla voidaan varmistaa ja osoittaa käsittelyn noudattavan asetusta. Toimenpiteet ovat sekä teknisiä että organisatorisia. Näitä toimenpiteitä tulee artiklan perusteella aina tarvittaessa päivittää ja tarkistaa. Asetuksessa rekisterinpitäjän vastuut ja velvoitteet on määritelty riskiperusteisesti.[110] Vastuuta koskevaa säännöstä tulee tulkita osana asetuksen kokonaisuutta, ottaen huomioon asetuksen tavoitteet. [111]

Tarkasteltaessa asetusta kokonaisuutena on sen tavoitteena rekisteröityjen oikeuksien toteutuminen ja henkilötietojen riittävä suojan taso. Asetus on kuitenkin sen verran vaikeaa luettavaa kokonaisuudessaan, että juuri kyseiseen tärkeään artiklaan olisi hyvä olla mahdollisuus säätää täsmällisempiä toimia, joilla rekisterinpitäjän vastuut toteutuvat. Artikla 24 ei tulkinnan perusteella sisällä kansallista liikkumavaraa,[112] jolla voitaisiin turvata juuri rekisterinpitäjän konkreettisia vastuutoimenpiteitä.

Artikla sisältää sekä velvoitteen toimia huolellisesti että velvollisuuden osoittaa, minkälaisiin toimenpiteisiin lainmukaisen käsittelyn varmistamiseksi on ryhdytty. Tällä artiklalla on tarkoitus täydentää tietosuoja-asetuksen 5 artiklan 2 kohdassa säädettyä osoitusvelvollisuutta, kun rekisterinpitäjältä edellytetään käsittelytoimien lainmukaisuuden osoittamista. Käsittelyn luonne, laajuus, asiayhteys, tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit vaikuttavat siihen, minkälaisia toimenpiteitä rekisterinpitäjältä edellytetään.[113] Rekisterinpitäjällä on tilivelvollisuus toimistaan. Osoitusvelvollisuuden kautta rekisterinpitäjän on pystyttävä osoittamaan, että rekisterinpitäjä ottaa huomioon tietosuojasäännökset käyttäessään henkilötietoja.

110 Andreasson – Riikonen – Ylipartanen 2019, s. 68.
111 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 269.
112 TATTI-työryhmän mietintö, s. 54.
113 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 268-270.

Rekisterinpitäjän on suunniteltava tietosuoja tuotanto- ja palveluprosessien suhteen huolellisesti (privacy by design). Tietosuoja on myös toteutettava oletusarvoisesti ja sisäänrakennetusti (privacy by default). [114] Rekisterinpitäjän vastuuta koskeva artikla täydentää osoitusvelvollisuuden artiklaa. Tarkoituksenmukaisempaa olisi kuitenkin, että nimenomaan vastuuta koskeva artikla olisi selkeä ja sitä olisi mahdollista täydentää kansallisella lainsäädännöllä. Mahdollisuus täydentää vastuuta koskevaa sääntelyä kansallisella tasolla turvaisi osaltaan rekisterinpitäjän todella ymmärtävän vastuun merkityksen. Tällä hetkellä asetus on vaikeasti luettavaa, kun eri artiklat liittyvät toinen toisiinsa ja lukeminen on rikkonaista. Selkeyttämällä rekisterinpitäjän vastuuta koskevaa artiklaa koko asetuksesta tulisi yhtenäisempi henkilötietojen suojan toteutumisen kannalta. Toisaalta tämän hetkinen asetus luo rekisterinpitäjille paljon liikkumavaraa suorittaa esimerkiksi osoitusvelvollisuus haluamallaan tavalla. Konkreettisempi vastuuartikla saattaisi johtaa rekisterinpitäjän toiminnan kannalta rajatumpaan valvontaan. Tällainen tarkempi vastuuartikla myös mahdollisesti kaventaisi rekisterinpitäjän liikkumavaraa.

Osoitusvelvollisuus on uusi tietosuoja-asetuksessa säädetty velvoite. Se konkretisoituu vaikutustenarvioinnin laatimisella ja selosteilla, joita laaditaan asetuksen perusteella käsittelytoimista. Osoitusvelvollisuuden tarkoituksena on mahdollistaa henkilötietojen suoja siten, että rekisterinpitäjällä on mahdollisuus luoda käytännölliset ja tehokkaat keinot suojan varmistamiseksi.[115]

Rekisterinpitäjän vastuun takana on arvio riskeistä, joita henkilötietojen käsittelyyn liittyy, sekä vahingoista, joita rekisteröidylle voi henkilötietojen väärinkäytöstä aiheutua. Asetuksen taustalla on riskiperusteinen lähestymistapa, jota ei määritellä missään asetuksen artiklassa. Kyseisessä lähestymistavassa mahdollisia riskejä ja ongelmia lähestytään *ennaltaehkäisevästi.* Tämä lähestymistapa on huomioitu kuitenkin monessa asetuksen artiklassa.[116] Asetuksen vastaisesta toiminnasta aiheutuva vahinko voi näyttäytyä eri tavoin. Rekisterinpitäjän lainvastaisen toiminnan mahdollistama petos tai identiteettivarkaus on esimerkiksi välitön syy taloudelliseen vahinkoon. Vahinkona nähdään myös se, että rekisteröidyltä evätään oikeus valvoa henkilötietojaan tai muuten hänelle kuuluvia oikeuksia

[114] Andreasson – Koivisto – Ylipartanen 2015, s. 9 – 10.
[115] Andreasson – Koivisto – Ylipartanen 2018, s. 95 – 97.
[116] Riskiperuste on huomioitu esim. TSA 32, 34 ja 35 artikloissa.

tai velvollisuuksia. Riskien arvioiminen tulee toteuttaa myös, kun arvioidaan henkilön henkilökohtaisia ominaisuuksia tai henkilötietojen joukko on suuri.

Konkreettisia toimia, joita rekisterinpitäjälle on asetettu, on esimerkiksi tietosuojavastaavan nimeäminen. Rekisterinpitäjän on nimettävä tietosuojavastaava toiminnalleen. Tietosuojavastaavalle asetettuina kriteereinä henkilön tulee olla ammatiltaan ja koulutukseltaan sellainen, joka pystyy seuraamaan ja noudattamaan asetusta ja suorittamaan velvollisuutensa menestyksellisesti.[117] Rekisterinpitäjän velvollisuuksiin kuuluu myös noiden jo aiemmin mainittujen vaikutustenarviointi siitä, mitä riskejä henkilötietojen käsittelyyn liittyy. Käytännön toteuttamismahdollisuus rekisterinpitäjän vastuun toteuttamisen kannalta on seuraavassa luvussa 3.2.2 käsiteltävä vaikutustenarviointi. Kyseistä 24 artiklaa on tulkittava vaikutustenarviointia koskevan säännöksen kanssa yhdessä.

Tietosuoja-asetuksen voimaan tultua ei riitä enää, että rekisterinpitäjä noudattaa lakeja, vaan asetus velvoittaa rekisterinpitäjän toimimaan aktiivisesti ja oma-aloitteisesti eri tavoin osoittaakseen, että tietosuojavaatimukset on otettu mukaan henkilötietojen käsittelyprosesseihin ja -käytäntöihin. Näitä aktiivisia toimenpiteitä ovat juuri dokumentointi, kirjalliset suunnitelmat, käytännesäännöt, sertifiointi sekä tietotilinpäätösten tekeminen. Aktiivisilla toimenpiteillä tarkoitetaan niin sanottua osoitusvelvollisuutta, asetuksen 5 artiklan 2 kohdan mukaisesti. [118]

3.2.2 Riskiperusteinen arvio ja vaikutustenarviointi

ENISA on esittänyt jo vuonna 2016 suuntaviivoja lähestymistavalle, joka ohjaa rekisterinpitäjiä (varsinkin pk-yrityksiä) hahmottamaan tietoturvariskejä ja toteuttamaan turvaavia toimenpiteitä. ENISAn toimittamassa raportissa käydään läpi vaikutustenarviointia ja sitä, millainen laadullinen prosessi siinä on kyseessä.[119] Tietosuoja-asetuksen mukainen vaikutustenarviointi (DPIO, data protection impact assessment) tulee

[117] Voigt -Von dem Bussche 2017, s. 3.
[118] Andreasson – Riikonen – Ylipartanen 2019, s. 25.
[119] European union Agency for cybersecurity -> Publications -> Enisa treat landscape report 2017..

tehdä, kun henkilötietojen käsittelyyn kohdistuu todennäköisesti korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille.[120]

Vaikutustenarviointia koskeva prosessi on jatkuvaa, eikä se ole kertaluonteinen tehtävä.[121] Rekisterinpitäjän tulee ottaa huomioon vaikutustenarvioinnissa henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Henkilötietojen käsittelyn luonteen arvioimisella pyritään tiedostamaan, sisältääkö henkilötietojen käsittely mahdollisesti jotain erityisiä henkilötietoryhmiä. Luonteeseen kuuluu myös huomioida rekisteröidyn heikko asema sekä uusi teknologia ja innovaatiot. Laajuuden arvioimisessa rekisterinpitäjän tulee selvittää, kuinka suuresta rekisteristä on kyse ja paljonko rekisteröityjä tulee olemaan. Myös tiedon määrä[122], mitä henkilötietoja tullaan keräämään ja millä perusteilla, kuuluvat tähän arvioon. Laajuuden arvioon vaikuttaa lisäksi se, miten laajasta soveltamisalasta henkilötietojen suhteen on kyse. Säilytysaika tulee myös arvioida, tullaanko tietoja säilyttämään lyhyt aika, jokin tietty määräaika vai onko tiedot tarkoitettu säilyttää pysyvästi. Tarkoitusten arviointi kohdistuu rekisteröityjen seurantaan ja valvontaan, henkilöiden arviointiin sekä automaattiseen päätöksentekoon. Tarkoituksen arviossa tulee huomioida, missä määrin rekisterinpidossa voidaan käyttää automaattista päätöksentekoa, jolla on oikeusvaikutuksia rekisteröityyn. Asiayhteyden arviointi pohjautuu luottamukseen. Tällöin rekisteröidyllä on oikeus luottaa, että tietoja käytetään vain siihen tarkoitukseen, johon ne on kerätty. Myös yksityisyyden turvaaminen tulee ottaa huomioon luottamuksen arvioimisessa. Luottamuksen arvioimisessa huomiota tulee kiinnittää henkilötietojen yhdistelyyn, kun henkilötietoja on kerätty eri yhteyksissä ja niitä aletaan yhdistelemään. [123]

Rekisteröidyn oikeuksille ja vapauksille aiheutettujen riskien tunnistamisen jälkeen rekisterinpitäjän tulee arvioida riskiä suhteessa siitä aiheutuvaan haittaan. Haitan vakavuus ja toteutumisen todennäköisyys ovat tällöin arvion perustana. Haitan vakavuus voi olla matala tai korkea, kun taas toteutumisen todennäköisyys voi olla kaukainen, mahdollinen tai hyvin mahdollinen. Riskejä tulee arvioida jatkuvasti ja tarvittaessa niitä on päivitettävä. Riskien suhteen rekisterinpitäjällä on myös osoitusvelvollisuus, jolla varmistetaan, että

120 Andreasson – Riikonen – Ylipartanen 2019, s. 67.
121 Andreasson – Riikonen – Ylipartanen 2019, s. 67.
122 Tietoja kerätään ja talletetaan enempi kuin rekisterinpidon kannalta olisi tarkoituksenmukaista. Näin selvittää esimerkiksi Sankari ja Wiberg artikkelissaan 2019.
123 Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi.

rekisterinpitäjä noudattaa riskiperusteista lähestymistapaa. [124] Käsittelytoimista aiheutuvat riskit on arvioitava jo ennen aloittamista, vaikka velvollisuutta varsinaiseen vaikutustenarvioinnin tekemiseen ei vielä olisi. Näin voidaan jo suunnitteluvaiheessa tunnistaa ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä hallitakseen riskit ja henkilötietojen asianmukaisen käytön.[125]

Riskit tulee arvioida rekisteröidyn näkökulmasta. Rekisterinpitäjän on arvioitava, mitä vaaraa rekisteröidyn oikeuksille ja vapauksille käsittelystä voi aiheutua sekä mitä fyysisiä, aineellisia tai aineettomia vahinkoja rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä.[126] Riskien arvioimiseksi on olemassa konkreettinen työkalu, vaikutustenarviointi. Tämä työkalu on pakollinen silloin, kun suunniteltu henkilötietojen käsittely voi aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille.[127] Tietosuoja-asetuksen 35 artiklassa säädetään tästä vaikutustenarvioinnista. Kyseisen artiklan 1 kohdan mukaan tietosuojaa koskeva vaikutustenarviointi tulee tehdä, jos tietyntyyppinen käsittely aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Korkean riskin voi aiheuttaa esimerkiksi uuden teknologian käyttäminen huomioiden käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Kun on laadittu yksi arviointi, voidaan tätä arviota käyttää samankaltaisiin korkeita riskejä aiheuttaviin käsittelytoimiin. Saman 35 artiklan 2 kohdan mukaan vaikutustenarviointia tehdessä rekisterinpitäjän tulee pyytää neuvoja tietosuojavastaavalta, jos sellainen on nimitetty. Saman artiklan 3 kohta puolestaan säätää siitä, milloin vaikutustenarviointi on erityisesti laadittava. Vaikutustenarviointi on laadittava erityisesti tapauksissa, joissa tehdään henkilökohtaisten ominaisuuksien järjestelmällinen ja kattava arviointi käyttäen automaattista käsittelyä, kuten profilointia, ja joka johtaa päätöksiin, joilla on oikeusvaikutuksia luonnollisten henkilöiden suhteen tai jotka muutoin vaikuttavat vastaavalla tavalla merkittävästi heihin. Vaikutustenarviointi on laadittava myös silloin, kun laajamittainen käsittely kohdistuu erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin tai on kyse yleisölle avoimen alueen järjestelmällisestä laajamittaisesta valvomisesta.

[124] Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi.
[125] Andreasson – Riikonen – Ylipartanen 2019, s. 71.
[126] Andreasson – Riikonen – Ylipartanen 2019, s. 71.
[127] Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi.

Näistä ensimmäinen vaatimus, jossa laaditaan henkilökohtaisten ominaisuuksien järjestelmällinen ja kattava arviointi, kytkeytyy osaltaan tietosuoja-asetuksen 22 artiklassa säädettyyn automaattisen päätöksenteon kieltoon. Tämä vaatimus kattaa kuitenkin automaattisen päätöksenteon lisäksi tilanteet, joissa ei tehdä automaattisia päätöksiä vaan joissa vain henkilötietoja käsitellään automaattisesti. Toinen vaatimus käsittää suuret määrät henkilötietoja, joita ollaan aikeissa käyttää alueellisesti, kansallisesti tai ylikansallisesti. Tällöin käsittely voi vaikuttaa suureen joukkoon ihmisiä ja käsittely aiheuttaa rekisteröidyn oikeuksiin ja vapauksiin kohdistuvaa korkeaa riskiä.

Vaikutustenarviointi on tehtävä myös silloin, kun henkilötietojen käsittely kohdistuu tietosuoja-asetuksen 9 artiklan mukaisiin *erityisiin henkilötietoryhmiin*, biometrisiin tietoihin tai tietoihin, jotka koskevat rikostuomioita ja rikkomuksia tai niihin liittyviä turvaamistoimenpiteitä tai henkilötietoja käsitellään luonnollisia henkilöitä koskevien päätösten tekemiseksi profilointiin perustuvan henkilökohtaisten ominaisuuksien järjestelmällisen ja kattavan arvioinnin perusteella; sekä aina muutenkin, jos toimivaltainen viranomainen katsoo käsittelyyn liittyvän todennäköisesti korkean riskin rekisteröityjen oikeuksien ja vapauksien kannalta. Riski näiden oikeuksien kannalta on korkea siitä syystä, että ne estävät rekisteröityjä käyttämästä oikeutta tai palvelua tai sopimusta, tai siitä syystä, että kyseiset toimet toteutetaan systemaattisesti laajassa mittakaavassa.[128]

Vaikutustenarviointi on tehtävä erityisesti silloin, kun tarkoituksena on käsitellä huomattavia määriä henkilötietoja. Laajamittaista käsittelyä määritettäessä on tietosuojatyöryhmä (WP 29) esittänyt, mitä tekijöitä ainakin tulee ottaa huomioon. Näitä huomioon otettavia tekijöitä ovat: asianomaisten rekisteröityjen lukumäärä, käsiteltävien tietojen tai tietoyksikköjen määrä, tietojenkäsittelytoimen kesto tai pysyvyys sekä maantieteellinen ulottuvuus.[129] Laaja-alainen tietojenkäsittely ei ole kyseessä silloin, kun yksittäinen lääkäri, muu terveydenhuollon ammattilainen tai lakimies käsittelee asiakkaiden henkilötietoja.[130]

Riskiperusteisen lähestymistavan perusteella rekisterinpitäjän tulee kartoittaa mahdolliset riskit, joita henkilötietojen käsittelyyn voi kohdistua hänen toimintaansa liittyen. Sen avulla pyritään ennakoimaan sitä, millaisia riskejä mahdollisesti kohdistuu kyseisiin henkilötietoihin ja kuinka niitä voidaan pyrkiä ennakoimaan. Vaikutustenarviointi on

[128] Tietosuoja-asetus, johdanto-osan 91 kappale. Luettelo ei ole tyhjentävä.
[129] WP 248, s. 12.
[130] Tietosuoja-asetus, johdanto-osa kohta (91).

riskiperusteisen lähestymistavan konkreettinen työkalu, joka tietyillä edellytyksillä on rekisterinpitäjän laadittava. Riskiperusteisesta lähestymistavasta ei ole säädetty omaa artiklaansa, mutta se oletetaan silti otettavan huomioon henkilötietojen käsittelyssä jo ennakolta. Vaikutustenarviointi työkaluna keskittyy siten ennakolliseen toimintaan, jolloin jälkikäteiset keinot jäävät arviointia vaille.

Vaikutustenarviointi on tietosuojan edistämisen työkalu. Se on yksi työkalu, jolla sisäänrakennettua tietosuojaa edistetään. Sen tarkoituksena on arvioida ennakkoon mahdollisia riskejä ja ratkaista niitä rekisterinpitäjän haasteita, joita tieto- ja yksityisyyden suojaan kohdistuu. Se on käytännössä lähestymistapa, jolla pyritään kartoittamaan sovelluksen, tuotteen tai palvelun merkitystä henkilötietojen käsittelyn kannalta, arvioimaan henkilötiedon käsittelyn vaikutuksia ja paljastamaan mahdollisia ongelmia ennakolta. Se pyrkii tunnistamaan riskit ja hallitsemaan niitä samalla, kun se huomioi vastakkaisten tavoitteiden tasapainottamisen sekä henkilötietojen suojan tavoitteet.[131]

3.2.3 Lainmukaiset henkilötietojen käsittelyn perusteet

Henkilötietojen käsittelyn oikeusperusteista säädetään tietosuoja-asetuksen 6 artiklassa. Henkilötietojen käsittely vaatii aina laissa säädetyn oikeusperusteen, jotta niitä voidaan käsitellä tai ryhtyä käsittelemään. Tämän lisäksi, kun käsitellään erityisiä henkilötietoryhmiä[132], tulee jonkin asetuksen 9 artiklassa säädetyt perusteet täyttyä.[133] Eräistä käsittelyperusteista on täydentävää sääntelyä kansallisessa tietosuojalaissa. Rekisterinpitäjälle on säädetty velvollisuus näyttää toteen, että käsittelyperuste on lainmukainen.[134]

Ennen henkilötietojen käsittelyn aloittamista rekisterinpitäjän täytyy määritellä oikeusperuste, johon käsittely perustuu. Oikeusperusteita on määritelty tietosuoja-asetuksessa kuusi eri käsittelyperustetta. Kun henkilötietojen käsittely on sidottu johonkin käsittelyperusteeseen, sitä ei voi enää vaihtaa toiseen. Käsittelyperusteita saattaa olla useampi kerrallaan käytössä, mutta tällöin ne on voitava erottaa toisistaan selkeästi.

131 Niinimäki-Rastas 2017, Edilex-julkaisu.
132 Erityisiä henkilötietoryhmiä ovat esimerkiksi etnistä alkuperää tai terveyttä koskevat tiedot jne. Näiden henkilötietoryhmien käsittely on lähtökohtaisesti kiellettyä.
133 Oikeusministeriö 2017, s. 19-22.
134 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 100.

Käsittelyperusteita voi siis olla useampi yhtä aikaa, mutta tietty käsittelyperuste tietyssä kohdassa ei voi muuttua toiseksi. Nämä perusteet vaikuttavat siihen, mitä oikeuksia rekisteröidyllä on suhteessa rekisterinpitäjään.[135] Eli, jos henkilötietoja käsitellään käsittelyperusteena suostumus ja sopimus, tulee molempien käsittelyperusteiden alle kuuluvat henkilötiedot erottaa. Jos henkilö on suostunut joihinkin henkilötietojen käsittelyihin tällä käsittelyperusteella, ei tämä käsittelyperuste voi kesken käsittelyn muuttua sopimukseksi.

Oikeusperusteista suostumus mahdollistaa rekisteröidylle laajimmat oikeudet suhteessa rekisterinpitäjään. Kun käsittelyperuste perustuu rekisteröidyn suostumukseen, on suostumuksen oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Rekisteröity hyväksyy näin henkilötietojensa käsittelyn. Suostumus voidaan toteuttaa kirjallisesti tai suullisesti antamalla suostumusta koskeva lausunto tai rekisteröity voi ilmaista suostumuksensa myös esimerkiksi rastittamalla ruudun internetsivustolla. Koska suostumus on helppo antaa, on se myös voitava peruuttaa yhtä helposti.[136] Jos rekisteröity peruu suostumuksen, peruuttaminen kohdistuu vain suostumuksen alaiseen käsittelyyn. Henkilötietojen käsittelyä voidaan kuitenkin muilta osin jatkaa, jos on vallinnut rinnakkain myös joku muu käsittelyperuste.

Suostumukselle on säädetty tiettyjä edellytyksiä, jotta se on pätevä. Pätevän suostumuksen on oltava yksilöity, tietoinen, aidosti vapaaehtoinen ja yksiselitteinen tahdonilmaisu. Suostumuksella pyritään mahdollistamaan rekisteröidylle mahdollisuus valvoa henkilötietojensa käsittelyä, ja mikäli henkilötietojen käyttötarkoitus muuttuu, tulee lähtökohtaisesti pyytää uusi suostumus rekisteröidyltä. Rekisterinpitäjän on määriteltävä käyttötarkoitus, johon henkilötietoja kerätään. Jos sama rekisterinpitäjän käsittelee useampaan eri käyttötarkoitukseen liittyviä henkilötietoja, on rekisteröidyn pystyttävä yksilöimään suostumuksensa. Jokainen käyttötarkoitus tarvitsee oman suostumuksen rekisteröidyltä, kun käsittelyperusteena on juuri suostumus.[137]

135 Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> milloin henkilötietoja saa käsitellä -> henkilön suostumus.
136 Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> milloin henkilötietoja saa käsitellä -> henkilön suostumus.
137 Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> milloin henkilötietoja saa käsitellä -> henkilön suostumus.

Suostumuksen vapaaehtoisuus edellyttää, että rekisteröity ei ole heikommassa asemassa suhteessa rekisterinpitäjään. Suostumus käsittelyperusteena ei välttämättä ole riittävä, kun rekisteröity toimii suhteessa rekisterinpitäjänä olevaan työnantajaan tai viranomaiseen. Tällöin rekisteröity voi olla heikommassa asemassa, jolloin suostumus ei ole aidosti vapaaehtoinen. Suostumuksen aitouteen liittyy myös se, että suostumus on voitava peruuttaa ilman haitallisia seurauksia yhtä helposti kuin sen antaminen tapahtuu. Peruminen on osa rekisteröidyn oikeuksia. Rekisteröidyllä tulee olla todellinen valinnan mahdollisuus, ja suostumuksen antamisen jälkeen rekisteröidyllä on oikeus perumiseen. Rekisteröityä ei saa johtaa harhaan, pakottaa tai rangaista suostumuksen antamatta jättämisestä. [138]

Koska suostumus on yksiselitteinen ja selkeä tahdonilmaisu, rekisteröity ei voi antaa suostumustaan vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jotakin tekemättä.[139] Sähköisesti pyydetty suostumus on yksiselitteinen ja selkeä, kun rekisteröity esimerkiksi rastittaa itse verkkosivustolla ruudun, jossa hän nimenomaisesti suostuu henkilötietojensa käsittelyyn. Suostumusta ei saa upottaa käyttö- ja sopimusehtoihin, jolloin se sekoittuu muihin tietoihin. Se on annettava selkeästi ja erillään muusta tiedosta, helposti ymmärrettävässä muodossa.[140] Suostumusta ei voi päätellä vain asiayhteydestä, se on annettava varta vasten.[141]

Rekisterinpitäjän tulee antaa rekisteröidylle suostumuksen pyytämisen yhteydessä tarpeeksi tietoja siitä, mihin rekisteröity suostumuksellaan suostuu. Rekisteröidyn on saatava tietää tahot, joille tiedot luovutetaan, kaikki käyttötarkoitukset, joita varten suostumus on pyydetty, tieto siitä, mitä tietoja rekisteröidyltä kerätään sekä rekisteröidyn oikeudesta peruuttaa suostumus ja tieto siitä, tullaanko henkilötietoja käyttämään automatisoitujen yksittäispäätösten tekemiseen tai profilointiin. Myös riskit tietojen siirrosta EU:n ulkopuolisiin maihin on saatava tietää, kun maan osalta ei ole tehty päätöstä tietosuojan tason riittävyyden osalta ja asianmukaisia suojatoimia ei ole toteutettu. Erikseen ei tarvitse yksilöidä niitä henkilötietojen käsittelijöitä, jotka käsittelevät kyseisiä suostumuksen alaisia tietoja rekisterinpitäjän lukuun. Rekisterinpitäjän tulee myös huomioida yleinen

138 Sankari – Wiberg 2019, s. 342.
139 Sankari – Wiberg 2019, s. 342.
140 Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> milloin henkilötietoja saa käsitellä -> henkilön suostumus.
141 Sankari – Wiberg 2019, s. 342.

informointivelvollisuus[142], joka edellyttää vastaanottajien yksilöintiä.[143] Huomionarvioista on, että suostumuksella ei voida kuitenkaan syrjäyttää tietosuoja-asetuksen 5 artiklassa mainittuja yleisiä henkilötietojen käsittelyperusteita.[144]

Sankarin ja Wibergin artikkelissa kritisoidaan suostumuksen tehoa käsittelyperusteena. Artikkelissa avataan testiä, jossa lähestytään sekä yksityisen puolen että julkisen puolen toimijoita ja pyritään selvittämään tietosuoja-asetuksen mukaisia toimenpiteitä ja toimijoiden suhtautumista asetuksen mukaiseen tietosuojaan. Tämän testin perusteella suostumus ei ole yhtä helppoa perua kuin antaa. Myöskään asetuksen mukaiset kriteerit eivät täyty, vaan suostumus tulee jossain yhteyksissä ymmärtää asiayhteydestä. Testin perusteella suostumus voidaan antaa vain luettelemalla tarpeellisia tietoja ääneen, kun taas peruuttaminen vaatii lomakkeiden täyttämistä. Myös suostumuksen peruuttaminen ja tietojen poistaminen sekoittuvat. [145]

Tietosuoja-asetuksen 6 artiklan 1 kohdan b kohdassa määritellään toiseksi lainmukaiseksi käsittelyperusteeksi sopimus. Käsittely on lainmukaista, jos käsittelyperusteena toimii sopimus, jossa rekisteröity on osapuolena. Tällöin rekisteröidyn henkilötietoja saa käsitellä, jotta sopimus voidaan laittaa täytäntöön. Sopimuksen sisältö ja perustavoite on tarpeen määritellä tarkasti, jotta niiden pohjalta voidaan arvioida käsittelyn tarpeellisuus. Sopimukseen perustuen henkilötietoja ei saa käsitellä yli sen, mikä on välttämätöntä. Kuitenkin, jos ennen sopimusta on suoritettava jotain käsittelytoimia, näiden suhteen voidaan käsitellä henkilötietoja jo rekisteröidyn pyynnön avulla. Tarpeellisuuden kannalta tarkasteltuna henkilötietojen käsittely on sallittua vain siltä osin, kun niiden avulla sopimus voidaan laittaa täytäntöön.[146] Kun käsittelyperusteena on sopimus, on rekisteröidyn oikeudet myös tällöin laajat. Tällöin erona suostumukseen kohdistuviin oikeuksiin on, että rekisteröidyllä on oikeus olla joutumatta automaattisen päätöksenteon kohteeksi ilman lainmukaista perustetta.[147]

Käsittelyperusteena voi olla myös lakisääteinen velvoite, josta säädetään tietosuoja-asetuksen 6 artiklan 1 kohdan c-kohdassa. Tällöin rekisterinpitäjällä on lakisääteinen

[142] Informointivelvollisuus on eri asia kuin henkilötietolain mukainen rekisteriseloste.
[143] Tietosuojavaltuutetun toimisto -> henkilötietojen käsittely -> milloin henkilötietoja saa käsitellä -> henkilön suostumus.
[144] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s.102.
[145] Sankari – Wiberg 2019, s. 344-345.
[146] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 102-103.
[147] Oikeusministeriö 2017. s. 27-29.

velvoite, johon rekisteröidyn henkilötietojen käsittely perustuu. Lakisääteisellä perusteella tarkoitetaan, että peruste on olemassa unionin oikeudessa tai rekisterinpitäjään sovellettavassa jäsenvaltion lainsäädännössä.[148] Lakisääteinen velvoite edellyttää, että rekisterinpitäjä käsittelee tiettyjä henkilötietoja. Tällainen velvoite voi koskea sekä yksityisellä että julkisella sektorilla toimivaa rekisterinpitäjää. Koska käsittelyperuste kohdistuu vain EU:n tai jonkin jäsenvaltion lainsäädäntöön, kolmansien maiden lainsäädäntöön perustuvat velvoitteet kuuluvat tämän velvoitteen piiriin vain, jos ne on sisällytetty EU:n tai jäsenvaltion oikeusjärjestykseen esimerkiksi kansainvälisellä sopimuksella.[149]

Lakisidonnaisuuden suhteen tulee huomioida perustuslaki sekä henkilötietojen suoja jo perusoikeutena. Perusoikeuksien suojasta säädetään lailla ja suojaa voidaan myös rajoittaa vain lain tasolla. Lakisidonnaisuuden suhteen tietosuoja-asetus ei edellytä, että jokaista tiedonkäsittelytilannetta varten olisi säädetty oma erityislakinsa, vaan kuten tietosuoja-asetuksen johdannossa sanotaan, voi yksi laki olla riittävä käsittelyperuste, kun se säätää useista käsittelytoimista.[150]

Elintärkeiden etujen suojaamisesta lainmukaisena käsittelyperusteena säädetään tietosuoja-asetuksen 6 artiklan 1 kohdan d alakohdassa. Henkilötietojen käsittely on lainmukaista, kun käsittelyperusteena on rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen. Elintärkeistä eduista on kyse, kun on kysymys elämästä ja kuolemasta tai uhista, jotka voisivat johtaa rekisteröidyn tai jonkun toisen loukkaantumiseen tai olla muuten terveydelle vahingollisia. [151] Sovellettavaksi tämä käsittelyperuste konkretisoituu silloin, kun käsittelylle ei ole muuta ilmeistä oikeusperustetta ja rekisteröity ei esimerkiksi kykene antamaan muuta suostumustaan. Myös suuren hädän vallitessa suostumusta ei välttämättä pystytä keräämään jokaiselta rekisteröidyltä erikseen. Elintärkeiden etujen suhteen rekisteröidyn kielto käsitellä henkilötietojaan ei päde, jos elintärkeän edun suojaaminen ylittää yksilön suojauksen tarpeen[152] tai jos kielto käsitellä jonkun rekisteröidyn henkilötietoja olisi este pelastaa joku suurempi joukko ihmisiä käsittelemällä tämän yhden kieltäytyneen henkilötietoja.

148 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 103.
149 Tietosuojavaltuutetun toimisto -> Henkilötietojen käsittely -> Milloin henkilötietoja saa käsitellä?
150 Tietosuoja-asetus, johdanto-osa kohta (45).
151 Tietosuojavaltuutetun toimisto -> Henkilötietojen käsittely -> Milloin henkilötietoja saa käsitellä?
152 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s.105-106.

Käsittely voi tietosuoja-asetuksen 6 artiklan 1 kohdan e ja f alakohtien perusteella olla laillista myös, kun käsittelyperusteena on yleinen etu ja julkinen valta tai rekisterinpitäjän oikeutettu etu. Henkilötietoja saa käsitellä, kun rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen tai yleinen etu vaatii sitä. Käsittelyperusteena tämä toimii sekä julkisella että yksityisellä sektorilla tilanteissa, joissa on kysymys Euroopan unionin tai jäsenvaltion yleisestä edusta tai julkisesta vallasta. Jotta tällainen käsittelyperuste on laillinen, on julkinen valta tai yleistä etua koskeva tehtävä tullut antaa lailla tai muilla oikeudellisilla säännöksillä. [153]

Oikeutettujen etujen toteuttamiseksi toteutettu henkilötietojen käsittely on sallittua, kun oikeutettu etu punnitaan tasapainotestillä. Tässä testissä rekisterinpitäjän tai kolmannen osapuolen intressiä punnitaan rekisteröidyn intressejä ja perusoikeuksia vasten ja selvitetään, onko oikeutettu etu tarpeen toteuttaa rekisterinpitäjän tai kolmannen osapuolen hyväksi. Tällainen oikeutettu etu käsittelyperusteena edellyttää, että sekä rekisteröidyn edut että oikeudet huomioidaan erityisen tarkasti. Oikeutettu etu käsittelyperusteena edellyttää, että rekisterinpitäjän ja rekisteröidyn välillä on jokin merkityksellinen suhde, kuten rekisteröity toimii rekisterinpitäjän alaisena tai asiakkaana. [154]

Tietosuojalain esitöissä (HE 9/2018 vp) on pyritty täsmentämään kansallista liikkumavaran puitteissa tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan mukaisia tilanteita. Asetuksen perusteella henkilötietojen käsittely kyseisen kohdan perusteella on lainmukaista ainoastaan, kun jokin kohdan edellytyksistä täyttyy. Tietosuojalain pyrkimyksenä on esitöiden perusteella kuitenkin säätää henkilötietojen käsittelyn oikeudellisesta perustasta tilanteissa, joissa kysymys on henkilön asemaa, tehtäviä ja niiden hoitamista julkisyhteisöissä, elinkeinoelämässä, järjestötoiminnassa tai muussa vastaavassa toiminnassa kuvaavista tiedoista ja käsittely on yleisen edun mukainen ja käsittely on oikeasuhtaista, kun vertaa sitä tietosuoja-asetuksen edellyttämään tapaan. Hallituksen esityksen perusteella oikeasuhtaisuutta tulisi arvioida sekä kerättyjen henkilötietojen määrän perusteella että lisäksi myös esimerkiksi käsittelytoimenpiteiden perusteella. Kansallisella tasolla on siten pyritty tietosuojalaissa täsmentämään niitä käsittelyperusteita, joihin

153 Tietosuojavaltuutetun toimisto -> Henkilötietojen käsittely -> Milloin henkilötietoja saa käsitellä?
154 Tietosuojavaltuutetun toimisto -> Henkilötietojen käsittely -> Milloin henkilötietoja saa käsitellä?

tietosuoja-asetus antaa kansallista liikkumavaraa. Näistä täsmennyksistä säädetään tietosuojalain 2 luvun 4 §:ssä.

Lainmukaisista käsittelyperusteista suostumuksen suhteen on koettu, että sen täyttäminen ei aina ole asetuksen mukaisesti toteutettu. Kuten Sankarin ja Wibergin artikkelissa kerrotussa testissä, ei suostumus aina ole yhtä helppoa peruuttaa kuin sen antaminen on. Lisäksi suostumuksen antamisessa rastitus on yleensä internet-sivustoilla helppoa, ja rasti riittää, että siitä pääsee eteenpäin. Sivustot eivät suostumusta kysyessään esimerkiksi vaadi lukemaan rastittamisen sisältöä.

Viranomaisten henkilötietojen käsittelyn perusteena on yleensä lakiin perustuva velvoite. Verohallinnon toiminta perustuu verohallinnon toiminnasta annettuun lakiin. Viranomaiset käsittelevät henkilötietoja yleensä viran puolesta ja viranomaisen tehtävien suorittamiseksi. Rekisteröidyillä on viranomaiseen kohdistuva oikeus pyytää häntä koskevia asiakirjoja nähtäväksi julkisuuslain 3 luvun perusteella. Lisäksi rekisteröidyllä on henkilötietojensa suhteen tietosuoja-asetuksessa määritellyt rekisteröidyn oikeudet. Viranomainen voi myös kieltäytyä antamasta tietoa rekisteröidyn pyytämästä asiakirjasta, mutta tällöin viranomaisen on perusteltava syy kiellolle.

3.2.4 Oikeussuojakeinojen rikkomisen seuraukset

Tietosuoja-asetuksen keskeisenä tehtävänä on ollut tehostaa seuraamusjärjestelmää. Asetuksen johdanto-osan 11 kappaleen mukaisesti tämä edellyttää EU:n alueella saman tasoisia valtuuksia valvoa henkilötietojensuojaa koskevien sääntöjen noudattamista sekä sitä, että seuraamukset sääntöjen rikkomisesta olisivat jäsenvaltioiden kesken saman tasoisia.

Seuraamusten osalta huomio on kiinnittynyt valvontaviranomaisen määräämiin hallinnollisiin sakkoihin.[155]Asetuksen 58 artiklan 2 kohdassa säädetään valvontaviranomaisen korjaavista toimivaltuuksista, joita ovat muun muassa varoitus tai huomautus käsittelytoimien asetuksen vastaisuudesta (a ja b alakohta). Varoitus tai huomautus voidaan antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle.[156] Muita

[155] Andreasson – Riikonen – Ylipartanen 2019, s. 35.
[156] Suomessa tietosuojavaltuutettu on antanut vasta huomautuksia tai varoituksia, ks. lisää finlex.fi.

korjaavia toimivaltuuksia ovat käsittelyn väliaikainen tai pysyvä rajoittaminen. Näiden lisäksi valvontaviranomainen voi määrätä tuon hallinnollisen sakon (i alakohta). Tietosuoja-asetuksen 83 artiklassa säädetään hallinnollisten sakkojen määräämisen yleisistä edellytyksistä.

Asetuksen myötä tullut viranomaisen mahdollisuus määrätä hallinnollisia sakkoja ja puuttua muilla valvontakeinoilla rekisterinpitäjän toimintaan on laajentanut valvontaviranomaisen toimivaltuuksia suoraan asetuksen nojalla.[157]

Tietosuojalain 22 §:ssä on säädetty tietosuojavaltuutetun mahdollisuudesta asettaa uhkasakko rekisterinpitäjälle sekä 24 §:ssä puolestaan on säädetty hallinnollisesta seuraamusmaksusta, jonka voi määrätä tietosuojavaltuutetun ja apulaistietosuojavaltuutetun yhdessä muodostama seuraamuskollegio. Seuraamusmaksu voidaan määrätä tietosuojalain 24 §:n 3 momentin perusteella tietosuoja-asetuksen 10 artiklan rikkomisesta, noudattaen kuitenkin mitä tietosuoja-asetuksen 83 artiklan 5 kohdassa ja tietosuojalaissa säädetään. Tähän seuraamusmaksun määräykseen voi hakea muutosta valittamalla hallinto-oikeuteen tietosuojalain 25 §:ssä säädetyllä tavalla. Seuraamusmaksua ei kuitenkaan voida määrätä valtion viranomaiselle, valtion liikelaitokselle, kunnalliselle viranomaiselle, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille (tietosuojalain 24.4 §).

Seuraamusmaksua ei voi Suomessa määrätä valtion viranomaiselle. Lain esitöiden perusteella viranomaiselle määrättävä hallinnollinen seuraamusmaksu on yleisen oikeusjärjestyksemme kannalta vieras menettely. Koska seuraamusmaksu on rajattu julkishallinnon osalta pois, oikeusjärjestys kohdistaa julkishallintoon muita erityisvaatimuksia perustelemaan kyseistä sääntelyratkaisua.[158] Joten valtio voi vuotaa tietoja, ja tällaisista tietovuodoista voidaan uutisoida hyvin pehmeästi, mutta se ei joudu siitä vastuuseen. Rekisteröity, eli kansalainen, ei voi näin nähdä valtion edes maksavan aiheutuneista tietovuodoista. Hallituksen esityksen perusteella valtiolle voidaan asettaa kuitenkin uhkasakko, jolla on tarkoitus mahdollistaa tietosuojavaltuutetun päätöksen

157 Andreasson – Riikonen – Ylipartanen 2019, s. 35.
158 Hallituksen esitys 9/2018 vp, kohta 25 §. Kohdassa erityisvaatimuksien osalta käsitellään viranomaisten hallinnon lainmukaisuusperiaatetta sekä viranomaisten virkavelvollisuutta. Ks. lisää

tehokkuutta. [159] Uhkasakon asettaminen valtion viranomaiselle on kuitenkin keino, millä tavalla kansalainen voi nähdä valtion joutuvan korvausvastuuseen aiheutuneista tietovuodoista.

TATTI-työryhmä on ennen tietosuojalain voimaantuloa antanut perustelunsa sille, että kansallista liikkumavaraa ei olisi käytetty sen suhteen, voidaanko viranomaisille määrätä hallinnollinen sakko. Tämän liikkumavaran käyttämättä jättämisen perusteluissa todetaan, että tietosuoja-asetuksen täytäntöönpanon tehokkuus edellyttää sen täytäntöönpanoa oikeasisältöisenä. Jotta yleisen tietosuoja-asetuksen mukaiset tavoitteet saadaan toteutettua, hallinnollinen sakko tulisi pystyä määräämään myös viranomaisille. Viranomaisia ei saisi jättää täysin hallinnollisen sakon määräämisen ulkopuolelle. Tämän perustelun puolesta todetaan myös, että viranomaisiin tulisi myös kohdistaa kansallisen valvontaviranomaisen toimesta tehokkaita, oikeasuhtaisia ja varoittavia seuraamuksia heidän rikkoessaan tietosuoja-asetusta. Tietosuoja-asetuksesta poikkeaminen vaatisi myös tällöin tehokasta seuraamusjärjestelmää, joka olisi vaihtoehtoinen hallinnolliselle sakolle. [160]

Yleisen tietosuoja-asetuksen vastaisen toiminnan tapahtuessa sääntelyviranomaisten korjaavien toimenpiteiden tulee olla tehokkaita, oikeasuhteisia ja varoittavia. Hallinnollisten seuraamusten on oltava tällöin kohtuullisia rikkomisen tyypin, vakavuuden ja siitä mahdollisesti aiheutuvien seurausten suhteen. Sääntelyviranomaisten on siis arvioitava nämä kaikki tosiseikat yhdenmukaisesti ja objektiivisesti perusteltavalla tavalla. Valittu korjaava toimenpide vaikuttaa myös siihen, mikä on tehokasta, oikeasuhtaista ja varoittavaa kussakin tapauksessa. Monet rikkomukset mahdollistavat hallinnollisten seuraamuksien määräämisen. Jäsenvaltioilla on mahdollisuus omassa kansallisessa lainsäädännössään sallia tai jopa vaatia seuraamusten määräämistä muiden kuin tietosuoja-asetuksen 9 artiklassa tarkoitettujen säännösten rikkomisesta. [161] Suomessa tähän on varauduttu juuri tietosuojalailla.

Hallinnollisten sakkojen määräämisessä jäsenvaltioiden välillä on eroavaisuuksia. Tämän vuoksi Euroopan tietosuojaneuvosto[162] on pyrkinyt jo ennen tietosuoja-asetuksen voimaantuloa määrittelemään yhteisiä arviointikriteereitä, joita yksittäiset

159 Hallituksen esitys 9/2018 vp, kohta 25 §.
160 Julkaisut.valtioneuvosto.fi 2020.
161 Datainspektionen.se ->Globalassets ->Document -> Riktlinjer for tillampning och fastställande av administrative sanktionsavgifter.
162 EDPB, European Data Protection Board.

valvontaviranomaiset voisivat käyttää hallinnollisten sakkojen määräämisessä.[163] Jäsenvaltioissa on jo Suomea lukuun ottamatta annettu sakkoja tietosuoja-asetuksen vastaisesta toiminnasta. GDPR Enforcement Tracker -sivuston perusteella Espanja on antanut eniten sakkoja tietoturvaloukkauksista. Nämä Espanjan määräämät sakot vaihtelevat 800 eurosta aina 60.000 euroon saakka. Yksityishenkilölle on määrätty 800 euron sakot artiklojen 5 ja 6 perusteella. Kovimmat sakot, 60.000 euroa on saanut esimerkiksi operaattoriyritys Vodafone España riittämättömästä tietoturvan tasosta (päätös annettu 3.2.2020). Sivuston perusteella 24 jäsenvaltiota 27stä[164] on jo antanut hallinnollisia sakkoja.[165]

EDPB:n arviointikriteereiden mukaan lähtökohtaisesti asetuksen rikkomisesta aiheutuvat seuraamukset tulisi olla saman tasoisia jäsenvaltioiden välillä.[166] Vastaava henkilötietojen suojan taso edellyttää mm. sitä, että seuraamukset olisivat saman tasoisia, mutta myös sitä, että jäsenvaltiot tekisivät tehokasta yhteistyötä estääkseen eroavaisuudet. Valvontaviranomaisten tulisi välttää korjaavien toimenpiteiden erilaisuutta samanlaisissa tapauksissa ja korjaavina toimenpiteinä tulisi määrätä sakkoja. Myös näiden sakkojen tulisi olla tehokkaita, oikeasuhteisia ja varoittavia, jotta ne tavoittaisivat päämääränsä. Toimenpiteitä arvioitaessa arvioidaan juuri tehokkuutta, oikeasuhtaisuutta ja varoittavuutta.

Tietosuoja-asetuksessa näihin oikeusseuraamuksiin on varauduttu rekisterinpitäjälle asetetulla vastuulla. Asetuksen 33 artiklan 1 kohdan mukaan rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta 72 tunnin kuluessa toimivaltaiselle viranomaiselle. Ilmoittaminen on tehtävä ilman aiheetonta viivytystä heti loukkauksen tultua ilmi tietosuoja-asetuksen 55 artiklassa tarkoitetulle viranomaiselle. Ilmoittaminen ei kuitenkaan ole välttämätöntä, jos henkilötietojen tietoturvaloukkaus ei todennäköisesti aiheuta luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Ilmoittamatta jättämisestä seuraa rekisterinpitäjälle velvollisuus antaa valvontaviranomaiselle perusteltu selitys. Tällä perusteella 72 tunnin ilmoittamisajasta voidaan poiketa. Jos rekisterinpitäjä ei tee ilmoitusta, on hänen kuitenkin selvitettävä objektiivisin perusteluin syitä siihen, mistä viivästyminen johtuu ja mitä viivästyksestä aiheutuu rekisteröidyn oikeuksille ja

[163] WP 253, 2017. s.4.
[164] Varsinaisia jäsenvaltioita on nykyään 27, kun Iso-Britannia erosi EU:sta alkuvuodesta 2020.
[165] Ks. lisää määrätyistä hallinnollisista sakoista osoitteesta enforcemenettracker.com. Kyseinen sivusto ei ole virallinen ja sitä tarkastellessa on huomioitava, että siellä raportoidaan myös keskeneräiset sakkomenettelyt.
[166] TSA, johdanto-osa kappale (10).

vapauksille.[167] Tietosuoja-asetuksen 33 artiklan 2 kohdan mukaisesti henkilötietojen käsittelijällä on myös velvollisuus ilmoittaa rekisterinpitäjälle viivytyksettä loukkauksen tapahtumisesta havaittuaan tällaisen tapahtuneen.

Tietoturvaloukkaukset ovat osa rekisterinpitäjän dokumentointivelvollisuutta. Rekisterinpitäjän tulee dokumentoida tapahtuneet tietoturvaloukkaukset osana osoitusvelvollisuuden toteuttamista. Tietosuoja-asetuksen 33 artiklan 5 kohta säätää tästä tietoturvaloukkauksien dokumentoinnista. Kohdan perusteella kaikki tietoturvaloukkaukset on dokumentoitava, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Dokumentoinnin avulla varmistetaan, että valvontaviranomainen voi tarkastaa artiklan noudattamisen.

Kansainvälisellä tasolla riskienhallinnan suojelemiseksi on laadittu toimenpiteitä. Vuonna 1980 OECD hyväksyi suosituksen,[168] joka koskee yksityisyyden suojaa ja kansainvälistä henkilötietojen siirtoa. Suositus sisältää henkilötietojen keräämistä, laatua, tietoturvaa, rekisteröidyn tarkastusoikeutta ja kansainvälistä tiedonsiirtoa koskevia yleisperiaatteita.[169] Koska digitalisaatio on kehittynyt, on tietojen laatu ja määrä muuttunut reilussa 30 vuodessa. OECD on vuonna 2013 antanut päivitetyt yksityisyyden suojaa koskevat suuntaviivat.[170] Näiden suuntaviivojen perusteella OECD on antanut erinäisiä ohjeita ja strategioita digitaalisen turvallisuuden riskien hallitsemiseksi. Digitaaliset turvallisuusuhat ovat lisääntyneet viime vuosina yhä enemmän, ja sen vuoksi on tarpeen määritellä turvallisuutta edistäviä strategioita.[171] Päivitetyissä suosituksissa on tuotu esille uusia käsitteitä tietosuojaan liittyen. Näistä käsitteitä ovat esimerkiksi tietosuojastrategiat ja tietoturvaloukkauksesta ilmoittaminen.[172]

ENISA on tarkastellut jo 2010-luvun alkupuolella jäsenvaltioiden voimassa olevia toimenpiteitä ja menettelyjä henkilötietojen rikkomusten suhteen. Vuonna 2011 se julkaisi

[167] Voutilainen 2019. s. 203.
[168] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.
[169] HE 96/1998 Vp. s.13.
[170] OECD Privacy Law Enforcement Co-operation. Oecd.org -> Internet -> Ieconomy -> Privacyguidelines.
[171] OECD Privacy Law Enforcement Co-operation. Oecd.org -> Internet -> Ieconomy -> Privacyguidelines.

[172]OECD Privacy Enforcement Co-operation. Oecd.org -> Internet -> Ieconomy -> Privacyguidelines.

sähköisen viestinnän tietosuojadirektiivin[173] (2002/58/EY) 4 artiklaan perustuen suosituksia siitä, miten tietosuojarikkomuksia voitaisiin havaita ja kuinka niihin voitaisiin valmistautua. Kyseisen direktiivin 4 artiklassa säädetään turvallisuudesta ja määritellään sähköisten viestintäpalveluiden tarjoajille tiettyjä kriteerejä, joiden perusteella voidaan varmistaa turvallisuus. Nämä ENISAn määrittelemät toimenpiteet ovat kuitenkin tietosuoja-asetuksen myötä täydentyneet, ja nykyisin tietosuoja-asetus määrittelee niistä tarkemmin.

3.2.5 Julkisuuslaki osana viranomaisen toimintaa

Valtion viranomaisten toimintaan kohdistuu omanaan laki viranomaisen toiminnan julkisuudesta (JulkL 621/1999). Tähän viranomaisen julkisuuteen liittyy tehtäviä, joilla on tarkoitus taata oikeusvarmuuden ja oikeusturvan toteutumista, mahdollistaa kansalaisten osallistuminen, vaikuttaminen ja valvonta, edistää avointa ja hyvää hallintoa, tukea sananvapautta, vahvistaa viranomaistoiminnan legitimiteettiä sekä mahdollistaa julkisten tietovarantojen hyödyntämistä. Julkisuuslailla on tarkoitus varmistaa viranomaisten käyttävän valtaa avoimesti, noudattavan hyvää tiedonhallintatapaa ja huolehtivan tarpeen vaatiessa tietojen salassapidosta.[174]

Julkisuuslain tavoitteena on, että jokaisella on oikeus saada tietoja viranomaisen julkisista asiakirjoista. Viranomaisen asiakirjat ovat kyseisen lain perusteella julkisia, jollei erikseen toisin säädetä (JulkL, 1 §). Suomessa vallitsee julkisuusperiaate. Tämän julkisuusperiaatteen mukaisesti jokaisella on oikeus saada tieto viranomaisen julkisesta vallankäytöstä ja viranomaisten muusta toiminnasta. Oikeus saada tieto viranomaisen toiminnasta on yleinen lähtökohta, josta voidaan tehdä poikkeuksia vain erityisin perustein. Poikkeukset on myös määriteltävä täsmällisesti lailla. Menettelyltä vaaditaan periaatteen mukaisesti ylipäänsä avoimuutta, ja se velvoittaa viranomaista tiedottamaan toiminnastaan.[175] Julkisuuslain 6 pykälän perusteella viranomaisen asiakirja on julkinen, kun se on valmis. Tämän jälkeen siitä voidaan antaa tieto, mikäli laki ei muuten estä tiedon antamista.

[173] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi).
[174] Lehtonen 2020.
[175] Mäenpää 2016, s. 2.

Euroopan unionin toiminnasta annetussa sopimuksen (SEUT) 298 artiklassa säädetään avoimesta eurooppalaisesta hallinnosta, johon myös julkisuusperiaate pohjautuu. Julkisuusperiaatteen toteuttamista tukee avoimuus. Avoimuudella tarkoitetaan viranomaisilla olevien tietojen saatavuutta ja käytettävyyttä. Julkisuusperiaatteen soveltamisala on lähtökohtaisesti viranomaisilla oleva, jossain muodossa tallennettu tieto. Julkisuusperiaatteen ulkopuolelle jäävät yksityiset toimijat. [176]

Hallituksen esityksen (HE 284/2018 vp) laiksi julkisen hallinnon tiedonhallinnasta sekä eräistä siihen liittyvistä laeista perusteella tämä laki olisi tiedonhallintaa koskeva yleislaki, jolla varmistettaisiin viranomaisten tietoaineistojen yhdenmukainen hallinta ja tietoturvallinen käsittely julkisuusperiaatteen noudattamiseksi. Hallituksen esityksen perusteella lailla olisi tarkoitus myös säätää viranomaisten tietojärjestelmien välillä tapahtuvasta tietojen luovuttamisesta sähköisesti. Tällä sääntelyllä olisi tarkoitus tehostaa viranomaisten tiedonhallintaa, jotta viranomaiset voivat tarjota hallinnon asiakkaalle palveluitaan noudattaen hyvää hallintoa laadukkaasti ja hoitaa tehtävänsä tuloksellisesti. Myös tietojärjestelmien ja tietovarantojen yhteen toimivuus on lain tarkoituksena.

WP 29 on antanut valtioille ohjeen, jossa annetaan jäsenvaltioiden lainsäätäjille ja toimivaltaisille laitoksille neuvoja, kuinka varmistaa avoimuus tietosuojaa kunnioittaen. Kyseisessä ohjeessa käytetään ”läpinäkyvyyden” käsitettä, kun puhutaan avoimuudesta, hyvästä hallintotavasta ja sen periaatteista, jotka on kirjattu Euroopan perussopimuksen 6 artiklan ja Euroopan unionin perusoikeuskirjan 7 artiklaan.[177]

Kyseisessä ohjeessa julkisten tehtävien suorittamisen avaimeksi tunnustetaan huippuosaaminen ja laadun varmistus, joilla saadaan toteutettua puolueettomuutta, avoimuutta ja ammatillista käytöstä. Ohjeen on tarkoitus helpottaa sen tasapainon löytymisessä julkisen sektorin, tietosuojan ja yksilöiden yleisen edun välillä. Lausunnossa neuvotaan, miten julkinen sektori voi varmistaa henkilöiden yhtäläiset tietosuojatasot kaikissa jäsenvaltioissa. Lausunto ottaa huomioon Euroopan ihmisoikeussopimuksen 10 artiklan sekä tietosuoja-asetuksen johdanto-osan kappaleet julkisen sektorin tietojen uudelleenkäytöstä. Näihin vedoten ohje pyrkii suosittelemaan tiettyjen ohjeessa mainittujen periaatteiden huomioon ottamista henkilötietoja käsiteltäessä, kun kyse on eturistiriitojen

176 Mäenpää 2016. s. 7-11.
177 Ec.europa.eu -> Justice -> Article 29 -> Documentation -> Opinion recommendation 2016, s. 4.

yhteydessä toteutettavien toimenpiteiden ja niihin liittyvän avoimuuden yhteydestä.[178] Ohjeen on tarkoitus toteuttaa avoimuutta ja ehkäistä eturistiriitoja, joita avoimuuden ja tietosuojan välillä syntyy.

Julkisuuslain ja tietosuoja-asetuksen yhteensovittaminen viranomaisissa on koettu olevan ristiriitaista. Viranomaisilla on hankaluuksia tulkita näiden säädösten yhteiseloa. Mäenpään mukaan julkisuuslaki säätää tiedon jakamisesta, kun taas tietosuoja-asetus ja tietosuojalaki sääntelevät tiedon keräämisestä ja käsittelystä. Voutilaisen käsityksen mukaan puolestaan Suomen viranomaiset eivät osaa tulkita kahta lakia ja kahta suomalaisten perusoikeutta oikein. Hänen käsityksensä on, että viranomaiset sekoittavat yksittäisen tiedon luovuttamisen ja tietojen massaluovutukset keskenään. Mäenpää korostaa, että lainsäätäjä ei nähnyt tietosuojalakia säätäessään tarpeelliseksi puuttua julkisuuslakiin, sillä julkisuuslaki koskee yksittäisten julkisten asiakirjojen luovuttamista. Vaikka nämä kaksi asiaa säätävät eri asioista, ei Mäenpää koe julkisuusperiaatteen ja tietosuojalainsäädännön rajanvetoa täysin ongelmattomaksi.[179]

Julkisen hallinnon tiedonhallinnasta annettu laki (906/2019) astui voimaan 1.päivänä tammikuuta 2020. Tällä lailla pyritään yhteen sovittamaan julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa. [180]

[178] Ec.europa.eu -> Justice -> Article 29 -> Documentation -> Opinion recommendation 2016, s. 4.
[179] Lehtonen 2020.
[180] Valtiovarainministeriö 2020-> vastuualueet -> Julkisen hallinnon ICT -> Tiedonhallinta ja tietopolitiikka -> Tiedonhallintalaki.

4 TIETOSUOJAA KOSKEVISTA PERIAATTEISTA

Henkilötietojen käsittelyssä aina tietojen kokoamisesta niiden tuhoamiseen asti on lähtökohtana käsittelystä säätäminen koko informaation elinkaaren ajan. Tietosuojalainsäädännön tarkoitus on kattaa koko tämä elinkaari. Tietosuojan periaatteet voidaan luokitella ryhmiin seuraavasti: 1. yleiset, kaikkia koskevat periaatteet, 2. ensisijaisesti henkilötietojen käsittelijöitä koskevat sekä 3. ensisijaisesti yksilön oikeuksia koskevat periaatteet.[181]

Lakisääteisyys, yksilön tunnistettavuus, avoimuus, tarpeellisuus, tietoturva, hyvä tietojenkäsittelytapa, automaattisen henkilöarvioinnin rajoittaminen, käytännesäännöt, viranomaiskoneiston olemassaolo ja sanktiojärjestelmä ovat yleisiin periaatteisiin kuuluvia oikeusperiaatteita.[182] Tarpeellisuus, suunnitelmallisuus, käyttötarkoitussidonnaisuus, huolellisuusvelvoite, tietoturvallisuus, laatuperiaate, tiedottamisvelvollisuus ja ankara vastuu ovat sen sijaan rekisterinpitäjää koskevia oikeusperiaatteita Saarenpään käsityksen mukaan. Suostumus, ensisijaisuus, arkaluonteisten tietojen sekä henkilötunnuksen erityisasema, tarkastus- ja oikaisuoikeus, markkinarauha, kielto ja vastustusoikeus sekä tietosuojaviranomaisten palvelut ovat yksilön kannalta tärkeitä tietosuojalainsäädäntöön perustuvia periaatteita.[183]

Voimassa olevan tietosuoja-asetuksen 5 artiklassa säädetään tietosuojaperiaatteista, jotka jokaisen rekisterinpitäjän tulee ottaa huomioon käsiteltäessä henkilötietoja. Periaatteilla pyritään takaamaan rekisteröidyn oikeuksien ja vapauksien toteutuminen. Nämä periaatteet ovat monilta osin aiemman henkilötietolain mukaisia periaatteita, mutta niitä on pyritty asetuksessa myös osittain täsmentämään. Tietosuojaperiaatteita ovat asetuksen 5 artiklan perusteella käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen täsmällisyys, tietojen säilytyksen rajoittaminen, tietojen eheys ja luottamuksellisuus sekä rekisterinpitäjän osoitusvelvollisuus.

Rekisterinpitäjällä on velvollisuus huolehtia, että tietosuojaperiaatteet tulevat huomioiduksi jokaisessa käsittelyvaiheessa. Tarvittaessa rekisterinpitäjän tulee myös pystyä osoittamaan, että periaatteita noudatetaan. Tällä rekisterinpitäjälle asetetulla vaatimuksella pyritään

181 Saarenpää 2015, s. 342.
182 Saarenpää 2015, s. 342.
183 Saarenpää 2015, s. 342, 355.

siihen, että henkilötietojen käsittely vaatii aiempaa tarkempaa suunnittelua ja dokumentointia.[184]

Lainmukaisesta henkilötietojen käsittelystä säädetään tietosuoja-asetuksen 6 ja 9–11 artikloissa. Niissä mainitaan käsittelyperusteet, joita on täsmennetty myös useissa kansallisissa erityislaeissa. Lainmukaisia käsittelyperusteita on 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. Tietosuoja-asetuksen 6 artiklan perusteella käsittely on lainmukaista ainoastaan silloin, kun vähintään yksi näistä edellytyksistä täyttyy.

Tietosuojaperiaatteista kohtuullisuus tarkoittaa käytännössä sitä, että rekisterinpitäjät eivät käytä henkilötietoja väärin, vaan ottavat niitä käsitellessään huomioon myös rekisteröidyn edut ja odotukset. Läpinäkyvyydellä haetaan informointivelvollisuutta. Läpinäkyvyydellä taataan ihmisten oikeus saada tietää, mitä ja miten heitä koskevia tietoja kerätään, käytetään tai muutoin käsitellään. Rekisterinpitäjällä on velvollisuus informoida rekisteröityjä, mikä puolestaan parantaa käsittelyn lainmukaisuutta.[185] Rekisterinpitäjän on kerrottava henkilötietojen käsittelystä ymmärrettävällä tavalla. Käsittelystä kerrottavat tiedot eivät saa johtaa harhaan, ja käsittelyä ei saa peitellä. Tiedot on annettava oikein, manipuloimatta vastaanottajaa. Käsittely tulee toteuttaa ennalta suunnitellusti, rekisteröidyn kannalta ilman turhia yllätyksiä.[186]

Rekisterinpitäjän tulee määritellä tietty, nimenomainen ja laillinen tarkoitus sille, mitä varten henkilötietoja kerätään. Niitä ei myöskään saa käyttää myöhemmin ohi sen tarkoituksen, mitä varten ne on kerätty. Tätä tarkoitusta ilmentää käyttötarkoitussidonnaisuuden periaate. Se rajoittaa rekisterinpitäjän mahdollisuuksia käyttää henkilötietoja ohi sen tarkoituksen, johon ne on alun perin kerätty. Se ei kiellä henkilötietojen käyttämistä johonkin toiseen käyttötarkoitukseen alkuperäisen käyttötarkoituksen lisäksi, kunhan uusi käyttötarkoitus ei ole ristiriidassa alkuperäisen käyttötarkoituksen kanssa.[187] Käyttötarkoitussidonnaisuuteen liittyy lisäksi myös tietojen minimointi.

[184] Tietosuojavaltuutetun toimisto -> Tietosuojaperiaatteet.
[185] Korpisaari– Pitkänen– Warma-Lehtinen 2018, s. 95.
[186] Tietosuojavaltuutetun toimisto -> Tietosuojaperiaatteet ->Lainmukaisuus ja läpinäkyvyys.
[187] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 96.

Jo henkilötietolain (523/1999, kumottu lailla 1050/2018) 7 §:ssä määritettiin käyttötarkoitussidonnaisuus. Lain perusteella henkilötietojen käsittelyssä tulee ottaa huomioon se, ettei käsittely saa olla yhteen sopimaton saman lain 6 §:ssä määritetyn henkilötietojen käsittelyn suunnittelemisen kanssa.[188] Nyt käyttötarkoitussidonnaisuutta yhdessä muiden tietosuojaperiaatteiden kanssa on täsmennetty tietosuoja-asetukseen.

Tietojen minimoinnin perusteella henkilötietoja saa kerätä vain välttämättömissä määrin. Rekisterinpitäjän tulee määritellä käyttötarkoitus henkilötietojen keräämiselle, jotta tietojen minimointi voidaan pyrkiä toteuttamaan. Tietojen minimointiin perustuen tarpeettomat henkilötiedot poistetaan ja virheelliset korjataan tai oikaistaan. Kun henkilötietoja ei enää tarvita siihen tarkoitukseen, johon ne on kerätty, tulee henkilötiedot poistaa. Lähtökohtaisesti henkilötietojen säilyttämisaika on hyvin lyhyt, ellei laista muuta johdu. [189]

Rekisteröidyllä on myös oikeus luottaa rekisterinpitäjään, jotta rekisteritietoihin eivät pääse ulkopuoliset. Tätä tarkoittaa tietojen eheys ja luottamuksellisuus. Eheyteen perustuen tietoja ei saa mennä muuttamaan ilman rekisterinpitäjän suostumusta, jotta tiedon oikeellisuus ei vaarannu. Rekisterinpitäjän on laadittava asianmukaiset tekniset ja organisatoriset toimet, jotta kukaan ei pääse käyttämään tietoja lainvastaisesti tai tiedot eivät pääse vahingossa häviämään, tuhoutumaan tai vahingoittumaan. [190]

Kaikki näistä tietosuojaperiaatteista konkretisoituvat osoitusvelvollisuuden avulla. Osoitusvelvollisuutta on käsitelty jo aiemmin luvussa 3.2.1 ja 3.2.2. Osoitusvelvollisuus toimenpiteenä on jälkikäteinen keino, mitä kuitenkin pyritään toteuttamaan ennakolta. Rekisterinpitäjän tulee osoitusvelvollisuuden perusteella pystyä osoittamaan, mitä toimenpiteitä se on suorittanut henkilötietojen suojan toteuttamiseksi, mutta kaikki toimenpiteet ovat tapahtuneet ennakolta. Toimenpiteet on tehty siinä vaiheessa, kun henkilötietoja on kerätty ja suunniteltu niiden keräämistä. Toimenpiteitä on myös tämän henkilötietojen keräämisen yhteydessä täsmennetty, mutta toimenpiteistä mikään ei pyri ratkaisemaan jälkikäteen suojan toteutumista.

[188] Pitkänen – Tiilikka – Warma 2013, s. 79.
[189] Tietosuojavaltuutetun toimisto -> Tietosuojaperiaatteet -> Tietojen minimointi.
[190] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 94-95.

5 TIETOTURVALOUKKAUKSET

5.1 Mitä tietovuodoilla tarkoitetaan?

Tietovuotoa ei määritellä erikseen missään laissa, mutta sillä voidaan tarkoittaa tiedon tarkoittamatonta siirtymistä suojatun järjestelmän ulkopuolelle.[191]

Suomen rikoslain 38 luvussa säädetään tieto- ja viestintärikoksista. Rikoslain 38 luvun 8 §:ssä määritellään *tietomurto* rikoksena. Pykälän perusteella henkilö on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi, jos kyseinen henkilö käyttää hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa. Myös sellaisen järjestelmän erikseen suojattuun osaan oikeudettomasti tunkeutuminen on rangaistavaa.

Tietovuoto voidaan lukea osaksi tietoturvaloukkauksia, joilla tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää tai ne muuttuvat. Tietoturvaloukkauksesta on kysymys myös tapahtumassa, jossa henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.[192] Tällaisen tapahtuman seurauksena voi rekisteröidylle aiheutua mittavia vaikeuksia, kuten identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen[193] tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen. Tietosuoja-asetuksen 4 artiklan 12 kohdassa määritellään henkilötietojen tietoturvaloukkaus. Kyseisessä kohdassa henkilötietojen tietoturvaloukkaus tarkoittaa tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.[194] Tietoturvaloukkaus koostuu siten käsittelystä, joka on aiheuttanut vahingossa tai lainvastaisella menettelyllä henkilötietojen tuhoutumisen, häviämisen, muuttamisen tai luvattoman luovuttamisen taikka tietoihin on päästy ilman perusteita vahingossa tai laittomasti. Mikä tahansa

[191] Vahtiohje.fi.

[192] Ks. tarkemmin tietoturvaloukkauksista esimerkkejä osoitteesta tietosuoja.fi. Tietoturvaloukkauksia voivat olla esimerkiksi hävinnyt tiedonsiirtoväline, varastettu tietokone, hakkerointi, haittaohjelmatartunta, kyberhyökkäys, tulipalo datakeskuksessa tai tiliotteen postitus väärälle henkilölle.

[193] Pseudonymisointi on TSA:n mukanaan tuoma uusi käsite, jolla tarkoitetaan henkilötietojen käsittelemistä niin, että niitä ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. ks. lisää Hanninen – Laine– Rantala – Rusi – Varhela 2017, s. 21.

[194] Lisää tästä määritelmästä ja yleisistä suuntaviivoista määritelmälle löytyy osoitteesta ec.europa.eu -> Newsroom -> Article 29.

tietoturvaloukkaus ei ole tietosuoja-asetuksessa tarkoitettu tietoturvaloukkaus.[195] Tietoturvaloukkauksen tapahduttua rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta voidaan välittömästi selvittää, onko kyseessä käsittelyssä tapahtunut tietoturvaloukkaus vai ei. Asiasta tulee viipymättä ilmoittaa valvontaviranomaiselle sekä antaa rekisteröidylle tiedoksi.[196]

Tietoturvaloukkauksesta voi aiheutua rekisteröidylle useita ongelmia, jos tällaisen loukkauksen tapahduttua siihen ei reagoida nopeasti. Tietoturvaloukkauksen seurausten minimointi yhdessä tehokkaan ja viivytyksettömän toteuttamisen kanssa on tärkeää rekisteröidyn oikeuksien ja vapauksien turvaamisen kannalta. Näillä loukkauksilla on aina jokin motiivi, yleensä taloudellinen, mutta se voi olla myös valtiollinen, poliittinen tai ideologinen. Niitä tapahtuu myös tahattomasti, inhimillisen virheen vuoksi. Loukkauksia voi tapahtua sekä fyysisessä että digitaalisessa maailmassa.[197]

Tietosuojatyöryhmä on julkaissut esimerkit helpottamaan tietoturvaloukkausten tunnistamista. Aineistolla on tarkoitus auttaa rekisterinpitäjää tunnistamaan tilanteet, milloin loukkauksista on ilmoitettava valvontaviranomaisille tai rekisteröidylle sekä määrittelemään tapauksen vakavuus. Tietosuojatyöryhmän esimerkkien avulla rekisterinpitäjän on helpompi määritellä, milloin tietoturvaloukkauksista tulee tehdä ilmoitus ja milloin henkilöiden oikeuksiin ja vapauksiin kohdistuu riskejä.[198]

Tietovuodot sisältyvät tietoturvaloukkauksen määritelmän piiriin. Asetuksen 32 artiklassa on määritetty tietoturvan osa-alueita. Yksittäinen tietoturvaloukkaus voi kuulua samanaikaisesti yhteen tai useampaan näistä osa-alueista. Osa-alueita tietoturvaloukkauksen näkökulmasta on *luottamuksellisuuden loukkaus*, *eheyden loukkaus* ja *saatavuuden loukkaus*. Luottamuksellisuuden loukkauksessa tietoja paljastuu luvattomasti tai vahingossa eteenpäin ilman perusteita tai vastaavasti niihin pääsee käsiksi sellainen taho, jolla ei kuuluisi olla niihin pääsyä. Eheyden loukkauksessa puolestaan henkilötiedot samoilla perusteilla muuttuvat, eli

195 Voutilainen 2019, s. 203.
196 TSA johdanto-osa, kohta 87.
197 Andreasson – Riikonen – Ylipartanen 2019, s. 137.
198 Ks. lisää näistä esimerkeistä ja niiden luokittelusta tietosuojatyöryhmän dokumenteista osoitteesta https://tietosuoja.fi/documents/6927448/8214536/Esimerkkejä+tietoturvaloukkauksista/754c16aa-152e-4f15-a458-d1579c5ea4b2/Esimerkkejä+tietoturvaloukkauksista.pdf.

niin tapahtuu luvatta tai vahingossa. Saatavuuden loukkauksessa henkilötiedot tai pääsy niihin menetetään luvattomasti tai vahingossa. Niihin ei enää päästä käsiksi tai ne tuhoutuvat luvatta tai vahingossa.[199]

5.2 Rekisterinpitäjän toimintavelvollisuudet tietoturvaloukkausten tapahduttua

Aiemmin luvussa 3.2.1. on käsitelty rekisterinpitäjän vastuun sisältöä. Asetuksen 24 artiklassa säädetään vastuun sisällöstä: tarvittavista toimenpiteistä asetuksen noudattamisen varmistamiseksi. Vastuut on määritelty riskiperusteisesti, ja ne tulee huomioida osana asetuksen kokonaisuutta. Kyseinen artikla ei anna kansallista liikkumavaraa, jolla toimia eri tietoturvaloukkausten tilanteissa voitaisiin täsmentää. Asetuksen perusteella vastuuta koskevaa säännöstä on tulkittava osana asetuksen kokonaisuutta, ottaen huomioon sen tavoitteet.[200]

Vastuun takana on rekisterinpitäjän suorittama arvio siitä riskistä, mitä vahinkoa väärinkäytöksistä esimerkiksi aiheutuu rekisteröidylle. Tämän riskiarvio osaltaan vaikuttaa siihen, kuinka rekisterinpitäjän tulee toimia tietovuototilanteissa. Asetuksen 33 artiklassa säädetään tietoturvaloukkauksesta ilmoittamisesta valvontaviranomaiselle. Asetuksen 33 artiklan perusteella tietoturvaloukkauksesta on ilmoitettava 72 tunnin kuluessa sen ilmitulosta. Loukkauksesta ei kuitenkaan tarvitse ilmoittaa, jos tietoturvaloukkauksesta ei aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos ilmoitusta ei anneta, on valvontaviranomaiselle kuitenkin annettava perusteltu selitys.

Rekisterinpitäjän on pitänyt jo ennen tietoturvaloukkauksen tapahtumista aloittaa prosessi vaikutustenarvioinnista. Sen on pitänyt arvioida riskit ja niiden suhde aiheutuvaan haittaan. Haitan vakavuus on myös tullut huomioida ja riskejä on pitänyt kartoittaa jatkuvasti yhdessä osoitusvelvollisuuden kanssa. Vaikutustenarviointi on tullut laatia etukäteisenä keinona kartoittaa riskit ja se, mitä henkilötietojen käsittelyssä voi tapahtua. Asetuksessa edellytetään, että henkilötietojen käsittelyn yhteydessä toteutetaan riskiä vastaavan

199 Pulkkanen 2018.
200 Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 269.

turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet 32 artiklan mukaisesti.

Tietoturvaloukkauksia ja niihin liittyviä tietovuototilanteita kuitenkin tapahtuu. Jotta luonnollisille henkilöille ei aiheutuisia monenlaisia vahinkoja, on loukkauksiin puututtava riittävän tehokkaasti ja nopeasti. Jos niihin ei puututa, voi rekisteröity joutua kärsimään huomattavia vahinkoja.[201] Tämän vuoksi tietoturvaloukkauksista on ilmoitettava 72 tunnin kuluessa valvontaviranomaiselle, joka Suomessa on tietosuojavaltuutettu.

Asetus ei lähtökohtaisesti jaottele rekisterinpitäjiä sen perusteella, onko se yksityinen vai julkinen toimija. Rekisterinpitäjän tavalla kerätä henkilötietoja ei myöskään ole merkitystä asetuksen määräysten kannalta. Tällä voisi kuitenkin nähdä olevan vaikutusta, kun verrataan tietojenkäsittelytapaa. Viranomaiset yleensä keräävät lähtökohtaisesti henkilötietoja lakiin perustuen, ja rekisteröidyn suostumuksella ei tällöin ole vaikutusta henkilötietojen keräämisen suhteen. Jos asetus ei erottele eri tietojen käsittelytapojen avulla erilaisia toimenpiteitä sille, mitä näiden tietoturvaloukkausten tapahduttua rekisterinpitäjän tulee tehdä suhteessa rekisteröityyn, on asetuksessa aukko. Tietojen keräämisen ja käyttämisen tarkoituksen perusteella voitaisiin asettaa rekisterinpitäjälle toimenpidevaatimuksia erilaisissa tietoturva- ja tietovuototilanteissa.

Koska asetus ei jaottele toimenpiteitä suhteessa siihen, mikä on peruste käsitellä henkilötietoja, ei valtio ole yksityiseen rekisterinpitäjään verrattuna mitenkään erityinen taho. Kuitenkin seuraamukset ovat näillä erilaiset, kun valtio ei joudu esimerkiksi korvausvelvolliseksi tai sille ei voida asettaa sakkoja toiminnastaan. Suhteessa rekisteröidyn oikeuksiin voivat oikeudet olla erilaiset riippuen käsittelyperusteesta. Käsittelyperuste voi vaikuttaa siihen, kuinka rekisteröity voi toteuttaa oikeuksiaan. Esimerkiksi valtio käsittelee henkilötietoja yleensä lakisääteisen velvoitteen tai julkisen vallan käytön perusteella. Tällöin rekisteröidyn suostumuksella ja siihen kohdistuvilla oikeuksien käytöllä ole merkitystä, kun käsittelyperuste pohjautuu jo laista.

Verrattaessa rekisterinpitäjän vastuuta rekisteröidyn oikeuksiin on rekisteröidyllä eniten oikeuksia suhteessa rekisterinpitäjään, kun oikeusperusteena on suostumus.[202] Tällöin vastakohtana sille, että rekisteröidyn oikeudet kasvavat, kun hän on suostumalla suostunut

[201] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 314.
[202] Tietosuojavaltuutetun toimisto -> Henkilötietojen käsittely -> Käsittelyperusteet.

henkilötietojen käyttöön, voidaan esittää, että rekisterinpitäjän vastuut sen sijaan kasvavat, kun rekisteröity ei ole voinut niin paljon vaikuttaa siihen, millä perusteella hänen henkilötietojaan käytetään. Eli esimerkiksi käsittelyperusteen perustuessa lakiin, tulisi tämän perusteen lisätä vastaavasti rekisterinpitäjän toimintavelvollisuuksia, koska se kutistaa rekisteröidyn oikeuksia.

Asetuksessa määritellyt vastuut sijoittuvat ajallisesti henkilötietojen keräämishetkeen ja siihen, kun pyritään ennakoimaan tietoturvaloukkausten tapahtumista. Asetus ei mahdollista kovin paljon toimenpiteitä puuttua jälkikäteisillä keinoilla aiheutuneisiin vahinkoihin. Asetus ei esimerkiksi säädä mitään jatkotoimenpiteitä tietoturvaloukkausten tapahduttua, millä pyrittäisiin entistä parempaan suojan tasoon. Asetus rakentuu vaikutustenarvioinnin ja osoitusvelvollisuuden varaan, ja niiden mukaisesti tehdään jatkuvaa seurantaa ja arviota siitä, millaiset vaarat kyseiseen rekisterinpitoon ja tietojen käsittelyyn kohdistuvat.

Jälkikäteiset keinot jäävät asetuksessa aukollisiksi, kun asetuksen perusteella määritellään vain hatarasti se, milloin tietoturvaloukkauksista tulee ilmoittaa rekisteriviranomaiselle ja milloin vastaavasti rekisteröidylle itselleen. Asetus selvittää vain, että ilmoitusta ei tarvitse tehdä tietosuojaviranomaiselle, *jos* henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.[203] Tätä riskiä arvioitaessa on asetuksen johdannon 76 kohdan mukaisesti otettava huomioon tietojenkäsittelyn luonne, laajuus, asiayhteys ja tarkoitus. Arviointi on tehtävä asetuksen perusteella *objektiivisesti*. Asetuksen lähtökohtana on se, että rekisterinpitäjä noudattaa informointivelvollisuutta. Tämä velvollisuus on asetettu asetuksessa erittäin tärkeään asemaan, ja sen perusteella rekisterinpitäjä osaltaan huolehtii rekisteröidyn oikeuksien toteutumisesta. Kuitenkin näyttää siltä, että jälkikäteisiin keinoihin informointivelvollisuus ei täysin ylety. Informointivelvollisuudesta puhutaan etukäteisten keinojen ja suunnittelun kannalta, mutta jälkikäteisissä keinoissa se huomioidaan muodossa ”jos”. Koska toimintavelvollisuuden piiriin ei kuulu automaattisesti informointivelvollisuuden toteuttaminen sekä tietosuojaviranomaiselle että rekisteröidylle, ei tämä velvollisuus kulje läpi asetuksen. Se otetaan huomioon ennakollisissa toimissa, mutta jälkikäteisissä keinoissa on jokaisen rekisterinpitäjän itse arvioitava, toteuttaako sitä vai ei.

[203] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 315.

Tietosuojalainsäädännön yhtenä oleellisena uudistamiskohteena oli vastata muuttuneeseen käsittely-ympäristöön sekä henkilötietojen käsittelyyn vaikuttavaan tekniseen kehitykseen.[204] Osoitusvelvollisuuden sisällön avulla pyrittiin auttamaan käsittely-ympäristön keskeisiä tarpeita. Tällä velvollisuudella rekisterinpitäjille lisättiin entistä enemmän velvollisuuksia verrattuna entiseen henkilötietodirektiiviin. [205] Jälkikäteisissä keinoissa osoitusvelvollisuus toteutuu, kun rekisterinpitäjällä on osoittaa ne keinot, joita hän toteutti ennakolta tarkoituksenmukaisesti henkilötietojen käsittelyn toteuttamiseksi. Jälkikäteisten keinojen osalta rekisterinpitäjä siis osoittaa sen, mitä teki ennakkoon estääkseen tietovuodon tapahtumisen. Osoitusvelvollisuuden piiriin ei siten kuulu mitään varsinaista osoitettavaa, mitä tehdä jälkikäteisesti ja miten suojata jo tietoturvaloukkauksen tapahduttua rekisteröidyn oikeuksia.

5.3 Rekisteröidyn oikeudet tietoturvaloukkaustilanteissa

Tietovuototilanteissa rekisteröidyn oikeuksien ei pitäisi heikentyä, vaan rekisterinpitäjällä tulisi olla toimintavalmiudet estää vahinkojen tapahtuminen. Kuitenkin, kun tietovuotoja tapahtuu, olisi syytä kiinnittää huomiota myös siihen, voidaanko rekisteröityä vastuuttaa sitä kautta, että hän on antanut esimerkiksi suostumuksen tietojensa käsittelyyn.

Tietosuoja-asetuksessa annetaan rekisteröidyille runsaasti oikeuksia, joilla pyritään takaamaan yksilöiden henkilötietoautonomia. Näiden oikeuksien turvaaminen on puolestaan jokaisen henkilötietoja käsittelevän rekisterinpitäjän vastuulla. [206]

Lähtökohtaisesti henkilötiedot ovat näkyvästi kaikkialla muiden nähtävillä erilaisissa sosiaalisen median rekistereissä, ja ihmiset eivät myöskään pelkää jakaa näitä tietoja oma-aloitteisesti. Pohdittaessa tietosuoja-asetuksen tavoitetta voisi yhtenä parantamisen kohteena esittää ihan omaa pykälää jopa perustuslakiin, joka koskisi henkilötietojen suojaa. Tämän hetkisen lainsäädännön mukaisesti tämä suoja sisältyy yksityis- ja perhe-elämän suojan pykälän (PL, 10.1 §) sisälle. Maailma kuitenkin digitalisoituu koko ajan yhä enemmän ja nopeammin, joten olisi tarpeen pohtia sitä, tarvitseeko henkilötietojen suoja nostaa perustuslain tasolla aivan omaksi pykäläkseen. Tällä tavalla voitaisiin varmistaa, että

[204] Uuden tekniikan vaikutusten huomioon ottamisesta ks. KOM (2010) 609, s.3.
[205] Vainio 2017, s. 48.
[206] Tietosuojavaltuutetun toimisto -> Rekisteröidyn oikeudet.

henkilötiedot saisivat myös mediassa ansaitsemansa huomion. Perustuslain 10 §:n 2 momentin mukaan *henkilötietojen suojasta säädetään tarkemmin lailla*. Kyseistä lakivarausta on perusoikeusuudistuksen esitöissä luonnehdittu toteamalla, että säännös viittaa tarpeeseen lainsäädännöllisesti turvata yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä. [207] Suomessa tämä henkilötietojen suoja on vakiintuneesti sijoitettu yksityiselämän suojan alakäsitteeksi,[208] mutta olisi tarkoituksenmukaista näin melkein 30 vuotta perusoikeusuudistuksen jälkeen tehdä muutoksia, jotka palvelevat nykyistä yhteiskuntaa. Nykyisin ihmiset ovat tietoisempia perusoikeuksistaan ja siten myös henkilötietojen suojasta.

Henkilötietojen suojan ollessa osa tiedollista itsemääräämisoikeutta voidaan tarpeellinen informointi rekisteröidylle tietoturvaloukkaustilanteissa nähdä myös tärkeänä yksilön oikeuksien kannalta. Jotta henkinen loukkaamattomuus ei vaarantuisi, on rekisteröityä tarpeen aina informoida loukkauksen tapahduttua. Jos yksilö ei lähtökohtaisesti ole voinut vaikuttaa henkilötietojensa käyttämiseen tarpeellisessa laajuudessa, on häntä koskevalla informaatiolla suurempi vaikutus. Tällöin ihmisellä ei välttämättä ole riittävää tietämystä henkilötietojensa käyttämisestä, kun käsittelyperusteena on jokin muu kuin oma suostumus. Jos käsittelyperuste on esimerkiksi lakiin perustuva tai oikeutettu etu, niin tällöin olisi syytä korostaa yksilön oikeutta tietoon. Tämä oikeus sisältää myös läpinäkyvyyden vaatimuksen yhteiskunnan ja yksilöiden välillä, joten tällä perusteella henkilön oikeudet pitäisi olla turvatummat. Myös oikeutta valtaan itseään koskevassa asiassa tulisi huomioida tietoturvaloukkausten tilanteissa. Tällaisten tilanteiden sattuessa henkilöllä tulisi olla mahdollisuus selvittää ilman turhaa byrokratiaa ne tiedot, jotka loukkaustilanteessa ovat kärsineet, ja onko näiden tietojen vuotamisesta aiheutunut tai aiheutumassa hänelle jotain väärinkäytösten seurauksia.

Toimivan yhteiskunnan kannalta on tärkeää, että yksilöt luopuvat osasta yksityisyyttään ja on tärkeää määritellä ehdot, jotka toimivat henkilötietojen käsittelyn perusteena.[209] Jos nämä ehdot määritellään näin, olisi myös syytä ottaa huomioon se, että tietosuoja-asetuksen ja sen kansallisen liikkumavaran puitteissa rekisterinpitäjillä olisi lähtökohtaisesti samanlainen asema riippumatta siitä, onko kyse julkisesta vai yksityisestä rekisterinpitäjästä. Tällä

[207] HE 309/1993 VP, S. 52-53.
[208] Viljanen 2011, s. 396 ss.
[209] Neuvonen 2014, s. 60.

hetkellä Suomessa viranomaisille rekisterinpitäjänä ei voida määrätä hallinnollista sakkoa, mikä taas on mahdollista yksityisille rekisterinpitäjille. Tämä asettaa rekisterinpitäjät lähtökohtaisesti eri asemaan riippuen siitä, mikä on rekisterinpitäjän status. Kuitenkin, jos tarkastellaan rekisterinpitäjiä ja heidän perustettaan, millä he käsittelevät henkilötietoja, on yksityisten toimijoiden rekisterinpidon lähtökohtana yleensä suuremmalla todennäköisyydellä esimerkiksi suostumus. Suostumus käsittelyperusteena takasi rekisteröidylle jo laajimmat mahdollisuudet pitää kiinni oikeuksistaan. Ja, jos nämä suostumusta käsittelyperusteena käyttävät rekisterinpitäjät ovat niitä, jotka voidaan tuomita Suomessa sakkoon, on tässä ristiriita. Viranomaisten pitämät rekisterit perustuvat yleensä lakiin, jolloin rekisteröidyllä on heikommat mahdollisuudet pitää kiinni oikeuksistaan, ja silti viranomaisille ei voida määrätä hallinnollista sakkoa rikkomuksesta, kuten taas yksityiselle rekisterinpitäjälle sellainen voidaan määrätä. Tämä on ristiriita, ja se heikentää yksilöiden oikeuksia, kun rekisterinpitäjänä on valtio.

Informointivelvollisuus on lähtökohta, jolla rekisterinpitäjä selvittää rekisteröidylle henkilötietojen käsittelyä jo keräämisvaiheessa. Kuten 3.1.2. kohdassa on selvitetty, on tämän velvollisuuden tavoitteena ollut varmistaa, että rekisteröidyllä olisi mahdollisuus käyttää oikeuksiaan kattavammin kuin tähän asti. Tämä velvollisuus olisi syytä kattaa myös jälkikäteisiin keinoihin, jossa rekisteröityä olisi syytä informoida tietovuototilanteissa - riippumatta siitä, mikä haitan aste on ollut. Tällä tavalla rekisteröidyllä olisi paremmat mahdollisuudet pitää huolta oikeuksistaan ja rekisterinpitäjän velvollisuudet vastaavasti olisivat tarkoituksenmukaisempia suhteessa aiheutuneeseen vaaraan tai vahinkoon. Rekisteröidyn ei tulisi joutua kärsijäksi, kun tietovuoto tai muu tietoturvaloukkaus tapahtuu, vaan rekisteröidyllä pitäisi olla samat oikeudet kuin muuten asetuksen näkökulmasta. Tällä hetkellä tietosuoja-asetus ei tältä osin takaa rekisteröidyn oikeuksia näissä jälkikäteisissä tilanteissa, vaan asetus lähtee ennakollisesta ohjautumisesta liikkeelle. Rekisterinpitäjän tulee ennakolta tehdä vaikutustenarviointi, ja sen tulee ennakolta informoida rekisteröityä. Kuitenkin tarvitaan myös jälkikäteisiä keinoja, joilla näiden tietovuotojen ja tietoturvaloukkausten jo tapahduttua voidaan varmistaa, että rekisteröidyn oikeudet eivät kärsi.

5.4 Tietovuototilanteiden haasteet

Haasteena tietoturvaloukkausten sattuessa voidaan nähdä se, että asetuksen tavoite ja pyrkimys siihen, millä toimilla tavoite saavutetaan, eivät kohtaa. Riippuen henkilötietojen käsittelyperusteesta rekisterinpitäjän velvollisuudet ovat lähtökohtaisesti samat, mutta suhteessa rekisteröidyn oikeuksiin, oikeudet kärsivät. Tietovuototilanteiden informointivelvollisuus ei saisi olla riippuvainen siitä, miten vaikutustenarviointi on huolehdittu ennakolta ja miten siinä on määritelty riskit ja niiden tasot. Informointivelvollisuus ei saisi olla lähtökohtaisesti riippuvainen aiheutuneesta vaarasta ja vahingosta, vaan sen tulisi olla jokaisessa tilanteessa käytettävissä oleva keino tuoda rekisteröidylle asti tieto siitä, mitä on tapahtunut.

Jotta nämä haasteet voidaan kohdata, on tietosuoja-asetuksessa määritelty informointivelvollisuus ulotettava koskemaan myös jälkikäteisiä ohjauskeinoja. Informointivelvollisuuden rekisterinpitäjän velvollisuutena olisi hyvä kattaa kaikki tietoturvaloukkausten tilanteet, eikä se saisi olla riippuvainen aiheutuneesta vahingosta. Näin rekisteröidyn oikeudet eivät olisi se kohde, joka kärsii.

Tämän hetken sääntelyn puitteissa rekisterinpitäjät asetetaan eri asemaan sen perusteella, onko rekisterinpitäjä julkinen vai yksityinen toimija. Tätä olisi myös syytä pohtia, toteutuvatko asetuksen tavoitteet täysin, kun se ei kohtele rekisterinpitäjiä tasapuolisesti. Ymmärrettävää on, että valtio ei voi maksaa itse itselleen hallinnollista sakkoa, mutta olisi tarpeen määritellä vaihtoehtoinen keino, millä myös viranomaisten toimesta tapahtuvat tietoturvaloukkaukset tulisivat rangaistusten piiriin.

Tietovuototilanteiden haasteena on myös se, että näitä tilanteita ei voida täysin ennakoida. Niitä tapahtuu ja niitä tulee tapahtumaan yhä jatkuvasti. Kappaleessa 3.1.5. on käsitelty hallituksen esitystä, jonka tavoitteena on luoda tietoturvallisuuden varmistaminen ja julkisuusperiaatteen huomioon ottaminen viranomaisen käsitellessä henkilötietoja. Jo ennen tietosuoja-asetuksen voimaantuloa on tietosuojatyöryhmä raportoinut eri jäsenvaltioissa esille tulleiden tietosuoja-aiheisten kohujen ja tietotovuotojen olevan puutteellisia teknisten järjestelmien tasolla. [210]

[210] WP 168, s. 19.

Tietosuoja-asetuksen näkökulmasta haasteena voidaan nähdä myös se, että vahingonkorvaus jälkikäteisenä keinona[211] ei ole tämän hetkisen selvityksen perusteella riittävä suojaamaan rekisteröidyn oikeuksia. Kun tietovuototilanteita tapahtuu väistämättä ja vahingonkorvauksella ei voida taata jälkikäteen rekisteröidyn oikeuksien toteutumista täysimääräisesti, ei asetus tällöin palvele täysin rekisteröidyn oikeuksia. Tietovuotojen, kuten myös muiden tietoturvarikkomusten suhteen, tulisi laatia riittävät jälkikäteiset keinot, joilla voidaan varmistaa rekisteröidyn oikeuksien toteutuminen.

Haasteena voidaan nähdä myös rikoslain 38 luvun 9 §:ssä säädetty tietosuojarikos, joka vaatii rekisterinpitäjältä tai henkilötietojen käsittelijältä *tahallisuutta* tai *törkeää huolimattomuutta* ja *loukkaa* toiminnallaan rekisteröidyn yksityisyyden suojaa tai *aiheuttaa* hänelle *muuta vahinkoa* tai *olennaista haittaa.* Kyseisen lainkohdan esitöissä peruslakivaliokunta on kiinnittänyt huomiota pykälän viittauksiin sekä tietosuoja-asetukseen, kahteen kansalliseen lakiin että epätäsmällisellä tavalla myös muuhun lakiin. Perustuslakivaliokunta ei ole kyseisessä lainkohdan esityössä täsmentänyt näitä tekotapaan liittyviä seurauksia, kuten, että mitä tarkoitetaan loukkaamisella teon yhteydessä tai mitä on *aiheuttaa muuta vahinkoa tai olennaista haittaa?* [212] Rikoslain 38 luvun 10 §:n mukaisesti syyttäjän on ennen tietosuojarikosta koskevan syytteen nostamista kuultava tietosuojavaltuutettua. Kyseinen pykälä tietosuojarikoksesta on ollut voimassa vasta pari vuotta, joten oikeuskäytäntö ei ole vielä ehtinyt muodostaa kuvaa siitä, mitä pykälän muun vahingon aiheuttamisella ja olennaisella haitalla tarkoitetaan. Tietovuototilanteiden suhteen ei kyse välttämättä ole myöskään rekisterinpitäjän tahallisuudesta, mutta myös törkeä huolimattomuus olisi syytä pyrkiä täsmentämään. Mikä aiheuttaa *törkeää huolimattomuutta*? Pykälän perusteella törkeän huolimattomuuden on lisäksi aiheutettava juuri rekisteröidyn oikeuksien loukkaaminen tai muu vahinko rekisteröidylle tai olennainen haitta.

[211] Ratkaisu *EIT 17.7.2008 I v. Suomi*.
[212] PeVL 14/2018 vp, kohta *laillisuusperiaate.*

6 JOHTOPÄÄTÖKSIÄ

Tutkielmassa olen tutkinut nykyisen tietosuoja-asetuksen mukaisia rekisterinpitäjälle asetettuja velvoitteita, joiden avulla pyritään ehkäisemään tietoturvaloukkausten tapahtumista. Olen myös tutkinut näiden velvoitteiden suhdetta rekisteröidyn oikeuksiin ja pyrkinyt selvittämään, ovatko asetetut keinot oikeassa suhteessa asetuksen tavoitteeseen.

Tietovuodot ovat osa tietoturvaloukkauksia, joita tapahtuu väistämättä koko ajan.[213] Kyberturvallisuuden avulla pyritään kehittämään keinoja näiden loukkausten estämiseksi. Nykyinen tietosuoja-asetus ja kyberturvallisuus eivät täysin kohtaa, kun rekisteröity ei saa täysimääräisesti digiturvallisuuden tavoittelemaa suojaa tietosuoja-asetuksen näkökulmasta.

Esimerkiksi Verohallinto valtion viranomaisena nauttii kansalaisten luottamuksesta. Kansalaisilla ei ole vaihtoehtoa Verohallinnolle, kuten ei monille muillekaan valtion viranomaisille. Kansalaiset rekisteröityinä ovat siten heikommassa asemassa verrattuna valtioon rekisterinpitäjänä. Näiden valtion viranomaisten suhteen kansalainen ei voi esimerkiksi harjoittaa oikeuttaan siirtää henkilötietojen käsittelyä järjestelmästä toiseen tietosuoja-asetuksen 20 artiklan mukaisesti, koska ei ole toista vastaavaa viranomaista, joka käsittelisi kyseisenlaisia tietoja kyseisessä asiassa.

Tietosuojan puitteissa pyritään varmistamaan yksityisyyden suojaa ja oikeusturvaa, jota rekisteröidyn oikeuksiksi on säännelty. Tietosuojan on tarkoitus ohjeistaa rekisterinpitäjiä toimimaan näiden oikeuksien turvaamiseksi riittävällä tavalla. Tietosuoja on osa perustuslain 10 § turvattua yksityisyyden suojaa, jota toteutetaan tietoturvan keinoin.

Kuten tutkielmassa tuon esille, tietosuoja-asetuksen tarkoituksena on ollut parantaa rekisteröityjen oikeusturvaa ja henkilötietojen suojaa. Laadittujen selvitysten perusteella kansalaiset ovat kokeneet henkilötietojensa suojan parantuneen asetuksen voimaantulon myötä. Tämä suojan taso on varmasti parantunut, kun rekisterinpitäjinä ovat yksityinen sektori ja yksityiset toimijat, kuten voidaan nähdä jo EU:ssa langetettujen sakkojen[214] perusteella. Tutkielman kannalta kritiikki kohdistuu *rekisterinpitäjän jälkikäteisiin toimintavelvoiteisiin tietoturvaloukkausten tapahduttua.* Asetus ei säädä tarpeeksi

[213] Ks. esim. Korpisaari 2019, joka on todennut, että tietovuotojen suhteen sinällään lainvastaisia tietovuotoja voidaan pitää oikeutettuina, jos ne johtavat esimerkiksi yhteiskunnallisesti tärkeän aiheen esiin tuomiseen.
[214] Ks. sakoista lisää osoitteesta enforcemetntracker.org. Sivusto sisältää myös keskeneräisiä menettelyjä, joten se ei aivan täysin anna realistista kuvaa sakkojen täytäntöönpanosta.

yksityiskohtaisesti näistä jälkikäteisistä toimintavelvollisuuksista. Kuten TATTI-työryhmä[215] on jo todennut mietinnössään, ei valtiolle voi Suomessa määrätä tietosuoja-asetuksen mukaista hallinnollista sakkoa. Ymmärrettävää on, että ei valtio voi maksaa valtion rahoista valtion kassaan sakkoja, mutta tällöin valtioon rekisterinpitäjänä tulisi kohdistua jotain suurempaa vastuuta. Kun tällä tavalla erotellaan lähtökohtaisesti rekisterinpitäjän status jo lain tasolla, se laittaa automaattisesti rekisterinpitäjät eri asemaan.

Ratkaisussa *EIT 17.7.2008 I v. Suomi* tutkielmani kannalta tärkeää on ratkaisun kohta 47, jossa todetaan, että jälkikäteinen vahingonkorvauksen mahdollisuus ei ole yksityisyyden suojan toteuttamiseksi riittävää. Jälkikäteinen vahingonkorvaus ei ole riittävää, koska yksityisyyden voi digitaalisessa maailmassa menettää vain kerran.[216] Ratkaisu on ajalta ennen tietosuoja-asetuksen voimaantuloa, mutta kyseinen ratkaisun kohta toteaa aukon olemassaolon. Lakia tai lain esitöitä ei voida koskaan laatia niin yksityiskohtaisiksi ja tarkoiksi, että kaikkiin mahdollisiin oikeusriitoihin voitaisiin ennakolta varautua. Ei ole olemassa sellaisia täsmällisiä ratkaisuohjeita, joita voitaisiin kaavamaisesti noudattaa ja päätyä aina oikeaan ratkaisuun.[217] Tietosuoja-asetuksen oikeussuojakeinoissa tämä olisi ehditty ottaa huomioon täsmällisemmin. Jälkikäteisestä vahingonkorvauksesta olisi voitu säätää asetuksessa ja myös ennakollisessa varautumisessa huomioida se, että kun näitä tietoturvarikkomuksia tapahtuu, on yksityisyys tällöin menetetty.

Vaikka jälkikäteinen vahingonkorvaus ei ole riittävä yksilön henkilötietojen suojan toteutumisen kannalta, tulisi jälkikäteisistä keinoista säätää aiempaa yksityiskohtaisemmin. Jälkikäteisinä keinoina rekisterinpitäjää voitaisiin esimerkiksi velvoittaa aina kertomaan rekisteröidylle tietoturvaloukkauksen tapahtumisesta. Rekisteröidyn suojan toteutumisen kannalta puolestaan rekisteröidylle voitaisiin tämän ilmoituksen vastaanottamisen perusteella mahdollistaa prosessi, jolla hän voisi vaatia enemmän selvitystä loukkauksesta sekä päättää itse, haluaako vaatia mahdollisia korvauksia vai ei. Mahdollisesti maksettavat korvaukset tulisi sitoa tietoturvaloukkauksen vakavuuteen, mutta lähtökohtaisesti tämä oikeus vaatia korvauksia olisi rekisteröidyllä itsellään. Tietovuototilanteille ei voi aina mitään, mutta jälkikäteisinä keinoina rekisterinpitäjän vastuu informoida rekisteröityä mahdollistaisi sen, että rekisteröidyllä olisi paremmat vaikuttamiskeinot oikeuksiensa

215 Ks. lisää osoitteesta julkaisut.valtioneuvosto.fi 2020.
216 Andreasson – Koivisto – Ylipartanen 2013, s. 20.
217 Korpisaari 2016, s. 28.

toteutumiseksi. Tällä tavalla tarkentamalla asetusta saataisiin sekä rekisterinpitäjien jälkikäteisiä vastuita kasvatettua, mutta myös rekisteröity pääsisi henkilökohtaisesti huolehtimaan paremmin oikeuksiensa toteutumisesta.

Ihmisoikeuksien väliset ristiriidat voivat ilmetä esimerkiksi sellaisissa oikeuksissa kuin oikeus tiedonsaantiin, ilmaisunvapauteen, oikeus yksityisyyteen ja kirjeen salassapitoon.[218] Tällä perusteella valtiolla rekisterinpitäjänä tulisi olla vastuu omissa rekistereissään tapahtuvista tietoturvaloukkauksista. Valtion tulisi pystyä ennakoimaan, mutta sen pitäisi myös pystyä kantamaan vastuu jälkikäteisesti. Tätä olisi syytä tarkentaa sekä kansallisella tasolla että myös EU:n tasolla.

Tietosuoja-asetus ei näyttäydy tasavertaisena sen suhteen, onko rekisterinpitäjä valtio vai yksityinen. Koska se ei ole tasavertainen, tulisi kehitellä jokin keino, millä varmistuttaisiin valtion tietoturvan tasosta.[219] Tällä hetkellä rekisteröityjen toimiessa vastoin asetusta toimenpiteet eivät näyttäydy tasapuolisesti, koska Suomi käytti kansallista liikkumavaraa määritellessään, ettei valtion viranomaisille voida määrätä hallinnollista sakkoa tietosuoja-asetuksen rikkomisesta. TATTI-työryhmän mietinnössä todetaan, että jos käytetään kansallista liikkumavaraa, niin valtion tulisi mahdollistaa vaihtoehtoinen tehokas seuraamusjärjestelmä, jolla saavutettaisiin tietosuoja-asetuksen tarvittava taso. Vaihtoehtoisen tehokkaan seuraamusjärjestelmän tutkiminen on jo oma tutkimuskohteensa, jota en tässä tutkielmassa sen tarkemmin tutki.

Tietosuoja-asetuksessa on aukko, kun jälkikäteisistä toimintavelvoitteista rekisterinpitäjälle säädetään vain suhteessa aiheutettuun vahinkoon. Se, että jokin vahinko nähdään niin lievänä, ettei sellaisesta ilmoittaminen ole tarpeen rekisteröidylle, ei palvele asetuksen tavoitetta.[220] Rekisteröidyllä ei ole mahdollisuutta tällaisessa tilanteessa huolehtia omista oikeuksistaan, ja vastaavasti rekisterinpitäjän velvollisuudet eivät toteuta näiden oikeuksien toteutumista. Tämän vuoksi ehdotan, että jokaisen rekisterinpitäjän olisi suoritettava vaikutustenarviointi ja vaikutustenarviointia koskevia suuntaviivoja riskien suhteen tulisi

[218] Sitek, Terem, Wójcicka 2015, s. 61-65.

[219] Tähän tavoitteeseen pyritään ainakin 1.tammikuuta 2020 voimaan astuneella tiedonhallintalailla. Lain tarkoituksena on 1.1 §:n perusteella varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen julkisuusperiaatteen toteuttaminen.

[220] Myös ajatus siitä, että joku toinen ihminen voi sanoa toisen puolesta, mikä henkilötieto on kenellekin tärkeä ja suojelemisen arvoinen, on ristiriitaista. Ja, koska se on ristiriitaista, on ristiriitaista myös se, että vahinko asetetaan järjestelmään tai riville ja mietitään sen perusteella, tarvitseeko tämän tiedon omistajan kuulla loukkauksen tapahtumisesta.

yhdenmukaistaa siten, että rekisteröidyllä olisi oikeus aina saada tieto häntä koskevasta tietoturvaloukkauksesta riippumatta määritellystä vahingosta.

Henkilötietojen suoja on perusoikeus, jota etenkin valtion tulee turvata. Tämän suojan toteutumisen kannalta olisi tarpeen määritellä lisää jälkikäteisiä keinoja, joilla voidaan turvata yksilöiden mahdollisuus pitää huolta oikeuksistaan. Koska perusoikeuden turvaaminen on valtion tehtävä, olisi Suomen myös syytä kehittää vaihtoehtoinen jälkikäteen toimiva korvausjärjestelmä valtiolle rekisterinpitäjänä, mikäli kansallinen liikkumavara sallii tämän.

Tietosuoja-asetuksen luettavuus on vaikea, ja eri artikloilla on yhteys toisiinsa eri tilanteissa. Tietosuojalaki ei tätä luettavuutta helpota, sillä se ei täsmentävänä lakina aina täsmennä, vaan sitä lukiessa tulee aina palata myös asetuksen artikloihin. Tässä luettavuudessa voidaan myös nähdä aukko rekisteröidyn oikeuksien kannalta, koska vaikealukuisuus ei helpota tilanteiden ymmärtämistä. Asetus ei kuitenkaan parin vuoden soveltamisaikana ole täysin päässyt tavoitteisiin kaikissa tilanteissa, ja tämän vuoksi jälkikäteiset keinot puuttua tietoturvaloukkausten tilanteisiin vaatisivat täsmennystä. Yksityisyys voidaan menettää digitaalisessa maailmassa vain kerran, mutta menettäessään sen tulisi yksilöllä olla oikeus olla tietoinen asiasta.

Tämän tutkielman kannalta lähitulevaisuudessa tehtäviä tutkimuksen kohteita voisivat olla ne toimenpiteet, joilla asetuksessa olevat jälkikäteiset keinot saavuttaisivat vahvan aseman korjauskeinoina tietoturvarikkomusten jo tapahduttua. Myös rekisterinpitäjien asemassa nähtävää aukkoa voitaisiin tutkia laajemmin, kun tietosuojavaltuutettu alkaa enemmän antamaan ratkaisuja tietoturva-asetuksen soveltamisen laiminlyömisestä. Mitä jatkotutkimukseen tulee, on tietosuoja-asetus vielä sen verran uusi ja ajankohtainen, että on aihetta jatkotutkimuksille. Myös rekisteröidyn oikeuksia kannattaa tutkia jatkossa lisää, koska oikeudet voidaan rajata esimerkiksi vain sosiaaliseen mediaan tai tutkia eri oikeuksien suhdetta toisiinsa.